International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Special Issue No. 01, May 2016
www.ijates.com
ijates
ISSN 2348 - 7550

# ECG SIGNAL STEGANOGRAPHY USING WAVELET TRANSFORMS

**Asha N S[1], Anithadevi M D[2], Dr. M Z Kurian[3]**

**ABSTRACT**

*Today, remote point of care (PoC) system is intensively used for moderating the medical traffic in hospitals. Dependability and confidentiality of the information's are the major problem in remote healthcare and PoC systems. In this paper, we have focused on encryption process in ECG steganography using wavelet transforms. This method provides reliability and confidentiality of the information in PoC system. Frequency domain steganography is implemented in which five level wavelet packet decomposition is applied. Data scrambles inside the ECG signal through scrambling matrix and shared key. In this method, we have collected the ECG signal of patients from body sensors and physionet. We have hidden the physiological parameters into biomedical signal and produced watermarked biomedical signal. We have also analyzed the energies of original ECG signal and encrypted ECG signal using different wavelets such as Coiflet, Biorthogonal and Symlets wavelets. From the result, it is observed that the energy of encrypted ECG signal using Coiflet wavelet transforms is higher than any other wavelet transforms.*

***Key Words: Confidentiality, ECG Signal, Energy, Steganography, Encryption, Watermarking.***

## I. INTRODUCTION

In the present days, patients are frequently admitted to the hospitals all over the world. Patients are suffering from various diseases especially related to the heart. With the increasing traffic in hospitals many patients can't get the appropriate medication in hospitals and they die. To avoid this problem health monitoring system and point of care (PoC) have become popular. With the support of these methodologies physiological information and ECG signal of the patients can be effortlessly transferred to doctor in hospital via internet. Doctor can evaluate all the parameters take reply and commencement the treatment instantaneously in emergencies without delay. Internet is the robust tool for communication. We can transmit and obtain much information by using internet. The transmission between patient and doctor is passing via internet, transmission needs privacy and confidentiality. The Health Insurance Portability and Accountability Act (HIPAA) conditions that patient medical information should be protected and private during the transmission via internet.

Researchers have proposed several methods to solve reliability, confidentiality, security problems. Digital watermarking is the one of the keys to these problems. In this technique, secret information will hide inside the host signal operating confidential key. Subsequently, stego signal is received via internet. This process is called encoding. The receiver is extracted that secret information from this signal using same secret key. This process is called decoding. There are numerous procedure for obtaining patient confidential information. Steganography technique is widely used for securing the information. In steganography technique original information hides inside the host data (images, video and audio) and forms the embed message. The embedded message delivers to

the authorized person via internet ant that person extracts the actual information from the host data. Steganography technique is based on encryption and decryption process but, it is not enough to secure patient information. We have implemented a new technique, which is established on wavelet transforms. A prevailing security technique is proposed which is shown in fig.1.

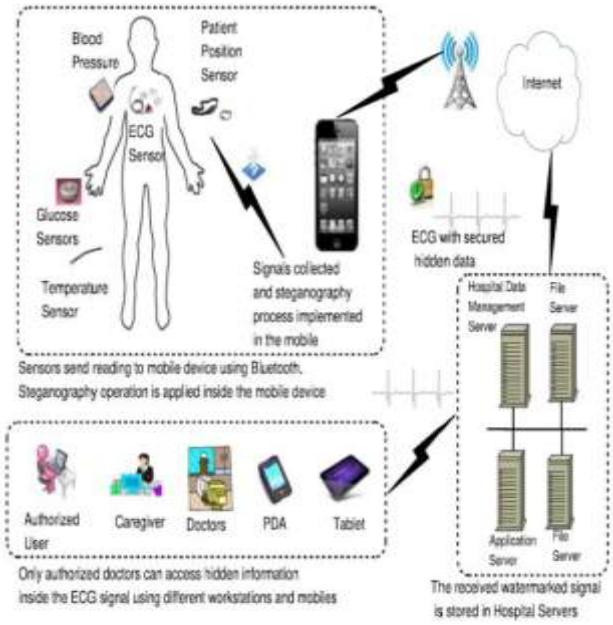


**Fig.1. Block diagram of ECG steganography scenario in point of care (PoC) systems.**

In this method, ECG signals are assembled from the different body sensors and physionet. Physiological parameters and patient personal information have taken from patient. This information send to patient PDA (Personal Digital Assistant) device such as mobile laptop, computer etc, via Bluetooth. Steganography technique is implemented in patient PDA device. Steganography technique obscures physiological parameters such as blood pressure, temperature, position and glucose level and patient personal information such as patient name, Medicare number, address etc, inside the ECG signal, which is transmitted to the hospital server over the internet. The watermarked ECG signal is accumulated at the hospital server. All doctors of hospital can see the watermarked ECG signal, but one certified doctor who has same secret key will extract the secret information by using same key from the host ECG signal.

## II. RELATED WORK

There are various techniques are existing to secure 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.

## III. PROPOSED METHODOLOGY

The sender side steganograpgy technique is implemented which is shown in fig.2. All the physiological parameters and patient information inside the ECG signal are encrypted by encryption method. Symmetric encryption method is applied in this method. A wavelet packet decomposition is implemented which decompose the signal into 32 sub bands coefficients. Afterwards, embedding process is implemented by using scrambling matrix and shared key and formed 32 watermarked wavelet coefficients. Finally, watermarked ECG signal is produced by inverse wavelet packet decomposition.

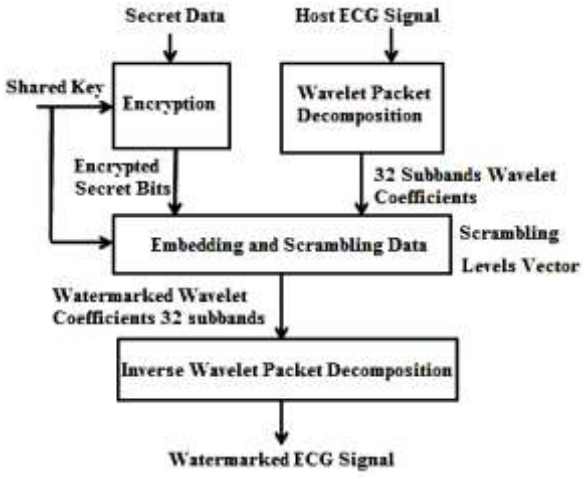


**Fig.2. Block diagram of Sender side steganography**

Frequency decomposition is proposed the embedding operation which produced the watermarked ECG signal. There are various stages are encompassed.

### 3.1.Encryption

Patient information is transmitted from sender to receiver via internet must be encrypted by using encryption technique. In this paper, XOR ciphering method is applied with an ASCII code. There are two types of encryption. First is the asymmetric key encryption, which has private and public keys. Second is the symmetric key encryption, which has only private key [6]. In this paper, symmetric key encryption is executed. Physiological parameters are collected and encrypt it inside the ECG signal. The resultant signal is called encrypted ECG signal.

### 3.2.Wavelet Decomposition

Wavelet transform represents the time frequency analysis (TFA). Wavelet transform shows the time and frequency component. DWT (Discrete Wavelet Transform) decompose the signal into coarse approximation and detailed information. DWT decompose the signal by using band filters [7]. The mathematical expression defined as

$$W(i, j)=\sum_{i}\sum_{j} X(i)\, \psi_{ij}(n) \qquad (1)$$

Where, W (i, j) shows the DWT coefficients, scale parameter is shown by I, shift parameter is shown by j and $\psi$ ij(n) shows wavelet basis time function. Five level wavelet packet decomposition is used in this paper and 32 sub bands wavelet coefficients are produced. Original ECG signal decomposes into two frequency components. First one is a low frequency component and another one is a high frequency component. Low frequency component has important features of ECG signal and high frequency component contains noise. This process has implemented up to five levels.

### 3.3.Embedding Technique

In this stage, Shared key and scrambling matrix is used. The patient physiological information is concealed inside the host ECG signal by using scrambling matrix and private key. 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 involved for making scrambling matrix.

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

Fig.3. shows the embedding operation. At embedding stage, sheared key is converted into ASCII codes. Row is read by sequence fetcher from the scrambling matrix. After getting the first row, patient information is embedded inside the 32 sub bands wavelet coefficients. In embedding operation, 32 sub band wavelet coefficients are read and converted into binary form. Secret bits are replaced by LSB bits of wavelet coefficients and produced the watermarked ECG signal.

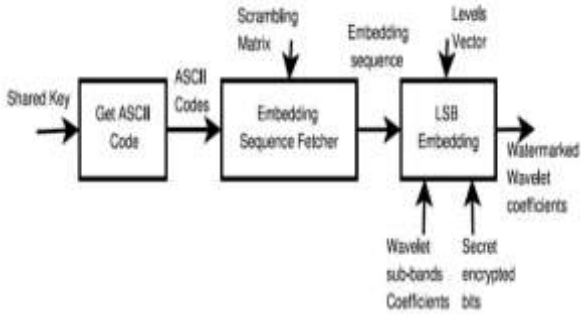


**Fig.3. Block diagram of Watermarked Embedding Operation.**

### 3.4.Inverse Wavelet Decomposition

Watermarked wavelet coefficients are recomposed in this final stage by applying inverse wavelet decomposition. After this, a new watermarked ECG signal is generated, which is similar to original ECG signal. It will repeat all the wavelet coefficients will be reconstructed. Finally, we produced the watermarked ECG signal.

## IV. EXPERIMENTAL RESULTS

ECG signals have taken from physionet. We have shown few results such as encrypted ECG signal and energies of different wavelets. Encryption algorithm is implemented by using five level wavelet packet decomposition. Different wavelets such as Biorthogonal6.8 wavelet, Symlets5 wavelet, Coiflet wavelet and Daubechies4 wavelet are used simultaneously [8]. Energy of original ECG signal and encrypted ECG signal are calculated by using different wavelets. First, we have loaded the ECG signal. The output of original ECG signal is shown in fig.4.

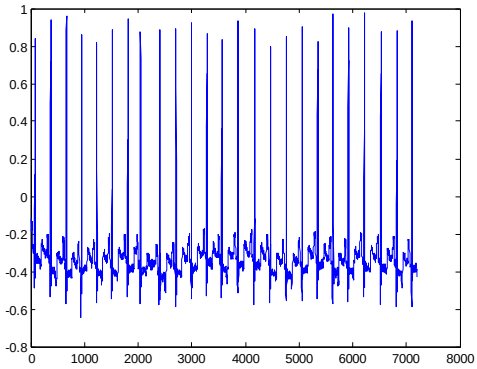


**Fig.4. Host ECG signal.**

Afterwards, ECG signal has decomposed. Consequently, embedding process is implemented by using scrambling matrix and shared 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.5.

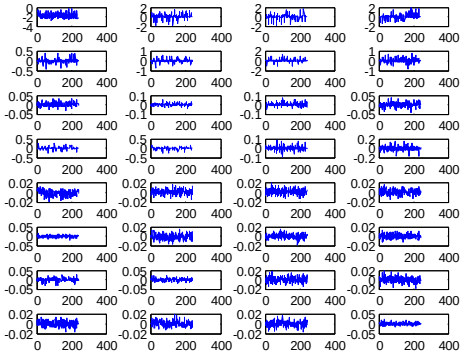

**Fig.5.32 sub band wavelet coefficients**

Then, a new watermarked ECG signal is produced by using inverse wavelet packet decomposition. The watermarked 32 sub band coefficients are shown in fig.6.

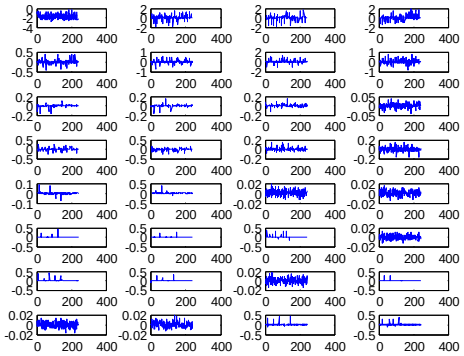

**Fig.6. Inverse wavelet 32 sub bands coefficients**

Then watermarked ECG signal is shown in fig.7.

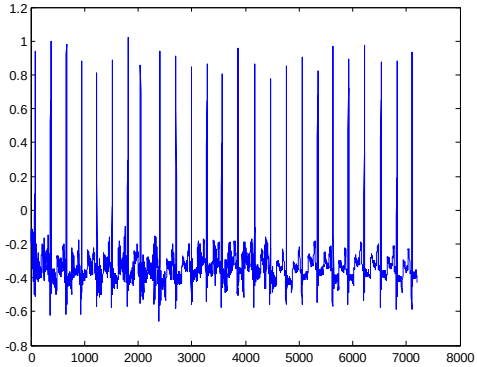

**Fig.7. Watermarked ECG signal**

The information is obtained which is shown in bellow notepad.

Enter the Key Value:=123

Enter the Key Value for Decryption:=123

Name: Ayman ibaida

Date of Birth:1/1/1970

Medicare Number: 1234567890

Telephone Number: 1234567890

Energy of Original Signal: =937.885150

Energy of Watermarked Signal: =941.161100

Table 1 shows the energies of original ECG signal and watermarked ECG signal using different wavelets. E (Original) represents energy of original ECG signal E (biorth6.8) represents energy of encrypted ECG signal using Biorthogonal wavelet, E (sym4) represent 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 |

## V. 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)."*et 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.