A Real Time Processing and Analysis of Watermarked ECG Signal in Remote Patient Monitoring Systems

Joby Jose[1], Anish M.P[2]

[1]Mahatma Gandhi University, University College of Engineering, Thodupuzha, Kerala 685 587, India

[2]Mahatma Gandhi University, University College of Engineering, Thodupuzha, Kerala 685 587, India

Abstract: ***Remote patient monitoring systems and Point-of-Care (PoC) technologies is gaining attention these days. These techniques reduce the medical labor cost and increasing traffic at hospitals. Most of the healthcare systems will collect ECG information on which the physiological readings are hidden and send to hospitals over internet. According to Health Insurance Portability and Accountability Act (HIPAA) while sending medical information over internet it should follow certain guidelines. This is to ensure patients confidentiality and data security inside the communication channels as well as information stored on the hospital server. Through this paper a real time implementation of remote patient monitoring system is being proposed. The processing of data based on encryption and steganography techniques and security analysis being done. The proposed design of remote monitoring system with watermarked ECG signal ensuring high data security, privacy and confidentiality and the retrieval of the physiological readings from the watermarked ECG is being carried out successfully.***

Keywords: PoC, XOR-ciphering, Steganography, DWT.

1. Introduction

Remote patient monitoring systems involve monitoring patients at their homes by collecting biomedical data along with physiological readings and sending it to hospitals over public communication network has got wide applications and advantages. This can reduce the medical labor cost and reduce the increasing traffic at hospitals. The number of old age homes is increasing day by day and a significant number of the inmates suffering from cardiac diseases. Point-of-Care (PoC) [1]-[3] techniques can play a great role in emergency services as well where immediate data exchange can be done and decisions can be made without any delay.

While sending information through internet a lot of security and privacy threats along with data integration issues arise. Data transmitted over public network should follow Health Insurance Portability and Accountability Act (HIPAA) regulations [4]. According to it the patient's privacy and data security is ensured by introducing security protocol and computer software. Introducing security protocol will give patient control on who can access his/her confidential health information, such as name, address, telephone number, and Medicare number. Computer software guarantees the security of the information inside the communication channels as well as the information stored on the hospital server. Of the several methods proposed by researchers a hybrid between encryption and steganography is proposed in this paper. Steganography is the art of hiding secret information inside another type of data called host data. The patients ECG signal is used as the host signal due to the fact that most of the healthcare systems will collect ECG information also the size of ECG signal is large compared to the size of other information.

The proposed model consists of both hardware and software. The hardware part is the ECG acquisition circuit consists of ECG clamps, Amplifier, Filter, Graphic LCD and Microcontroller. The software employed is MATLAB to implement the processing of ECG signal. Processing of the data includes encryption wavelet decomposition and embedding the encrypted data in wavelet coefficients. For security of information inside the communication channel and hospital server encryption of the secret data is done. For encryption the technique employed is XOR-chipering. This will provide data authentication by preventing unauthorized access to medical information and physiological data send along with the ECG signal. Through wavelet decomposition the ECG signal in the time domain is converted into coefficients representing frequency components of the signal at a given time. After wavelet packet decomposition the embedding operation is performed using a special apparatus the scrambling matrix. Before transmission inverse wavelet recomposition is performed to convert the signal back to time domain. At the receiver the watermark (hidden data in ECG signal) is extracted. The proposed model also performs a security analysis to guarantee the maximum security. The block diagram of the proposed model is shown in Figure 1.

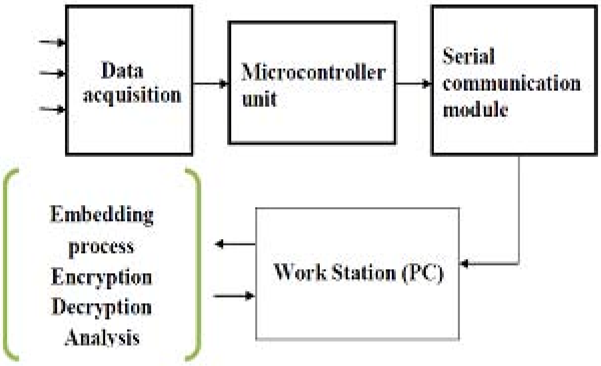

Figure 1: Block diagram of proposed model

2. Current Works and Developments

Many approaches to secure patients sensitive data have been implemented [3], [5]-[7]. Zheng and Qian [8] proposed a new reversible data hiding technique based on wavelet transform. Golpira and Danyali [9] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. Kaur *et al.* [10] proposed new digital watermarking of ECG data for secure wireless communication. Ibaida and khalil [1] proposed a wavelet-based ECG steganography for protecting patients confidential information in Point-of-Care (PoC) systems. Discrete Wavelet Transform (DWT) is applied to signal through band filters resulting in high-frequency and low-frequency components.

3. Methodology

The proposed model consisting of a data acquisition circuit and microcontroller unit in the transmitter section and the workstation where the encryption and embedding operations are performed using software help. The different stages in the acquisition transmission reception process are explained below.

3.1 Data Acquisition

The block diagram of ECG acquisition circuit is shown in Figure 2. ECG clips are connected to AD620 instrumentation amplifier. Instrumentation amplifier amplifies the difference between the signals. Equation for calculating gain of the instrumentation amplifier is given as in (1).

$$G = (49.4k/R) \tag{1}$$

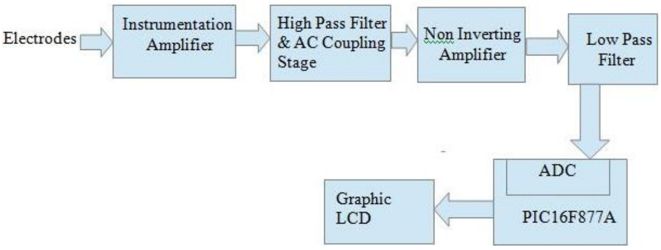

Figure 2: Block diagram of data acquisition circuit

Output of the instrumentation amplifier is given to clamper circuit using operational amplifier for clamping above reference voltage, after that another operational amplifier is used as band-pass filter. Here IC 7660 is used to generate -5V and IC 7805 for +5V. The microcontroller unit employed is PIC 16F877A. The output of the PIC is an 8 bit binary sequence ranging values from 0 to 255. The analog ECG is displayed on the graphic LCD.

3.2 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's confidential information. XOR ciphering technique is used with an ASCII coded shared key which will play the role of the security key.

3.3 Wavelet Decomposition

Wavelet transform [11] is a powerful tool to combine time domain with frequency domain in one transform.

In this stage of processing Discrete Wavelet Transform (DWT) being applied using band filtering creating 32 level sub-bands of ECG signal as high and low frequency components [12].

3.4 Embedding

At this stage the proposed technique will use a special security implementation to ensure high data security (a second level data security). A scrambling operation is performed using two parameters. First is the shared key known to both the sender and the receiver and second is the scrambling matrix, which is stored inside both the transmitter and the receiver. Each transmitter/receiver pair has a unique scrambling matrix.

The embedding stage starts with converting the shared key into ASCII codes; therefore each character is represented by a number from 1 to 128. For each character code, the scrambling sequence fetcher will read the corresponding row from the scrambling matrix. The steganography level is determined according to the level vector which contains the information about how many LSB bits will be changed for each sub-band. Accordingly, the selected steganography level for bands from 1 to 17 is 5 bits and 6 bits for the other bands. This is because hiding data in some sub-bands will highly affect the original signal while hiding in other sub-bands would result in small distortion effect. The operations performed in the embedding process are shown in Figure 3.

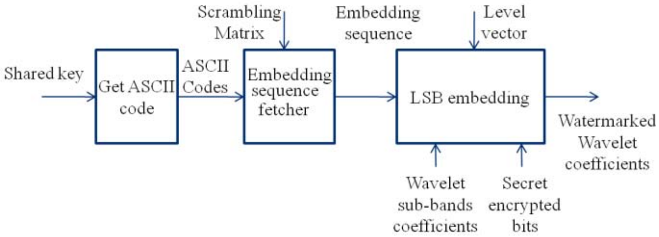

Figure 3: Block diagram of watermark embedding operation

3.5 Inverse Wavelet Recomposition

In this stage the wavelet coefficients are converted into time domain. The resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet recomposition. The result of this operation is the new watermarked ECG signal. The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain. Therefore, the newly reconstructed watermarked ECG signal will be very similar to the original ECG signal.

3.6 Watermark Extraction

In this stage the secret bits from the watermarked ECG signal is extracted at the receiver end. The extraction process is done only if the shared key value, scrambling matrix, and steganography levels vectors are known. The stages in the extraction process are shown in Figure 4. The first step is to apply five-level wavelet packet decomposition to generate the 32 sub-bands signals. Next, using the shared key and scrambling matrix the extraction operation starts extracting the secret bits in the correct order according to the sequence rows fetched from the scrambling matrix. Finally, the extracted secret bits are decrypted using the same shared key.

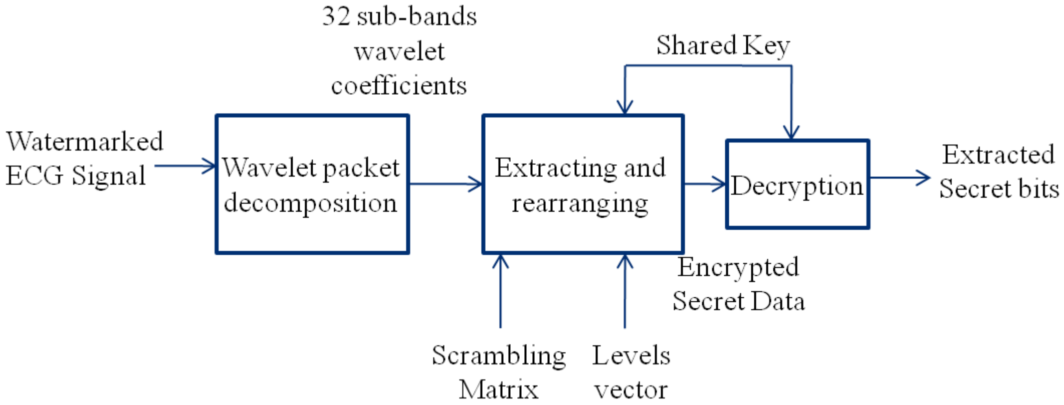

Figure 4: Block diagram of receiver steganography

4. Security Analysis

The proposed model's capability to ensure data security is based on the encryption and steganography techniques. The security key for encryption and shared key for embedding can be different by doing so it will provide a second level off security for the hidden data. The scrambling matrix is stored in the transmitter/receiver pair and it will not be transmitted. To guarantee the maximum security, the length of the key (L) used should satisfy (2).

$$L = \text{Max}\ (B/180,\ M) \quad (2)$$

Where B is the size of the embedded data in bits and M represents the minimum key size.

The amount of data that can be stored is calculated using (3).

$$b = (t*fs/32)*180 \quad (3)$$

Where b is the total number of bits stored, t is the total signal time in seconds, and fs are the sampling frequency.

5. Conclusion

In this paper remote patient monitoring system being studied and implemented in real time and processing techniques being described. The watermarked ECG signal can be used for diagnoses purpose also the watermarks can be successfully extracted. Analysis for security measures being done. It is found that it can be implemented successfully for commercial applications. In future this can be implemented in android mobile phones by developing applications that can perform the encryption and steganography operations.

References

[1] A. Ibadia, and I. Khalil "Wavelet-based ECG steganography for protecting patients confidential information in Point-of-Care systems," IEEE Trans. Biomed. Eng. Vol. 60, no. 12, pp. 3322-3330, Dec. 2013.

[2] Y. Lin, I. Jan, P. Ko, Y. Chen, J. Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport," IEEE Trans. Inf. Technol. Biomed., vol. 8, no. 4, pp. 439–447, Dec. 2004.

[3] 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. Inf. Technol. Biomed., vol. 11, no. 6, pp. 619–627, Nov. 2007.

[4] 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.

[5] 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.

[6] A. De la Rosa Algarin, S. Demurjian, S. Berhe, and J. Pavlich Mariscal, "A security framework for xml schemas and documents for healthcare," in Proc. IEEE Int. Conf. Bioinf. Biomed. Workshop, pp. 782–789, Oct. 2012.

[7] M. Li, S. Yu, Y. Zheng, 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.

[8] K. Zheng and X. Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms," in Proc. Int. Conf. Comput. Intell. Security, vol. 1, pp. 295–299, Dec. 2008.

[9] 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., pp. 31–36, Dec. 2009.

[10] 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., pp. 140–144, Mar. 2010.

[11] A. Poularikas, Transforms and Applications Handbook. Boca Raton, FL, USA: CRC Press, 2009.

[12] 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.

Author Profile

Joby Jose, BTech in Electronics and Communication from NSS College of Engineering, University of Calicut. Now doing Mtech Applied electronics in M.G University College of Engineering. **Anish M.P,** Lecturer Dept. of ECE, University college of Engineering. Thodupuzha, Kerala.