ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(24), DOI: 10.17485/ijst/2015/v8i24/80448, September 2015* ISSN (Online) : 0974-5645

Wavelet based ECG Steganography for Protecting Patient Confidential Information

M. Sucharitha[1]* and K. Parimala Geetha[2]

[1]ECE, Noorul Islam University, Kumaracoil - 629180, Tamil Nadu, India; sucharitha_m2002@yahoo.co.in
[2]ECE, Ponjesly College of Engineering, Nagercoil - 629502, Tamil Nadu, India

Abstract

With the growing number of aging population and most of the patients are suffering from cardiac diseases, it is conceivable that remote ECG patient monitoring systems are expected to be widely used as Point-of-Care (PoC) applications in hospitals around the world. Therefore, huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and are then diagnosed by remote patient monitoring systems. It is utterly important that patient confidentiality is protected while data is being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems. In this paper, a wavelet based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. It is found that the proposed technique provides high security protection for patients data and ECG data remains diagnosable after watermarking (i.e. hiding patient confidential data) and as well as after watermarks (i.e. hidden data) are removed from the watermarked data.

Keyword: ECG Signal, Steganography, Watermarking, Wavelet Transform

1. Introduction

In Point-of-Care (PoC) systems, a patient is connected to the hospital server for constant monitoring of cardiovascular disease diagnosis and emergency response services[3]. In such a system the patient's ECG signal is acquired using sensors and then transmitted by using zigbee transmitter[5]. The mobile then transmits this ECG signal to the hospital server through public internet[1]. The hospital server on the other hand receives the patient's ECG signal and validates it with ECG based biometric security system. After successful validation, the identity of the patient is known to the hospital and the services for which the patient is subscribed for. The signal is then used for diagnostic purposes.

In the above system, the patient's ECG signal is transmitted without being encrypted resulting into the data being vulnerable to access from an unauthorized entity. Therefore if this unencrypted ECG signal falls into the wrong hands, then the patient's privacy is compromised. This compromised data then can be sold to various organizations. Since ECG signals are also used in biometric security systems, the compromised data can also be used to gain unauthorized access to various systems that use biometric security.

To protect the patient's confidential information, the ECG signal needs to be encrypted. In previous researches many approaches were established to secure patient sensitive data. Many of them proposed to secure the confidential data based on steganography techniques to hide information[4]. Permutation cipher is used to encrypt the confidential data whereas in noised smearing technique is used to alter the original ECG signal which can then be reverted back to its original state using a security key.

*Author for correspondence

Several researchers have proposed various security protocols to secure patient confidential information. In this proposed method a steganography technique based on wavelet transformation for securing the patient information is implemented.

2. Related Work

F. Hu, et al.[2] uses a low-cost low-power sensor and wireless communication technology for ECG monitoring purposes. Based on wireless sensor network technology, wearable mobile platforms are distributed to the patients of concern. These mobile platforms are responsible for gathering patient vital sign using a three-lead ECG monitoring system. The gathered data are transmitted wirelessly over radio to the receiving station connected to a workstation where the data are processed. These data provide meaningful information for the diagnosis of possible cardiovascular diseases. In this method human processing is not only time consuming for some tasks but also error prone.

H. Wang, et al.[7] proposed BSN architecture and its corresponding algorithms for healthcare monitoring applications, especially ECG-based applications.

De la Rosa Algarin A., et al.[9] has proposed an XML security framework that has addressed the issue of providing security in meta-systems that utilize security policies defined after the different access control models (RBAC, MAC and DAC). In these cases, it is not enough to utilize the security requirements of the newly developed system. These are many approaches to secure patient sensitive data. However, one approach proposed to secure data is based on using steganography techniques to hide secret information inside medical images.

K. Zheng and X. Qian[13] proposed a new reversible data hiding technique based on wavelet transform. Their method is based on applying B-spline wavelet transform on the original ECG signal to detect QRS complex. This method has low capacity since it is shifting one bit. Furthermore for security purpose it does not use a user defined key. Finally, this algorithm is based on normal ECG signal in which QRS complex can be detected but for abnormal signal QRS complex cannot be detected.

H. Golpira and H. Danyali[12] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of this algorithm is low and no encryption key is involved in its watermarking process.

S. Kaur, et al.[11] quantized each ECG sample is using 10 bits and is divided into segments. The segment size is equal to the chirp signal and a patient ID is used in the modulation process of the chirp signal. The resulting watermarked signal is 11 bits per sample. The final signal consists of 16 bits per sample with 11 bits for watermarked ECG and 5 bits for the factor and patient ID. The digital watermarking of the ECG signal for secure communication is proposed.

3. Proposed Method

The first step is to apply 5-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. The watermark extraction process is almost similar to the watermarking embedding process except that instead of changing the bits of the selected node, it is required to read values of the bits in the selected nodes, and then resetting them to zero. Figure 1 and Figure 2 shows the sender steganography and receiver steganography.

3.1 Sender Steganography

3.1.1 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 this stage XOR ciphering technique is used with an ASCII coded shared key which will play the role of the security key. XOR ciphering is selected because of its simplicity.

3.1.2 Wavelet Decomposition

Wavelet transform is a process that can decompose the given signal into coefficients representing frequency components of the signal at a given time.

In this work, 5-level wavelet packet decomposition has been applied to the host signal and hence 32 sub-bands are resulted from this decomposition process. In decomposition iteration the original signal is divided into two signals.

Therefore, one of the resulting signals will represent the high frequency component and the other one represents

the low frequency component. Most of the important features of the ECG signal are related to the low frequency signal. In our proposed technique different number of bits will be changed in each wavelet coefficient (usually called steganography level) based on its sub-band.

3.1.3 Embedding Operation

At this stage the proposed technique will use a special security implementation to ensure high data security[8]. In this technique a scrambling operation is performed using two parameters[6]. First is the shared key known to both the sender and the receiver. Second is the scrambling matrix, which is stored inside both the transmitter and the receiver. Each transmitter/receiver pair has a unique scrambling matrix.

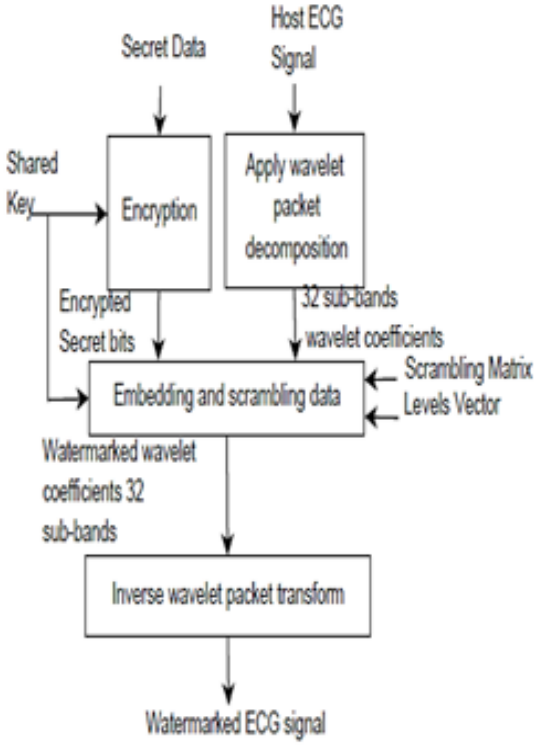

Figure 1. Block diagram for sender steganography.

3.2 Receiver Steganography

3.2.1 Inverse Wavelet Transform

Resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet decomposition. 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.

3.3 Extraction and Rearranging

In this stage the encrypted and decomposed data is extracted by the use of the wireless zigbee transmitter and the microchip Tarang f4 it receives the encrypted signal and it rearranges the signal which are fed into the ECG signal and it is done by the help of the scrambling matrix.

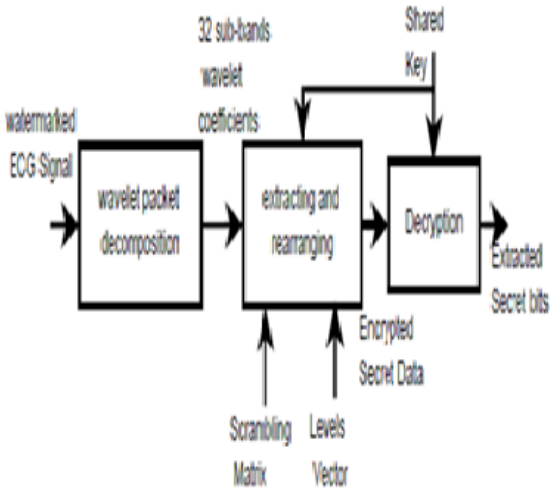

Figure 2. Block diagram for receiver steganography.

3.4 Decryption

Finally, the extracted secret bits are decrypted using the same shared key.

4. Experiments and Results

The ECG signal in which the data is to be hided is shown in Figure 3.

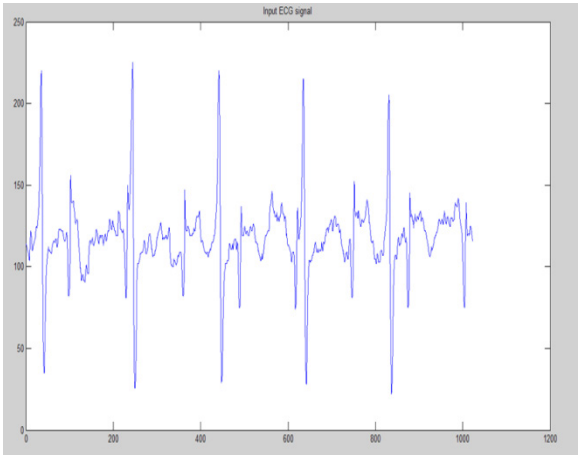

Figure 3. Raw ECG signal.

The data such as patient information to be hided is saved in the form of text document. In the embedding operation, both the encryption key and data hiding key is activated and is shown in Figure 4.

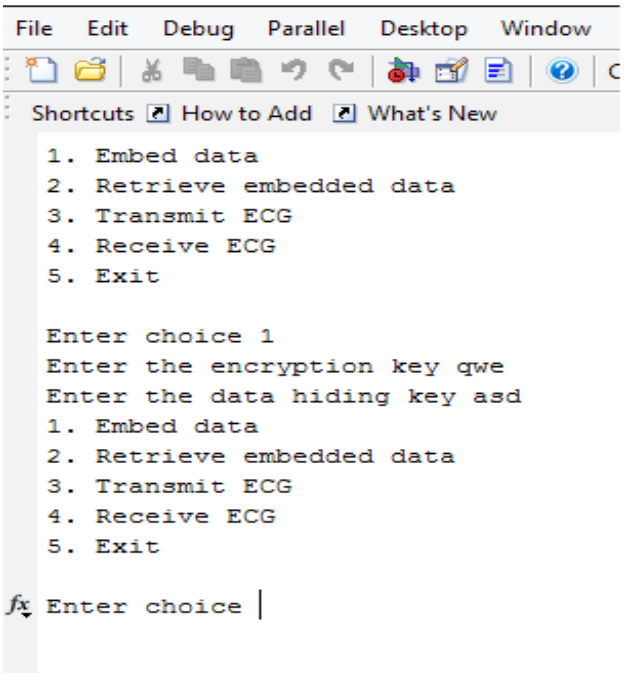

Figure 4. Embedding Operation

In Figure 5 data are hidden in the ECG signal and is transmitted to maintain confidentiality about the patient information.

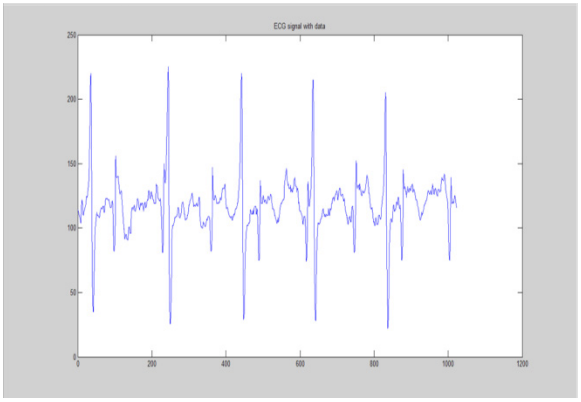

Figure 5. **Hidden data in the ECG signal.**

At the receiver section the patient information such as Blood pressure, Glucose level, temperature is retrieved from the ECG signal is shown in Figure 6.

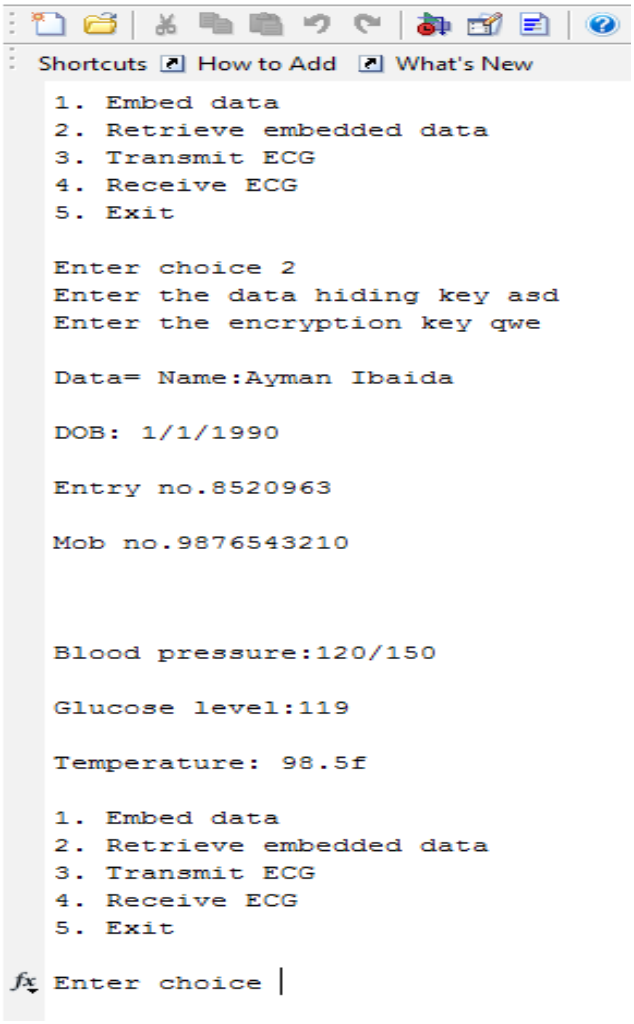

Figure 6. Retrieving data from ECG signal.

5. Conclusion

In this paper a novel steganography algorithm is proposed to hide patient information inside ECG signal. This technique will provide a secured communication and confidentiality in a Point-of-Care system. A 5-level wavelet decomposition is applied. A scrambling matrix is used to find the correct embedding sequence based on the user defined key. The hidden information in the ECG signal can be extracted and it is transmitted to another PC through wireless zigbee transceiver and it's again retrieved.

6. References

1. Lin Y, Jan I, Ko P, Chen Y, Wong J, Jan G. A wireless PDA-based physiological monitoring system for

patient transport. IEEE Trans Inform Tech Biomed. 2004; 8(4):439–47.
2. Hu F, Jiang M, Wagner M, Dong D. Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software code sign. IEEE Trans Inform Tech Biomed. 2007; 11(6):619–27.
3. Ibaida A, Khalil I, Sufi F. Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using Principal Components Analysis (PCA). IEEE 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP); 2010. p. 207–12.
5. Malasri K, Wang L. Addressing security in medical sensor networks. Proceedings of the 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments; 2007. p. 12.
6. Maglogiannis I, Kazatzopoulos L, Delakouridis K, Hadjiefthymiades S. Enabling location privacy and medical data encryption in patient tele-monitoring systems. IEEE Trans Inform Tech Biomed. 2009; 13(6):946–54.
7. Wang H, Peng D, Wang W, Sharif H, Chen H, Khoynezhad A. Resource-aware secure ECG healthcare monitoring through body sensor networks. IEEE Wireless Comm. 2010; 17(1):12–9.
8. Marvel L, Boncelet C, Retter C. Spread spectrum image steganography. IEEE Trans Image Process. 1999; 8(8):1075–83.
9. De la Rosa Algarin A, Demurjian SA, Berhe S, Pavlich-Mariscal J. A security framework for XML schemas and documents for healthcare. IEEE Trans Inform Tech Biomed. 2012. p. 782–9.
11. Kaur S, Singhal R, Farooq O, Ahuja B. Digital watermarking of ECG data for secure wireless Communication. IEEE International Conference on Recent Trends in Information, Telecommunication and Computing; 2010. p. 140–4.
12. Golpira H, Danyali H. Reversible blind watermarking for medical images based on wavelet histogram shifting. IEEE International Symposium on Signal Processing and Information Technology; 2010. p. 31–6.
13. Zheng K, Qian X. Reversible data hiding for electrocardiogram signal based on wavelet transforms. International Conference on Computational Intelligence and Security; 2008.