Survey on Wavelet based ECG Stegnography for Protecting Patients Confidential Information

Muhusina Ismail[1] Shiney Thomas[2]
[2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Amal Jyothi College of Engineering Kanjirappally, Kottayam, India

Abstract— In this modern era, the use of e-health application is widely increased. Majority of the aging people are suffering from cardiac dis-eases, so it is very crucial important to save the patient's life by diagnosing cardiac diseases on time, by make use of these e-health applications. The best example of this is of Remote Cardiac Patient Monitoring application. Thus Point of Care systems make use of this application. With the growth of human rights, people are more and more concerned about the privacy of their information and other important data. The objective of this paper is to makes use of electrocardiography (ECG) data as host signal in order to protect individual information. An ECG signal can not only be used to analyze dis-ease, but also to provide crucial biometric in-formation for identification and authentication. Thus we are integrating patients physiological readings like blood pressure, temperature, glucose level, etc into patients ECG, and this host signal will watermarked and transmitting to re-mote patient monitoring system via public net-work. This paper introduces a wavelet-based steganography technique which combines encryption and scrambling technique to protect patient confidential data. After several experiments and evaluation this study proves that host signal will not affect any distortion and is less than 1%.

Key words: ECG, Reversible Data Hiding, voltage balance

I. Introduction

The number of elderly patients is increasing dramatically due to the recent medical advancements.

Accordingly, to reduce the medical labour cost the use of remote healthcare monitoring systems and Point-of-Care (PoC) technologies have become popular. Monitoring patients at their home can drastically reduce the increasing traffic at hospitals and medical centers. Moreover, Point-of-Care solution can provide more re-liability in emergency services as patient medical in-formation (ex. for diagnosis) can be sent immediately to doctors and response or appropriate action can be taken without delay. However, Remote health care systems are used in large geographical areas essentially for monitoring channel used to exchange information. Typically, patient biological signals and other physiological readings are collected using body sensors. Next, the collected signals are sent to the patient PDA device for further processing or diagnoses. At last, the signals and patient confidential information as well as sending the diagnoses report or any urgent alerts to the central hospital servers via the Internet. Those biomedical signals are then checked by doctors and possibly make a decision in case of an emergency from anywhere using any device [2]. Using Internet as main communication channel, which leads to new security and privacy threats as well as data integration issues? Based on the Health Insurance Portability and Accountability Act (HIPAA), information through the Internet should be protected and secured. HIPAA mandates that a patients privacy and confidentiality be protected, while information are transmitting through the internet as follows:

A. *Patient privacy:*

It is of crucial importance that a patient can control who will use his/her confidential health information, such as name, address, telephone number, and Medicare number. As a result, the security protocol should provide further control on who can access patients data and who cannot.

B. *Security:*

The security of the information inside the communication channels as well as the information stored on the hospital server should be guaranteed by the methods of computer software. Accordingly, it is of crucial importance to implement a security protocol which will have powerful communication and storage security.

Cardiovascular diseases (CVD) are the Number One killer of the modern era. Wireless cardiovascular monitoring facilities are widely used to provide continuous patient monitoring and to send urgent alerts to the specialists in case of any emergency or abnormal life threatening cardiac behaviour. Accordingly, Electrocardiogram (ECG) signals are widely used in these monitoring systems. ECGs are electrical signals that reflect the heart electrical functionalities over time and they are collected using electrodes. Consequently, the development of portable wireless monitoring facilities such as body sensors has increased significantly with the aim of utilizing ECG signals to diagnose most cardiac diseases. The use of E-health applications is increasing to a great extent around the globe. Many health-care organizations such as insurance companies, hospitals, and government health sec-tors require access to patient information and records including their archived biomedical signals. There-fore, patient records need to be stored in a centralized repository which will allow other health-care organizations to access these records. Service can be facilitated by cloud. In typical wireless tele-monitoring systems with body sensor networks, patients wear one or more body sensors to collect their ECG signals. Next, the collected biomedical signals are transmitted to the patients smart-phone where any processing required is implemented. Finally, the collected signals as well as other patient information are transmitted to the medical cloud using the Internet.

II. Problem Statement

Several researchers have proposed various security protocols to secure patient confidential information. Techniques used can be categorized into two sub-categories. Firstly, there are techniques that are based on encryption and cryptographic algorithms. These techniques are used to secure data during the communication and storage. As a result, the final data will be stored in encrypted format. The disadvantage of using encryption based techniques is its large computational overhead. Therefore, encryption based methods are not suitable in resource-constrained mobile environment.

Other techniques are called steganography techniques; Steganography is the art of hiding secret information inside another type of data called host data [6].

III. PROBLEM FORMULATION

Many security techniques are based on the fact that hiding its sensitive information inside another insensitive host data, without bothering about the host data size increment and huge computational overhead. These techniques are called steganography techniques. Steganography is the art of hiding secret information inside another type of data called host data. However, steganography techniques alone will not solve the authentication problem and cannot give the patients the required ability to control who can access their personal information as stated by HIPAA.

IV. RELATED WORK

To secure patient sensitive data several methods has been introduced. However, among these, one approach that is used to secure data is based on using steganography techniques to hide secret information inside medical images [3] [4] [5]. The challenging factors of these techniques are how much information can be stored, and to what extent the method is secure. Finally, what will be the resultant distortion on the original medical image or signal.

A. Reversible Data Hiding Technique:

The method [4] is based on applying B-spline wavelet transform on the original ECG signal to detect QRS complex. After detecting R waves, Haar lifting wavelet transform is applied again on the original ECG signal. Next, the non QRS high frequency wavelet coefficients are selected by comparing and applying index subscript mapping. Then, the selected coefficients are shifted one bit to the left and the watermark is embedded. Finally, the reverse haar lifting wavelet transform is applied to reconstruct the ECG signal. Moreover, before they embed the watermark, for watermark scrambling, Arnold transform is applied. Since it is shifting one bit, this method has low capacity. As a result for each ECG sample value only one bit can be stored. Furthermore, the security in this algorithm relies on the algorithm itself, it does not use a user defined key. Finally, this algorithm is based on normal ECG signal in which complex can be detected. However, for abnormal signal in which QRS complex cannot be detected, the algorithm will not perform well.

B. Reversible Blind Watermarking Technique:

The technique is for medical images based on wavelet histogram shifting [5]. In these work medical images such as MRI is used as host signal. A two dimensional 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 second threshold's right histogram part to the right. For inserting the binary watermark data the locations of the zero points and the thresholds are used. This algorithm will not perform well for ECG host signals but for MRI images. Moreover, the capacity of these algorithms is low and no encryption key is involved in its watermarking process.

C. A New Digital Watermarking Technique:

This is a new digital watermarking [3] of ECG data for secure wireless communication. Here, each ECG sample is quantized using 10 bits, and is divided into segments. The segment size is equal to the chirp signal that they use. Therefore, a modulated chirp signal is added for each ECG segment .In the modulation process of the chirp signal, Patient ID is used. Next, multiplying the modulated chirp signal with a window dependent factor, and then added to the ECG 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. However, in this algorithm the size of ECG signal is increased from 12 bits/sample to 16 bits/sample. This behavior overrides completely the concept of using steganography and the main purpose of steganography that does not increase the original size of the host signal.

D. Time Domain Special Range ECG Steganography:

In recent e-health systems the usage of ECG signal has increased significantly to provide highly qualified remote medical services. Here, a new steganography technique [6] [1] is introduced that is able to hide the secret message in any position in the host signal without distorting the original signal.

This technique provides high security for the secret message by selecting more secured positions (such as MSB) in the host ECG signal that are unexpected to the intruders. This model consists of four sequential steps. The first step is responsible for shifting up and scaling the ECG signal to avoid the negative values and converting the signal floating point numbers into integers the function of this step represents the first level of security of the steganography technique by hiding the values of both shifting and scaling factors that are mandatory parameters for extracting the secret information. A number of special values in the ECG signal samples are found to be relevant hosts that can hide the secret bits in the most significant positions with the condition of inverting the values of the right hand bits to the secret bit position. The data hiding process is to hide the secret bits using the shifted value as a host, then the resultant value would be shifted back to its original level. ECG Signal Scaling and Level Correction is done - finally to extract the hidden data from the host signal the receiver needs to know two parameters, the used range and signal pre-processing parameters.

E. Frequency Domain Wavelet based ECG Steganography:

The sender side of this steganography technique [6] [1] consists of four integrated stages. The proposed technique is designed to ensure secure 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. The main target of steganography is to put out of sight the secret message in the other cover media so that nonentity can see that and both participants are converse in secret way. By combining the techniques of steganography and the other techniques, information security has improved noticeably. Steganography are of two types:

1) Fragile:

In this type of steganography, if the file is modified then the embedded information is destroyed.

2) Robust:

This steganography, embed information into a media which cannot be simply destroyed.

The steganography are used, mainly because of its capacity and security. Here it ensures complete confidentiality over patients secret information. This guarantees minimum distortion of the host signal, which carries the patients confidential information as well as physiological readings for diagnoses. Capacity of this is high and computational overhead is less.

Parameters	**Reversible Data Hiding**	**Reversible Blind Watermarking**	**Digital Watermarking**	**Time Domain ECG Steganography**	**Frequency Domain Wavelet based ECG Steganography**
Accuracy	low	medium	low	medium	high
Capacity	low	low	medium	medium	high
Distortion	high	high	high	medium	low
Security	low	medium	medium	medium	high
Computation Overhead	high	high	medium	high	medium

Table 1: Comparison Table

V. Summary and Conclusions

Several algorithms were proposed to hide patient information as well as diagnostics information inside an patients biomedical signal. These techniques will provide a secured communication and confidentiality in the current e-health system. A time domain steganography technique is proposed which is based on applying special range transform to provide the ability to hide the data in any bit position with minimum error. In the frequency domain technique, a 5-level wavelet decomposition is applied. A scrambling matrix is used to find the correct embedding sequence 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 by experimental methods. It was found that the resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted. The wavelet based steganographic technique [1] guarantees minimum distortion and it ensure security and confidentiality over patients confidential information.

References

[1] Ayman Ibaida, Ibrahim Khalil “Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems, "IEEE Transactions On Biomedical Engineering., Dec.2013., vol. 60, no. 12,

[2] F. Hu, M. Jiang, M. Wagner, and D. Dong, “Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hard-ware” software code sign, "IEEE Trans. Inf. Tech-nol. Biomed., Nov. 2007., vol. 11, no. 6, pp. 619627

[3] S. Kaur, R. Singhal, O. Farooq, and B. Ahuja, “Digital watermarking of ECG data for secure wireless communication," in Proc. Int. Conf. Re-cent Trends Inf. Telecommun. Comput., Mar. 2010, pp. 140144.

[4] K. Zheng and X. Qian, “Reversible data hiding for electrocardiogram signal based on wavelet trans-forms," in Proc. Int. Conf. Comput. Intell.Security, Dec. 2008, vol. 1, pp. 295299

[5] 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., Dec. 2009, pp. 3136

[6] L. Marvel, C. Boncelet, and C. Retter, “Spread spectrum image steganography," in Proc. IEEE Trans. Imag. Process, Aug. 1999, vol. 8, no. 8, pp. 10751083,