Asian Journal of Electrical Sciences (AJES)
Vol.3.No.1 2015pp 10-12.
available at: www.goniv.com
Paper Received : 08-03-2015
Paper Accepted: 20-03-2015
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

ECG STEGANOGRAPHY IN POINT-OF-CARE SYSTEMS

R.PRABHU, T.SARANYA & T.V.SUDHIRAA
Final Year B.Tech IT
P.S.R Engineering College.

ABSTRACT

Remote ECG patientmonitoring systems are expected to be widely used as point-of-care (PoC) applications in hospitals around the world. Therefore, huge amount of ECG signal co;llected by body sensor networks from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level, etc., and diagnosed by those remote patient monitoring systems. It is utterly important that patient confidentiality is protected while data are 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. The proposed technique provides high-security protection for patients data with low (less than 1%) distortion and ECG data remain diagnosable after watermarking (i.e., hiding patient confidential data) and as well as afterwatermarks (i.e., hidden data) are removed from the watermarked data.

IndexTerms—Confidentiality, ECG, encryption, steganography,watermarking, wavelet.

I. INTRODUCTION:

PoC solutions can provide more reliability in emergency services as patient medical information (e.g., diagnosis)can be sent immediately to doctors and response or appropriate action can be taken without delay. The signals collected using the sensor and patient confidential information as well as diagnoses report or any urgent alerts are sent to the central hospital servers via the Internet. Doctors can check those biomedical signals and possibly make a decision in case of an emergency from anywhere using any device. Using Internet as main communication channel introduces new security and privacy threats as well as data integration issues. According to the Health Insurance Portability and Accountability Act (HIPAA), information sent through the Internet should be protected and secured.

Several researchers have proposed various security protocols to secure patient confidential information. Techniques used can be categorized into two subcategories. First, there are techniques that are based on encryption and cryptographic algorithms.These techniques are used to secure data during the communication and storage. The disadvantage of using encryption-based techniques is its large computational overhead. Therefore, encryption-based methods are not suitable in resource-constrained mobile environment. Alternatively, many security techniques are based on hiding its sensitive information inside another insensitive host data without incurring any increase in the host data size 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 [8]. 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.

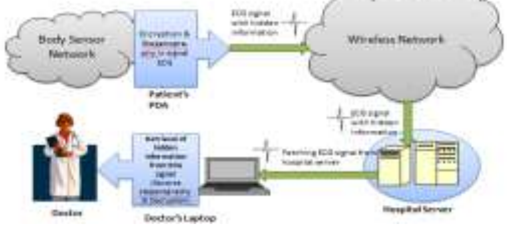

Body Sensor Network
Patient's PDA
ECG signal with hidden information
Wireless Network
ECG signal with hidden information
Fetching ECG signal from hospital server
Hospital Server
Doctor
Doctor's Laptop

Fig. a. ECG steganography scenario in Point-of-Care (PoC) systems

In this model(Fig:(a)) body sensor nodes will be used to collect ECG signal, glucose reading, temperature, position and blood pressure,the sensors will send their readings to patient's PDA device via Bluetooth. Then, inside the patient's PDA device the steganography technique will be applied and patient secret information and physiological readings will be embedded inside the ECG host signal. Finally, the watermarked ECG signal is sent to the hospital server via the Internet. As a result, the real size of the transmitted data is the size of the ECG signal only without adding any overhead, because the other information are hidden inside the ECG signal without increasing its size. At hospital server the ECG signal and its hidden information will be stored. Any doctor can see the watermarked ECG signal and only authorized doctors and certain administrative personnel can extract the secret information and have access to the confidential patient information as well as other readings stored in the host ECG signal. Hence this method satisfies the HIPAA's criteria over protecting the information.

II. RELATED WORK

The challenging factors of the proposed technique is that 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. S. Kaur and B. Ahuja, proposed a Digital watermarking of ECG data for secure wireless communication. In their work, 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, for each ECG segment a modulated chirp signal is added. Patient ID is used in the modulation process of the chirp signal. Next, the modulated chirp signal is multiplied by 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.

III.METHODOLOGY:

The sender side of the proposed steganography technique consists of four integrated stages as shown in Fig.b.

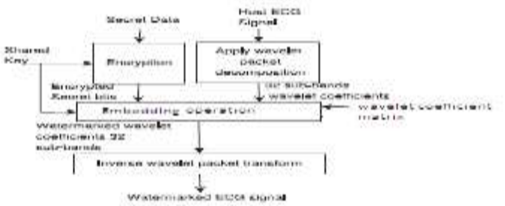

Secret Data
Host ECG Signal
Shared Key
Encryption
Apply wavelet packet decomposition
Encrypted Secret bits
32 subbands wavelet coefficients
Embedding operation
wavelet coefficient matrix
Watermarked wavelet coefficients 32 subbands
Inverse wavelet packet transform
Watermarked ECG signal

Fig. b. Block diagram of the sender steganography which includes encryption, wavelet decomposition, and secret data embedding.

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.

A. 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 this stage, XOR ciphering technique is used because of its simplicity.It can be easily implemented inside a mobile device.

B. Stage 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. Wavelet transform can be defined as
follows:

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

where ψ represents wavelet function. S and P are positive integers representing transform parameters. C represents the coefficients which is a function of scale and position parameters. Wavelet transform is a powerful tool to combine time domain with frequency domain in one transform. In most applications, discrete signals are used. Therefore, discrete wavelet transform (DWT) must be used instead of continuous wavelet transform. DWT decomposition can be performed by applying wavelet transform to the signal resulting in four different signals. Therefore, in our proposed technique different number of bits will be changed in each wavelet coefficient(usually called steganography level) based on its subband.

C. Stage 3: The Embedding Operation

At this stage, the proposed technique will use a special security implementation to ensure high data security. The embedding operation is performed using two parameters. First is the shared key known to both the sender and the receiver. Second is the wavelet coefficient matrix, which is stored inside both the transmitter and the receiver. Each transmitter/receiver pair has a unique wavelet coefficient matrix. The embedding operation performs the data hiding process in the wavelet coefficients.This process will start by reading the current wavelet coefficient in subband and changing its LSB bits. On the other hand, the steganography level is determined according to the level vector which contains the information about how many LSB bits will be changed for each subband.

D. Stage 4:Inverse Wavelet Recomposition

In this final stage, the resultant watermarked 32 subbands 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 unwatermarked ECG signal. Finally, the coefficient matrix will be shifted again and rescaled to return its original range and inverse wavelet transform is applied to produce the watermarked ECG signal.

E) Watermark Extraction Process

To extract the secret bits from the watermarked ECG signal,the following information is required at the receiver side.

1) The shared key value.

2) Wavelet coefficient matrix.

The stages of the extraction process can be shown in Fig.c.The first step is to decompose the watermarked signal. Next, using the shared key and wavelet coefficient matrix the extraction operation starts extracting the secret bits in the correct order. Finally, the extracted secret bits are decrypted using the same shared key. The watermark extraction process is almost similar to the watermarking embedding process.

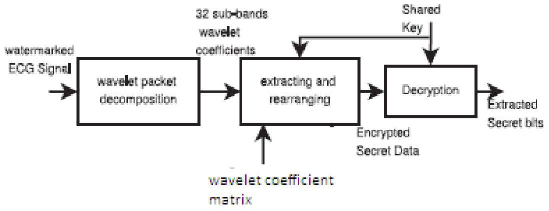


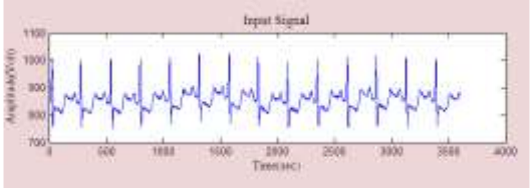
Fig.C. Block diagram of the receiver steganography which includes wavelet decomposition, extraction, and decryption.

VII. CONCLUSION

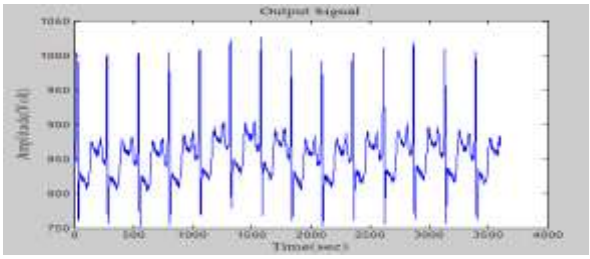
In this paper, steganography technique is proposed to hide patient information, since it provides a secured communication and confidentiality in a PoC system. The ECG signal within which the data is hidden is sent successfully and the receiver is thus able to extract the hidden data from this signal without any larger distortion in the original signal.

RESULT:

Original signal:



Watermarked signal:



REFERENCES

[1] 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.

[2] 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.

[3] 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.

[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] 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.

[6] L. Marvel, C. Boncelet, and C. Retter, "Spread spectrum image steganography," IEEE Trans. Imag. Process., vol. 8, no. 8, pp. 1075–1083, Aug. 1999.

[7] M. Li, S. Yu, Y. Zheng, K. Ren, andW. 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] 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.

[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., Dec. 2009, pp. 31–36.

[10] 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.