ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

ECG Steganography Based Privacy Protecting Of Medical Data for Telemedicine Application

N. Suganya[1], M. Marimuthu[2]

PG Student, Department of Applied Electronics, Sri Subramanya College of Engineering and Technology, Palani, Tamilnadu, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Sri Subramanian College of Engineering and Technology, Palani, Tamilnadu, India[2]

ABSTRACT: The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in ECG signals. The proposed encryption technique used to encrypt the confidential data into unreadable form and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After data encryption, the data hider will conceal the secret data into the ECG signal coefficients. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using chaos crypto system. This is the reason a new security approach called reversible data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. Here the discrete wavelet transformation is used to decompose an ECG signal to different frequency sub bands. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the high frequency coefficients. In the data extraction module, the secret data will be extracted by using relevant key for choosing the relevant data to extract the data. By using the decryption keys, extracted text data will be decrypted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery.

KEYWORDS*:* ECG, Steganography, Encryption, Wavelet, Watermarking, Confidentiality.

I. INTRODUCTION

A. MOTIVATION OF THE PROJECT

The number of elderly patients is increasing dramatically due to the recent medical advancements. Accordingly, to reduce the medical labor cost, the use of remote healthcare monitoring systems and Point-of-Care (Pock) technologies have become popular Monitoring patients at their home can drastically reduce the increasing traffic at hospitals and medical centers. Moreover, Point-of-Care solutions can provide more reliability in emergency services as patient medical information (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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

large geographical areas essentially for monitoring purposes, and, the Internet represents the main communication 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. Finally, the signals 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.

B. OVERVIEW

A new security technique is proposed to guarantee secure transmission of patient confidential information combined with patient physiological readings from body sensors. The proposed technique is a hybrid between the two preceding categories. Firstly, it is based on using steganography techniques to hide patient confidential information inside patient biomedical signal. Moreover, the proposed technique uses encryption based model to allow only the authorized persons to extract the hidden data.

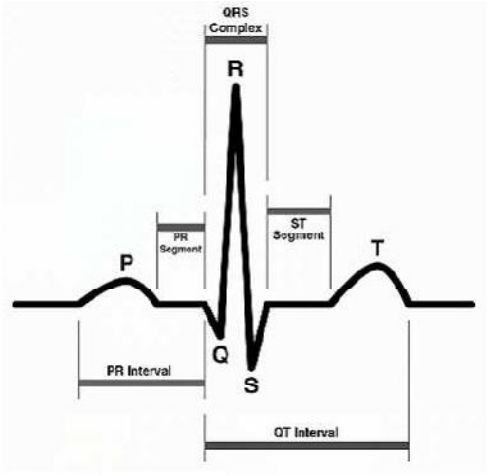

Figure.1 .ECG Signal.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Electrocardiogram (ECG) is a diagnosis tool that reported the electrical activity of heart recorded by skin electrode. The morphology and heart rate reflects the cardiac health of human heart beat . It is a noninvasive technique that means this signal is measured on the surface of human body, which is used in identification of the heart diseases . Any disorder of heart rate or rhythm, or change in the morphological pattern, is an indication of cardiac arrhythmia, which could be detected by analysis of the recorded ECG waveform. The amplitude and duration of the P-QRS-T wave contains useful information about the nature of disease afflicting the heart. The electrical wave is due to depolarization and re polarization of Na+ and kilns in the blood. Detection of the different elements of an ECG trace is the basis of some of the ECG recognition methods; therefore, in this section these elements and their temporal and frequency characteristics are briefly discussed. The amplitude of a wave is measured with reference to the ECG baseline level and the duration of a wave is defined by two time instants at which the wave either deviates significantly from the baseline or crosses it. However, since there is no universal method to determine the onset and end of these elements , it is sometimes problematic to exactly localize the boundaries between the waves of an ECG trace.

An electrocardiogram (ECG or EKG, abbreviated from the German Electrocardiogram) is a graphic produced by an electrocardiograph, which records the electrical activity of the heart over time. The signal is constructed by measuring electrical potentials between various points of the body using a galvanometer. Understanding the various waves and normal vectors of depolarization and depolarization is very important to obtain useful diagnostic information. ECG signals have a wide array of applications throughout the medical field in determining whether the heart is functioning properly or suffering from any abnormalities. ECG analysis is the gold standard for the evaluation of cardiac arrhythmias, it guides therapy and risk stratification for patients with suspected acute myocardial infarction. The baseline voltage of the electrocardiogram is known as the is electric line. A typical ECG tracing of a normal heartbeat (or cardiac cycle) consists of a P wave, a QRS complex and a T wave. A small U wave is normally visible in 50 to 75% of ECGs.

The patient ECG signal is used as the host signal that will carry the patient secret information as well as other readings from other sensors such as temperature, glucose, position, and blood pressure. The Electrocardiogram (ECG) signal is used here due to the fact that most of the healthcare systems will collect ECG information. Moreover, the size of the ECG signal is large compared to the size of other information. Therefore, it will be suitable to be a host for other small size secret information. As a result, the proposed technique will follow HIPAA guidelines in providing open access for patients biomedical signal but prevents unauthorized access to patient confidential information. In this model 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. The proposed steganography technique has been designed in such a way that guarantees minimum acceptable distortion in the ECG signal, Furthermore, it will provide the highest security that can be achieved. The use of this technique will slightly affect the quality of ECG signal.

II. PROPOSED SYSTEM

The sender side of the proposed steganography technique consists of four integrated stages as shown in Fig 2. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

from extracting the hidden information.

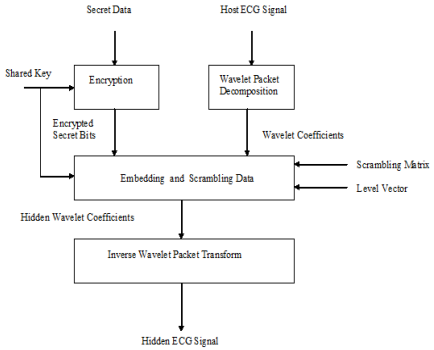

Fig 2. Block Diagram of the sender steganography which includes encryption wavelet decomposition and secret data embeddeing.

A. 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. As a result, XOR ciphering can be easily implemented inside a mobile device.

The exclusive or (XOR) is a logical test that checks if exactly one of two conditions is true. A condition is simply something that is true or false. In binary, true is represented by a 1, and false is represented by a 0. Since the exclusive is a type of test, it will also return a true (1) or a false (0). A true will be returned if exactly one condition of the test is true, and a false will be returned if no conditions are true or both conditions are true. Here is a list of the four possible XOR tests:

```
1 XOR 1 = 0
1 XOR 0 = 1
0 XOR 1 = 1
0 XOR 0 = 0
```

B. Wavelet Decomposition

The discrete wavelet transform (DWT) was developed to apply the wavelet transform to the digital world. Filter banks are used to approximate the behavior of the continuous wavelet transform. The signal is decomposed with a high-pass filter and a low-pass filter.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The Haar transform is the simplest of the wavelet transforms. This transform cross-multiplies a function against the Haar wavelet with various shifts and stretches, like the Fourier transform cross-multiplies a function against a sine wave with two phases and many stretches. The attracting features of the Haar transform, including fast for implementation and able to analyse the local feature, make it a potential candidate in modern electrical and computer engineering applications, such as signal and image compression.

C. The Embedding Operation

At this stage the proposed technique will use a special security implementation to ensure high data security. In this technique a scrambling operation is performed using two parameters. First is the shared key known to both the sender and the receiver. Second is the scrambling matrix, which isstored inside both the transmitter and the receiver. While building the matrix we make sure that the following conditions are met:

1. The same row must not contain duplicate elements
2. Rows must not be duplicates.

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 embedding operation performs the data hiding process in the wavelet coefficients according to the sub-band sequence from the fetched row. The embedding process will start by reading the current wavelet coefficient in sub-band 32 and changing its LSB bits. Then, it will read the current wavelet coefficient in sub-band 22 and changing its LSB bits, and so on. 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 sub-band. For example if the data is embedded in sub-band 32 then 6 bits will be changed per sample, while if it is embedded into wavelet coefficient in sub-band 1 then 5 LSB bits will be changed.

D. Inverse wavelet re-composition

In this final stage, the resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet re-composition. 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. The detailed embedding algorithm is shown in Algorithm 1.The algorithm starts by initializing the required variables.

Next, the coefficient matrix will be shifted and scaled to ensure that all coefficients values are integers. Then, the algorithm will select a node out of 32 nodes in each row of the coefficient matrix. The selection process is based on the value read from the scrambling matrix and the key. The algorithm will be repeated until the end of the coefficient matrix is reached. Finally, the coefficient matrix will be shifted again and re-scaled to return its original range and inverse wavelet transform is applied to produce the watermarked ECG signal.

E. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

2. Scrambling matrix
3. Steganography levels vector

The first step is to apply wavelet packet decomposition to generate the 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.

III.SECURITY ANALYSIS

The security of the proposed algorithm is mainly based on the idea of having several parameters shared between the transmitter and the receiver entities. Any change in any parameter will lead to extraction of wrong data. As a result, even if the key is stolen the attacker will require to know the scrambling matrix as well as the steganography levels vector. The scrambling matrix is stored inside the transmitter/receiver pair and it will not be transmitted under any circumstance. For example, each patient could have his own device from his medical service provider and the matrix is burnt on this device. Therefore, for each pair of transmitter and receiver, it must be a unique scrambling matrix.

IV.CONCLUSION

In this paper a novel steganography algorithm is proposed to hide patient information as well as diagnostics information inside ECG signal. This technique will provide a secured communication and confidentiality in a Point-of-Care system. To reduce the medical labor 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 centres. Remote health care systems are used in large geographical areas essentially for monitoring purposes, and the Internet represents the main communication 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. Finally, the signals 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. According to the Health Insurance Portability and Accountability Act (HIPAA), information sent through the Internet should be protected and secured. It is found that the resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted.

REFERENCES

[1]. L. Marvel, C. Boncelet, and C. Retter, "Spread spectrum image steganography," IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075–1083, 1999.

[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 Transactions on information technology in biomedicine, vol. 8, no. 4, pp. 439–447, 2004

[3]. D. Stinson, Cryptography: theory and practice. CRC press, 2006.

[4]. A. Al-Fahoum, "Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure," IEEE Transactions on Information Technology in Biomedicine, vol. 10, no. 1, 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[5]. F. Hu, M. Jiang, M. Wagner, and D. Dong, "Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/ software codesign," IEEE Transactions on Information Technology in Biomedicine,, vol. 11, no. 6, pp. 619–627, 2007.

[6]. K. Malasri and L. Wang, "Addressing security in medical sensor networks," in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments. ACM, 2007, p. 12.

[7]. K. Zheng and X. Qian, "Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms," in International Conference on Computational Intelligence and Security, 2008. CIS'08, vol. 1, 2008.

[8]. W. Lee and C. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," IEEE Transactions on Information Technology in Biomedicine,, vol. 12, no. 1, pp. 34–41, 2008.

[9]. I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," IEEE Transactions on Information Technology in Biomedicine,, vol. 13, no. 6, pp. 946–954, 2009.

[10]. A. Poularikas, Transforms and Applications Handbook. CRC, 2009.

[11]. S. Kaur, R. Singhal, O. Farooq, and B. Ahuja, "Digital Watermarking of ECG Data for Secure Wireless Commuication," in 2010 International Conference on Recent Trends in Information, Telecommunication and Computing. IEEE, 2010, pp. 140–144.

[12]. H. Wang, D. Peng, W. Wang, H. Sharif, H. Chen, and A. Khoynezhad, "Resource-aware secure ecg healthcare monitoring through body sensor networks," Wireless Communications, IEEE, vol. 17, no. 1, pp. 12–19, 2010.

[13]. H. Golpira and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting," in IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2009. IEEE, 2010, pp. 31–36.

[14]. A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009. IEEE, 2010, pp. 207–212.

[15]. A. De la Rosa Algarin, S. Demurjian, S. Berhe, and J. Pavlich-Mariscal, "A security framework for xml schemas and documents for healthcare," in Bioinformatics and Biomedicine Workshops (BIBMW), 2012 IEEE International Conference on, 2012, pp. 782–789.

[16]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 1, pp. 131–143, 2013.