International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

An approach of ECG Steganography to Secure the Patient's Confidential Information

Ms.Vedanti M.Khandare, Dr. Siddharth A. Ladhake, Mr.U. S. Ghate

Student,Department of Electronics and Telecommunication, Sipna College of engineering and technology, Amravati(M.S.),India

Principal, Sipna College of engineering and technology, Amravati(M.S.),India

Assistant Professor, Department of Electronics and Telecommunication, Sipna College of engineering and technology, Amravati(M.S.),India

---

Abstract - *The number of aging population are growing significantly. In accordance with Health Insurance Portability and Accountability Act (HIPAA) the patient's privacy and security is important in the protection of healthcare privacy. 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. Many times patients ECG signal and other physiological readings are collected by using Body Sensor Networks and that will be transmitted and diagnosed by remote patient monitoring systems. So there is need to provide more security that may combines both encryption and decryption for data confidentiality as well as for data integrity.In this paper, work will be done for security purpose where wavelet-based steganography technique is used.*

Key Words*:* Confidentiality, Encryption, Wavelet, Steganography, ECG signal.

1.INTRODUCTION

When the patient's confidential information transmitted through the public network it should be protected so the proper diagnosis is to be done. Patient privacy is important that a patient can control who will use his/her confidential health information and who cannot. In case of emergency situations people always cannot reach medical centers as it takes long time to reach so that, people may contact physical health care centers to get health tips or first aid.Sometimes people may get treatment from doctor transmitting physiological readings of patients to the hospital server and in turn they provide treatments accordingly. During that time exchange of database, hospitals needs efficient transmission and storage techniques. This exchange involves large amount of vital patient information such as bio-signals and medical images. In order to provide security for data to be protected while it being transmitted over the public network as well as when they are stored in servers.So there is a need to apply some technique that provide security to data against the hacking,tampering etc.

An important sub discipline of hiding information is steganography. Steganography is the science of hiding data (message) inside of other host data (cover). In terms of steganography, these data are protected by their secret existence inside the cover.This method involves, hiding patient data which is confidential, inside ECG signal of patient that can be called as host signal. Additionally, the proposed method uses model which involves encryption to allow extracting the data which is hidden.

That data can be extracted by only the authorized persons like doctors

2. LITERATURE REVIEW

There are many approaches to secure patient sensitive data. However, the challenging factors of these techniques are how much information can be stored, and to what extent the method is secure.

Zheng and Qian[1] 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. 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 1 bit to the left and the watermark is embedded. Finally, the ECG signal is reconstructed by applying reverse haar lifting wavelet transform.

Golpira and Danyali[2] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting.In this paper, medical images such as MRI is used as host signal. A 2-D wavelet transform is applied to the image. Then, the histogram of the high-frequency subbands 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. The locations of the thresholds and the zero points are used for inserting the binary watermark data.Moreover, no encryption key is involved in its watermarking process.

Finally,Kaur[3] proposed new digital watermarking of ECG data for secure wireless communication.This work shows that, each ECG sample is quantized using 10 bits, and is divided into segments.Patient ID is used in the modulation process of the 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 Identification. In this project a signal called low frequency chirp is used to embed watermark in which patient's data taken as 15 digit code. The watermarking scheme used here is the blind recovery of the watermark is used at the receiver end and the embedded watermark can be removed.

A wavelet based ECG steganography is proposed by Ibrahim Khalil and A. Ibaida [4]for protecting patient confidential information in point-of-care system. The first stage of this method is to encrypt the patient confidential information. In this stage XOR ciphering technique is used.Wavelet transform is a process of decomposition which results in coefficients representing frequency components of the signal at a given time. Band filters are used to perform DWT decomposition. It will result in two different signals: one will be related to the high frequency components and the other related to the low frequency components of the original signal. If this process is repeated multiple times, then it is called multi-level packet wavelet decomposition. Here 5-level wavelet packet decomposition has been applied to the host signal. Accordingly, 32 sub-bands resulted from this decomposition process. As a result, a small number of the 32 sub-bands will be highly correlated with the important ECG features while the other sub bands will be correlated with the noise. The next stage is embedding stage which starts with converting the shared key into ASCII code . Then in the final stage, the resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet recomposition.

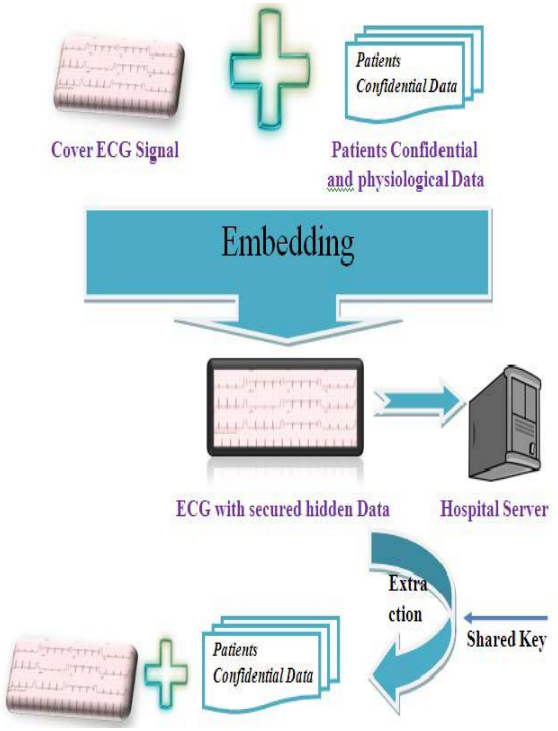
3. PROPOSED WORK

Using Internet as main communication channel introduces new security and privacy threats as well as data integration issues. While transmitting information through the internet a patient's privacy and confidentiality should be protected.

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 u

Figure 1 shows the approach of ECG Steganography.By using this technique it provide the data security to the patients confidential information.In which basically patient confidential data is embedded in cover ECG signal to get ECG with secured data and ex process.the stego ECG signal which is obtained is either transmitted over public network or stored within hospital servers.

Figure 2 shows sender steganography which includes various stages like encryption,wavelet decomposition.



. Figure 1. Approach of steganography using ECG signal for protecting the patients confidential information

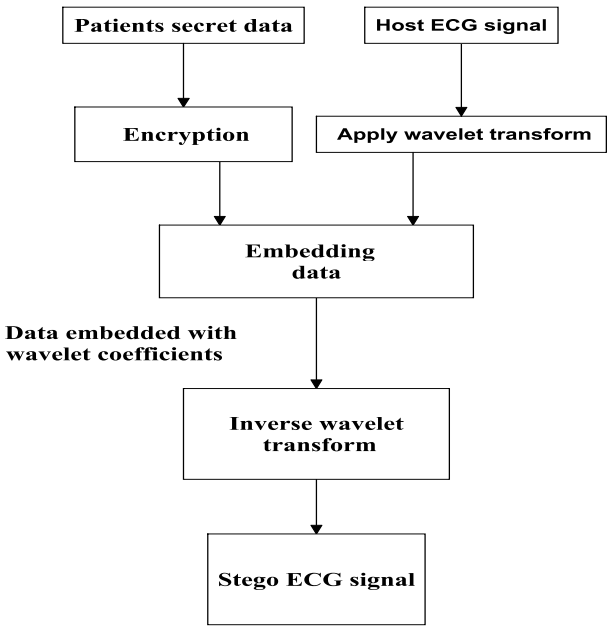


Figure 2. Block diagram of the sender steganography

***I) Data Encryption*:** The process of transforming plain text to an unreadable format using a cipher is called encryption. Data Encryption is used to encrypt the confidential data to prevent any unauthorized access. 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 it uses an ASCII coded shared key which plays the role of a security key. This shared key is known to the encrypter and the decrypter. XOR ciphering is selected because of its simplicity

***II) Signal transformation* :** To provide high data security, an embedding operation is carried out which hides the information in the ECG signal. In order to hide the data we should convert the time domain signal into the frequency domain. In this section we discuss transformation techniques that can be applied to the ECG signal.

Discrete Wavelet Transformation:The Wavelet Transform provides a time-frequency model of the signal. It uses multi-resolution technique by which dissimilar frequencies are evaluated with different resolutions. It is a tool that separates the information into different frequency components. It decomposes the given signal into coefficients representing frequency components of the signal at a given time.

***III) The Embedding Operation*:** In this section we discuss the method to embed the encrypted data into the host signal. We will perform a scrambling operation to ensure high-data security. The scrambling operation is implemented using two parameters:

a) Shared key
b) Scrambling matrix

The shared key is known to both the sender and the receiver whereas the scrambling matrix is stored in both the transmitter and the receiver. The scrambling matrix is a 128x32 size matrix and is build using the following conditions:

The same row must not contain duplicate elements

Rows must not be duplicates

$$S = s1,1 \quad s1,2 \ldots\ldots\ldots s1,32$$
$$s2,1 \quad s1,2 \ldots\ldots\ldots s2,32$$
$$s128,1 \quad s128,2 \ldots s128,32$$

The embedding operation begins with converting the security key into ASCII code, thus converting each character into a number from 1 to 128. These numbers are then used to select one of the rows of the scrambling matrix. The rows of the scrambling matrix contain the sub-band number of the signal. After a row is selected data is embedded into the wavelet coefficients according to the sequence of the sub-bands stated in the selected row and the steganography levelof the subband. The steganography level is determined by the level vector. The data is embedded using LSB embedding. In this algorithm the bits of the hidden message is inserted into the least significant bits of the sub-bands wavelet coefficients. As the secret data is inserted into the LSB bits there not much change in the host signal and the steganographed signal.

***IV) Inverse Wavelet Re-Composition*:** In the final phase of the process the steganographed subbands are recomposed using inverse wavelet re-composition. This transforms the signal from time and frequency domain to the time domain resulting into an ECG signal which is very similar to the host ECG signal. The first step in inverse wavelet decomposition is restoring the signal from decomposed signal. As a signal is decomposed in multilevel sub-bands then that signal is recomposed from the decomposed signal. These new ECG contain the confidential information which is hide inside it and high level security is provide to this signal by using embedding operation.

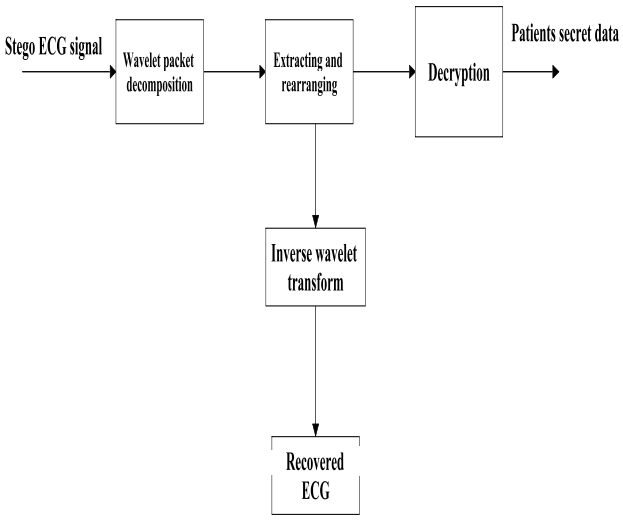


Figure 3. Block diagram of the receiver steganography

Above figure shows the the receiver steganography which includes various stages like wavelet decomposition, extraction, and decryption

***V) Data Extraction*:** In this phase we extract the hidden data from the steganographed signal. In extraction process most of the steps used in embedding are repeated but in the reverse order i.e.: First the steganographed ECG is transformed using DWT to obtain the wavelet coefficients. Then the scrambling matrix is scanned in a predefined order using the shared key to get the signal coefficients. The secret bits are then extracted from the LSBs of wavelet coefficients and decrypted using the security key

4.CONCLUSION

This paper discusses an innovative idea using the steganography approach to provide security to the data when it is transmitted in the public networks as well as when stored on servers.The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological parameters thus it provide integration between ECG and the rest.The suggested technique provides an authentication to prevent unauthorized persons from gaining access to the confidential data.

REFERENCES

[1] K. Zheng and X. Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms"

[2] 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.

[3] 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

[4] Ibaida and I. Khalil. "Wavelet based ECG steganography for protecting patient confidential information in point-of-care systems."IEEE transaction on bio-medical engineering 2013.

[5] A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)"

[6] Y. Lin, I. Jan, P. Ko, Y. Chen, J.Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport

[7] 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.

[8] 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.

[9] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 946–954, Nov. 2009.

[10] 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.

[11] 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 pages 207–212.

[12] Shashikala Channalli et al, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141 137.

[13] Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003

[14] Pradeep Kumar Jaisal, Dr. Sushil Kumar, Dr. S.P Shukla, "A Survey of Electrocardiogram Data Capturing System using Digital Image