PRIVACY PROTECTION OF MEDICAL DATAS USING ECG STEGANOGRAPHY

[1]R Mekala, [2]S Vanitha
[1]PG Scholar, Department of ECE, SNS College of Technology, Coimbatore
[2]Assistant professor, Department of ECE, SNS College of Technology, Coimbatore
[1]mekala48@gmail.com, [2]vanitharajanneel@gmail.com

Abstract: In wireless networks, the bio-medical data may be vulnerable to attacks like tampering, hacking etc. This paper proposes wavelet based steganography technique which is used to provide more security which combines encryption and concealing technique to protect patient confidential data while transmitted over the public network. To evaluate the effectiveness of the proposed technique on the ECG signal, distortion measurement metrics such as Percentage RMSE Difference (PRD) and the other error performance metrics such as PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error).

Index Terms: Confidentiality, conceal, ECG, encryption, steganography, watermarking, wavelet.

1. INTRODUCTION

In remote areas, 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 in case of emergency situations. Sometimes people may get treatment from doctors transmitting physiological readings of patients to the hospital server or medical practitioners and in turn they provide treatments accordingly. During that time exchange of database between hospitals needs efficient and reliable transmission and storage techniques to cut down the cost of health care. This exchange involves large amount of vital patient information such as bio-signals and medical images. 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. Information hiding, steganography, and watermarking are three closely related fields that have a great deal of overlap and share many technical approaches. However, there are fundamental philosophical differences that affect the requirements, and thus the design of a technical solution. Digital watermarking is mainly used in copyright protection; 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. The transmitted data (hidden data and cover) are passed through the network like any other data and anyone who sees them ignores the hidden items. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the information is hidden. Information to be hidden + cover object = stego object\

To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have the key. A stego object is one, which looks exactly same as cover object with an hidden information.

2. RELATED WORKS

The method used in [5], uses new digital watermarking of ECG data for secure wireless communication. In this method 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.

Another method used in [6], uses a reversible blind watermarking for medical images based on wavelet histogram shifting. In this , 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 right histogram part of the second threshold to the right. The locations of the thresholds and the zero points are used for inserting the binary watermark data. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of this algorithm is low. Moreover, no encryption key is involved in its watermarking process.

The method used in [7], uses a new reversible data hiding technique based on wavelet transform . In this 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 one bit to the left and the watermark is embedded. Finally, the ECG signal is reconstructed by applying reverse haar lifting wavelet transform. Moreover, before they embed the watermark, Arnold transform is applied for watermark scrambling. This method has low capacity since it is shifting one bit. As a result only one bit can be stored for each ECG sample value. 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 QRS complex can be detected. However, for abnormal signal in which QRS complex cannot be detected, the algorithm will not perform well.

In this paper[8], a new steganography technique is proposed that helps embed confidential information of patients into specific locations (called special range numbers) of digital ECG host signal that will cause minimal distortion to ECG, and at the same time, any secret information embedded is completely extractable. As a result of the large demand of sending and receiving confidential information of patients in e- health care systems, and the fact that ECG samples are large in size, they can be used as hosts to carry confidential information as secret bits. A new steganography technique is proposed to hide personal information of patients inside ECG signals that are capable of hiding the secret bits in any position of the digital signal samples including the most significant bit. In this paper, it has been proven that the proposed steganography technique does not affect the significant features of the ECG signals as the modifications performed on host signals in order to secret data are not noticeable by naked eyes. The PRD of modified watermarked ECG segments were very low for both normal and abnormal ECGs. The proposed technique uses very simple mathematical equations which can be easily implemented inside the patient PDA device. On the other hand, the receiver should know the signal pre-processing parameters in addition to the selected special range as the secret key to extract the embedded data.

3. EXISTING SYSTEM

3.1EMBEDDING PROCESS

A new security technique is used to guarantee secure transmission of patient confidential information. 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. In this method, the patient ECG signal is used as the host signal that will carry the patient secret information. The various stages involved are:

First stage is to encrypt the patient confidential information in such a way that prevents unauthorized persons and 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.

Second stage is the Wavelet decomposition [5], which is applied to the host signal. Accordingly, sub-bands resulted from this decomposition process. In each decomposition iteration the original signal is divided into two signals. Moreover, the frequency spectrum is distributed on these two signals. Most of the important features of the ECG signal are related to the low frequency signal is called the approximation signal(A).On the other hand, the high frequency signal represents mostly the noise part of the ECG signal is called detail signal (D). As a result, a small number of the sub-bands will be highly correlated with the important ECG features while the other sub bands will be correlated with the noise components in the original ECG signal .

Third stage is the Embedding process [4],is used to conceal the encrypted data and the wavelet decomposed input signal. 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 is stored inside both the transmitter and the receiver. Each transmitter/receiver pair has a unique scrambling matrix.

Final stage is the inverse wavelet process which 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 unwater marked ECG signal.

3.2EXTRACTION PROCESS

Extraction is the process of extracting the secret information from the watermarked signal. In the extraction process, first Step is to apply wavelet decomposition on watermarked signal 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.

In this steganography method, four bits can be embedded with a maximum alternation of two bits. The drawbacks of this technique are low data hiding capacity and more distortion due to hiding process, so it may degrade the image quality.

4. PROPOSED SYSTEM

The proposed method presents 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. Finally, Signal and hidden text will be recovered without any loss based same methods which are used at embedding stage. Privacy Protection system for Confidential data transmission based on the Secret data concealment within ECG signal done using Chaos encryption, Wavelet filters and adaptive least significant bit replacement technique. Data extraction can be done using the secret key and decryption takes place by reverse process that takes place at sender side of secret data. The overview of the proposed system is shown below in figure 1.

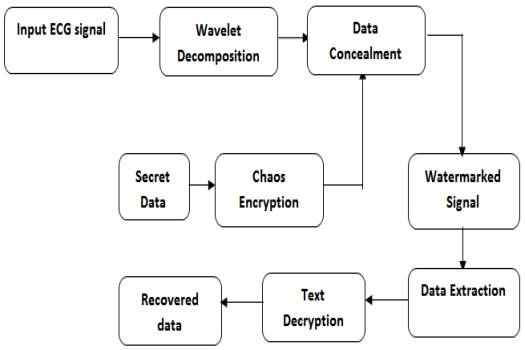

Figure 1: Overview of the proposed system

Chaotic Encryption Method seems to be much better than traditional encryption methods used today. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and loss of information Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography [4]. Therefore, chaotic cryptosystems have more useful and practical applications. One-dimensional chaotic system with the advantages of high-level efficiency and simplicity [14], such as Logistic map, has been widely used now. Chaos encryption method is one of the advanced encryption standard to encrypt the image for secure transmission .It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit xor operation .Here logistic map is used for generation of chaotic map sequence.

The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. A detailed coefficients obtained

from wavelet domain are used here for concealment process and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first bit selected coefficient and the second bit of message is embedded into the second bit location and so on. The resultant watermarked signal which holds the secret message with original form and difference between the input signal and the watermarked signal is not visually perceptible.

In the extraction process we nearly repeat most of the steps in the embedding process but in the reverse order, and the wavelet coefficients of the watermarked ECG signal are constructed. Then, scanning is performed on the matrix in a predefined way using the secret keys to find signal coefficients. By using the secret key we find coefficients in highest detail coefficients of the matrix and then according to their position other coefficients in the lowest scale will be found. Finally matrix of wavelet coefficients of the ECG will be constructed, and then inverse discrete wavelet transform (IDWT) is applied to the matrix in order to reconstruct the extracted watermark signal respectively.

5. CONCLUSION

In this method, a 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 various systems. Wavelet decomposition is applied on the ECG signal image to get high and low frequency components so that encrypted data is hidden inside high frequency components results in watermarked signal. The resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted but the data hiding capacity is low in this method. The proposed method allows hiding more data using adaptive LSB embedding and provides more security using non-linear chaos encryption method. The performance comparison of steganographic method using images and ECG signal can be analyzed

ACKNOWLEDGEMENTS

We are grateful to the management of SNS College of Technology, Coimbatore for providing the facilities in the Department of Electronics and Communication Engineering to carry out the research work. We acknowledge Dr. S Chendur Pandian, Principal, for his constant encouragement and guidance provided in all respects.

REFERRENCES

[1] Ayman Ibaida∗ and Ibrahim Khalil, ―Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems‖, IEEE transactions on biomedical engineering, vol. 60, no. 12, December 2013.

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

[3] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Had- jiefthymiades, ―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.

[4] 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.

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

[6] 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.

[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] Ayman Ibaida, Ibrahim Khalil and Dhiah Al-Shammary,‖ Embedding Patients Confidential Data in ECG Signal for HealthCare Information Systems‖ 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina, August 31 - September 4, 2010.

[9] F. Hu, M. Jiang, M. Wagner, and D. Dong, ―Privacy- preserving tele cardiology sensor networks: toward a low-cost portable wireless hard-ware/software co-design,‖ IEEE Transactions on Information Technology in Biomedicine,, vol. 11, no. 6, pp. 619–627, 2007.

[10] 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 as- sisted living environments. ACM, 2007, p. 12.[9] 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. Workshops (BIBMW), 2012 IEEE International Conference on, 2012, pp. 782–789

[11] 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.

[12] 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.

[13] 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

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

[15] A. Al-Fahoum, ―Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure,‖ IEEE Transactions on In- formation Technology in Biomedicine, vol. 10, no. 1, 2006.

[16] Ayman Ibaida∗ and Ibrahim Khalil, ―Wavelet-Based ECG Steganography for Protecting Patient Confidential information in Point-of-Care Systems‖, IEEE transactions on biomedical engineering, vol. 60, no. 12, December 2013.

[17] A. Giakoumaki, S. Pavlopoulos, and D. Koutouris, ―A medical image watermarking scheme based on wavelet transform,‖ in Proc. IEEE Conf. Engineering in Medicine and Biology Society (EMBS'2003), vol. 1, Sept. 2003, pp. 856 - 859.

[18] V. H. Vallabha, ―Multiresolution Watermark Based on Wavelet Transform for Digital images,‖ Cranes Software International Limited, 2003.

[19] S.-J. Lee, and S.-H. Jung, ―A survey of watermarking techniques applied to multimedia,‖ in Proc. IEEE International Symposium on Industrial Electronics, vol. 1, Jun. 2001, pp. 272-277.

[20] G. Xuan, Q. Yao, C. Yang, J. Gao, P. Chai, Y. Shi, and Z. Ni, ―Lossless Data Hiding Using Histogram Shifting Method Based on Integer Wavelets,‖ Lecture Notes in Computer Science (LNCS 4283), pp.323–332,2006.