Encrypted Data Concealment in Electrocardiogram Signal using Chaos Encryption Method

Preeti Motwani[1], Dimple Chaudhari[2]

[1, 2]Department of Electronics & Telecommunication, Yadavrao Tasgaonkar Institute of Engineering & Technology, Bhivpuri Rd, Karjat. India.
[1]preeti.motwani@tasgaonkartech.com
[2]dimple.chaudhari@tasgaonkartech.com

ABSTRACT

In this paper, a security technique is proposed for the enhancement of protection system for secret data transmission by concealment of encrypted data in ECG signals. The proposed technique encrypts the secret data by using chaos encryption method. This method does not replace cryptography but makes easier to be realized. After encryption, the secret data is concealed into ECG signal co-efficient which makes the secret message into unreadable form and inaccessible to any intruder having random method. Also, DWT decomposition is performed on ECG signal resulting into different frequency sub-bands in which the data is embedded using LSB replacement technique. To get the original information, extracted data will be decrypted using decryption key. Thus, this scheme provides a better encryption and data hiding based on image and data recovery.

Keywords — ECG signal, DWT, Chaos Encryption, Watermarking, Confidentiality.

1. INTRODUCTION

The number of patients suffering from cardiac diseases is increasing dramatically, so it is necessary to provide immediate and appropriate action by means of Point-of-care (PoC) technologies which have become popular. The use of PoC technology not only reduces the medical labor cost but also provide more reliability in emergency services. These technological improvements in medical systems enhance the quality of services provided to the patients. A computer based emergency health-care systems are expanding in order to support large geographical areas and the Internet represents the main communication channel used to exchange information. As internet plays the major role in sending important data through communication channel it introduces security & privacy threats as well as data integration issues. According to the Health Insurance Portability & Accountability Act (HIPPA), information send through the internet should be protected & secured .Also, patient's privacy & confidentiality should be protected. Thus, it is of crucial importance to implement a security protocol for powerful communication & storage security of private data. Various techniques have been proposed to protect data confidentiality and privacy that are based on encryption & cryptographic algorithm.

In this paper, a new security technique is proposed to guarantee secure transmission of patient's confidential information along with patient's physiological readings. Steganography technique is used to hide patient confidential data inside patient biomedical signal. The proposed method uses chaos encryption method to allow only authorized person to extract hidden data.

2. RELATED WORK

There are many ways to secure patient sensitive data [2], [5], [6], [7]. Steganography technique is one of the approach [1], [3], [4], [9] used to secure data by means of hiding information inside medical images/signals. The challenges faced in these

techniques are how much data is stored and to what extend the method is protected. Also what will be the resultant distortion on the original medical images or signal K.Zheng and X.Qian [9] proposed a reversible data hiding for ECG based on wavelet transforms. This method is based on applying B-spline wavelet transform on original ECG signal to detect QRS complex. Also, Haar lifting wavelet transform is applied on the original ECG signal after R waves is detected. Then by applying index subscript mapping, the non-QRS high frequency wavelet coefficients are selected and are shifted one bit to the left and watermark is embedded. Before applying water marking, Arnold transform is applied for watermark scrambling. Only one bit can be stored for each ECG sample value, hence this method has low capacity. Also security in this algorithm relies on algorithm itself, and it does not use a user defined key. Finally, this algorithm is based on normal ECG signals and for abnormal signals; this algorithm will not perform well because detecting QRS complex in such signals is not possible.

H.Golpira and H.Danyali [4] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. In their paper, MRI (medical image) is the host signal. On this image, a two dimensional wavelet transform is applied. Then, the histogram of high frequency sub- bands is determined. Next, to insert binary watermarking data, the locations of thresholds and zero points are required. To obtain them, two thresholds are selected, first in the beginning and other in the last portion of histogram. Now, for each threshold, a zero point is generated by shifting left histogram part of first threshold to the left and shifting right histogram part of second threshold to the right. This algorithm performs well for MRI images but not for ECG signals. Also no encryption is involved in its watermarking process and the capacity is also low for this algorithm.

W.Lee and Chien-Ding Lee proposed A cryptographic Key management solution for HIPPA privacy regulations. In their proposed scheme, to protect the data integrity of the patient health information, symmetric cryptosystem and cryptographic checksum are combined. Also smart cards equipment are used to store important key data, identification data, and so on. The patients need to understand the rules of their protected health information (PHI) and sign the consent in the registration phase. This way the PHI is encrypted to ensure confidentiality. However, there is a restriction on dependence on the smart card as it requires a well-established card application environment.

3. PROBLEM DEFINITION

3.1 Existing Method

3.1.1. RSA Encryption Algorithm:

In this system, encryption key is public and differs from decryption key which is kept secret. This method has limitations such as factoring problem, it can be attacked easily, and is deterministic encryption algorithm (does not have random component).

3.1.2. Bit Modification Technique:

This is a conventional technique and vulnerable to steganalysis. The data is hidden in least significant bits only. Thus, one can easily trace the information and can change the values. So, we can't get the original information that we hided.

3.1.3. Data Embedding using Pixel Difference Expansion:

In this method, DE technique discovers extra storage space by exploring redundancy in image content and reversibly embeds a payload into digital images .During data embedding, modification of all changeable difference values, by either adding a new LSB or modifying its LSB .It has low computational capacity.

4. PROPOSED METHODOLOGY

Privacy Protection system for Confidential data transmission is based on ,Secret data concealment within ECG signal using Chaotic map based on text encryption ,Wavelet filters, Adaptive Least Significant Bit Replacement technique. Data recovery by decryption, Parameter Analysis (MSE, PSNR, Correlation, Elapsed time). The proposed scheme is shown in fig.1 and fig.2

4.1. Proposed Block Diagram

4.1.1. Embedding

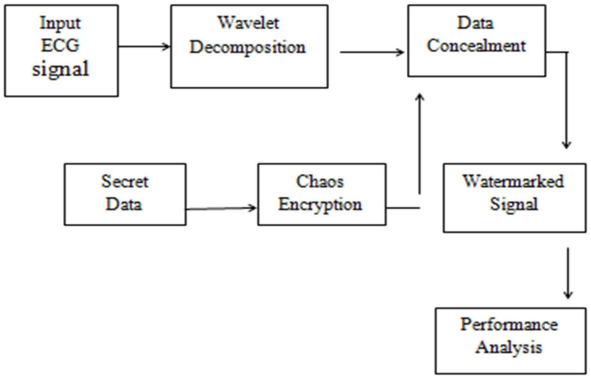


Figure.1. Block diagram of data embedding

4.1.2 Extraction

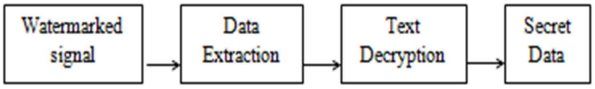
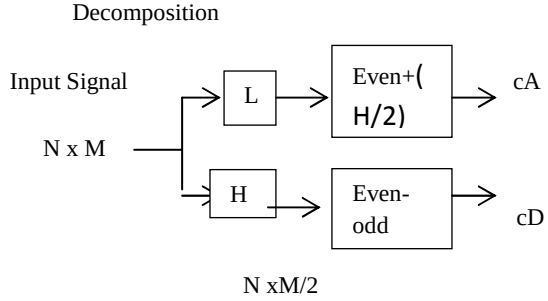


Figure.2. Block diagram of data extraction

4.1.3. Lifting Wavelet Transform:

LWT decomposes the signal into different sub band coefficients, L and H for embedding the messages in the approximation and detailed coefficients of sub bands. Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information. L sub band contains the significant part of the spatial domain signal. High-frequency sub band contains the detailed with noisy information of signal. These coefficients are selected as reserved space for hiding the text data. The secret text data is embedded into the wavelet coefficients of high frequency sub bands because it is non-sensitive to human visual system.

Wavelet Decomposition



Where,

cA- Approximation coefficients , cD – Detailed coefficients

L – Low Pass Filter , H – High Pass Filter

4.1.4 Chaos Encryption:

This method is one of the advanced encryption standard to encrypt the privacy data for secure transmission. It encrypts the original text data's 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. It is very useful to transmit the secret data through unsecure channel securely which prevents data hacking.

4.1.5 LSB Embedding:

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. The quality of the signal however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output signal and it is determined by mean square error and Peak signal to noise ratio determines the signal quality.

4.1.6 Parameter Evaluation:

Percentage Residual Difference (PRD): It is used to measure the difference between original ECG signal and watermarked signal and it is expressed by,

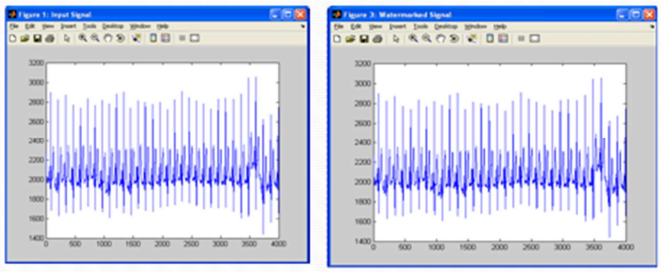
PRD = sqrt (sum ((x – y) ^2)/sum(x))

Where,

x – Original signal

y – Watermarked signal

5. EXPECTED RESULT



6. CONCLUSION

The project proposes the secret data protection of patients through steganalysis approach for telemedicine application. Here, the text message is concealed in ECG signal and is concentrated on preserving signal quality .The Chaos encryption scheme is used to encrypt the text before hiding into signal. Through simulations of result we will regenerate watermarked signal with least error and measures the PRD. Thus this scheme is suitable for data protection in hospitals.

REFRENCES

[1] Ayman Ibaida, Ibrahim Khalil, “Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems”, IEEE Transaction on Biomedical Engineering.

[2] Amjed.S.Al-Fahoum, “Quality Assessment of ECG Compression Techniques Using a Wavelet-Based Diagnostic Measure”, IEEE Transaction on Information Technology in Biomedicine, vol 10, n0. 1, Jan 2006.

[3] S.kauf, R.singhal, “Digital Watermarking of ECG data for secure wireless Communication”, 2010 International Conference on Recent Trends in Information, Telecommunication and Computing.

[4] 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

[5] Ilias Mag, Leo Kaz, Kons Dela, and S.Hadji, Enabling Location Privacy and Medical Data Encryption in Patient TeleMonitoring Systems”, IEEE Transactions on Information Technology in Biomedicine,vol.13,no.6,Nov 2009.

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

[7] 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.

[8] Jun Tian, “Reversible Data Embedding Using a Difference Expansion”, IEEE Transactions on circuits and systems for video technology, vol.13, No.8, August 2003.

