MAT JOURNALS

Journal of Signal Processing
Volume 4 Issue 2

Literature Survey on Biomedical Steganography

[1]S. Thenmozhi, [2]Sureka.P
[1]Associate professor, [2]M.Tech student
Department of EC, Dayanandasagar College of Engineering

Abstract
The word "steganography" comes from the Greek origin "concealed writing". With escalating significance on security, fraud, Steganography is gaining its value due to exponential growth and transmission of secret information through multimedia like internet. In other words, it can be stated as invisible communication. In biomedical steganography, the secret communication is accomplished, where a patient's information is embedded into a biomedical signal (ECG, EEG, PPG) or image which is taken as a cover signal or image. This survey analysis various steganography techniques used for biomedical signal or image.

Keywords: *biomedical signals (ECG, EEG, PPG) or biomedical image, secret data, key, steganography.*

INTRODUCTION

In the digital era, advancement of medical field in the area of telemedicine, necessitates secure transmission of medical data for proper analysis and treatment. Steganography provides refuge to the biomedical signal or image while transmitting through a public network. In steganography approaches, a bio medical signal or image is used as a cover signal and the private confidential information is embedded in cover signal or image using various transformations. Patient's confidential information can be (1) personal data like name, DOB, details, (2) diagnosis such as blood pressure, temperature, and pulse rate. The patient's data is hidden in the biomedical signal or image. The embedded signal or image is called as stego signal or image. At the retrieval side the biomedical signal or image and patient data is extracted separately. Where the doctors can diagnose the patient based the biomedical signal extracted. Here the extracted signal or image should be similar to the transmitted signal or image and the transmitted signal/image should be confidential except the sender and the receiver providing high security to the information transmitted. Different evaluation parameters are discussed in this survey for providing security and privacy for the information transmitted through the network. This paper compares various techniques of steganography used in medical field.

LITERATURE REVIEW

In [1], an effort is made to use curvelet transform which allows identifying the important coefficients that store crucial data about diagnoses. To achieve less degradation, the coefficients around the value zero are modified while embedding the patient data. To avoid the overlapping of the watermark, (n x n) sequence is used for embedding the patient data. Their main goal of the proposed method is to preserve the diagnosability while minimizing the signal degradation. They analyzed the effect of modifying the coefficients at three levels are: near zero, minimum, maximum of the cover bio-medical signal. Based on studying their three different levels, for better result, the coefficients around zero are modified. Authors in this paper have proposed ECG steganography where, ECG is taken as a cover medium. 1D ECG is converted into a 2D image using Discrete Curvelet transform. Discrete Curvelet

transform is applied to the cover and patient data is converted into a binary format which is embedded in ECG signal using LSB embedding. Authors have evaluated on peak signal to noise ratio (PSNR) (range from 43-75), percentage residual difference (PRD) (range from 0.0018-0.0132) and kullback leibler distance (KL) (range from 0.0018-2.94). The proposed approach doesn't affect diagnosability which is measured using kullback-leibler divergence (KL) and allows reliable steganography and the proposed algorithm can be used in case for successful bio-medical steganography.

In [2], their basic demand is, ECG signal should entirely be restored after extracted in-order to diagnose the patient's illness accurately for the doctors. Both the proposed methodologies are reversible according to the results obtained. Authors have proposed Two Reversible Data Hiding (RDH) method. First method is by applying Conventional reversible data hiding, which gives high visual quality of ECG signal, and Huffman encrypted patient data is embedded into the ECG signal using local linear predictor (LLP). First method evaluates PRD (range from 0.018 -1.7) and (BPS) bits/sample (range from 0.05 – 0.45). And second method, a unified embedding-scrambling Reversible Data Hiding (RDH) along with local linear predictor (LLP) as predictor is used to embed patient data in ECG signal. Second method evaluates PRD (range from 1.16e+03 – 930.20) and (BPS) bits/sample (range from (7.4 – 8.3).This paper assures perfect restoration of patient data and ECG signal at the extracting side. Security of both ECG signal and patient data is guaranteed by embedding scrambling. First method using Conventional reversible data hiding guarantees distortion to be equal to 1%. And second method using unified embedding-scrambling Reversible Data Hiding (RDH) guarantees, high embedding capacity of 7.8 bits/sample where ECG signal quality is not a concern. Result shows both the methods are reversible making it suitable for real-time.

In [3], Authors have proposed DCT (discrete-cosine-transform) to achieve minimum distortion. ECG signal is decomposed using DCT (discrete-cosine-transform) and patient's data is converted in binary form. Converted patient data is embedded in ECG signal using LSB technique. To secure the information that is transmitted through the public network, the proposed technique provides an effective way to secure the data transmitted. Using matlab GUI, authors claim ECG has less distortion and it can be used for diagnoses.

In [4], authors propose encoding system that assures privacy and security to 1D bio-medical signal. The proposed 1D SPIHT (set partitioning in hierarchical trees) method compresses 1D signal, to avoid distortion the data is embedded in compressed domain. The proposed method is tested using two bio-medical signals from the standard database for ECG and EEG. SPHIT architecture can be extended to higher dimension for the bio-medical signal, as encoding relies on SPHIT algorithm. Set partitioning in hierarchical trees (SPHIT) is applied to ECG/EEG signals and AES encrypted patient data is embedded in ECG/EEG signal by hash function. This paper focuses on achieving security and efficiency. This has higher embedding capacity within the bio-medical signal (3kb- resting ECG, 200kb-stress tests, 30MB-ambulatory ECG) and encoder achieves a compression ratio of 3-real time to 5-offline operation. Results show high embedding capacity (up to 89%) and PRD (7-9).

In [5], the authors proposed wavelet-based-steganography i for protecting the

patient's information by combining encryption and scrambling-technique. Embedding sequence is created by using the scrambling matrix and the user defined key. Five-level of Discrete wavelet transform (DWT) is applied to the ECG cover signal. This practice provides security and privacy in POC and patient data is scrambled using XOR ciphering-technique. LSB embedding technique is used to embed patient data into the ECG signal. The WEWPRDs criterion appears to be a correct representation of the amount of signal distortion at all sub-bands and robust to insignificant errors in some bands. This paper guarantees secure communication and minimum distortion. Experimental results show PRD (range from 0.315 – 0.319) and WWPRD (range from 0.454 – 0.457).

In [6], authors proposed an algorithm aims to conceal patient data along with the diagnostic data within the ECG signal. Patient information is scrambled using chaos. Multi level wavelet decomposition is applied to the ECG cover signal and chaos scrambled patient data is entrenched using LSB technique. This technique gives low distortion while protecting bio-medical information. Results show evaluation parameters for PRD (range from 0.08 – 0.28).

In [7], DWT is used to decompose the bio-medical signal and SVD to hide important data within the decomposed signal. The singular-values of decomposed signal is replaced by singular-value of important information, the secrete data in embedded into the selected sub-band of the decomposed ECG signal. Signal degradation using this method is less because of the application of SVD for cover signal as well as secrete information. By applying inverse DWT, patient data can be extracted. DWT discrete wavelet transform is applied to the ECG signal and secret data is subjected to SVD and the obtained SVD of patient data is replaced in ECG signal using (SVD) singular value decomposition. The proposed method is capable of embedding secrete information in ECG signal and it's observed that HH-band is best to hide secrete information. This approach gives signal degradation < 0.6% allowing proper diagnoses and also retrieval of patient data. The result gives PRD (0.068), PSNR (69dB), BER (4.3).

In [8], reversible watermarking technique is developed for ECG signal based on wavelet transform for high data-hiding-capacity. Since the QRS wave has the energy of the ECG signal, so the wavelet-coefficients that is hidden in the ECG signal should avoid distortion of QRS wave. Since the modification is done on non-QRS wave, imperceptibility of embedded watermark within the ECG bio-signal is well guaranteed. Authors applied haar-wavelet-based on lifting scheme transform to the ECG signal and patient data is encrypted using Arnold transform which is embedded into ECG signal using shifting operation. Using this method, high-degree of invisibility is achieved as, the watermark is embedded in high frequencies of Haar-wavelet transform which corresponds to non-QRS wave of the original signal. This paper proves originality of the ECG signal and efficiency. The result shows NRSME (0.092 – 0.192), capacity (up to 74kb).

In [9], the proposed method is carried out in a point-of-care system, where the testing can be done at bed side of the patient, so as to save patients life. DWT helps in providing security to the patient's information, as it makes use of encryption and scrambling methods. DWT is applied to the ECG signal and RSA encrypted patient data is embedded into the ECG signal using LSB technique. This paper provides security and privacy for

transferring ECG signal and patient data. Outcome of this technique improves security and performance in health-care-systems and saves elderly patients live. Experimental results show PRD (up to 2.87 x 10^{-4}) and WWPRD (9.026 x 10^{-6}).

In [10], by applying integer-wavelet transform, the host-image component is mapped to the integer-wavelet coefficient. Considering high frequency-sub-band of transformed image, the watermark data is embedded in those sub-bands. Two thresholds (T1, T2) are selected according to capacity required for watermarking. And two-zero points (Z1, Z2) are required to shift beginning and end part of histogram. Histogram region that is located between the thresholds are not changed. Authors propose a 2D wavelet transform (DWT) which is applied to the medical image and binary watermarked-data is embedded into medical image by shifting method. The proposed method allows loss-less re-construction for the watermarked and the cover image. Considering the advantage of low distortion in high-frequency sub-bands and allowing center region unchanged in the histogram. Binary watermarked-data is inserted in locations of threshold and zero-points. Experiment result shows high PSNR (up to 58 dB).

In [11], to secure the transmitted data which mainly consist of bio-medical signal and patient sensitive data, this paper introduces a steganography technique that assures privacy of the patient data , by concealing within the signal employing the secrete key. Fast Walsh Hadamard Transform is used to increase hiding. In this paper Fast Walsh-Hadamard Transform is applied to the any of the three bio-medical signals like ecg, eeg, ppg. The serene data is scrambled using AES encryption algorithm with the help of a secret key for safe data transmission. AES encrypted patient data is entrenched into the bio-medical signal using discrete-wavelet-transform (DWT)-Haar wavelet Transform. To increase pay load capacity, Fast Walsh –Hadamard transform is used to convert signals into a group of coefficients. To assure least amount of deformation, only less vital coefficient values are selected. To enhance security, key is employed in 3D coefficients, reform to yield a 3D order used in the processing of concealing. This paper assures to have high embedding –level by using the proposed Fast Walsh-Hadamard Transform, where the signal is obtained in the frequency domain coefficient. Experimental results of this paper work show evaluation parameters for PRD for stego image (0.21 – 0.96) and the extracted signal (0.045 – 0.77).

Table 1: *The Table Gives Different Technique's Used and Evaluation Parameter Measured In Each Paper.*

Sl. No	method	Evaluation parameter
[1]	ECG=>discrete curvelet transform Patient data=>binary format Embedding=watermark embedding	PRD Kullback leibler distance (KL)
[2]	ECG=>Reversible Data Hiding (RDH) Patientdata=>Huffman encryption Embedding= local linear predictor(LLP)	PRD (BPS) bits/sample
[3]	ECG=>DCT (discrete-cosine-transform) Patient data=>binary format LSB Embedding	---------
[4]	ECG=> Set partitioning in hierarchical trees (SPHIT) Patient data=>AES Embedding using hash function	PRD Embedding capacity
[5]	ECG=>DWT	PRD

	Patient data=> XOR ciphering-technique LSB Embedding	WWPRD
[6]	ECG=>DWT Patient data=> chaos cryptography LSB Embedding	PRD
[7]	ECG=>DWT Patient data=>SVD Embedding using SVD	PRD PSNR BER
[8]	ECG=>haar wavelet Patientdata=>Arnold transform Embedding is through shifting operation	NRMSE
[9]	ECG=>DWT Patient data=>RSA Embedding using LSB	PRD WWPRD
[10]	Image=>DWT Patient data=> binary watermarked data Embedding is done with the help of shifting method	PSNR
[11]	ECG/EEG/PPG=>Fast-Walsh-Hadamard- transform (FWHT) Patient data=> AES Embedding=> discrete-wavelet-Transform (DWT)	PRD

CONCLUSION

This literature survey gives overview of bio-medical signal or image steganography used transmit the patient data secretly inside bio-medical signal or image according to the algorithms proposed. Paper [1].[4].[6],[7],[11] gives lower PRD compared to other papers and PSNR in paper [17],[10] gives higher values. For any proposed methodology, PRD should be low and PSNR should be high. Future research work may include a technique that reduces PRD and to increase PSNR.

REFERENCES

1. S. Edward Jero, Palaniappan Ramu, Ramakrishnan. 'ECG steganography using curvelet transform'. Biomedical Signal Processing and Control 22 (2015) 161–169.
2. Hui Wang, Weiming Zhang, Nenghai Yu. "Protecting patient confidential information based on ECG reversible data hiding'. springer 20 May 2015.
3. Dr.K.V.Padmaja, Ankitha.O.P, Anshu Singhania, Preethi.M.R, Rashmi R Nayak. 'DCT based ECG Steganography for Protecting Patient's Confidential Data in Point-of-Care Systems'. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 5, Issue 7, July 2016.
4. Oscar J. Rubio, Álvaro Alesanco, Jose Garcia. "Secure information embedding into 1D biomedical signals based on SPIHT". Journal of Biomedical Informatics 46 (2013) 653–664.
5. 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.
6. S. P. PREDEEP KUMAR and E. BABU RAJ. "An Enhanced Cryptography for ECG Steganography to Satisfy HIPAA Privacy and Security Regulation for Bio-Medical Data's". Biomedical & Pharmacology Journal. Vol. **9**(3), 1087-1094 (2016).
7. S Edward Jero & Palaniappan Ramu & S Ramakrishnan." Discrete Wavelet Transform and Singular Value Decomposition Based ECG Steganography for Secured Patient

Information Transmission". Springer J Med Syst (2014).
8. Kai-mei Zheng, Xu Qian. "Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms". International Conference on Computational Intelligence and Security. 2008
9. ANKITA G. SHIRODKAR. "SECURE STEGANOGRAPHY, COMPRESSION AND TRANSMISSION OF ECG IN POINT-OF-CARE SYSTEM". International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009 (2015).
10. Hemin Golpira1, Habibollah Danyali. " Reversible Blind Watermarking for Medical Images Based on Wavelet Histogram Shifting". In Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on, pages 31–36. IEEE,2009.
11. Alsharif Abuadbba, Khalil. "Walsh-Hadamard Based 3D Steganography for Protecting Sensitive Information in Point-of-Care. IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING. 0018-9294 (c) 2016