RESEARCH ARTICLE OPEN ACCESS

Result Paper on Protecting confidential information in POC System ECG Steganography

[1]Miss.Ankita K.Ramekar, [2]Prof.M.A.Pund

[1]ME student(PRMIT&R,Badnera)
[2]Professor(PRMIT&R,Badnera)

Abstract:

This paper proposes the development of Secure system for secret data communication through encrypted data hiding in ECG signals. The proposed encryption technique used to encrypt the secret data into unreadable form and 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 hide 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 is the reason a new security approach called reversible data hiding arises. It's art of hiding the data in another transmission medium to get secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. Here the DWT(Discrete Wavelet Transform) is used to decompose an ECG signal to different frequency sub bands. Hence, patients ECG signal and other readings such as blood pressure, glucose reading, position,etc., are collected at home by using Body Sensor Networks (BSNs) will be transmitted and diagnosed by remote patient monitoring systems. At the same cost that the patient privacy is protected against intruders while data traverse in open network and stored in hospital servers. In this project, to fulfill HIPAA act, a Discrete Wavelet Transform based steganography technique has been proposed. DWT technique allow ECG signal to put out of sight the patient confidential data and thus guarantees the patient's privacy and confidentiality.

Keywords— **ECG, Steganography, Encryption, Wavelet, Watermarking, Confidentiality.**

1. INTRODUCTION:

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. The primary goal is to provide confidentiality,integrity, and availability. Steganography is a branch of cryptography that involves hiding information "in plain sight".Hiding a message reduces the chance of a message being detected. The main aim is to hide patient's confidential data and other physiological information in ECG signal. ECG signal is used because the size of ECG is large compared to other medical images. Therefore, patients ECG signal and other physiological readings such as temperature, blood pressure, glucose reading, position, etc., are collected at homes by using Body Sensor Networks (BSNs) will be transmitted and diagnosed by remote patient monitoring systems. At the same cost that the patient confidentiality is protected against intruders while data traverse in open network and stored in hospital servers.

This technique allow ECG to put out of sight the patient
confidential data and thus guarantees the patient's privacy and confidentiality. The aim is to show that both the Host ECG and stego ECG signals can be used for diagnoses and the difference would be undetectable.
The work of this project is motivated by investigations
from the above and similar research findings. Our first
objective is to save patient confidential data from harm by using steganography method. From the proposed model, we then formulate new steganography technique using ECG and introduce their respective algorithms, which are fast and scalable, but are also capable of providing high-quality and consistent performance. The main target of steganography is to put out of sight the secret message in the other cover media so that nonentity can see that and both participants are converse in secret way. By combining the techniques of steganography and the other techniques, information security has improved noticeably. Steganography is used as copyright, averting e-document forging, ensure data confidentiality. Such carriers are text, document, audio, image, video, 3D models recording, etc.,Hiding a message reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection.
Main requirements of steganography
1) The integrity of the embedded information inside
the cover media must be truthful for the receiver and
sender.
2) The stego entity must unchanged to the naked eye
3) And always assume that the attacker may knows that
there is hidden data inside the cover object.
Steganography are of two types
1) Fragile: In this type of steganography, if the file is
modified then the embedded information is destroyed.
2) Robust: This steganography, embed information into a media which cannot be simply destroyed.
Goals of Steganography are capacity and security.
Several researchers have been proposed to secure patient confidential data. There are techniques that are based on encryption and cryptographic algorithms. These techniques are used to secure data during the communication and storage. As a result, the final data will be stored in encrypted format.The limitations of using encryption based techniques is its large computational overhead. Therefore, encryption based methods are not suitable in resourceconstrained
mobile environment.

2. Literature Review

Many approaches have been established to secure patient
confidential data [2], [4], [5], [16], [17]. However, these approaches are [15], [7], [6], [8] proposed to secure data based on steganography techniques to hide secret information inside medical images.
Ibaida and Khalil [15] shows that, it embed confidential data of patients into a position which is called special range numbers, of the ECG host signal which is in digital that will provide minimum distortion to ECG, and any secret information embedded is completely extractable. In this, that there are many possible SRN create it tremendously difficult for attackers to recognize the locations of private bits. This experiments display that percentage residual difference (PRD) of watermarked ECGs for normal and abnormal ECG segments. This method has high computational overhead. This algorithm is developed for normal ECG signal of the patient but not for abnormal ECG signals such as Ventricular

tachycardia, fibrillation, etc., Moreover, the capacity of this algorithm is low. No encryption key is involved in its watermarking process. S.Kaur, R. Signghal [7] 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.

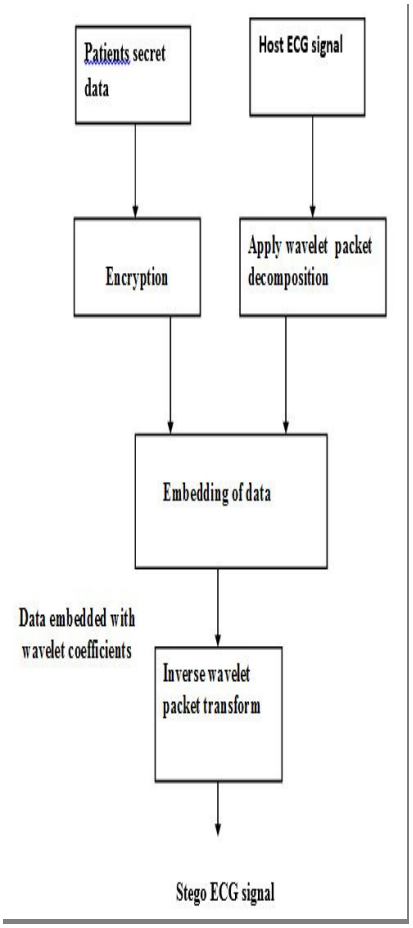
The final signal consists of 16 bits per sample, with 11 bits for watermarked ECG and 5 bits for the factor and patient Identification. In this project a signal called low frequency chirp is used to embed watermark in which patient's data taken as 15 digit code. The watermarking scheme used here is the blind recovery of the watermark is used at the receiver end and the embedded watermark can be removed. Original size of host signal increased after watermarking. Not more secure compared to other techniques. Same as normal image steganography. The watermarking process has no encryption key method.

K.Zheng and Xu-Qian [6] shows that, reversible watermarking algorithm has developed for electrocardiogram (ECG) signal based on wavelet transforms. This method is based on applying wavelet transform on the original ECG signal to detect QRS complex. Next, the non QRS coefficients are selected, are shifted one bit to the left and the watermark is embedded. In electrocardiogram signal, the energy is concentrated in QRS complex waves. So the selection of wavelet coefficients for hiding should avoid making QRS complex waves distort obviously. The algorithm hides bits in the expansion of selected coefficients of high frequency subband of Haar wavelet transform based on lifting scheme. The performance has been evaluated in terms of ECG signal distortion and embedding capacity. This method has low

capacity since it is shifting one bit. So, one bit can be stored for each ECG sample value. Finally, this algorithm is for normal ECG signal. However, for abnormal signal in which QRS complex cannot be detected.

3. Proposed Work

For Embedding:



Patient secrete data:

Patient secrete data which we want to stored in an ECG signal.It contain Name of patient, address, medical parameters such as temperature, blood pressure, blood sugar.

Host ECG signal :

ECG signal which we are going to use as a cover media to conceal patient confedential information.

Encryption:

In cryptography encryption is the process of encoding a message or information in

such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Wavelet packet decomposition:

For n levels of decomposition the WPD produces 2^n different sets of coefficients (or nodes) as opposed to (3n + 1) sets for the DWT. However, due to the downsampling process the overall number of coefficients is still the same and there is no redundancy.From the point of view of compression, the standard wavelet transform may not produce the best result, since it is limited to wavelet bases that increase by a power of two towards the low frequencies. It could be that another combination of bases produce a more desirable representation for a particular signal. The best basis algorithm by Coifman and Wickerhauser[1]finds a set of bases that provide the most desirable representation of the data relative to a particular cost function (e.g. entropy).There were relevant studies in signal processing and communications fields to address the selection of subband trees (orthogonal basis) of various kinds, e.g. regular, dyadic, irregular, with respect to performance metrics of interest including energy compaction (entropy), subband correlations and others.

For Extraction:

Extraction:

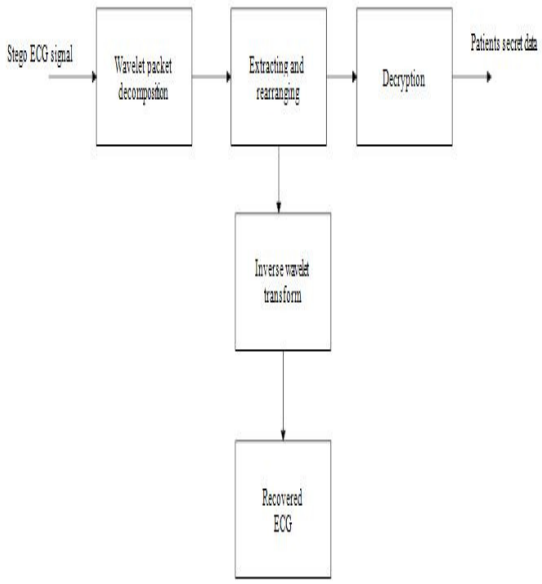
Data extraction is the act or process of retrieving data out of (usually unstructured or poorly structured) data sources for further data processing or data storage (data migration). The import into the intermediate extracting system is thus usually followed by data transformation and possibly the addition of metadata prior to export to another stage in the data workflow. Usually, the term data extraction is applied when (experimental) data is first imported into a computer from primary sources, like measuring or recording devices. Today's electronic devices will usually present an electrical connector (e.g. USB) through which 'raw data' can be streamed into a personal computer.Typical unstructured data sources include web pages, emails, documents, PDFs, scanned text, mainframe reports, spool files, classifieds, etc. Which is further used for sales / marketing leads.Extracting data from these unstructured sources has grown into a considerable technical challenge where as historically data extraction has had to deal with changes in physical hardware formats, the majority of current data extraction deals with extracting data from these unstructured data sources, and from different software formats. This growing process of data extraction from the web is referred to as Web scraping.

Decryption:

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some

companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.



4. Result:

In the implementation, the patients confidential information such as name, date of birth, age, address, Medicare number, phone number, and other physiological readings such as patient location, temperature, glucose, hemoglobin, blood pressure are not sent to the receiver as a separate message, but, instead, transmitted along with the ECG signal as cover or host medium to hide the above specified datas. Specifically, this scheme hide patient personal data and physiological in the ECG signal together using our hiding scheme.

We consider the following performance parameter.

1. Root Mean square (RMS):

   The root mean square deviation (RMSD) or root mean square error (RMSE) is a frequently used measure of the differences between values (sample and population values) predicted by a model or an estimator and the values actually observed. The RMSD represents the sample standard deviation of the differences between predicted values and observed values. Peak Signal to Noise Ratio:

2. PSNR:

   The PSNR block computes the peak signal to noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image.

3. Signal To Noice Ratio:

Signal to noise ratio (abbreviated SNR or *S/N*) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0dB) indicates more signal than noise.While SNR is commonly quoted for electrical signals, it can be applied to any form of signal (such as isotope levels in an ice core or biochemical signaling between cells).The signal to noise ratio, the bandwidth, and the channel capacity of a communication channel are connected by the Shannon–Hartley theorem Signaltonoise ratio is sometimes used metaphorically to refer to the ratio of useful information to false or irrelevant data in a conversation or exchang

Analysis Table:

File size	I/P Signal &Stego Signal	I/P Signal & recover Signal
1k	MSE: 0.0012 MAE:0.0012 SNR:73.6441 PSNR:77.3988 CC:1.0000	MSE:0.0000 MAE:0.0000 SNR: Inf db PSNR: Inf db CC:1.0000
2k	MSE:0.0103 MAE:0.0103 SNR:64.7702 PSNR:68.0078 CC:1.0000	MSE:0.0000 MAE:0.0000 SNR: Inf db PSNR: Inf db CC:1.0000

5. Conclusuion:

In this project, a novel steganography algorithm is proposed to hide patient confidential and physiological data in the ECG signal using Discrete Wavelet Transform. The HIPAA regula-tion comply in this paper i.e., information sent through the public network will be protected and secured. ECG signal hides the corresponding patient confidential data and thus guarantees the patient's privacy and confidentiality. The proposed algorithm provide significantly improved security, efficiency and performance. Three tier of security is provided. Any doctor can see the Stego ECG signal and only authorized doctors can extract the secret information and have access to the confidential patient information as well as other readings stored in the host ECG signal. The distortion will be less. The difference will be undetectable in Stego ECG signal, and both the Stego ECG and Host ECG can be used for diagnoses. 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.

6. References:

[1] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su, "Reversible data hiding", IEEE *Trans. on Circuits and Systems for Video Technology*, vol. 16, No. 3, Mar. 2006.

[2] Jun Tian, "Reversible data embedding using a difference expansion", IEEE *Trans. on Circuits and Systems for Video Technology*, vol. 13, No. 8, Aug. 2003.

[3] Mehmet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp, Eli Saber, "Lossless generalized-LSB data embedding", IEEE *Trans. on Image Processing*, vol. 14, No. 2, Feb. 2005.

[4] Pramod Kumar, Pushpendra Kumar Pateriya, "RC4 enrichment algorithm approach for selective image encryption", *International Journal of Computer Science & Communication Networks*, vol. 2(2), 181-189.

[5] Chinmaya Kumar Nayak, Anuja Kumar Acharya, Satyabrata Das, "Image encryption using an enhanced block based transformation algorithm", *International Journal of Research and Reviews in Computer Science*, vol. 2, No. 2, Apr. 2011.

[6]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.

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

[8] 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.

[9] 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.

[10]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.

Websites:
https://in.mathworks.com/products/mat ab-drive.html
https://physionet.org/physiobank/database/mitdb/