An approach to maximize efficiency in ECG steganography technique

Gagandeep kaur Randhawa
M.Tech Scholar, Dept of Electronic and Communication GCET
Gurdaspur India

Damandeep Kaur
Assistant Professor
Department of Electronic and Communication GCET
Gurdaspur India

Abstract

Today number of people are suffering from cardiac disease therefore telecardiology is used widely. So ECG signals and confidential information of patient is transmitted through internet. Thus abstraction of this information is ECG signal is must to protect data of patient. In this paper we proposed a technique of ECG steganography that is based on encryption of image and text data into ECG signal. The simulation result will be shown in terms of PSNR, MSE, BER parameters.

Keywords: ECG steganography, security, PSNR, MSE

Introduction

In modern world data can be shared worldwide anywhere through different mode of sharing. Apart from the technologies which facilitate an ease of sharing of data, security of information from any eavesdropper/ third party client is a bigger concern. In the field of healthcare, patient information is transmitted from one place to nearby hospitals for proper observation of the patient. This information is solely important for his health records and observations hence need to protect from various threats[1] This can be done with the help of the electrocardiogram (ECG) signals.Also, Diagnose the cause of chest pain, proper use of early intervention in myocardial infraction depends upon it. Human heart generates distinct deflections on the ECG[2]. Such deflections can be recorded in the forms of waves named as P, Q, R, S and T waves. P wave in the upward directions represents depolarization. Q wave represents a downward deflection and depict septal depolarization [3]. Similarly, R wave depicts ventricular depolarization; S wave represents late ventricular depolarization and T wave shows repolarization of the ventricles [4]. Hence, these waves track the activates of heart. As technology grows number of portable devices are increases which record ECG activities over time span and transmit the patient data remotely. Shimmer and Alivecor iPhone are examples of these systems. The data acquired from ECG signal can be stored in different formats like ecgML,XML-ECG, Philips XML, DICOM-ECG etc.[5]

Steganography in ECG

As a technology grows, monitoring patients at their home instead of hospital is also increases, which fortunately suppress the number of visitors in a hospital. These Point of care (POC) techniques [6] can provide a reliable information about patient's health and can be transmitted to the expert or doctors from anywhere at any time. Internet remains the common medium of transmitting this information which reveals this information to some threats of communication

Many techniques based on cryptography has been evolved in past to protect the data.

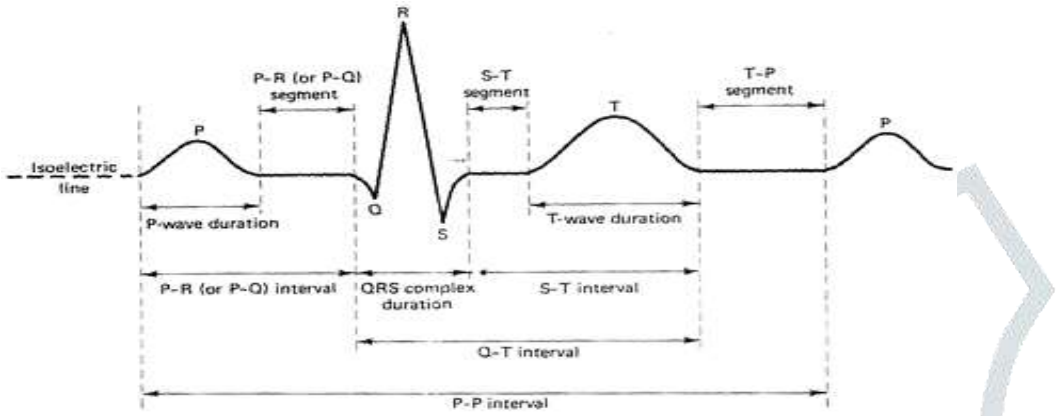


Fig.1. P, Q, R, S, and T wave of Electrocardiogram

These techniques provide a desirable security to the patient information by employing some encryption. However, this lead to a complex computational data and not considered for POC techniques. Steganography i.e. hiding information (patient information in current scenario) [7]in another signal to protect[6] it from any threats provide solution to above problem. This reduces the overall data overheads as well as original signal can be recovered from watermarked signal. There are two distinct domain of ECG steganography classified as Time domain and Frequency domain. The later one can hide large number of information but yield to lower performance. On the other hand, Time domain ECG steganography has higher rate of performance but store less amount of data [8]. Patients health data (like ECG signal, temperature etc.) can be acquired with the help of sensors. The collected data is then sent to PDA [8] via some mode of communication. Before transferring the data, a stenography technique has been applied where patient information is hide into a ECG signal (using ECG as host signal). The resultant watermarked signal [9] is then transferred to the hospital through the use of internet. On the receiver end (hospital) this hidden information is retrieved successfully. This reduced the overall size of size of encrypted signal and reduces overheads.

Literature Survey

Steganography is way to encryptthe data in particular media and making a data in accessible form. Stenography is a technique which encodes the data can be implemented in terms of picture and sound. The

following mechanism will be used in case of steganography. The various mechanism like encryption and decryption. The encryption is mechanism which converts the plain text into ciphertext and decryption is the process of converting cipher text into plain text.

[10]The fast advancement of information correspondence in present day time requests secure trade of data. Steganography is a built up technique for accessing data in media. Steganographic strategies accessed data in various record organizations, for example, picture, content, sound, and video. Security as far as PSNR and power are the key difficulties to steganography. In this paper, a novel picture steganography strategy in light of most noteworthy bits (MSB) of picture pixels is proposed.On the basis of syntax the software engineering focus on LSB bits for extracted the data. The proposed technique uses the MSB bits that make it more secure the information.

[11]The accessibility of generally computerized items combined with the higher transmission capacity and nature of administration. The wired and remote accessibility systems have transmit, and convey advanced information with high quality. In such a situation steganography has been considered. It has been discovered valuable for data security. Steganography also used for exchange of secret data over a correspondence channel. The information to be installed is separated in squares and each packet is inserted in the cover media under control of a secure key.

[12]ECG steganography is a developing field of research for secure information. Two or three procedures have been proposed for shading picture steganography. The shading pictures are transmit on web because of their size. In this paper, we proposed hashing based approach for steganography in dark scale pictures. The proposed approach is more efficient and successful that gives a more secure method for information transmission at higher speed. The displayed approach is actualized into a model device coded in VB.NET. The introduced approach is successful in way record configurations, for example, bmp, gif, jpeg. An arrangement of test pictures were prepared with the device and the aftereffects of the underlined analysis show the capability of the displayed approach as far as secure steganography as well as regarding quick information transmission over web.

[13] We show a method to install information to a picture, called data covering up or steganography. We use some straightforward watched connections between the pixel. the dark code picture, and the usage of a basic Exclusive-OR operation in light of N pictures accessible to the sender and the recipient, called the cover pictures. We display the calculations for installing the information in the adjusted, last picture, N+l, called the stego picture; and also removing this information on the accepting side. We display some pictures to demonstrate that the methodology we propose has a high PSNR, and a practically non-difference histogram when contrasted with the before stego picture. We additionally examine the power ofthis calculation strategies, for example, steganalysis.

PROPOSED SYSTEM

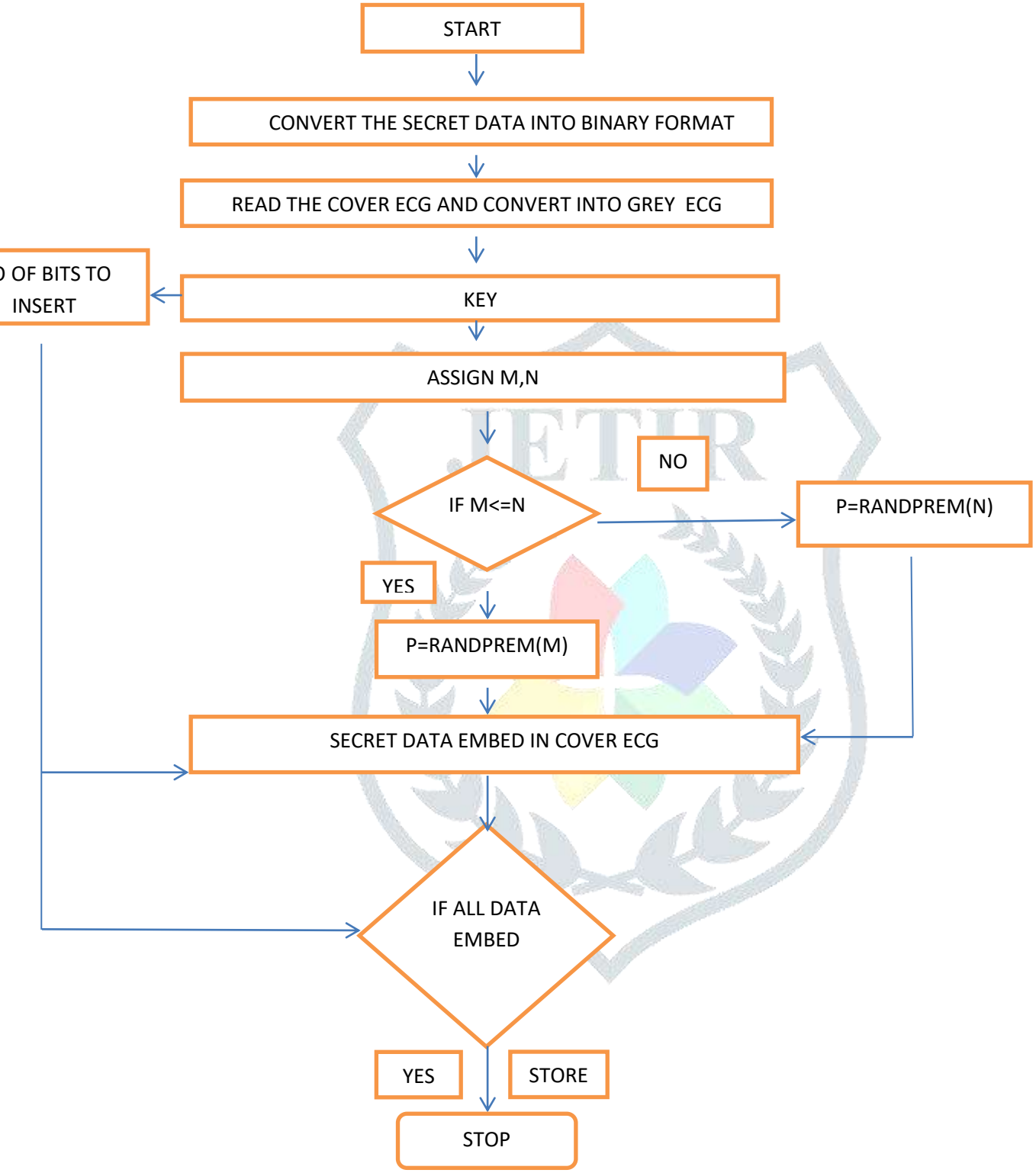


Figure 1: SHOWING FLOWCHART OF PROPOSED SYSTEM

System being studied takes out the ECG from source and encrypt message onto the ECG. ECG contain encrypted information. That information along with ECG is transferred towards the destination. Key for decryption is also transferred along with the ECG. At the receiver end decryption is performed. Decryption

is possible only if valid key is received by the receiver. Recived message is stored within the buffer and algorithm terminates.

5.1 ALGORITHM OF THE PROPOSED SYSTEM

1. Begin
2. Input: Cover ECG, Secret Message, Secret Key;
3. Transfer Secret Message into Text File;
4. Message Text File;
5. Convert Text File to Binary Codes;
6. Convert Secret Key into Binary Codes;
7. Set Bits Per Unit to Zero;
8. Encode Message to Binary Codes;
9. Add by 2 unit for bits Per Unit;
10. Output: Stego ECG;
11. End

The flow of the algorithm is given by the following figure:-

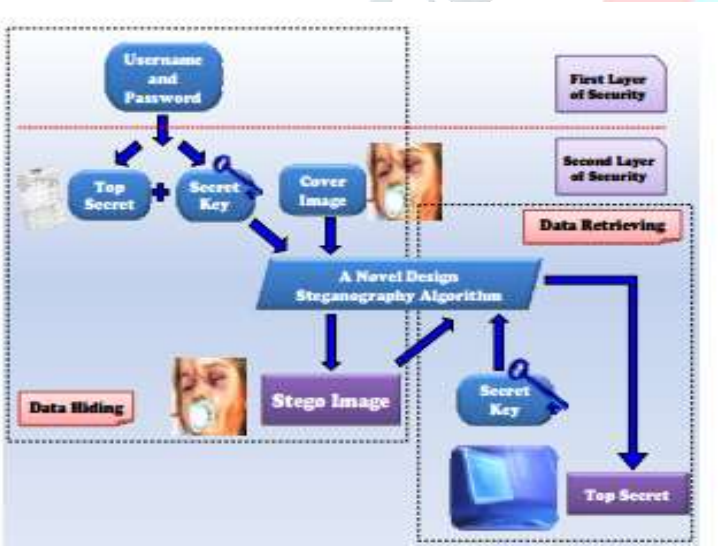


Figure 6:- The framework for the system

Performance Evaluation Parameters

Mean Square Value

Mean Square error (MSE) is defined as the measure of degree of similarity or it's the extent offeror/distortion between two signals. MSE could also be thought of a measure of signal quality. Y is original signal of M predictions and Y' compared signal. [26]

$$MSE(Y, Y') = \frac{1}{M} \sum \frac{M}{i=1} (Y - Y')^2$$

Peak Signal to Noise Ratio

Peak signal-to-noise ratio (PSNR) is the ratio of the maximum possible power of pixel value to the power of noise. It is generally calculated in logarithmic scale and its value is always represented in db. MAX stands for maximum value of signal.

$$PSNR = 20 * log10\ (MAX) - 10 * log10\ (MSE)$$

Percentage Residual Difference

PRD (percentage residual difference) is tool used to measure the difference between the actual ECG host signal and the watermarked ECG signal.

$$\text{PRD} = \sqrt{\sum_{I=1}^{N}((Y - Y')^2} \Big/ \sum_{i=1}^{N}(Y')^2$$

Y represents the original ECG signal and *Y'i*s the watermarked signal.

Bit Error Rate (BER)

BER can be evaluated as the ratio of number of errors occurred to the number of bits sent in a transmission system.

Wavelet Based Weighted Percentage Residual Difference (WWPD)

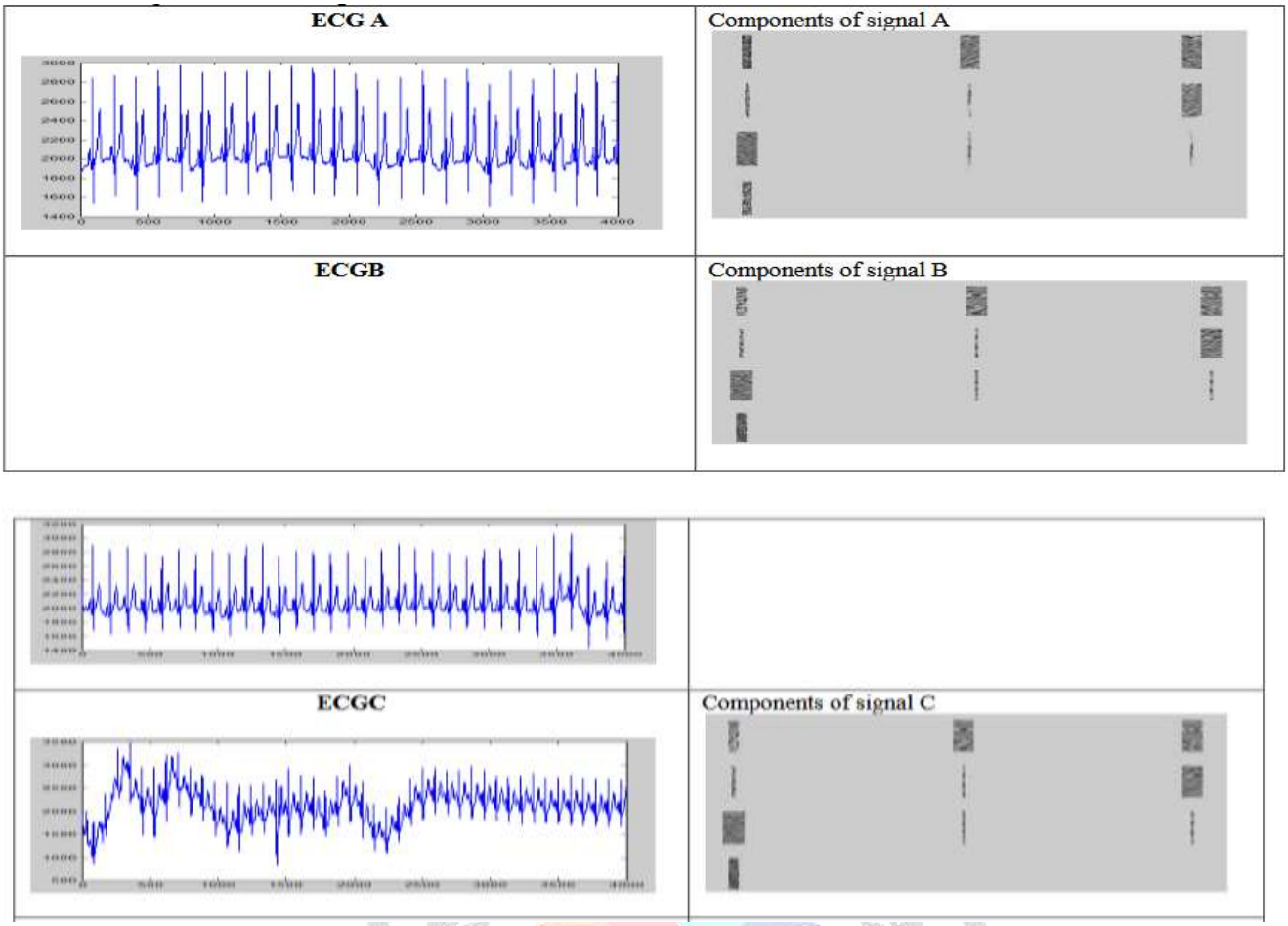
WWPRD is based on biological wavelet decomposition. Mathematically, it defined as:

$$\text{WWPRD} = \sum_{j=0}^{Nm} w'WPRD'$$

where Nm is total number of sub bands, w' represents the weight value related to sub band j and WPRD' depicts the wavelet-based percentage residual difference.

RESULTS

The ECG signal is as given below:



Conclusion and future Scope

Steganography is used in order to hide the information within the ECG and then transfer the information towards the destination. It is one f the most complete encryption slandered which is followed in order to enhance security levels in sensitive data transfer. Optical medium is commonly followed for transfer hence enhancing speed and reduce time consumed in transmitting the data. ECG compression and noise handling mechanism are also utilized to enhance quality of ECG. Results obtained are better as compared to existing literature in terms of PSNR, MSE, BPP and CR.

In future, Steganography can be merged with the random key in order to enhance security further.

References

[1] H. Wang, W. Zhang, and N. Yu, "Protecting patient confidential information based on ECG reversible data hiding," 2015.

[2] S. E. Jero, P. Ramu, and S. Ramakrishnan, "Discrete Wavelet Transform and Singular Value Decomposition Based ECG Steganography for Secured Patient Information Transmission," 2014.

[3] S. E. Jero, P. Ramu, and S. Ramakrishnan, "Biomedical Signal Processing and Control ECG steganography using curvelet transform," *Biomed. Signal Process. Control*, vol. 22, pp. 161–169, 2015.

[4] S. Chen, Y. Guo, and H. Huang, "Hiding Patients Confidential Datainthe ECG Signal viaa Transform-Domain

Quantization Scheme," pp. 1–8, 2014.

[5] "Review Paper on Denoising of ECG Signal."

[6] R. R. Bond, D. D. Finlay, C. D. Nugent, and G. Moore, "A review of ECG storage formats," *Int. J. Med. Inform.*, vol. 80, no. 10, pp. 681–697, 2011.

[7] P. Comp, "Scie enceDir rect ScienceDirect ECG Elec ctrode Configura ation to Extract Real Tim me FEC G Signa als Niyan n a *, Gourish," 2018.

[8] A. Ibaida, I. Khalil, and D. Al-shammary, "Embedding Patients Confidential Data in ECG Signal For HealthCare Information Systems," pp. 3891–3894, 2010.

[9] A. Ibaida and I. Khalil, "Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems," vol. 60, no. 12, pp. 3322–3330, 2013.

[10] C. Wang, N. Wu, C. Tsai, and M. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," vol. 81, pp. 150–158, 2008.

[11] F. Hu, M. Jiang, and M. Wagner, "Privacy-Preserving Telecardiology Sensor Networks : Toward a Low-Cost Portable Wireless Hardware / Software Codesign," vol. 11, no. 6, pp. 619–627, 2007.

[12] S. Shen and L. Huang, "SC," *Comput. Secur.*, 2014.

[13] E. J. S, P. Ramu, and R. Swaminathan, "Imperceptibility — Robustness tradeoff studies for ECG steganography using Continuous Ant Colony Optimization," vol. 49, pp. 123–135, 2016.