Sharing of Patient confidential data using ECG steganography

V.Sankari [1], K. Nandhini [2]

Abstract— In accordance with Health Insurance Portability and Accountability Act (HIPAA) the patient's privacy and security is important in the protection of healthcare privacy. At the same time, the number of aging population are growing significantly. Point-Of-care (PoC) applications in hospitals are used widely around the world. The Security Regulations are implemented to provide data integrity, confidentiality, and availability. Therefore, patients ECG signal and other physiological readings such as temperature, blood pressure, glucose reading, position, etc., are collected at home by using Body Sensor Networks (BSNs) .It will be transmitted and diagnosed by remote patient monitoring systems (RPM). At the same cost ,patient confidentiality 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 allows ECG signal to put out of sight the patient confidential data and thus guarantees the patient's privacy and confidentiality. In addition the following mechanism were incorporated in this project: (1) encryption and decryption for data confidentiality and integrity (2) a three-tier security for data (3) ECG based Steganography to exchange data. A degree of high privacy is guaranteed for patient and simultaneously the Stego ECG remains diagnosable. Our scheme also ensures security, scalability, and efficiency.

Index Terms— Confidentiality, DWT, ECG, HIPAA, RPM, Steganography, Wavelet.

1 Introduction

In accord with HIPAA regulations, the patients confidential information sent through the public network should be protected and secure. Patient privacy is important that a patient can control who will use his/her confidential health information, such as name, address, telephone number, and Medicare number and who can access patient's data and who cannot. At the same time number of aging population is increasing significantly, monitoring patients at their home can reduce the increasing traffic at hospitals and medical centres. 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.

Information Security is to prevent the unauthorized access, misuse of data, content modification, or denial of access, facts(data), etc., The primary goal is to provide confidentiality, integrity and availability. The good security in reality is compile of these solutions. The solid physical security is essential to guard substantial assets like papers, records. Communication security (COMS) is essential to guard information in transmit. Computer security (COMPS) is essential to control access over others computer systems, and Network security (NET) is vital to secure the local area network. Together, these concepts provide Information security (INFOS). You guard these things against threats, vulnearbility.

Among these, an important sub discipline of hiding information is steganography. Information hiding is recent techniques have become important in a number of applications. It is important that communication must be secured by encrypting the secret messages. While cryptography protect the content of the messages, steganography concealing the secret message. Usually means hiding information in other information.

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.

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 [2], [4], [16], [17]. The limitations of using encryption based techniques is its large computational overhead. Therefore, encryption based methods are not suitable in resource-constrained mobile environment.

Rest of the paper is organized as follows. Section II briefly discusses the related works in this area. In section III , the basic methodology, system design, the embedding process and the extraction process is discussed. Section IV shows the result of the project. Finally, section V concludes the paper.

2 Related Work

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 sub- band 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.

H. Danyali and H. Golpira [8] proposes a technique based on histogram shifting in wavelet transform domain, in which blind reversible watermarking approach for medical images are proposed. In their work MRI medical image is used as host data. The watermark data is embeded into a subband regions which is in high frequency of the transformed image. Two thresholds were used based on the watermarking. One in the initial part and the other in the ending part of the histogram. The histogram located between the two thresholds remains unchanged. A two dimensional wavelet transform is applied to the image, to extract the watermarked data in the cover media. Therefore the hidden watermarked data are extracted. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of this algorithms is low.

3 Methodology.

The sender side of the proposed ECG steganography method consist of three stages. This proposed technique has authentication stage that prevent unauthorized users from extracting the hidden data and it is designed to secure the information of patients hiding with minimal distortion of the host ECG signal.

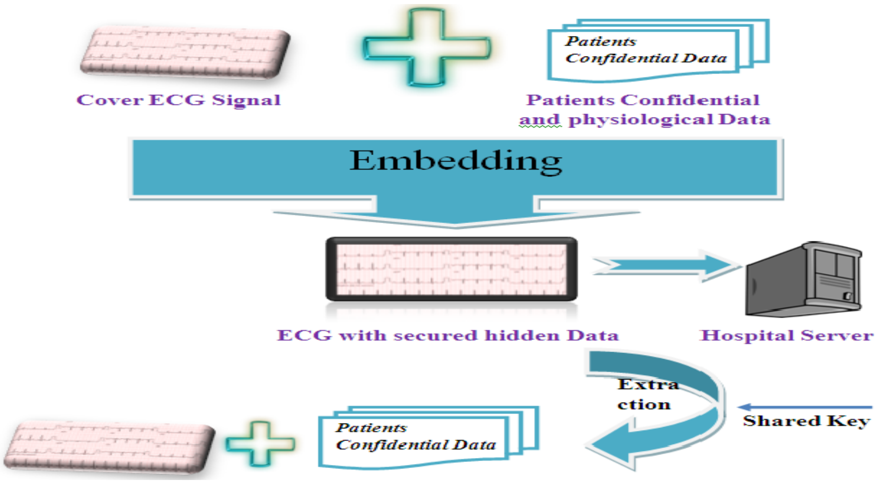
Cover ECG Signal
Patients Confidential Data
Patients Confidential and physiological Data
Embedding
ECG with secured hidden Data
Hospital Server
Extra ction
Shared Key
Patients Confidential Data

Fig. 1. Scenario of ECG Steganography that embed patient confidential data in ECG signal to get ECG with secured data and extraction process.

3.1 Generation Of ECG Signal

Electrocardiogram Tracing of heart's electrical activity, the rhythm of the heart in term of beats per minute (bpm). 10 electrodes in total are placed on the patient. 6 are chest electrodes called V1-V6. 4 are limb electrodes as right arm, left arm, right leg, left. The format of ECG signal consist of Q wave, R wave, S wave, the QRS complex, P and T waves. The signal normally begins with P wave that following the QRS wave or QRS complex. Then it was followed by the corresponding T and U waves. A U-wave may be present and lies after the T-wave. The QRS complex is the most important component in the ECG signal because of its high amplitude and speared nature, it process more electrical activity, it indicates depolarization of the ventricles which have superior muscles. The subsequent processing of the ECG signal such as calculation of the RR interval, P and T waves for ventricular fibrillation and tachycardia, etc are estimated by detection of QRS complex. The two types of ECG signal used and generated in this project are as follows 1) Normal Signal and 2) Tachycardia(abnormal). A heart rate above 150 bpm called Tachycardia.

3.2 Data Encoding

For Security purpose, the patient's data are first encrypted using Public key cryptosystem. The patient confidential information is encrypted in such a way that prevent unauthorized persons who does not have the shared key from accessing confidential data. Encryption is the initial security solution for communicating in open network Therefore, encryption itself does not provide security. Encryption does not save data from hacking but it prevents the intruder from modify or reading the content of data that is encrypted. It may protect valuable data that is in stored encrypting files.

3.3 Stego ECG Signal

In this stage to ensure high data security, the embedding operation is performed which hides data in the wavelet coefficients and propose high data security. In this stage a discrete wavelet transform operation is performed. Then the stego ECG signal with patients confidential information is further encrypted for strong and high security purpose.

3.4 Data Decoding

To extract the secret data from the stego ECG signal, the following information is required at the receiver side. The shared key value for decrypting data. Shared key for decrypting digital stego ECG.

This is necessary that the encryption algorithm should run in the reverse order. It requires the cipher text of patient data and the secret shared key and produces the original data.

In this stage the receiver should undergo the reverse operaion to retrieve patients confidential information and the original ECG signal. They should have the shared key for decrypting the digital stego ECG signal and shared key for decrypting information. The security of this system is based mainly on the idea of having secure shared key between the sender and the receiver entities. Any changes in any key value in the encryption and decryption process will not allow to extract the data. Using the shared key, the extraction operation starts extracting the secret bits in the correct order according to the sequence rows. The extracted secret bits are decrypted using the same shared key.

ALGORITHM

```
1: $S_C$ ecg : the host ecg signal (cover)
2: $S_S$ : calculate the size of ecg signal
3: $S_D$ : read the secret data
4: b bits : the secret bits
5: bs : size of secret bits
6: k : encryption key (asymmetric)
7: ks : size of the key
8: $ES_D$ : encrypted secret data
   of pateint
9: $ES_D \leftarrow S_D + k$
10: convert the encrypted data into binary so as to obtain individual bits of the data.
11: $B(ES_D)$ : binary digits of $ES_D$
12: $AS_C$ : analog ecg signal
13: $DS_C$ : digital ecg signal
14: $DS_C \leftarrow S_C + A/D$
15: convert the $DS_C$ into binary notation so as to obtain individual bits of the signal.
16: Prepare the secret data to embed
17: Decompose the $S_C$ using DWT
    $W(i,j) = \sum_{i}^{j} X(i)\varphi ij(n)$    (1)
18: secg ← embed (bits (b) in LCF of $S_C$)
19: Repeat step 18 until all the data bits are embedded
20: to increase security encrypt the secg using xor
21: end
22: $AS_C \leftarrow S_C + D/A$
23: ECG ← apply inverse dwt and decryption (recomposition)
24: Finally the secret data can be obtained by converting the extracted binary to data bit
```

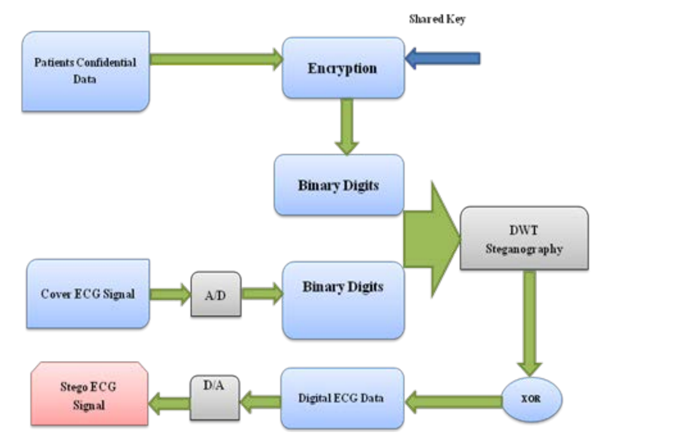

Fig. 2. Block Diagram of proposed steganography which includes encryption, dwt, decryption.

4 Results

This scheme has implemented and conducted some tests. 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, haemoglobin, 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 hides patient personal data and physiological data in the ECG signal.

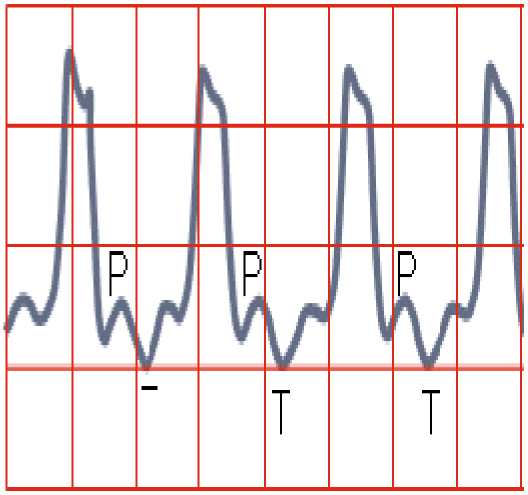

Fig. 3. Sample ECG Signal

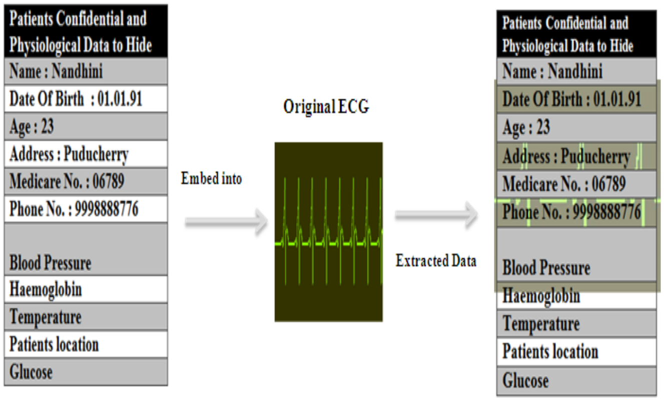

Fig. 4. Embedding patient confidential information in the ECG signal

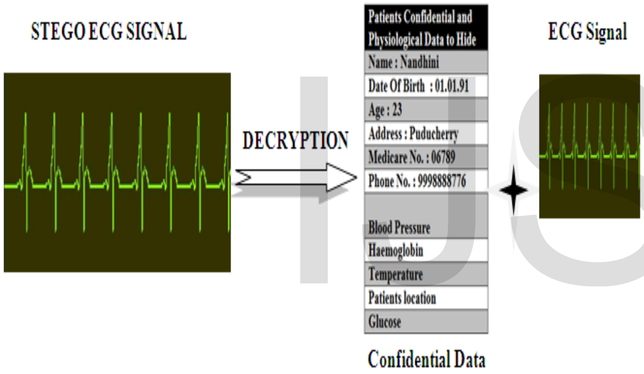

Fig. 5. Decoding process extracting patient data from the ECG signal

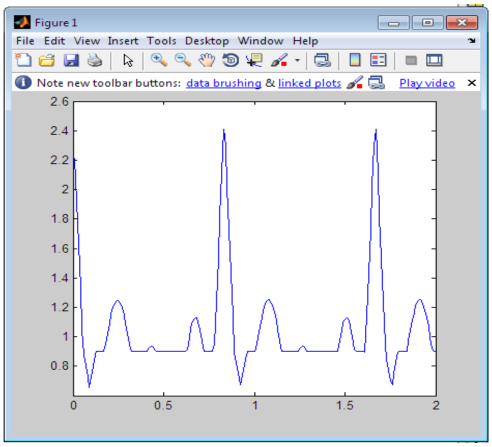
Figure 1
File Edit View Insert Tools Desktop Window Help
Note new toolbar buttons: data brushing & linked plots Play video
2.6
2.4
2.2
2
1.8
1.6
1.4
1.2
1
0.8
0
0.5
1
1.5
2

Fig. 6. Generated original normal ECG signal using MATBAB

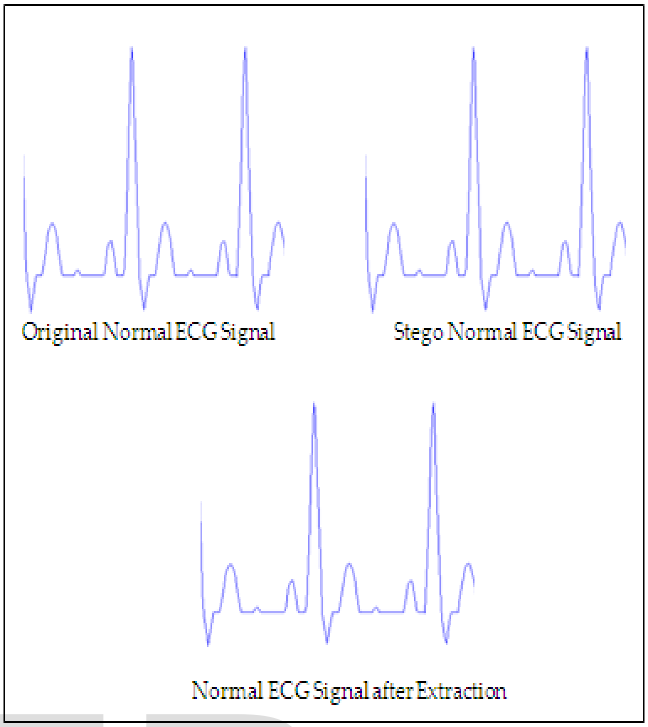

Fig.7. Normal ECG Signal before applying the steganography operation and after the steganogarphy operation as well as after extracting the secret data.

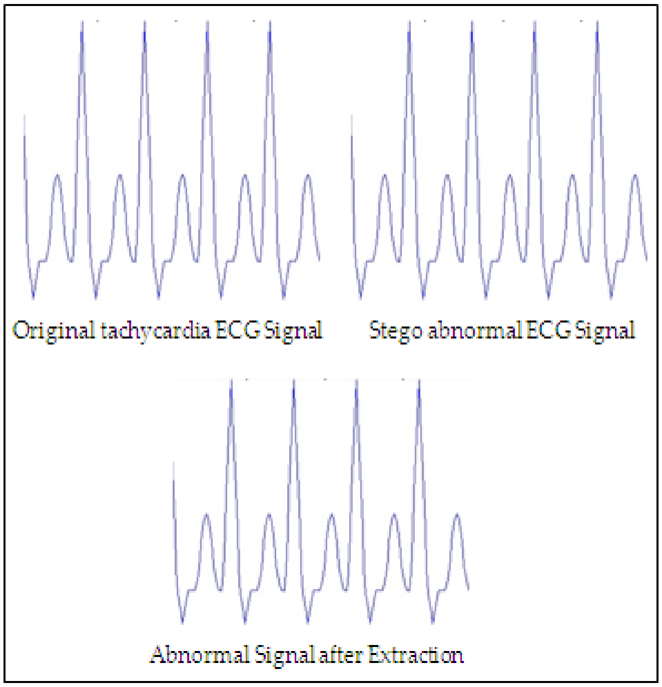

Fig.8. Abnormal ECG Signal before the steganography operation and after steganogarphy operation as well as after extraction.

5 Conclusion

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 regulation 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.

References

[1] Ayman Ibaida, Ibrahim Khalil "Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems" IEEE Transactions On Biomedical Engineering.

[2] 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.

[3] 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 assisted living environments. ACM, 2007, p. 12.

[4] 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.

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

[6] 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.

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

[8] 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.

[9] Eric Maiwald "Fundamentals of Network Security" Himal Impression Press, 2008.

[10] Arvind Kumar, Km. Pooja "Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[11] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.

[12] Shashikala Channalli et al, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141 137.

[13] Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003

[14] Pradeep Kumar Jaisal, Dr. Sushil Kumar, Dr. S.P Shukla, "A Survey of Electrocardiogram Data Capturing System using Digital Image Processing: A Review", IJCST Vol. 3, Iss ue 1, Jan. - March 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

[15] Ibaida, A. ; Sch. of Comput. Sci. & IT, RMIT Univ., Melbourne, VIC, Australia ; Khalil, I. Al-Shammary, D. , "Embedding patients confidential data in ECG signal for healthcare information systems", Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE.

[16] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "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.

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

[18] Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, "Spread Spectrum Image Steganography" Jr., Member, IEEE, and Charles T. Retter, Member, IEEE.

[19] Ying Wang, Member, IEEE, and Pierre Moulin, Fellow, IEEE "Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions", Transaction on Information theory, Vol. 54, No. 6, June 2008.

[20] Weiming Zhang, Shuozhong Wang, and Xinpeng Zhang, "Improving Embedding Efficiency of Covering Codes for Applications in Steganography", Vol. 11, No. 8, August 2007

- *Mrs. V. Sankari received B.Tech degree inV.R.S College of Engineering and Technology,villupuram from Anna University, India, in the year 2005 and M.E degree in Rajalakshmi Engineering college, Chennai from Anna University, India, in the year 2009 and currently working as Assistant Professor in Manakula Vinayagar Institute of Technology, Pondicherry University, India. PH-9894201681. E-mail: tosankari@gmail.com*
- *Ms. K. Nandhini received the B.Tech. degree in Information Technology from Dr. Pauls Engineering College, Anna University, India, in 2012 and currently pursuing masters degree program in Computer Science and Engineerng in Pondicherry University, India, PH-9943796831. E-mail: nandhini21b.e@gmail.com*