Hiding Patient Confidential Information in ECG Signal Using DWT Technique

Ms. Pawar Kshetramala Dilip, Prof. V. B. Raskar

Abstract- **the patient's confidential data should be safe and secure these is Act by Health Insurance Portability and Accountability Act (HIPAA). At the same time, there is a significantly growth in population. Numbers of patient care centers are used usually around the world in a Point - Of - care (PoC) applications. The Security systems are implemented to provide data integrity, privacy, and accessibility. Therefore, ECG signal of the patients and other physiological data of the patient's like body temperature, glucose level, blood pressure, position, etc., are collected by Body Sensor Networks (BSNs) at home. After that it will transmitted over network and then stored at hospital server. In this paper, it used the steganography method which is depending on discrete wavelet transform to accomplish HIPAA act. DWT technique is applied on the ECG signal to hide confidential information of the patient which provides privacy to confidential information. High degree privacy is provided to patient, also Stego ECG remains diagnosable. In this paper the steganography technique is used to provide the three tire securities to patient's data. Our system also ensures safety, scalability, and effectiveness.**

Index Terms— ECG, Steganography, Encryption, Wavelet, Watermarking.

I. INTRODUCTION

Hiding the confidential data in to other form of data is call as data steganography. The HIPAA regulations act says that, there should be a protection and security is provided to the patient's confidential information which is sent through the public network. As the patient privacy is important so patient can control his/her confidential health information that if anyone can access or control the information like name, age, gender, ID no., address, telephone number. Monitoring patients at their home can reduce due to increasing rush at hospitals and care centers like medical.

Hiding patient's confidential information and other physiological data in ECG signal is the main goal. Provide secrecy, integrity, and accessibility to confidential information. The main branch of cryptography is steganography that involves hiding information in other secondary information. Hiding the information decrease the chance of the information being detected. Medical images has smaller size were the ECG signal has greater size. Therefore instead of medical image ECG signal is used in steganography process. The ECG signal of the patients is used to hide physiological data of patient like temperature, glucose level, blood pressure, position, etc., which are collected by using Body Sensor Networks (BSNs) at home and stored on hospital server by transmitted via network. Then that data is diagnosed by monitoring systems at hospital. At the same cost that the patient privacy is protected against intruders while data navigate in open network and stored in hospital servers. This technique allows hiding the confidential information of the patient in to ECG signal and thus gives guarantees the patient's privacy and discretion.

The main objective of steganography is to put the undisclosed message in the other coated media so that nobody can see that and both doctor and patient can communicate in secret way. The data security has improved by combining the more number of methods of steganography and the other techniques related to data hiding.

The first steganography method is on hiding patient data which is confidential, inside ECG signal of patient which can be called as host signal. Additionally, the proposed method uses model which involves encryption to allow extracting the data which is hidden. That data can be extracted by only the authorized persons like doctors. In this paper, for the host signal, the ECG signal of patient is used and the patient private information and other physiological reading are hiding inside it. The main fact is that the ECG signal which is used here as a host signal because ECG information will collect by many of the healthcare systems. As compare to other host signal, ECG signal has large size thus it can hide more data than hiding data in other host signal.

Therefore, for the small size secrete data the ECG signal will be right as a host. The proposed technique fallows the HIPPA, by providing open access for ECG signal and provides security for patient's confidential information from unauthorized access. In this method the ECG signal with temperature, blood pressure and glucose level are collected by using body sensor network. By using Bluetooth the physiological readings collected from sensor are transfer to patient's PDA device. The patient's PDA device contains steganography technique and embedding operation which embed the patient secret information and patient physiological data inside the. ECG signal i.e. host signal.

II. LITERATURE SURVEY

To provide security to patient confidential data, there is no. of methods [4], [1], [5]. However, one approach proposed which is on using steganography. Were, to protect confidential information of the patient it used medical image to stored secret information. How much data can be stored in medical image are the challenging factors of this method and up to which level this method is safe.

Kai-meiZheng and XuQian [8] proposed a fresh technique for data hiding which is reversible and depending on wavelet transform. Furthermore, this method dose not used user define key, so in this algorithm the security is depends only on algorithm. At last, this algorithm is not useful for the abnormal ECG signal because in it QRS complex is absent. However this algorithm is depending only on normal ECG signal were QRS complex can be easily find.

ISSN: 2278 – 1323

H. Danyali and H. Golpira [7] proposed a new technique where medical images are used like host signal. So this technique is not useful for ECG signal. Moreover, this algorithm has low capacity. Additionally, the encryption key is not concerned in its watermarking process.

In our approach to use ECG signal in data hiding process. To decompose the ECG signal DWT technique is used. Then the patient's confidential information is embedded with share key inside decomposed ECG signal. XOR ciphering method is used with a shared key which is an ASCII coded. Here first security is provided with a shared key which is an ASCII coded. Second security is provided at the time of embedding operation by applying inimitable scrambling matrix. And third security is providing by selection steganography level vector at the time of inverse wavelet transform. So here three tier securities are provide to the patient's confidential information.

III. IMPLEMENTATION DETAILS

The sender side steganography technique containing of four stages and receiver steganography side consists of three stages which is shown in Fig 1. In this technique to decompose ECG signal discrete wavelet transform is used. Then data hide inside that decomposed signal. The two main part of this method are sender steganography and receiver steganography.

A) Sender Steganography:

The sender side steganography technique contains encryption, wavelet decomposition and data embedding operation. Firstly, secrete data are encrypted and then embedded in to ECG signal. Scrambling matrix and level vector are used in the embedding process. Shared key is taken for security purpose. The detailed block diagram of sender steganography is shown in Fig. 2.

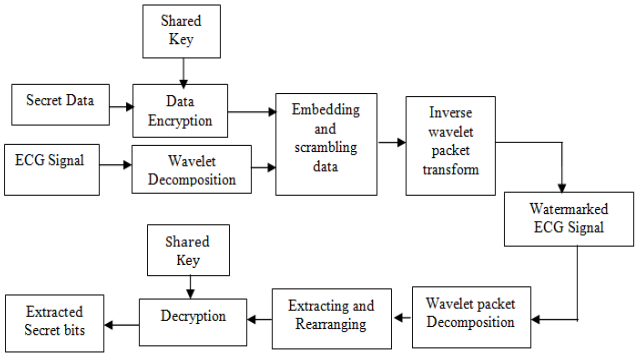

Fig.1. *Block diagram of ECG Steganography*

1) Encryption:

This stage has main aim to provide security to the confidential information of the patient by encrypting data in like the way that prevents illegal persons to accessing the private information. For this stage the main part is XOR ciphering which involves the technique for share key in security purpose. Because of simplicity XOR ciphering is selected. Additionally, XOR ciphering can be implemented easily within a mobile device.

a) Confidential Information:

For Security purpose, Public key cryptosystem is used to encrypt the patient's data first. The confidential information of the patient is encrypted like the way that prevents illegal persons to accessing the private information to which share key is unknown. In open network communication, the initial security is given by Encryption. Data hacking does not prevent by encryption but it prevents from modify or reading the encrypted data content. The ECG signal of the patient and other physiological data of the patient like blood pressure, body temperature, glucose level, position and also patient name, patient age, patient gender, etc. this private information should be protected and secure. For that purpose these information encrypted with shared key.

b) XOR Ciphering:

Exclusive-OR encryption is not like RSA, is roughly unbreakable through brute force methods. Exclusive-or encryption requires share key for both Encryption and descriptor algorithm, while is simple and unbreakable. Exclusive-OR encryption depends on the Boolean algebra function, exclusive-OR (XOR). XOR is a binary operator (meaning that it adds two arguments). By its name, exclusive-OR, it returns true if one operator is true out of two operators.

XOR ciphering method is used with a shared key which is an ASCII coded. Here first security is provided with a shared key which is an ASCII coded.

2) Wavelet Decomposition:

For the correct analysis it takes multistage wavelet decomposition. The fig. 4 shows 'h' is low-pass filter, 'g' is high-pass filter, and '↓2 'is down sampling. Wavelet transform is a process that decomposes the given signal into high frequency and low frequency coefficients.

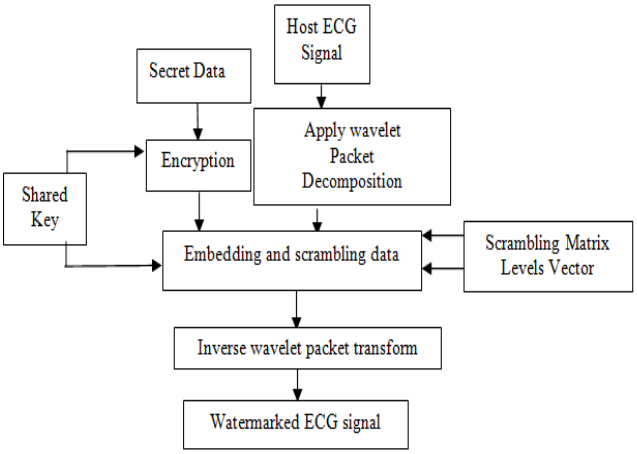

Fig.2. *Block diagram of the sender steganography*

$$C(S, P) = \int_{-\infty}^{\infty} f(t)\psi(S, P)dt \qquad (1)$$

In eq. 1, S and P are two positive integers used to representing transform parameters. C expresses the coefficients which is the function of position parameter and scale and position. Time domain and frequency domain can be combining in one transform using wavelet transform. For more number of applications discrete signals are used. Therefore, instead of continuous wavelet transform it uses Discrete Wavelet

ISSN: 2278 – 1323

Transform (DWT). The decomposition of DWT can be done by applying wavelet transform to the signal with band filters. The output of the band filtering operation will be two different signals of high frequency components and low frequency components of the main signal. To repeat this process for multiple times it takes multi-level wavelet decomposition. The eq. 2 expresses Discrete Wavelet transform.

$$W(i,j) = \sum_i \sum_j X(i)\psi_{ij}\ (n) \qquad (2)$$

Where W (i, j) represents the coefficients of DWT. I is the scale parameter and j is the parameter of shift transform, and is the t basis time function of wavelet with fast decay and finite energy. The eq. 3 expresses wavelet function.

$$\psi_{ij}(n) = 2^{-i/2}\ \psi(2^{-i}n - j) \qquad (3)$$

In this paper, a host signal is decomposed in to 32 sub-bands by applying a5-level wavelet packet decomposition. The main signal is divided into two signals in each of the decomposition level. One of them represents components of high frequency and second one represents components of the low frequency. The approximation signal (A) is a low frequency signal which contains the ECG signals important feature. Were On the other side, the signal (D) is the ECG signals noise part which is related to high frequency signal. As a result, a small number of the 32 sub-bands are related with signal A i.e. approximation signal and other sub bands will be related with the noise components in the main ECG signal. Therefore, our proposed method is depending on sub-band in which for each sub-band different number of bits of wavelet coefficient will be changed (usually called steganography level).

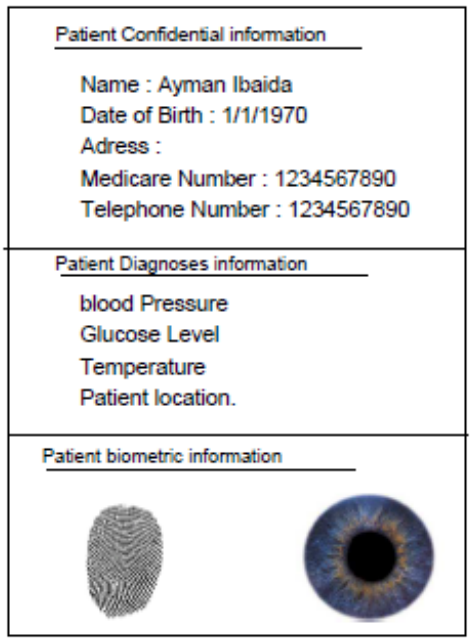

Fig. 3. *Confidential information of patient..*

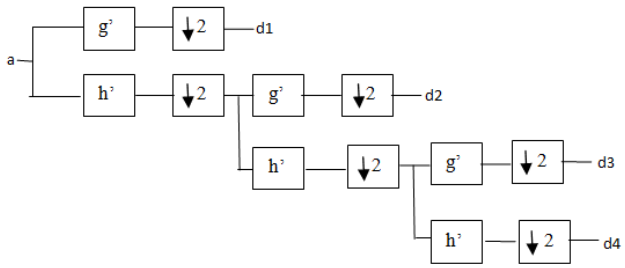

Fig. 4. *Multilevel Decomposition*

To reduce the distortion in the stego ECG signal, different levels of steganography for the host signal will be selected. Hiding data in some sub-bands to minimize the distortion will highly affect the main ECG signal. Accordingly, there are 5 bits for bands from 1 to 17 in selected steganography level and for other band there are 6 bits.

3) The Embedding Operation:

For the high data security the technique is implemented which involves embedding operation. There are two parameters in scrambling operation. First parameter is shared key. Sender side and the receiver side should know the share key which same for both sides. Second parameter is scrambling matrix. The transmitter and the receiver both stores same scrambling matrix inside in, thus for each pair of transmitter/receiver has a same scrambling matrix defined by Eq. 4

$$S = \begin{pmatrix} S_{1,1} & S_{1,2} & \cdots\cdots & S_{1,32} \\ S_{2,1} & S_{2,2} & \cdots\cdots & S_{2,32} \\ . & . & \cdots\cdots & \\ . & . & \cdots\cdots & \\ S_{128,1} & S_{128,2} & \cdots\cdots & S_{128,32} \end{pmatrix} \qquad (4)$$

Were scrambling matrix S has size 128×32. The element S is a number which is in between 1 and 32. To build the matrix there are some conditions are as following:

- There should not be duplicate element in the same row.
- Rows should not be duplicates.

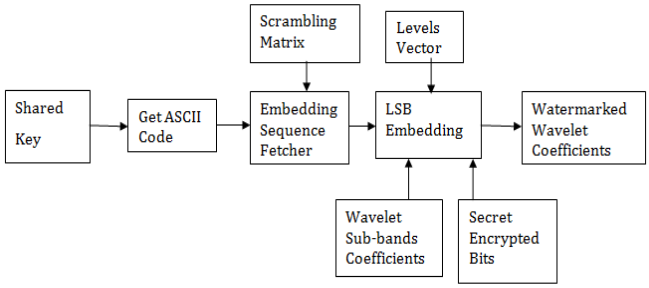

Fig. 5.Block diagram of Embedding operation

The detailed block diagram for the embedding process is shown in Fig.5. The first step in embedding matrix is converting the shared key into ASCII coded value, therefore the result in ASCII code number is in between 1 to 128 for each character. The main function of scrambling sequence fetcher is, read the corresponding row for each character code from the given scrambling matrix. The fetched row example can be shown in Eq. 5

ISSN: 2278 – 1323

$$S=\begin{pmatrix} 32 & 22 & 6 & 3 & 15 & 11 & 30 & 7 \\ 28 & 17 & 14 & 8 & 5 & 29 & 21 & 24 \\ 31 & 26 & 27 & 19 & 16 & 1 & 23 & 2 \\ 4 & 18 & 25 & 13 & 9 & 20 & 10 & 12 \end{pmatrix} \quad (5)$$

For data hiding the embedding operation performs according to fetched row result which is sub-band sequence. For example, in eq. 5 if the fetched row is present, then from 32 sub-bands the wavelets coefficients are read and change its LSB bits by the embedding process. Then, it will read the first wavelet coefficients from the 32 sub-bands and change the LSB bit in 32 number sub-band. Then it will change the LSB bit of 22 number sub-band and so on. According to level vector it decides the steganography level. The main work of level vector is to maintain the record of sub-bands and the LSB bit changed numbers. For example it will changed 6 bits for 32 sub-band per sample while for the 1 sub-band it will change 5 LSB bits.

4) Inverse Wavelet Decomposition:

The first step in inverse wavelet decomposition is restoring the signal from decomposed signal. As a signal is decomposed in multilevel sub-bands then that signal is recomposed from the decomposed signal. In practical, there is multistage reconstruction technique is used for small waves. For accurate analysis signal should be reconstructed. Fig. 6 shows the multi- stage reconstruction diagram for decomposed wavelet signal. Were 'h' indicate low-pass filter, 'g' indicate high-pass filter and '↑2' means up sampling.

The final watermarked ECG signal is recomposed from the original signal in 32 sub-bands. These new watermarked signal of ECG contain the confidential information which is hide inside it and high level security is provide to this signal by using embedding operation. The signal before the wavelet decomposition is in time domain, that signal is then converted in to time domain instead of time and frequency domain in the reverse wavelet decomposition process. Therefore the new watermarked and original signal of ECG is same.

B) Receiver Steganography:

The receiver side includes watermark decomposition, extraction & decryption process. The received ECG watermarked signal is extracted with the help of shared key.

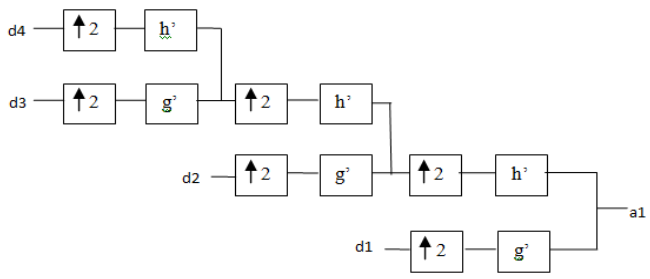

Fig.6 *Multi-stage reconstruction*

1) Watermarked Extraction Process:

In the watermarked secret bit extraction, the receiver side should know the following information.

1) The shared key value
2) Scrambling matrix
3) Steganography levels vector

Fig. 7 shows the detailed block diagram of receiver steganography. The shared key value and the scrambling matrix should be same at both side.The first steps is to get the extracted information from the watermarked ECG signal. To generate the 32 sub-bands signals it applies 5-level wavelet packet decomposition to ECG signal. Then the main step to extract hidden data or secret data from stego signal is to apply known scrambling matrix value to signal. Then that secret data is fetched sequentially according to scrambling matrix using row fetched sequencer. Finally, to decrypt the extracted secret bits apply the shared key value which is same at both sender and receiver side.

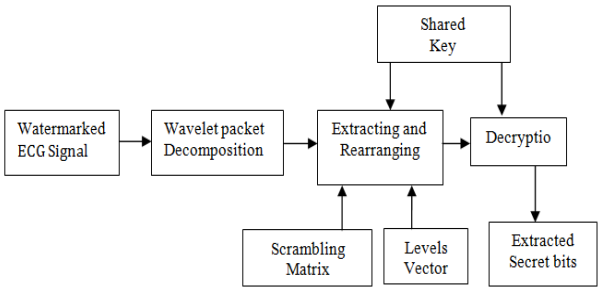

Fig. 7 *Block diagram of the receiver steganography*

IV. Result And Discussion

In this paper three stages are implemented out of eight stages, which are required to implement the project. Those three stages are XOR ciphering, Encryption and wavelet decomposition. In the implementation, the patient's confidential information like name, age, gender are encrypted with share key and transmitted along with the ECG signal specifically, this scheme hides patient personal data and physiological data in the ECG signal.

A) Data Encryption:

The patient's confidential information such as name, age, gender, glucose level, blood pressure are encrypted with shared key. XOR ciphering method is used with a shared key which is an ASCII coded value.

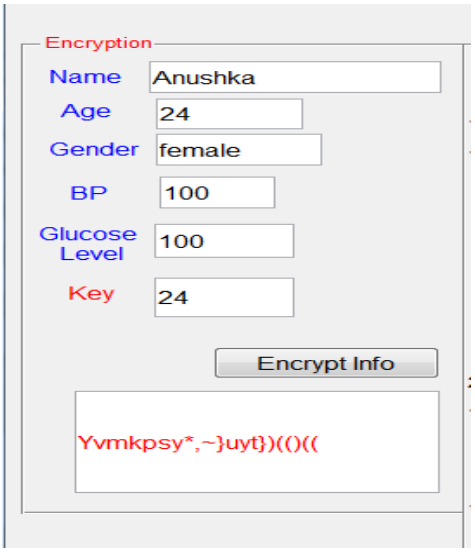

Fig.8. *Data Encryption*

B) Offset Removal of ECG Signal:

ISSN: 2278 – 1323

Figure shows the GUI representation of ECG signal. There is lead 1 & lead 2 ECG signal shown in result. Offset corrected signal is also shown in figure.

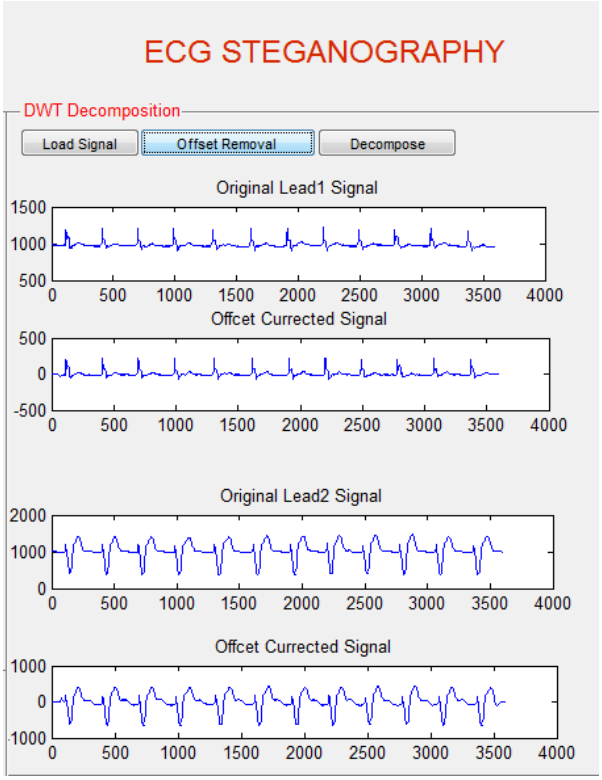

Fig. 9. *Offset Removal*

C) Decomposition of ECG Signal:

The host ECG lead 1 & lead 2 signals are decomposed in to two part, Approximation & detailed signal. Were approximation signals are low frequency signals & detailed signals are high frequency signals. ECG signals are related with low frequency signals. After decomposing the ECG signal, the encrypted information is embedded in to decomposed ECG signal.

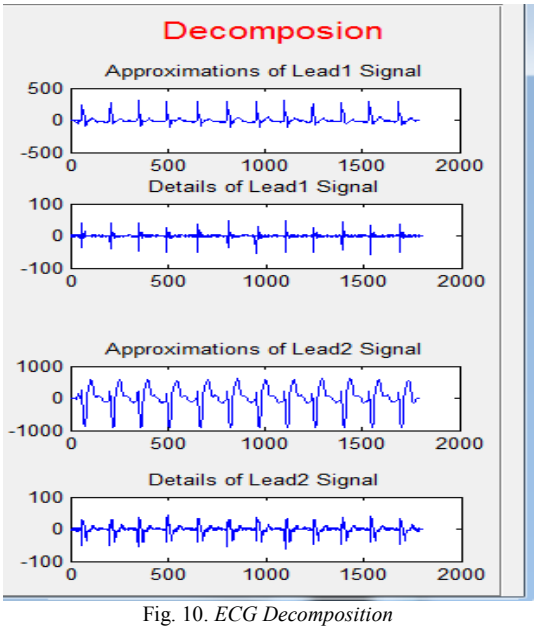

Fig. 10. *ECG Decomposition*

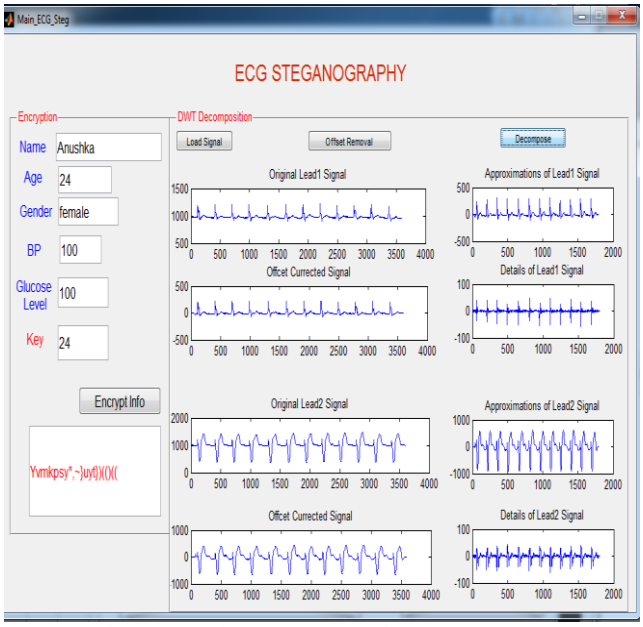

Fig. 11. *Signal Decomposion and Data Encryption*

V. CONCLUSION

In this paper, the confidential data of the patient is hiding inside ECG signal and thus guarantees the patient's confidentiality and privacy using Discrete Wavelet Transform. The proposed algorithm provides secrecy, integrity, and accessibility to confidential information. Three tier of security is providing. . Any doctor from the hospital can access the watermarked ECG signal but only certified doctors can extract the secrete data from ECG watermarked signal. Also the authorised person can only access to the confidential patient's data as well as other physiological data of patient which is stored inside the host ECG signal. The distortion will be less.

REFERENCES

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

[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]. 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.

[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]. A. Al-Fahoum, "Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 1, 2006.

[6]. 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.

[7]. H. Golpira and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting," in *IEEE*

ISSN: 2278 – 1323

International Symposium on Signal Processing and Information Technology (ISSPIT), 2009. IEEE, 2010, pp. 31–36.

[8]. 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.

First Author-Ms. Pawar Kshetramala Dilip, perusing M. E. in Electronics and Telecommunication from ICOER, JSMP's Wagholi, Pune.

Second Author- Prof. V. B. Raskar, Received ME.(Digital Signal) in Electronics and Telecommunication from RSCOE, JSMP's Tathawade, Pune. Now working as a Assistant Professor in ICOER, JSPM's Wagholi, Pune.

ISSN: 2278 – 1323