Secure Steganography, Compression and Transmission of ECG signal for Protecting Patient Confidential Information in Point-of-Care Systems

Dr. Bijith Marakarkandy¹, Mr. Raghupati Tiwari²

¹ Associate Professor (Electronics & Telecommunication Engineering), TCET, Kandivali, Mumbai, India
² Pursuing Master of Engineering in Electronics & Telecommunication, TCET, Kandivali, Mumbai, India

ABSTRACT
Considering the growth in population and many of the people are in troubled from cardiovascular diseases, The ECG patient remotely observing systems are probable to be broadly used as point-of-care in hospitals and also all over world. Hence, very large number of ECG data obtained by patient body sensor networks by remote patients from their places will send with physiological information that is temperature, glucose level, blood pressure, so on. It is more important that patient’s confidential data are secured when it is placed on the server of a hospital and also used by remote watching system when required. Thus, in this paper recommended to use Wavelet based steganography method which make combination of encryption and scramble method to secure patients confidentiality. These proposed technique permits ECG signals to hide patient’s confidentiality and also other physiological data’s hence also provide integration of ECG signal and patients private data. To estimate the good effects of the given method on the ECG signals, there are two distortion measurements metrics are used - the percentage of residual difference and wavelet weighted PRD. It is discovered that this process provides very high-security system for patients information with less distortion and ECG signal being diagnosable after of watermarking and along with after watermarks are eliminated from the watermarked data. It is expected that the water-marked ECG signal are used for diagnose and the hidden information all are removed.

Keywords: ECG, Steganography, DWT, Water marking.

1. INTRODUCTION
According to the HIPAA rules and regulations, the patients secret information sends through the public Network should be took care of and safe. Patient getting care rights not to be public means that his privacy is most important that any patient can control who would use his or her secret health medical information, such as contact number, name, Medicare number, and who can take patients data and also who cannot. At the similar time number old enough population are increasing more looking at patients to their house can decrease the people at hospitals and also at medical centers. The main objective is to get integrity, availability, confidentiality. Steganography is the branch of a cryptography that concern to hiding of information. Hiding an information decrease the possibility of information being identified. The most important thing is to hide all the confidential information’s of the patients and other information which are present in ECG signal. ECG signal are taken due to the size of all ECG is more in comparison to other medicals footage. As an outcome of that, patient getting care ECG signal and also other physiological readings collects at the home by using BSN (Body sensor Networks) will also be sent and diagnose by remote patients observing system. In any way the patients getting care there confidential information are secured against the intruder when information is on the public network and stored on hospitals server. This method lets ECG to put out of sight the patients getting care to keep secret data and make sure to the patients getting care privacy and there confidentiality. The purpose is that both host ECG and the stego ECG information can be used for diagnosis and difference is being undetected. This project work is motivated by inspection from many and similar researches findings. Our main objective is that to protect patients confidential information is being harmed due to steganography technique. From proposed technique, we made a new technique of steganography utilizing ECG signal and from that we introduce algorithm of that, which is fast and also scalable, and it is also has capability to provide high quality and also consistent performance. In typical wireless tele-monitoring systems with body sensor networks, patients wear one or more body sensors to collect their ECG signals. Next, the collected biomedical signals are transmitted to the patient’s smart-phone where any processing required is implemented. Finally, the collected signals as well as other patient information are transmitted to the medical cloud using the Internet [52]. Alternatively, patients at hospital can also send their biomedical signals with their information to the centralized medical cloud. However, in this scenario, many challenges arise.
1. Patient confidential information should be transmitted to the medical cloud along with patient physiological signals. In this case, confidential information requires a special mechanism for protection against intruders.
2. ECG signals are of enormous sizes. A typical electrocardiogram observing device makes large volume of the digital data. Depending on the application for the data, the sampling rate varies from 125 to 1024 Hz. Each data sample may be represented using 8 to 16 bit binary number. Up to 12 different streams of data may be obtained from various sensors placed on the patient’s body. If this large amount of data is transmitted wirelessly to the medical cloud then it will require a large bandwidth as well as very considerable power.

2. Proposed Work
This security technique will provide us secure transmission of patient’s confidential data with all the patient physiological data from the body sensors. Thus proposed method is with two techniques. First, it is depend on steganography method to hide the patient’s confidential data into patient’s bio-medical signal. However, this proposed method uses encryption technique because only known person can only remove the hidden information. In this technique, the patient’s ECG signal are use as host signal which will take the patient secret data and also other information from other sensors like blood pressure, glucose level, temperature and position. The ECG signals are use because of the health care system will gather ECG data. Since, the sizes of the ECG signal are more as compared to other information size. Hence, the proposed method has been follows the HIPAA rules and regulations which provide access for all patients’ details such as medical signal but it also prevents the signal from unauthorized person access to the patient’s information which is confidential. This paper technique BSN (body sensor nodes) which are uses to gather ECG information, blood pressures, temperature, glucose level and position, thus sensors will be used to send readings to the patient’s device such as PDA device through Bluetooth. Into the patient PDA device will be applied a steganography method and patient’s confidential data and also physiological data will embedded into the ECG host signals. The watermarked ECG signals are sends to the hospitals server through Internet. The actual size of transmitted information are of a size of the ECG signal, since the all other information’s are hidden into the ECG signal not increased it size. In the hospitals server the hide information and are stored. Any doctor will be able to see the watermarked ECG signal and no other can see but approved doctors and also patient can take his/her secret medical data and the confidential data. This system is shown in Fig. 1. The given Steganography method have been made in a way that make sure of less acceptable distortions in ECG signal, moreover, it must provide the largest security that can be accomplished. If this method will be used it will slightly affect on quality of the ECG signal. Although, watermarked ECG signal would be going to use in this paper for the diagnosis purposes. In the paper, the given research question has been answered.

![ECG steganography scenario in point-of-care (PoC) systems where body sensors collect different readings as well as ECG signal and watermarking process implemented inside the patient’s mobile device.](image)

1) Will be given method going to protect the patient’s confidential information as given in the HIPAAAs securities and also privacy guidelines?
2) What would be the effects upon the original ECG signal following applying the given Steganography method in term of size and quality?

3. Methodology
At sender side in the given steganography method has 4 integrated stages shown in following fig.3. Thus proposed method has been designed in such a way that it makes sure of hiding of information in secure way with less distortion of the host signal. However, this method has a authentication stage to prevents an unauthorized user from taking the hidden data.
A. Encryption
The eagerness of this stage is to encrypt the patient individual information in a well-known a manner that prevents unwanted persons—who does not have the shared key from accessing patient confidential data. In this stage, RSA Algorithm is used of an ASCII coded shared key which will be the security key. As shown in figure 2.

B. Wavelet Decomposition
Wavelet transform are a technique which can decomposes given signals into coefficient are represents frequency component of an signal at the given time. Wavelet transform formed as shown in below equations.
Such as ψ represent the wavelet functions. P and S are positive integers representing transform parameters. C represent coefficient which are function of the scale and the position parameters. Wavelet transform is a robust method to merge time domain with mutually frequency domain in one method. In many implementations, discrete signals are performed. Therefore, discrete wavelet transform (DWT) mostly used ideally of continuous wavelet transform. DWT decomposition may be done by trying wavelet transform on the signal for band filters. The outcome of the band filtering performance is two separate signals. First one is equivalent to the high-frequency section and the second is related to the low-frequency section of the original signal. If this method is restated many times, hence called multilevel packet wavelet decomposition.

\[
C(S,P) = \int_{-\infty}^{\infty} F(t) \varphi(S,P) dt \quad (1)
\]
DWT can be defined as follows:

\[ W(i,j) = \sum_{i} \sum_{j} X(i,j) \Psi_{ij}(n) \]  

Such as \( W(i,j) \) represents the DWT coefficients, \( i \) and \( j \) are the scale and shift transform parameters, and \( \Psi_{ij}(n) \) is the wavelet basis time function with finite energy and fast decay.

**B. Embedding Operation**

In this method we would use some security technique to make high data security. In Proposed technique, a scrambling action will used with two parameters. First one is shared key will have both side at sender and receiver. Second will be scrambling matrix that stored into both transmitters and receivers.

i) The identical row should not have duplicate elements.

ii) Rows should not be similar.

The block diagram of the data embedding process is as shown in Fig.4. The embedding method begins with changing the shared key into ASCII codes; therefore each letter is expressed by a number from 1 to 128. For all letter code, the scrambling sequence fetcher further study the equivalent row from the scrambling matrix.

\[ Sr = 31 \ 42 \ 63 \ 26 \ 21 \ 30 \ 7 \ 18 \ 17 \ 14 \ 8 \ 6 \ 29 \ 21 \ 35 \ 31 \ 25 \ 26 \ 19 \ 15 \ 1 \ 23 \ 2 \ 4 \ 19 \ 25 \ 13 \ 8 \ 20 \ 11 \ 12. \]  

**Fig.4** Block diagram showing the detailed construction of the watermark embedding operation.

The embedding operation performs the data hiding process in the wavelet coefficients according to the sub band sequence from the fetched row. For example, if the fetched row is as in (3), the embedding process will start by reading the current wavelet coefficient in sub band 32 and changing its LSB bits. Then, it will read the current wavelet coefficient in sub-band 22 and changing its LSB bits, and so on. On the other hand, the Steganography level is determined according to the level vector which contains the information about how many LSB bits will be changed for each sub-band. For example, if the data are embedded in sub-band 32 then 6 bits will be changed per sample, while if it is embedded into wavelet coefficient in sub-band 1 then 5 LSB bits will be changed.

**D. Inverse Wavelet Recomposition**

In this last stage, the occurring watermarked 32 sub-bands can be recomposed with inverse wavelet packet recomposition. The outcome of this suggested method is the recent watermarked ECG signal. Inverse wavelet method will change the signal to the time domain rather merge both time domain and frequency domain. As an outcome of that, the newly remade watermarked ECG signal would be very much identical to the first form un-watermarked ECG signal. The complete embedding as shown in Algorithm. Thus Algorithm begins by initializing all required variables. Further, the coefficient matrix would be moved and scaled to make certain that each coefficient gains are complete numbers, not parts. Then, the Algorithm will a node from 32 nodes in each rows of coefficient matrix. Thus chooses procedure is depending on the gain study of the scrambling matrix and the key. The Algorithm will be redone unless the conclusion of the coefficient matrix is reached. Further, the coefficient matrix will be modified in position again and rescaled to restore its first form and inverse wavelet transform is sent in name for to make the watermarked ECG signal.

**E. Watermark Extraction Process**

To get out the secret bits from the watermarked ECG signal, the supporters information is needed at the receiver side.

1) The shared key value.

2) Scrambling matrix.

3) Steganography levels vector.

The stages of the extraction process can be given view in Fig. . The first step is to put to use five-level wavelet small parcel decomposition to produce the 32 sub-bands signals. Further, applying shared key and scrambling matrix, the extraction procedure begins getting from secret data in right pattern according to the rows orderly fetched from
scrambling matrix. Ultimately, the removed secret bits are decrypted applying the identical shared key. The watermark separation procedure is nearly close to the watermarking embedding procedure given in Algorithm 1, excluding that rather modifying the bits of the choose node, it is instructed to study gains of the bits in the chosen nodes, and then starting again from zero.

F. Parameter Evaluation

Percentage Residual Difference (PRD) : PRD are used to find the difference into the original signal and watermarked signal and is expressed as

$$PRD = \sqrt{\frac{\sum_{i=1}^{N} (x_i - y_i)^2}{\sum_{i=1}^{N} (x_i)^2}}$$

(4)

Where, $x$: original signal  $y$: watermarked signal.

4. EXPERIMENTAL RESULTS

To verify the proposed technique, it is checked on ECG signals & PRD is measured in between original ECG signal and resulting watermarked signal.

![Input ECG signal](image1)

**Fig.5** Input ECG signal

![Wavelet reconstructed ECG signal](image2)

**Fig.6** Wavelet reconstructed ECG signal

![Secure Steganography, Compression and Transmission of ECG in POC](image3)

**Fig.7** Final extracted patient data from the ECG signal
5. CONCLUSION

The steganography technique is used to hide the patient’s secret information and also diagnoses data which are present in ECG signal. This proposed method will provide a confidential communication and security in the PoC system. The five-level-wavelet decomposition is also applied. A scrambling matrix are used to detect the accurate embedded sequences depend on the public defined key. Steganography techniques are determined for all sub-bands by the experimental procedure. Thus, we had checked the diagnosis quality of distortion. It has been discovered that resultant watermarked-ECG signal are used for diagnoses purpose and the hidden secret information can be fully extracted.

REFERENCES


