# Secured e-Healthcare through Physiological Signal's Steganography

[1]Dipti D. Patil, [2]Anish Singh Shekhawat, [3]Arnav Jain, [4] Shamala T. Mantri
[1]Associate Professor, [2]Student, [3]Student, [4]Assistant Professor

[1]Department of Information Technology,
[1]MKSSS's Cummins College of Engineering for Women, Pune, India

***Abstract :*** Now a days point of care systems are providing preventive healthcare facilities with great ease. With increased use of these e-healthcare systems, confidentiality of patient's identity and its health data have become an important issue. Steganography is the art of hiding information into some host in plain sight. It involves hiding messages in other harmless messages. This paper discusses the technique in which patient's confidential data is steganographed with their physiological signal i.e ECG signal. It will be useful in transmitting the patient's data securely through public networks in remote monitoring systems and can also be used for biometric authentication. The proposed method hides a confidential patient's data in normal as well as abnormal ECG signal. Percentage residual difference distortion measurement technique has been used to calculate the effectiveness of the algorithm. It is observed that the proposed technique provides high protection for patient's data with low distortion. Also after stenography, ECG data remains diagnosable.

***IndexTerms*** **– Steganagraphy, e-healthcare, Security and Privacy, signal processing, ECG**

## I. INTRODUCTION

In today's Point-of-Care (POC) systems [1, 2], a patient is under constant monitoring for possible cardiovascular diseases and response services in the event of an emergency. In these systems, the patient's physiological signal ie. ECG signal is acquired using body sensors and transmitted to their cell phone via Bluetooth. The signal is then transmitted to the hospital servers, from the phone, via Internet. The drawback of these systems is the lack of measures to ensure that the patient's data doesn't fall into the hands of unauthorized personnel, which leads to the patient's confidential data being compromised. Such information can be then be sold to organizations like the insurance companies. As ECG signal can also be used for human identification and biometric authentication [3, 4] any unauthorized entity can use it to gain access to systems where such system is in place.

In this paper we discuss a technique of securing the patient's data using his ECG signal, so that only authorized person is able to access the patient's confidential information. In this case confidential data is nothing but all patients' personal information like name of patient, date of birth, address, Medicare number, blood pressure, sugar level, location and biometric information. Some researchers are proposed to secure the confidential data based on steganography techniques to hide information inside medical images [5]. In [6, 7] permutation cipher is used to encrypt the confidential data whereas in [8] noised smearing technique is used to alter the original ECG signal which can then be reverted back to its original state using a security key. In [9] reversible watermarking algorithm was developed for ECG signal based on wavelet transformation.

## II. ARCHITECTURE

The proposed architecture for the system first collects the patient's normal as well as abnormal ECG signal or any other pathological signal using the biomedical sensors attached to his body as shown in Fig. 1. These signals are then transferred to a mobile like devices which also receives the encrypted data from the patient using some encryption technique. Wavelet transform is then applied to the signal and wavelet coefficients are obtained. The encrypted data is then embedded into these wavelet coefficients using LSB substitution.

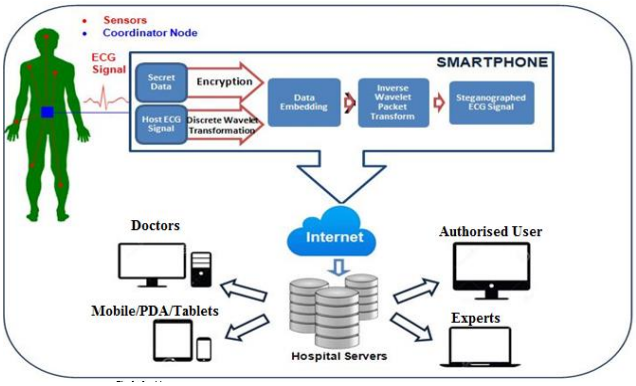


Fig. 1 Architecture for ECG steganography and transmission of steganographed ECG signal[5]

After data embedding, the transformed signal is recomposed into the ECG signal using inverse wavelet transform. This steganographed signal is then transferred to the hospital servers through the internet where only authorized personnel can access the patient's information. The secret key is provided to the authorized personnel by the patient, using which he can gain access to the patient's information in the ECG signal.

At the hospital server the doctor signs into the system using his unique login id and password. He is then asked for the secret key of the patient to access his personal information. After providing the key the received ECG signal is decomposed and data is extracted from the wavelet coefficients obtained after wavelet transformation. The data is in encrypted format which is then decrypted using the shared secret key.

## III. METHODODLOGY

The technique discussed in this paper assures that the patient's private data is securely transmitted over the internet using his/her own ECG signal. The various stages involved in this technique are:

### A. AES Encryption

The process of converting the plain text to an unreadable format using a cipher is called encryption. Data encryption is used to prevent any unauthorized access of the data. Encryption is carried out before embedding to provide a greater level of security. In our proposed model length of ECG signal is 5 seconds with sampling rate is 300 can embedded 1K bytes data in ECG signal by using following equation (1):

$$b = (t*fs)*180/32 \quad (1)$$

Where t is total time of ECG signal in seconds and fs is sampling rate.

Advanced Encryption Standard (AES) is a symmetric key block cipher technique. It encrypts data by dividing the data into blocks of 128-bits and encrypting these blocks one by one.

We use a 256-bit key to encrypt the data provided by the user. The data is encrypted in the mobile like devices with the help of predefined AES encryption.

### B. Discrete Wavelet Transform

To ensure high level of security we hide the data into the ECG signal. In order to do this we need to convert the signal from time domain to frequency domain.

Signal transformation is just an alternative form of representing the signal. The information present in the signal remains unchanged. In most Digital Signal Processing applications, the frequency detail of the signal is vital.

The Fourier transformation (FT) is perhaps the most common transform used to acquire the frequency detail of a signal. But as given in [10], the Fourier Transform is only suitable for stationary signals, i.e., signals whose frequency does not change with time and not for non-stationary signals which have different features at different space and time. This is because FT cannot specify at which time intervals the frequency components of a signal occurs. Image and speech signals like most of the biomedical signals such as, EEG, ECG, EMG, etc., vary with time and space and thus are non-stationary signals. To analyse these signals, both frequency and time data are required simultaneously, i.e., a time-frequency model of the signal is needed.

The Wavelet Transform provides a representation of the signal in the time-frequency domain. It uses multi resolution technique by which different frequencies are analysed with different resolutions. The Discrete Wavelet Transform (DWT) is an implementation of the wavelet transform on the discrete signal using a set of discrete wavelet scales and translations following some specified rules. DWT can not only be applied to extract the time-frequency information, it can also be exploited for noise suppressing.

In the above mentioned technique, we perform a discrete wavelet transformation on the ECG signal. The transformation used here is the discrete Haar Wavelet Transform (HWT). Like all other wavelet transforms, the Haar transform also divides a discrete signal into two sub bands of half its length. One sub band is a running average or trend known as approximation sub band; the other sub signal is a running difference or fluctuation known as detail sub band mentioned in equation 2a, 2b and 2c.

For a function f, the HWT is defined as:

$$f \rightarrow (a^L \mid d^L) \quad (2a)$$

$$a^L = (a_1, a_2, \ldots a_{N/2}) \quad (2b)$$

$$d^L = (d_1, d_2, \ldots\ldots d_{N/2}) \quad (2c)$$

Where L is the decomposition level, 'a' is the approximation sub band and 'd' is the detail sub band. The mathematical operations performed to obtain the above sub bands are shown with eqs 3a and 3b :

$$a_m = (f_{2m} + f_{2m-1})/\sqrt{2} \text{ for } m = 1,2\ldots..N/2 \quad (3a)$$

$$d_m = (f_{2m} - f_{2m-1})/\sqrt{2} \text{ for } m = 1,2\ldots..N/2 \quad (3b)$$

In this technique we apply a 5-level HWT to the original signal. It has been pointed out in [11] that the decomposition level plays an important part in wavelet transform. If the number of decomposition level exceeds certain value then some important signal detail would be removed and if it is less than that certain value then the signal would contain some noise. In [11, 12], after experimentations a decomposition level of 5 is regarded as the most appropriate decomposition level for an ECG signal.

### C. Data Embedding

After the signal is decomposed into wavelet coefficients, the encrypted data is then embedded into the obtained coefficients. The data is embedded using the LSB embedding technique in which the data is embedded into the least significant bits of the sub bands wavelet coefficients. The embedding operation is performed bit by bit using the encrypted data. As the data is embedded into the LSB of coefficients there is not much change in the signal values.

### D. Inverse DWT

After embedding the data the decomposed signal is then recomposed using inverse wavelet transform. This converts the time and frequency domain signal into time domain signal resulting in an ECG signal which is very similar to the host ECG signal.

### E. Data Extraction

The data is extracted on the hospital side using the same operations that were performed to hide the signal but in the reverse order. Hence first the steganographed signal is decomposed using HWT. After decomposition the data is extracted from the sub band coefficients. The data that is extracted is still in the encrypted form. Hence the extracted data is then decrypted using the shared key as shown in fig. 2.

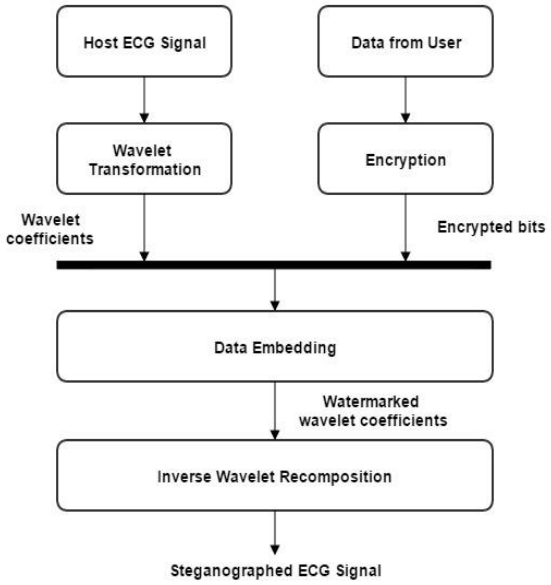


Fig.2. Block diagram of the sender steganography which includes encryption, wavelet decomposition, and data embedding

## IV. RESULTS

We have used the ECG signal generated by [13, 14], an ECG waveform generator for experimentation. Three different types of ECG signals are used for the experimentation. For the experimentation total 40 ECG samples are used. . The set of samples consist of 16 normal (NSR) ECG samples, 12Ventricular fibrillation ECG samples and 13 Ventricular Tachycardia ECG samples. Each sample is of 5s long with 300-Hz sampling frequency. Data is embedded into the signal using the same procedure as mentioned above. To evaluate the proposed technique, PRD (Percentage Residual Difference) is used to measure the variance between the original ECG signal and the steganographed ECG signal as shown in Equation 4.

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N} {x_i}^2}} \qquad (4)$$

Where x denotes the host ECG signal, and y is the steganographed signal.

Fig 3 (a) & (b) shows the host ECG signal and the steganographed ECG signal. From these two figures we can see that the change in host ECG signal is very less and the signal is hardly distorted.

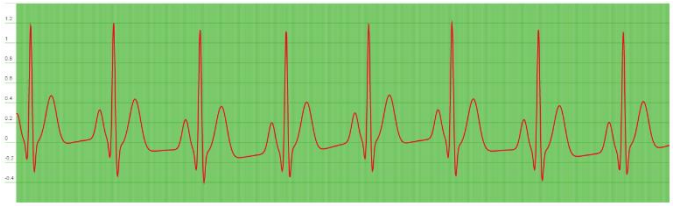

Fig.3a Original ECG Signal of the Patient

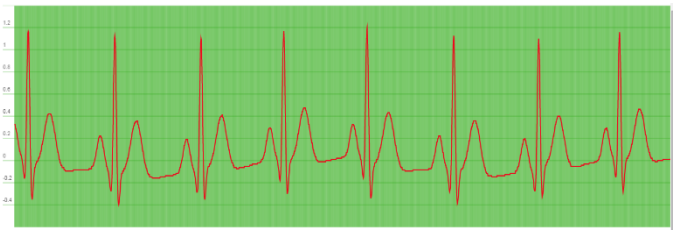

Fig.3b Steganographed ECG Signal of the Patient

Table.1. shows the results obtained for 16 normal ECG samples. It can be seen that a maximum PRD measured was 0.3%. Hence, this proves that the above mentioned technique does not affect the diagnostic feature of the host ECG signal.

Table 1: PRD and WWPRD results for different normal ECG segments.

| Sample No | PRD % | WWPRD % |
|---|---|---|
| 1 | 0.43446 | 0.39338 |
| 2 | 0.56804 | 0.4371 |
| 3 | 0.59837 | 0.44557 |
| 4 | 0.51656 | 0.43133 |
| 5 | 0.53641 | 0.41908 |
| 6 | 0.58602 | 0.43386 |
| 7 | 0.5064 | 0.62222 |
| 8 | 0.26013 | 0.59378 |
| 9 | 0.4634 | 0.6083 |
| 10 | 0.51913 | 0.63338 |
| 11 | 0.5055 | 0.61394 |
| 12 | 0.45053 | 0.595 |
| 13 | 0.45692 | 0.50512 |
| 14 | 0.41861 | 0.50547 |
| 15 | 0.36499 | 0.42618 |
| 16 | 0.42648 | 0.33541 |

Table.2 shows the results obtained for 12 Ventricular Tachycardia ECG samples. It can be seen that a maximum PRD measured was 0.5%. Hence, this proves that the above mentioned technique does not affect the diagnostic feature of the host ECG signal.

Table 2: PRD and WWPRD results for Ventricular Tachycardia ECG samples

| Sample No | PRD % | WWPRD % |
|---|---|---|
| 1 | 0.24973 | 0.25439 |
| 2 | 0.27853 | 0.30552 |
| 3 | 0.29892 | 0.29903 |
| 4 | 0.24248 | 0.2822 |
| 5 | 0.26566 | 0.26055 |
| 6 | 0.27017 | 0.25964 |
| 7 | 0.28042 | 0.27871 |
| 8 | 0.47009 | 0.5803 |
| 9 | 0.16381 | 0.28317 |
| 10 | 0.19697 | 0.30666 |
| 11 | 0.27231 | 0.26876 |
| 12 | 0.32276 | 0.32799 |

Table.3 shows the results obtained for 12 Ventricular Tachycardia ECG samples. It can be seen that a maximum PRD measured was 0.5%. Hence, this proves that the above mentioned technique does not affect the diagnostic feature of the host ECG signal.

Table 3: PRD and WWPRD results for Ventricular Fibrillation ECG samples

| Sample No | PRD % | WWPRD % |
|---|---|---|
| 1 | 0.65061 | 0.84787 |
| 2 | 0.58442 | 0.78362 |
| 3 | 0.54158 | 0.78223 |
| 4 | 0.40013 | 0.41339 |

| | | |
|---|---|---|
| 5 | 0.30265 | 0.38706 |
| 6 | 0.30569 | 0.4287 |
| 7 | 0.20551 | 0.43169 |
| 8 | 0.19213 | 0.31981 |
| 9 | 0.47881 | 0.50826 |
| 10 | 0.38448 | 0.3726 |
| 11 | 0.48817 | 0.4968 |
| 12 | 0.48814 | 0.48671 |

This encouraging result clearly demonstrates that the steganographed ECG signals can be used for diagnostic purposes.

## V. DISCUSSION

The technique discussed in this paper causes less distortion of the signal than the one that uses a direct approach of embedding the data directly into the signal[16,17]. Wavelet transformation not only helps to lower the distortion significantly but can also be used as a noise suppressing technique. This can be done by setting a threshold value with which the wavelet coefficients can be compared to see if it's a desirable part of the original signal.

The ECG signal used in this research for experimentation was from a synthetic ECG signal generator [14] and had no noise component unlike the real ECG signals. This however should not undermine the discussed technique as the wavelet transformation used for steganography can also be used for noise suppression and thus would perform equally if not better than the results above.

In future research different compression techniques can be applied to the signal and data so that more data can be embedded into the signal and also so that storage of these signals takes less space at the hospital servers for historical analysis of the patient.

## VI. CONCLUSION

This paper discusses an innovative idea of hiding the user's confidential data into his/her ECG signals. This can be used to provide a secure communication in remote health monitoring systems. The use of encryption provides an authentication capability to prevent unauthorized persons from gaining access to the confidential data.

As this technique doesn't distort the signal much, it can be used for diagnosis purposes without revealing the confidential data embedded in it. In future this technique can be used in biometric security systems using ECG signals to provide data privacy, authentication and verification.

## REFERENCES


[1] Ibaida and Khalil (2013), "Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems", in IEEE Transactions on Biomedical Engineering , Vol. 60, No. 12 , Dec. 2013

[2] F. Hu, M. Jiang, M. Wagner, and D. Dong, "Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign," IEEE Trans. Inf. Technol. Biomed., vol. 11, no. 6, pp. 619–627, Nov. 2007.

[3] Wtibbeler G, Stavridis M, Kreiseler D, Bousseljot RD, Elster C. Verification of humans using the electrocardiogram. Pattern Recognition Letters 2007;28: 1172-75.

[4] Wang Y, Agrafioti F, Hatzinakos D, Plataniotis K. Analysis of human electrocardiogram for biometric recognition. EURASIP Journal on Advances in Signal Processing 2008.

[5] Anish Singh Shekhawat, Arnav Jain, Dipti Patil, "A Study of ECG Steganography for Securing Patient's Confidential Data based on Wavelet Transformation", International Journal of Computer Applications (0975 – 8887) Volume 105 – No. 12, November 2014

[6] Sufi F, Fang Q, Khalil I, Mahmoud SS. Novel methods of faster cardiovascular diagnosis in wireless telecardiology. IEEE Journal on Selected Areas in Communications 2009; 27(4): 537–552.

[7] Sufi F, Khalil I. Enforcing secured ecg transmission for realtime telemonitoring: a joint encoding, compression, encryption mechanism. security and communication networks. Security and Communication Networks 2008; 1(5): 389–405.

[8] Sufi F, Khalil I. A new feature detection mechanism and its application in secured ecg transmission with noise masking. Journal of Medical Systems 2009; 33(3): 121–132.

[9] 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.

[10] Swati Kumravat, "An Efficient Steganographic Scheme Using Skin Tone Detection and Discrete Wavelet Transformation" International Journal of Computer Science & Engineering Technology ; Vol. 4 No. 07: 2229-3345

[11] D. W. Yan-Fang Sang and J.-C. Wu, "Entropy-based method of choosing the decomposition level in wavelet threshold de-noising," Journal of Entropy and Information Studies, Jun. 2010.

[12] Lei Lei, Chao Wang, and Xin Liu, "Discrete Wavelet Transform Decomposition Level Determination Exploiting Sparseness Measurement", World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Electronics and Communication Engineering Vol:7, No:9, 2013

[13] McSharry PE, Clifford GD, Tarassenko L, Smith L. A dynamical model for generating synthetic electrocardiogram signals. IEEE Transactions on Biomedical Engineering 50(3): 289-294; March 2003.

[14] McSharry PE, Clifford GD, ECGSYN - A realistic ECG waveform generator. [Online]: http://www.physionet.org/physiotools/ecgsyn/

[15] Seedahmed S. Mahmoud, "A generalised wavelet packet-based anonymisation approach for ECG security application", Security and Communication Networks, 2017.

[16] Y. Lin, I. Jan, P. Ko, Y. Chen, J.Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport," IEEE Trans. Inf. Technol. Biomed., vol. 8, no. 4, pp. 439–447, Dec. 2004.