A Study of ECG Steganography for Securing Patient's Confidential Data based on Wavelet Transformation

Anish Singh Shekhawat
Computer Engg. Dept.
MITCOE, Pune, India

Arnav Jain
Computer Engg. Dept.
MITCOE, Pune, India

Dipti Patil, Ph.D.
Associate Professor, Computer Engg. Dept.
MITCOE, Pune, India

ABSTRACT
The ECG signal is popularly used for diagnosis of various cardiovascular diseases. In recent times, the ECG signal is also being used for biometric security systems. As the ECG signals contain private health information, along with personal identification data, it needs to be secured before transmission through various public networks to avoid the data being compromised. This paper discusses various data encryption techniques along with data embedding using signal transformation to ensure that the sanctity of the information.

General Terms
Biometric Security, ECG Steganography

Keywords
ECG Signals, Confidentiality, DWT, Encryption, Steganography, Wavelet

1. INTRODUCTION
In point-of-care systems (PoC) [1, 2], a patient is connected to the hospital server for constant monitoring of cardiovascular disease diagnosis and emergency response services. In such a system the patient's ECG signal is acquired using sensors and then transmitted to his cell phone via Bluetooth. The cell phone then transmits this ECG signal to the hospital server through public internet.

The hospital server on the other hand receives the patient's ECG signal and validates it with ECG based biometric security system. After successful validation, the identity of the patient is known to the hospital and the services for which the patient is subscribed for. The signal is then used for diagnostic purposes.

In the above system, the patient's ECG signal is transmitted without being encrypted resulting into the data being vulnerable to access from an unauthorized entity. Therefore if this unencrypted ECG signal falls into the wrong hands, then the patient's privacy is compromised. This compromised data then can be sold to various organizations like the insurance companies. Since ECG signals are also used in biometric security systems, the compromised data can also be used to gain unauthorized access to various systems that use biometric security.

To protect the patient's confidential information, the ECG signal needs to be encrypted (as it is being done for medical images [3]). In previous researches many approaches were established to secure patient sensitive data. Many of them proposed to secure the confidential data based on steganography techniques to hide information inside medical images. In [4, 5] permutation cipher is used to encrypt the confidential data whereas in [6] 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 [7] reversible watermarking algorithm was developed for ECG signal based on wavelet transformation. This method is only for normal ECG signal and cannot detect any abnormal signal.

The challenging factors of these techniques are how much information can be stored, and to what extent the method is secure. The above mentioned techniques are computationally expensive for mobile and embedded devices without low computational capacity.

In this paper, we discuss a novel steganography technique based on wavelet transformation for securing the patient information. We discuss different methods to encrypt the data, their feasibility as well as how effective they are to secure patient's data.

2. ARCHITECTURE
The proposed architecture for the system as shown in Figure.1 first collects the patient's ECG signal and other physiological readings using different body sensors. The signals are then sent to the smart phone via Bluetooth on which the secret data of the patient is stored. The secret data is encrypted in the smart phone using some encryption technique. The signals are then transformed into discrete wavelets using Discrete Wavelet Transformation (DWT). The five-level DWT applied on the host signal results into 32 sub-bands. The encrypted data is then embedded into the sub-band's coefficient using LSB substitution.

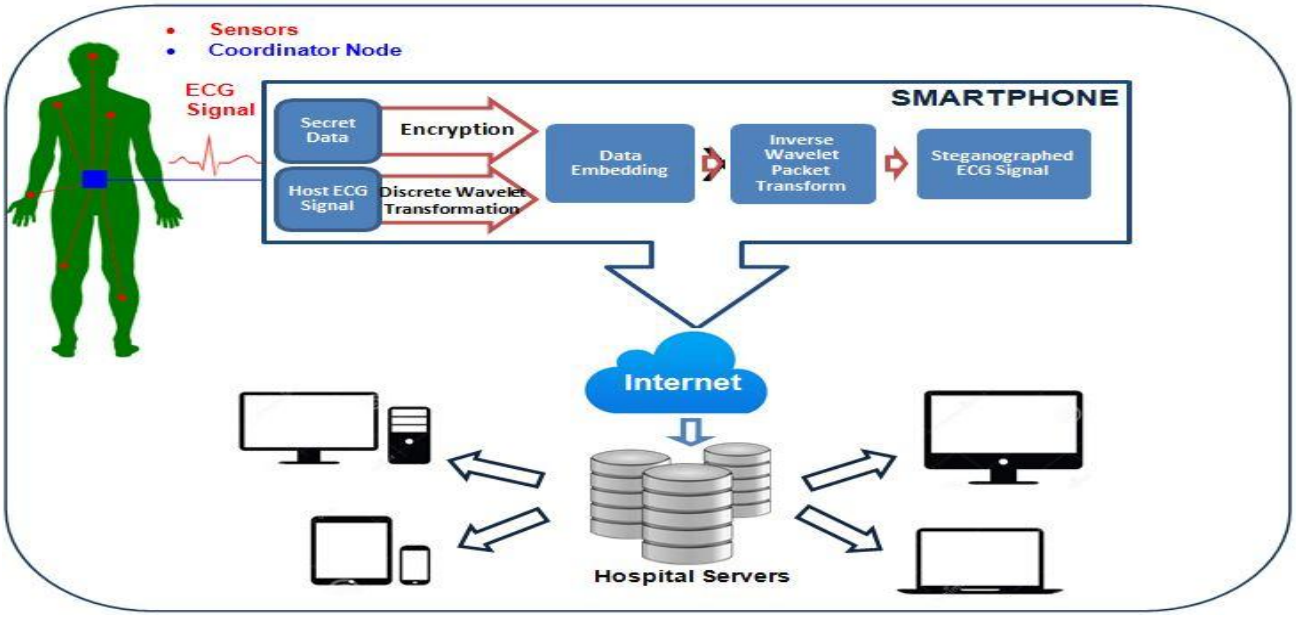

Figure.1: Architecture for ECG steganography and transmission of steganographed ECG signal

The 32 steganographed sub-bands are recomposed using inverse wavelet re-composition into a single steganographed ECG signal. The smart phone then sends the signal to the hospital server through Internet. The hospital server extracts the data from the host signal which can then be accessed by authorized personnel. Only the authorized people have the security key to access the hidden data.

3. METHODOLOGY

The new security technique used in [8] guarantees secure transmission of confidential information is based on using steganography techniques to hide confidential information inside the ECG signal. Moreover, the technique uses encryption to allow only the authorized persons to extract the hidden data. In this method, the patient ECG signal is used as the host signal that will carry the patient secret information.

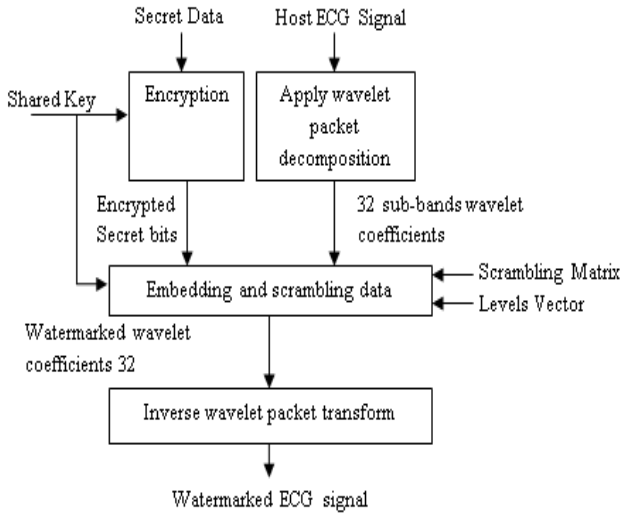

Figure.2: Block diagram of the sender steganography which includes encryption, wavelet decomposition, and secret data embedding.

The various stages involved in ECG steganography are:

3.1 Data Encryption

The process of transforming plain text to an unreadable format using a cipher is called encryption. Data Encryption is used to encrypt the confidential data to prevent any unauthorized access. Data Encryption is carried out before embedding of data into the signal to provide additional security. Various encryption techniques are available to encrypt the data but not all are possible to implement inside a smartphone due to computational limitations. The processors used on mobile devices are less capable than the ones used on a desktop system. Only few devices have the computational prowess to implement high-end encryption techniques. In this section we discuss different encryption techniques that can be used for encryption inside cell phones.

3.1.1 XOR Ciphering

XOR Ciphering is an additive ciphering technique. It uses the basic principle of a bitwise XOR operation to encrypt the data. XOR ciphering uses an ASCII coded shared key which plays the role of a security key. This shared key is known to the encrypter and the decrypter. This techniques works on the following principles:

a) 0 + 0 = 0
b) 0 + 1 = 1
c) 1 + 0 = 1
d) 1 + 1 = 0
e) A + (B + C) = (A + B) + C

3.1.2 AES

XOR Ciphering technique is extremely common these days. A simple XOR cypher can be easily broken using frequency analysis. XOR operator is also vulnerable to a known plaintext attack. Another well-known technique for data encryption is AES encryption. It is one of the most secure and frequently utilized encryption algorithms available today. The algorithm described by AES is also a symmetric key algorithm, meaning the same key is used for both encrypting and decrypting the data. This encryption process is based on several linear transformations, substitutions and permutations; each performed on data blocks of 16 byte – hence the term block cipher. Those operations are performed several times,

called "rounds" during which a unique round key is computed out of the encryption key, and incorporated into the calculations. Based on this block structure of AES; if a single bit in the key or in the plaintext block is altered then the computation results in an entirely different block of cipher text – a clear improvement over traditional XOR cipher.

Another advantage of AES is that most of the cell phones running android already have support for implementing 128-bit AES encryption. AES is also faster than most of the encryption standards in both hardware and software. As of today, no realistic attack against AES exists. Thus, AES remains the ideal choice of encryption standard.

Encryption is the initial security solution in open system. Therefore, encryption itself does not offer security. Encryption does not avert information from hacking however it keeps the hacker from altering or interpreting the data.

3.2 Signal transformation

To warrant high data security, an embedding operation is carried out which hides the information in the ECG signal. In order to hide the data we should convert the time domain signal into the frequency domain.

The transformation of a signal is nothing but representing the signal in a different form. There is no change in the information inside the signal. In this section we discuss two transformation techniques that can be applied to the ECG signal.

3.2.1 Discrete Fourier Transformation

Fourier transformation is applied to transform the signal between time domain and frequency domain. The Discrete Fourier Transform (DFT) is probably the most prevalent transform used to attain the frequency spectrum of a signal.

But one of the major drawbacks of DFT is that they are only appropriate for stationary signals, i.e. whose frequency does not vary with time. The Fourier Transform, although it gives us the various frequencies that exist in the signal, it does not give us the period when these frequencies occur. Signals that have different features at different intervals of time are non-stationary signals. Biological signals such as ECG signal are non-stationary. To evaluate these signals, both frequency and time data are needed simultaneously, i.e., a time-frequency model of the signal is required.

3.2.2 Discrete Wavelet Transformation

The Wavelet Transform provides a time-frequency model of the signal. It uses multi-resolution technique by which dissimilar frequencies are evaluated with different resolutions. It is a tool that separates the information into different frequency components. It decomposes the given signal into coefficients representing frequency components of the signal at a given time. Wavelet transform can be defined as follows.

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

Where ψ denotes wavelet function, S and P are transform parameters and are both positive integers. C is a function of scale and position parameters and represents the coefficients [9].

DWT decomposition can be achieved by applying wavelet transform to the signal using band filters. The outcome of the band filtering operation will be two different signals; one will be related to the high-frequency components and the other related to the low-frequency components of the original signal. If this procedure is replicated multiple times, then it is called multilevel packet wavelet decomposition. DWT can be defined as shown in Equation 2:

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

where W(i, j) represents the DWT coefficients, i and j are the scale and shift transform parameters, and Ψij (n) is the wavelet basis time function. The wavelet function can be defined as follows:

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

In this paper we apply five-level wavelet packet decomposition to the host signal. As each wavelet decomposition process results into two different signals, the five-level wavelet decomposition will lead to 32 sub-signals. As the frequency spectrum is divided into two signals after each decomposition process, one of the resulting signals will denote the high-frequency component and the other denotes a low-frequency component. Most of the important characteristics of the ECG signal fall in the low-frequency range whereas the high-frequency range consists of mostly noise. Therefore out of 32 sub-bands only a small number of sub-bands are related to the important ECG characteristics while others are associated with noise components of the signal [10]. Thus different number of bits will be changed in each wavelet coefficient depending on the sub-band level. Hence for minimal distortion of the significant characteristics of the host signal, different steganography levels are assigned for each band. The steganography level for bands 1 to 17 is 5 bits whereas it is 6 bits for the remaining bands.

3.3 The Embedding Operation

In this section we discuss the method to embed the encrypted data into the host signal. We will perform a scrambling operation to ensure high-data security. The scrambling operation is implemented using two parameters:

a) Shared key
b) Scrambling matrix

The shared key is known to both the sender and the receiver whereas the scrambling matrix is stored in both the transmitter and the receiver. The scrambling matrix is a 128x32 size matrix and is build using the following conditions:

a) The same row must not contain duplicate elements
b) Rows must not be duplicates

$$S = \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,32} \\ s_{2,1} & s_{1,2} & \cdots & s_{2,32} \\ \vdots & \vdots & \ddots & \vdots \\ s_{128,1} & s_{128,2} & \cdots & s_{128,32} \end{bmatrix} \tag{4}$$

The embedding operation begins with converting the security key into ASCII code, thus converting each character into a number from 1 to 128. These numbers are then used to select one of the rows of the scrambling matrix. The rows of the scrambling matrix contain the sub-band number of the signal. After a row is selected data is embedded into the wavelet coefficients according to the sequence of the sub-bands stated in the selected row and the steganography level of the sub-band. The steganography level is determined by the level vector.

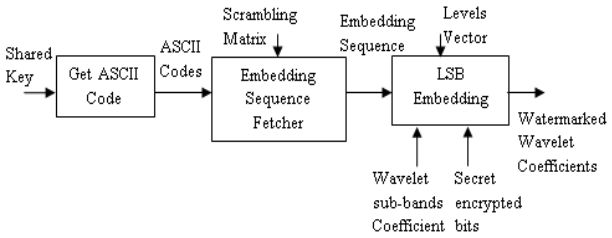

Figure.3: Block diagram showing the detailed construction of the watermark embedding operation.

The data is embedded using LSB embedding. In this algorithm the bits of the hidden message is inserted into the least significant bits of the sub-bands wavelet coefficients. As the secret data is inserted into the LSB bits there not much change in the host signal and the steganographed signal.

3.4 Inverse Wavelet Re-Composition

In the final phase of the process the 32 steganographed sub-bands are recomposed using inverse wavelet re-composition. This transforms the signal from time and frequency domain to the time domain resulting into an ECG signal which is very similar to the host ECG signal.

3.5 Data Extraction

In this phase we extract the hidden data from the steganographed signal. In extraction process most of the steps used in embedding are repeated but in the reverse order i.e.: First the steganographed ECG is transformed using DWT to obtain the wavelet coefficients. Then the scrambling matrix is scanned in a predefined order using the shared key to get the signal coefficients. The secret bits are then extracted from the LSBs of wavelet coefficients and decrypted using the security key.

4. SECURITY ANALYSIS

The security analysis [8] of the algorithm discussed in this paper is based on the security key shared between the sender and the receiver and the scrambling matrix. Slightest change in any of the parameters will lead to wrong data. Since both the parameters are required for the successful extraction of the data the scrambling matrix is never transmitted in any form. The scrambling matrix is hardwired in the sender and the receiver and is unique to the pair.

5. RESULTS

In [11] three different types of ECG signals were used for experimentation. Data was first embedded and then extracted from the signal using the same procedure as mentioned above. To evaluate the proposed model, PRD (Percentage Residual Difference) is used to measure the variance between the host ECG signal and the resulting steganographed ECG signal as shown in Equation 5.

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N} {x_i}^2}} \qquad (5)$$

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

Table.1. shows the results obtained for 18 normal ECG samples. It can be seen that a maximum PRD measured was 0.6%. Second, it can be observed that the difference between the normal PRD and the wavelet-based PRD for diagnoses measurement is very small. Hence, this proves that the steganography process does not affect the diagnostic feature of the host ECG signal. This table also shows the PRD measured after data extraction. It is obvious from the table that removal of the watermark will have a small impact on the PRD value. To guarantee unbiased results, Ventricular Fibrillation and Ventricular Tachycardia ECG samples were also experimented. As can be seen from Table.2 and Table.3, the maximum PRD for Ventricular Tachycardia host signal is only 0.5% whereas it is 1% for Ventricular Fibrillation.

Table 1: PRD results for different normal ECG segments.

Sample No	PRD %	WWPRD %	PRD % extracted	WWPRD % extracted
1	0.43446	0.39338	0.57647	0.52692
2	0.56804	0.4371	0.79583	0.59282
3	0.59837	0.44557	0.80906	0.62531
4	0.51656	0.43133	0.72957	0.60578
5	0.53641	0.41908	0.72213	0.56855
6	0.58602	0.43386	0.80906	0.61782
7	0.5064	0.62222	0.70934	0.873
8	0.26013	0.59378	0.35179	0.81591
9	0.4634	0.6083	0.63565	0.82741
10	0.51913	0.63338	0.70037	0.85416
11	0.5055	0.61394	0.6874	0.84694
12	0.45053	0.595	0.60611	0.79233
13	0.45692	0.50512	0.61693	0.68123
14	0.41861	0.50547	0.56098	0.68459
15	0.36499	0.42618	0.50238	0.59443
16	0.42648	0.33541	0.57897	0.45032
17	0.44176	0.34352	0.59529	0.46326
18	0.42957	0.34337	0.59061	0.47203

Table 2: PRD results for Ventricular Tachycardia ECG samples

Sample No	PRD %	WWPRD %	PRD % extracted	WWPRD % extracted
1	0.24973	0.25439	0.33705	0.34314
2	0.27853	0.30552	0.37474	0.41137
3	0.29892	0.29903	0.40912	0.41751
4	0.24248	0.2822	0.33029	0.38589
5	0.26566	0.26055	0.37705	0.36925
6	0.27017	0.25964	0.37263	0.36044
7	0.28042	0.27871	0.37983	0.38101
8	0.47009	0.5803	0.49603	0.65555
9	0.16381	0.28317	0.22884	0.4103
10	0.19697	0.30666	0.27143	0.41038
11	0.27231	0.26876	0.37796	0.38309
12	0.32276	0.32799	0.43247	0.44159

Table 3: PRD results for Ventricular Fibrillation

Sample No	PRD %	WWPRD %	PRD % extracted	WWPRD % extracted
1	0.65061	0.84787	0.89994	1.1713
2	0.58442	0.78362	0.7944	1.0715
3	0.54158	0.78223	0.74391	1.0733
4	0.40013	0.41339	0.55157	0.56329
5	0.30265	0.38706	0.41009	0.53588
6	0.30569	0.4287	0.41517	0.58034
7	0.20551	0.43169	0.27795	0.5915
8	0.19213	0.31981	0.26104	0.43105
9	0.47881	0.50826	0.66257	0.71434

10	0.38448	0.3726	0.52747	0.51307
11	0.48817	0.4968	0.66364	0.677
12	0.48814	0.48671	0.66386	0.66023

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

6. CONCLUSION

This paper discusses an innovative idea using the AES encryption to encrypt ECG signals. According to the security analysis this algorithm can be used to hide confidential data inside the ECG signal. The suggested technique provides an authentication technique to prevent unauthorized persons from gaining access to the confidential data. This confidential data can be patient information to provide a secure communication in Point-of-Care systems and in remote health care systems. It can be implemented into a patient's smartphone which uses the ECG signals transmitted by body sensors to the smartphone via Bluetooth.

Thus this algorithm can be used for secure transmission in cardiac monitoring systems and also for storage of patient information in the cloud. It can also be used for secure transmission of user identification data for validation using biometric wrist bands where data privacy is critical.

This technique can be used to provide a lower layer of a complex role based access control framework that can restrict the access to only the required information in the concealed data.

7. REFERENCES

[1] 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.

[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] Hu J, Han F. A pixel-based scrambling scheme for digital medical images protection, Journal of Network and Computer Applications. 2009; 32: 788–794.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Ayman Ibaida, Ibrahim Khalil "Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Sys-tems" IEEE Transactions On Biomedical Engineering 2013, 60(12):3322---3330.

[9] A. Poularikas, Transforms and Applications Handbook. BocaRaton, FL, USA: CRC Press, 2009.

[10] A. Al-Fahoum, "Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure," IEEE Trans. Inf. Technol.Biomed., vol. 10, no. 1, pp. 182–191, Jan. 2006.

[11] Ayman Ibaida, "Electrocardiograms in Wireless Body Sensor Networks", 2014, School of Computer Science and Information Technology, Science, Engineering, and Technology Portfolio, RMIT University, Melbourne.