

Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems

Ayman Ibaida* and Ibrahim Khalil

Abstract—With the growing number of aging population and a significant portion of that suffering from cardiac diseases, it is conceivable that remote ECG patient monitoring systems are expected to be widely used as point-of-care (PoC) applications in hospitals around the world. Therefore, huge amount of ECG signal collected by body sensor networks from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level, etc., and diagnosed by those remote patient monitoring systems. It is utterly important that patient confidentiality is protected while data are being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems. In this paper, a wavelet-based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. To evaluate the effectiveness of the proposed technique on the ECG signal, two distortion measurement metrics have been used: the percentage residual difference and the wavelet weighted PRD. It is found that the proposed technique provides high-security protection for patients data with low (less than 1%) distortion and ECG data remain diagnosable after watermarking (i.e., hiding patient confidential data) and as well as after watermarks (i.e., hidden data) are removed from the watermarked data.

Index Terms—Confidentiality, ECG, encryption, steganography, watermarking, wavelet.

I. INTRODUCTION

THE number of elderly patients is increasing dramatically due to the recent medical advancements. Accordingly, to reduce the medical labor cost, the use of remote healthcare monitoring systems and point-of-care (PoC) technologies have become popular [1], [2]. Monitoring patients at their home can drastically reduce the increasing traffic at hospitals and medical centers. Moreover, PoC solutions can provide more reliability

in emergency services as patient medical information (e.g., diagnosis) can be sent immediately to doctors and response or appropriate action can be taken without delay. However, remote health care systems are used in large geographical areas essentially for monitoring purposes, and, the Internet represents the main communication channel used to exchange information. Typically, patient biological signals and other physiological readings are collected using body sensors. Next, the collected signals are sent to the patient PDA device for further processing or diagnoses. Finally, the signals and patient confidential information as well as diagnoses report or any urgent alerts are sent to the central hospital servers via the Internet. Doctors can check those biomedical signals and possibly make a decision in case of an emergency from anywhere using any device [3].

Using Internet as main communication channel introduces new security and privacy threats as well as data integration issues. According to the Health Insurance Portability and Accountability Act (HIPAA), information sent through the Internet should be protected and secured. HIPAA mandates that while transmitting information through the internet a patient's privacy and confidentiality be protected as follows [4].

- 1) *Patient privacy*: It is of crucial importance that a patient can control who will use his/her confidential health information, such as name, address, telephone number, and Medicare number. As a result, the security protocol should provide further control on who can access patient's data and who cannot.
- 2) *Security*: The methods of computer software should guarantee the security of the information inside the communication channels as well as the information stored on the hospital server.

Accordingly, it is of crucial importance to implement a security protocol which will have powerful communication and storage security [5].

Several researchers have proposed various security protocols to secure patient confidential information. Techniques used can be categorized into two subcategories. First, 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], [6], [7]. The disadvantage of using encryption-based techniques is its large computational overhead. Therefore, encryption-based methods are not suitable in resource-constrained mobile environment. Alternatively, many security techniques are based on hiding its sensitive information inside another insensitive host data without incurring

Manuscript received February 15, 2013; revised April 23, 2013; accepted May 14, 2013. Date of publication May 21, 2013; date of current version November 18, 2013. Asterisk indicates corresponding author.

*A. Ibaida is with the Department of Computer Science and Information Technology, RMIT University, Melbourne VIC 3082, Australia (e-mail: aymoon1978@gmail.com).

I. Khalil is with the Department of Computer Science and Information Technology, RMIT University, Melbourne VIC 3082, Australia (e-mail: ibrahim.khalil@rmit.edu.au).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TBME.2013.2264539

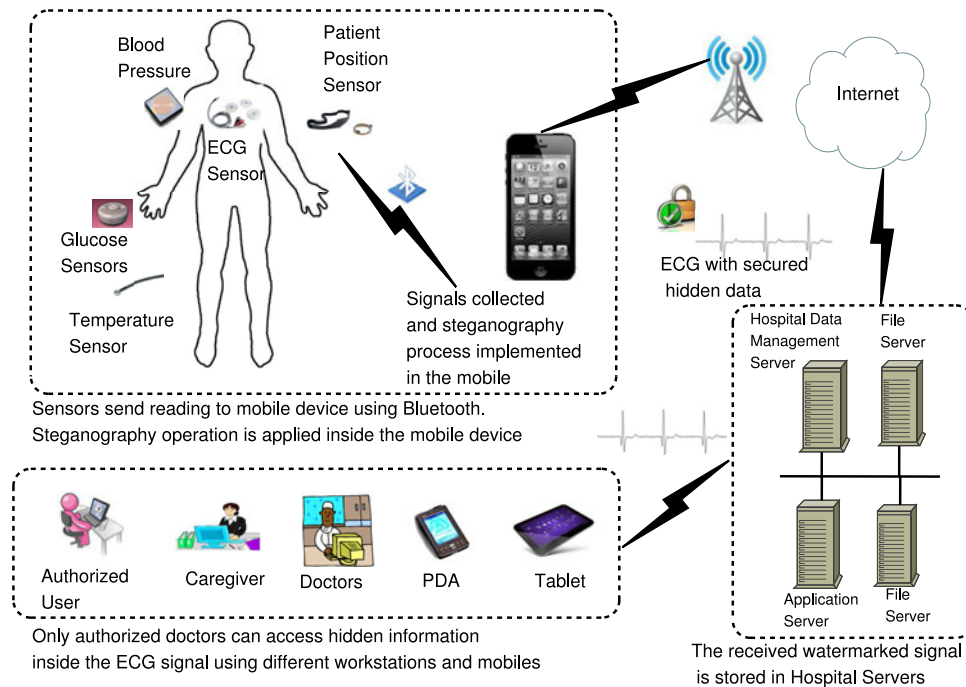


Fig. 1. ECG steganography scenario in Point-of-Care (PoC) systems where body sensors collect different readings as well as ECG signal and watermarking process implemented inside the patient's mobile device.

any increase in the host data size and huge computational overhead. These techniques are called steganography techniques. Steganography is the art of hiding secret information inside another type of data called host data [8]. However, steganography techniques alone will not solve the authentication problem and cannot give the patients the required ability to control who can access their personal information as stated by HIPAA.

In this paper, a new security technique is proposed to guarantee secure transmission of patient confidential information combined with patient physiological readings from body sensors. The proposed technique is a hybrid between the two preceding categories. First, it is based on using steganography techniques to hide patient confidential information inside patient biomedical signal. Moreover, the proposed technique uses encryption-based model to allow only the authorized persons to extract the hidden data. In this paper, the patient ECG signal is used as the host signal that will carry the patient secret information as well as other readings from other sensors such as temperature, glucose, position, and blood pressure. The ECG signal is used here due to the fact that most of the healthcare systems will collect ECG information. Moreover, the size of the ECG signal is large compared to the size of other information. Therefore, it will be suitable to be a host for other small size secret information. As a result, the proposed technique will follow HIPAA guidelines in providing open access for patients biomedical signal but prevents unauthorized access to patient confidential information.

In this model body sensor nodes will be used to collect ECG signal, glucose reading, temperature, position and blood pressure, the sensors will send their readings to patient's PDA device via Bluetooth. Then, inside the patient's PDA device the steganography technique will be applied and patient secret in-

formation and physiological readings will be embedded inside the ECG host signal. Finally, the watermarked ECG signal is sent to the hospital server via the Internet. As a result, the real size of the transmitted data is the size of the ECG signal only without adding any overhead, because the other information are hidden inside the ECG signal without increasing its size. At hospital server the ECG signal and its hidden information will be stored. Any doctor can see the watermarked ECG signal and only authorized doctors and certain administrative personnel can extract the secret information and have access to the confidential patient information as well as other readings stored in the host ECG signal. This system is shown in Fig. 1.

The proposed steganography technique has been designed in such a way that guarantees minimum acceptable distortion in the ECG signal, Furthermore, it will provide the highest security that can be achieved. The use of this technique will slightly affect the quality of ECG signal. However, watermarked ECG signal can still be used for diagnoses purposes as it is proven in this paper. In this paper, the following research questions are answered.

- 1) Can the proposed technique protect patient confidential data as explained in the HIPAA security and privacy guidelines?
- 2) What will be the effect on the original ECG signal after applying the proposed steganography technique in terms of size and quality?

Rest of the paper is organized as follows. Section II briefly discusses the related works and what other researchers did in this area. In Section III, we discuss the basic system design, the embedding process (i.e., patient sensitive data into ECG signal), and the extraction process. Next, in Section IV security analysis is proposed. Then, Section V explains diagnosability measurement. Section VI shows the results of PRD calculated before

and after secret data extraction. Finally, Section VII concludes the paper.

II. RELATED WORK

There are many approaches to secure patient sensitive data [2], [7], [9], [10]. However, one approach [11], [12], [13] proposed to secure data is based on using steganography techniques to hide secret information inside medical images. The challenging factors of these techniques are how much information can be stored, and to what extent the method is secure. Finally, what will be the resultant distortion on the original medical image or signal.

Zheng and Qian [13] proposed a new reversible data hiding technique based on wavelet transform. Their method is based on applying B-spline wavelet transform on the original ECG signal to detect QRS complex. After detecting R waves, Haar lifting wavelet transform is applied again on the original ECG signal. Next, the non-QRS high-frequency wavelet coefficients are selected by comparing and applying index subscript mapping. Then, the selected coefficients are shifted 1 bit to the left and the watermark is embedded. Finally, the ECG signal is reconstructed by applying reverse haar lifting wavelet transform. Moreover, before they embed the watermark, Arnold transform is applied for watermark scrambling. This method has low capacity since it is shifting 1 bit. As a result only 1 bit can be stored for each ECG sample value. Furthermore, the security in this algorithm relies on the algorithm itself, it does not use a user-defined key. Finally, this algorithm is based on normal ECG signal in which QRS complex can be detected. However, for abnormal signal in which QRS complex cannot be detected, the algorithm will not perform well.

Golpira and Danyali [12] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. In this paper, medical images such as MRI is used as host signal. A 2-D wavelet transform is applied to the image. Then, the histogram of the high-frequency subbands is determined. Next, two thresholds are selected, the first is in the beginning and the other is in the last portion of the histogram. For each threshold, a zero point is created by shifting the left histogram part of the first threshold to the left, and shifting the right histogram part of the second threshold to the right. The locations of the thresholds and the zero points are used for inserting the binary watermark data. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of this algorithms is low. Moreover, no encryption key is involved in its watermarking process.

Finally, Kaur *et al.* [11] proposed new digital watermarking of ECG data for secure wireless communication. In their work, each ECG sample is quantized using 10 bits, and is divided into segments. The segment size is equal to the chirp signal that they use. Therefore, for each ECG segment a modulated chirp signal is added. Patient ID is used in the modulation process of the chirp signal. Next, the modulated chirp signal is multiplied by a window-dependent factor, and then added to the ECG 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 ID.



Patient Confidential information	
Name :	Ayman Ibaida
Date of Birth :	1/1/1970
Address :	
Medicare Number :	1234567890
Telephone Number :	1234567890
Patient Diagnoses information	
blood Pressure	
Glucose Level	
Temperature	
Patient location.	
Patient biometric information	
	

Fig. 2. Original data consisting of patient information and sensor readings as well as patient biometric information.

III. METHODOLOGY

The sender side of the proposed steganography technique consists of four integrated stages as shown in Fig. 4. The proposed technique is designed to ensure secure information hiding with minimal distortion of the host signal. Moreover, this technique contains an authentication stage to prevent unauthorized users from extracting the hidden information.

A. Stage 1: Encryption

The aim of this stage is to encrypt the patient confidential information in such a way that prevents unauthorized persons—who does not have the shared key—from accessing patient confidential data. In this stage, XOR ciphering technique is used with an ASCII coded shared key which will play the role of the security key. XOR ciphering is selected because of its simplicity. As a result, XOR ciphering can be easily implemented inside a mobile device. Fig. 2 shows an example of what information could be stored inside the ECG signal [14].

B. Stage 2: Wavelet Decomposition

Wavelet transform is a process that can decompose the given signal into coefficients representing frequency components of the signal at a given time. Wavelet transform can be defined as follows:

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

where ψ represents wavelet function. S and P are positive integers representing transform parameters. C represents the coefficients which is a function of scale and position parameters [15]. Wavelet transform is a powerful tool to combine time domain with frequency domain in one transform. In most applications, discrete signals are used. Therefore, discrete wavelet transform (DWT) must be used instead of continuous wavelet transform. DWT decomposition can be performed by applying wavelet

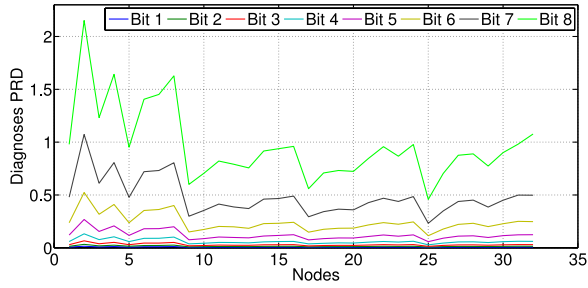


Fig. 3. Effect of applying steganography using different levels on the resulting PRD for each of the 32 subbands.

transform to the signal using band filters. The result 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 process is repeated multiple times, then it is called multilevel packet wavelet decomposition. DWT can be defined as follows:

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

where $W(i, j)$ 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. The wavelet function can be defined as follows:

$$\Psi_{ij}(n) = 2^{-i/2} \Psi(2^{-i}n - j). \quad (3)$$

In this paper, a five-level wavelet packet decomposition has been applied to the host signal. Accordingly, 32 subbands resulted from this decomposition process as shown in Fig. 7. In each decomposition iteration, the original signal is divided into two signals. Moreover, the frequency spectrum is distributed on these two signal. Therefore, one of the resulting signals will represent the high-frequency component and the other one represents the low-frequency component. Most of the important features of the ECG signal are related to the low-frequency signal. Therefore, this signal is called the approximation signal (A). On the other hand, the high-frequency signal represents mostly the noise part of the ECG signal and is called detail signal (D). As a result, a small number of the 32 subbands will be highly correlated with the important ECG features while the other subbands will be correlated with the noise components in the original ECG signal [16]. Therefore, in our proposed technique different number of bits will be changed in each wavelet coefficient (usually called steganography level) based on its subband. As a result, a different steganography level will be selected for each band in such a way that guarantees the minimal distortion of the important features for the host ECG signal. The process of steganography levels selection was performed by applying lot of experimentation as shown in Fig. 3. It is clear that, hiding data in some subbands will highly affect the original signal, while hiding in other subbands would result in small distortion effect. Accordingly, the selected steganography level for bands from 1 to 17 is 5 bits and 6 bits for the other bands.

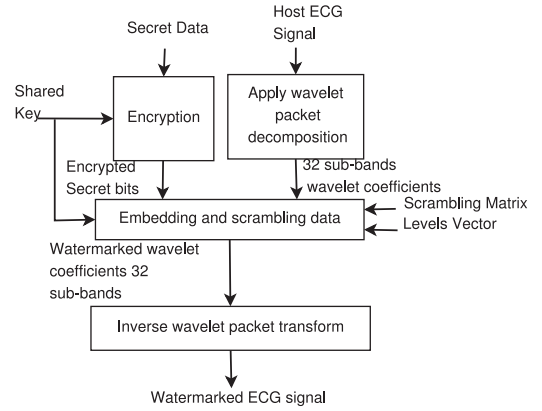


Fig. 4. Block diagram of the sender steganography which includes encryption, wavelet decomposition, and secret data embedding.

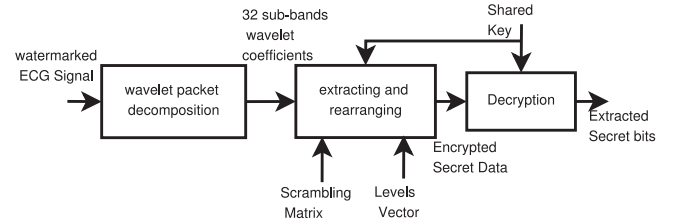


Fig. 5. Block diagram of the receiver steganography which includes wavelet decomposition, extraction, and decryption.

C. Stage 3: The Embedding Operation

At this stage, the proposed technique will use a special security implementation to ensure high data security. In this technique, a scrambling operation is performed using two parameters. First is the shared key known to both the sender and the receiver. Second is the scrambling matrix, which is stored inside both the transmitter and the receiver. Each transmitter/receiver pair has a unique scrambling matrix defined by

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

where S is a 128×32 scrambling matrix and s is a number between 1 and 32. While building the matrix we make sure that the following conditions are met.

- 1) The same row must not contain duplicate elements.
- 2) Rows must not be duplicates.

The detailed block diagram for the data embedding process is shown in Fig. 6. The embedding stage starts with converting the shared key into ASCII codes, therefore each character is represented by a number from 1 to 128. For each character code, the scrambling sequence fetcher will read the corresponding row from the scrambling matrix. An example of a fetched row can

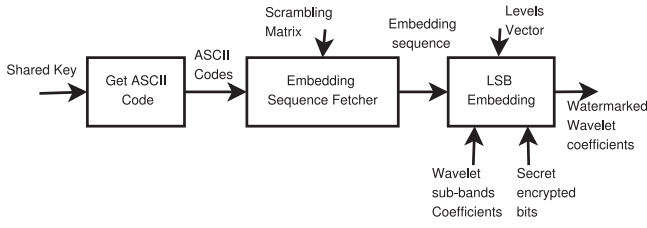


Fig. 6. Block diagram showing the detailed construction of the watermark embedding operation.

be shown as follows:

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

The embedding operation performs the data hiding process in the wavelet coefficients according to the subband sequence from the fetched row. For example, if the fetched row is as in (5), the embedding process will start by reading the current wavelet coefficient in subband 32 and changing its LSB bits. Then, it will read the current wavelet coefficient in subband 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 subband. For example, if the data are embedded in subband 32 then 6 bits will be changed per sample, while if it is embedded into wavelet coefficient in subband 1 then 5 LSB bits will be changed.

D. Stage 4: Inverse Wavelet Recomposition

In this final stage, the resultant watermarked 32 subbands are recomposed using inverse wavelet packet recombination. The result of this operation is the new watermarked ECG signal. The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain. Therefore, the newly reconstructed watermarked ECG signal will be very similar to the original unwatermarked ECG signal. The detailed embedding algorithm is shown in Algorithm 1.

The algorithm starts by initializing the required variables. Next, the coefficient matrix will be shifted and scaled to ensure that all coefficients values are integers. Then, the algorithm will select a node out of 32 nodes in each row of the coefficient matrix. The selection process is based on the value read from the scrambling matrix and the key. The algorithm will be repeated until the end of the coefficient matrix is reached. Finally, the coefficient matrix will be shifted again and rescaled to return its original range and inverse wavelet transform is applied to produce the watermarked ECG signal.

E. Watermark Extraction Process

To extract the secret bits from the watermarked ECG signal, the following information is required at the receiver side.

Algorithm 1 The embedding algorithm

```

1: bits: the secret bits array
2: bs: size of bits array
3: b: index of the current bit of the secret bits array
4: ecg: the host ECG signal
5: key: encryption key
6: kl: size of key
7: kc: index of the current character in the secret key
8: scra: The scrambling matrix  $128 \times 32$ 
9: sl: steganography embedding level
10: coef: wavelet packet coefficients at level 5 which has 32 columns
11: cs: number of rows of coef matrix
12: s: index of the current row of the coefficients matrix
13:  $coef \leftarrow coef + 20$ 
14:  $coef \leftarrow coef \times 10000$ 
15:  $b \leftarrow 1$ 
16:  $kc \leftarrow 1$ 
17:  $s \leftarrow 1$ 
18: while  $s < cs$  do
19:   for  $i = 1$  to 32 do
20:      $node \leftarrow scra(ascii(key(kc)), i)$ 
21:      $bnode \leftarrow sl(node)$ 
22:     for  $j = 1$  to  $bnode$  do
23:        $coef(s, node) \leftarrow embed(bits(b), position(j))$ 
24:        $b \leftarrow b + 1$ 
25:       if  $b > bs$  then
26:          $b \leftarrow 1$ 
27:       end if
28:     end for
29:   end for
30:    $s \leftarrow s + 1$ 
31:    $kc \leftarrow kc + 1$ 
32:   if  $kc > kl$  then
33:      $kc \leftarrow 1$ 
34:   end if
35: end while
36:  $coef \leftarrow coef / 10000$ 
37:  $coef \leftarrow coef - 20$ 
38:  $necg \leftarrow wavletpacketrecomposition(coef)$ 

```

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

The stages of the extraction process can be shown in Fig. 5. The first step is to apply five-level wavelet packet decomposition to generate the 32 subbands signals. Next, using the shared key and scrambling matrix the extraction operation starts extracting the secret bits in the correct order according to the sequence rows fetched from the scrambling matrix. Finally, the extracted secret bits are decrypted using the same shared key. The watermark extraction process is almost similar to the watermarking embedding process shown in Algorithm 1 except that instead of changing the bits of the selected node, it is required to read values of the bits in the selected nodes, and then resetting them to zero.

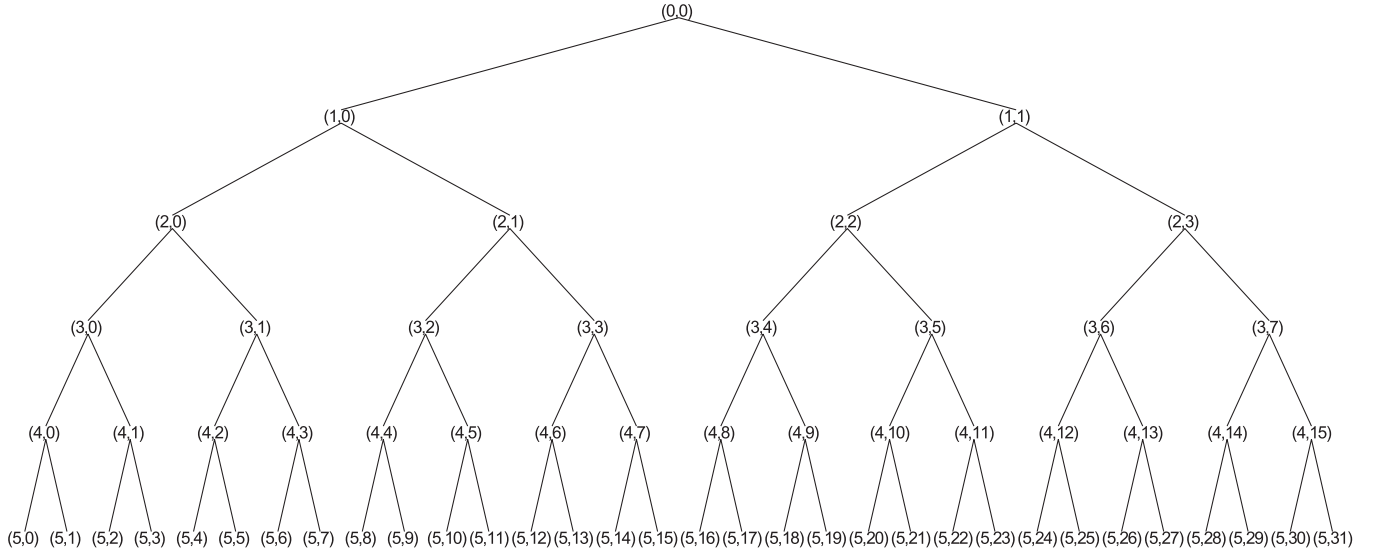


Fig. 7. Five-level wavelet decomposition tree showing 32 subbands of ECG host signal and the secret data will be hidden inside the coefficients of the subbands.

IV. SECURITY ANALYSIS

The security of the proposed algorithm is mainly based on the idea of having several parameters shared between the transmitter and the receiver entities. Any change in any parameter will lead to the extraction of wrong data. Accordingly, the receiver and transmitter should agree on the following information.

- 1) The scrambling matrix.
- 2) The encryption key (ASCII text string), i.e., shared secret.
- 3) Steganography levels vector.

As a result, even if the key is stolen the attacker will require to know the scrambling matrix as well as the steganography levels vector. The scrambling matrix is stored inside the transmitter/receiver pair and it will not be transmitted under any circumstance. For example, each patient could have his own device from his medical service provider and the matrix is burnt on this device. Therefore, for each pair of transmitter and receiver, it must be a unique scrambling matrix. As a result the total number of devices pairs (that can be supported) with a unique scrambling matrix can be calculated as follows:

$$N = 32! \times 128! \approx 3.8562 \times 10^{+215}. \quad (6)$$

As shown in (6) the total number of devices that we can support is larger than the IPv6 protocol address space. On the other hand, the sequence of rows fetched from the scrambling matrix is totally related to the user defined key. As a result, the longer the key is, the stronger the steganographic technique will be. To guarantee the maximum security, the length of the key used (L_{key}) should satisfy the following condition:

$$L_{key} = \text{Max} \left(\frac{B}{180}, M \right) \quad (7)$$

where B is the size of the embedded data in bits and M represents the minimum key size. Accordingly, Table I shows the probabilities to break the proposed technique using different key lengths and the minimum data size that can be hidden to achieve the maximum security for each key length.

TABLE I
SECURITY STRENGTH FOR DIFFERENT KEY LENGTHS

key length	minimum data size (bits)	probabilities
4	720	1E+224
8	1440	2.7E+232
16	2880	2E+249
32	5760	1E+283
40	7200	7.4E+299

The amount of data that can be stored inside the ECG host signal using the proposed model totally depends on the steganography levels vector. In our proposed model and for ECG with 10-s length and sampling rate of 360, a 2531 bytes (2.4 kB) of data can be embedded inside ECG host signal. The amount of data that can be stored is calculated using

$$b = \frac{t \times f_s}{32} \times 180 \quad (8)$$

where b is the total number of bits stored, t is the total signal time in seconds, and f_s is the sampling frequency.

V. DIAGNOSABILITY MEASUREMENT OF THE WATERMARKED ECG SIGNAL

In this paper, the work done by Al-Fahoum [16] has been implemented and used as a diagnosability measure to determine the effect of the watermarking process on the usability of the resultant ECG for diagnoses purposes. In this model, a five-level wavelet decomposition is applied to the original and watermarked ECG signal. As a result, the original signal will be divided into number of subbands denoted by A_5, D_5, D_4, D_3, D_2 , and D_1 . It is found that band A_5 includes most of the T-wave contribution and some of the P-wave contribution. Therefore, its weight should include the significance of P and T. Moreover, band D_5 includes most of the P-wave contribution, part of the T-wave contribution, and a relatively low percentage of the QRS-complex contribution. The weight of D_5 should maintain the highest weight contribution of P, T, and QRS. Band D_4 also

TABLE II
WEIGHTS FOR EACH SUBBAND USED IN MEASURING DIAGNOSABILITY

Wavelet Bands	A5	D5	D4	D3	D2	D1
Bands weights	6/27	9/27	7/27	3/27	1/27	1/27

contains most of the QRS-complex contribution, and a little portion of P-wave. The weight of D_4 is higher than A_5 but lower than D_5 . D_3 includes some portions of the QRS-complex, and so its weight is lower than QRS weight itself. Bands D_2 and D_1 are weighted less than any other band as they do not contribute to the spectrum of any of the main features. However, they cannot be excluded where late potentials and delta waves may exist. The researchers used a heuristics weights to mark the contribution of each subband. The weights used are shown in Table II.

After applying five-level wavelet decomposition a PRD measure of each subband is calculated as

$$\text{WPRD}_j = \sqrt{\frac{\sum_{i=1}^N (c_i - \tilde{c}_i)^2}{\sum_{i=1}^N (c_i^2)}} \quad (9)$$

where c_i is the original coefficient within subband j and \tilde{c}_i is the coefficient of subband j for the watermarked signal. Finally, to find the weighted wavelet PRD (10) is used

$$\text{WWPRD} = \sum_{j=0}^{N_L} w_j \text{WPRD}_j \quad (10)$$

where N_L is the total number of subbands, w_j denotes the weight value corresponding to subband j , and WPRD_j represents the calculated wavelet-based PRD for subband j .

VI. EXPERIMENTS AND RESULTS

In this paper, three different types of ECG signals are used for the experimentation. A testbed of 59 ECG samples is used for the experimentation. The set of samples consist of 19 normal (NSR) ECG samples, 27 Ventricular fibrillation ECG samples, and 13 Ventricular Tachycardia ECG samples. Each sample is 10 s long with 250-Hz sampling frequency.

To evaluate the proposed model, the PRD (percentage residual difference) is used to measure the difference between the original ECG host signal and the resulting watermarked ECG signal as

$$\text{PRD} = \sqrt{\frac{\sum_{i=1}^N (x_i - y_i)^2}{\sum_{i=1}^N x_i^2}} \quad (11)$$

where x represents the original ECG signal and y is the watermarked signal.

Alternatively, to evaluate the diagnostic distortion caused by the watermark, a wavelet-based PRD is used as detailed in the previous section. These measures have been calculated for each sample. Accordingly, to measure distortion caused by the extraction process, PRD and diagnoses PRD have been calculated. Finally, to evaluate the reliability of the extracted information bit error rate has been used as follows:

$$\text{BER} = \frac{B_{\text{err}}}{B_{\text{total}}} \times 100\% \quad (12)$$

TABLE III
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 IV
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 V
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
13	0.41675	0.45275	0.57517	0.63255
14	0.45104	0.46792	0.60064	0.61633
15	0.38447	0.39853	0.5267	0.55549
16	0.32621	0.32604	0.4417	0.43772
17	0.66713	0.93723	0.91967	1.2995
18	0.79696	1.3659	1.0728	1.8144
19	1.0732	0.96977	1.454	1.2749
20	1.0514	0.99681	1.4297	1.3527
21	0.84326	0.99305	1.1607	1.3767
22	0.71059	0.97451	0.96605	1.3123
23	0.61859	1.066	0.8545	1.4892
24	0.66063	1.0684	0.91559	1.4727
25	0.79912	1.2993	1.1125	1.8225
26	0.92514	1.1759	1.2979	1.6486

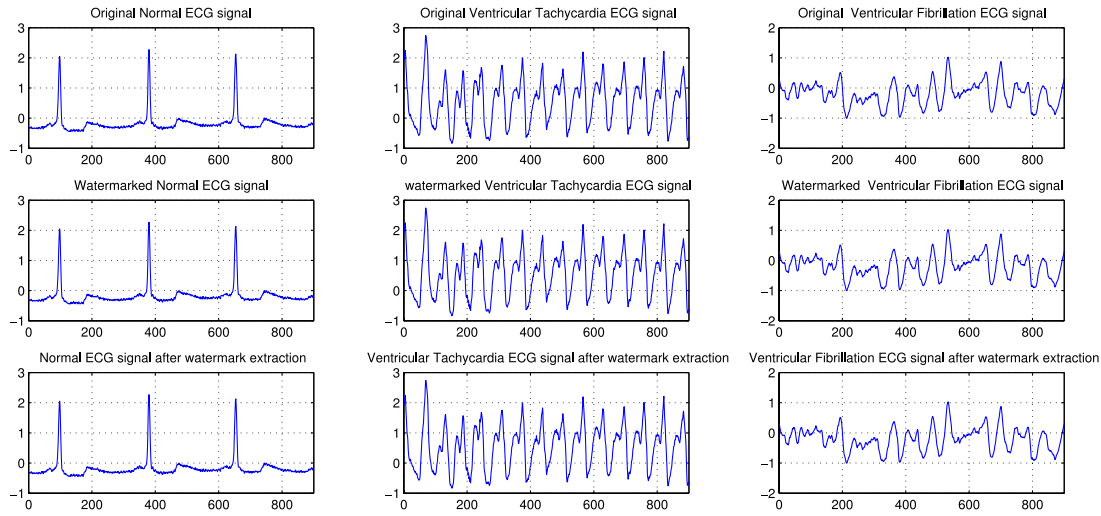


Fig. 8. ECG signals for normal, VT and VF signal before applying the steganography operation and after the steganography operation as well as after extracting the hidden data.

TABLE VI
AVERAGE PRD RESULTS FOR DIFFERENT SCRAMBLING MATRICES

Case No	PRD %	WWPRD %	PRD % extracted	WWPRD % extracted
1	0.316605	0.340602	0.424484	0.454439
2	0.316308	0.338725	0.424643	0.455201
3	0.31775	0.333594	0.423802	0.455167
4	0.317904	0.338432	0.425399	0.456254
5	0.316824	0.337616	0.42462	0.455501
6	0.318639	0.341384	0.425632	0.457272
7	0.319365	0.338233	0.424424	0.455365
8	0.315372	0.337196	0.425761	0.45611
9	0.317598	0.34042	0.425144	0.455971
10	0.317847	0.343214	0.424329	0.456203

where BER represents the bit error rate in percentage, B_{err} is the total number of erroneous bits, and B_{total} is the total number of bits.

Table III shows the results obtained for 18 normal ECG samples. It can be seen from the table that a maximum PRD measured was 0.6%. Second, it can be noticed that the difference between the normal PRD and the wavelet-based PRD for diagnoses measurement is very small. Accordingly, this proves that the watermarking process does not affect the diagnosability. Finally, this table shows the PRD measured after extracting the watermark. It is obvious from the table that removal of the watermark will have a small impact on the PRD value. As a result, the ECG signal can still be used for diagnoses purposes after removing the watermark.

To guarantee unbiased results, we also experimented with VT and VF samples and the results are shown in Tables V and IV, respectively. It is obvious from these results that the maximum PRDs for VT host signal are only 0.5% and 1% for VF. This encouraging result clearly demonstrates that the watermarked ECG signals can be used for diagnoses. Fig. 8 shows three ECG signal types, and the resultant watermarked signals before and after watermark extraction process.

Previous results have been obtained by using the same scrambling matrix. To generalize our results, we performed the same experiments and calculated the average PRD values for differ-

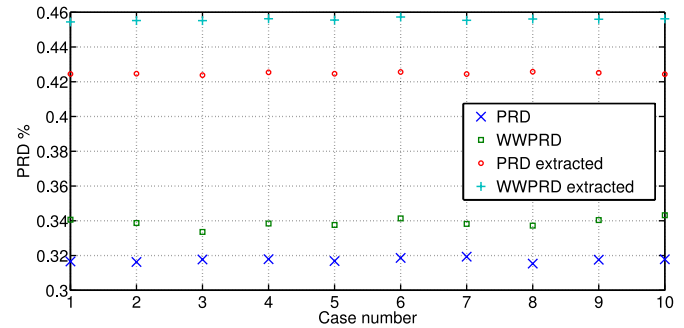


Fig. 9. Average PRD results for different scrambling matrices.

TABLE VII
DOCTORS DIAGNOSES RESULTS

Doctor	Normal similarity	Normal diagnosability	Abnormal similarity	Abnormal diagnosability
1	99%	Yes	99%	Yes
2	100%	Yes	100%	Yes

ent cases of scrambling matrices. Table VI shows ten different cases taken and their corresponding average PRD values. It can be clearly seen how the values are approximately equal for different cases. The obtained results further prove that our proposed technique will cause minimum distortion for different cases of the scrambling matrix. This is clearly shown in Fig. 9.

To validate diagnosability of the digitally processed ECGs, two specialist doctors were consulted. Sixty ECG segments (each 10-s length) for both normal sinus rhythm and abnormal (Ventricular Tachycardia, Ventricular Fibrillation) cases were shown to them before and after watermarking, and also after removal of watermarks. They were asked the following questions.

- 1) How similar is the original and the watermarked ECG?
- 2) Can the watermarked ECG be used for diagnoses?

Both the specialist doctors admitted that the similarity is so high that the difference is undetectable and the both watermarked and unwatermarked signals can be used for diagnoses. The detailed results are shown in Table VII.

VII. CONCLUSION

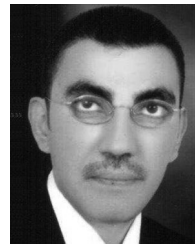
In this paper, a novel steganography algorithm is proposed to hide patient information as well as diagnostics information inside ECG signal. This technique will provide a secured communication and confidentiality in a PoC system. A five-level wavelet decomposition is applied. A scrambling matrix is used to find the correct embedding sequence based on the user-defined key. Steganography levels (i.e., number of bits to hide in the coefficients of each subband) are determined for each subband by experimental methods. In this paper, we tested the diagnoses quality distortion. It is found that the resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted.

ACKNOWLEDGMENT

The authors would like to thank Dr. L. Asaf and Dr. S. Hermiz from Settlement Rd Clinic, 258 Settlement Rd Thomastown, Vic., Australia, for their time and effort in finding the similarity between the original and watermarked ECG signals. Finally, the author would like to thank the anonymous reviewers for their constructive suggestions.

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] A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in *Proc. 5th Int. Conf. Intell. Sens. Netw. Inf. Process.*, Dec. 2010, pp. 207–212.
- [4] W. Lee and C. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 1, pp. 34–41, Jan. 2008.
- [5] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in *Proc. 1st ACM SIGMOBILE Int. Workshop Syst. Netw. Supp. Healthcare Assist. Living Environ.*, 2007, p. 12.
- [6] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 946–954, Nov. 2009.
- [7] H. Wang, D. Peng, W. Wang, H. Sharif, H. Chen, and A. Khoynzhad, "Resource-aware secure ECG healthcare monitoring through body sensor networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 12–19, Feb. 2010.
- [8] L. Marvel, C. Boncelet, and C. Retter, "Spread spectrum image steganography," *IEEE Trans. Imag. Process.*, vol. 8, no. 8, pp. 1075–1083, Aug. 1999.
- [9] A. De la Rosa Algarin, S. Demurjian, S. Berhe, and J. Pavlich-Mariscal, "A security framework for xml schemas and documents for healthcare," in *Proc. IEEE Int. Conf. Bioinf. Biomed. Workshop*, Oct. 2012, pp. 782–789.
- [10] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.
- [11] S. Kaur, R. Singhal, O. Farooq, and B. Ahuja, "Digital watermarking of ECG data for secure wireless communication," in *Proc. Int. Conf. Recent Trends Inf. Telecommun. Comput.*, Mar. 2010, pp. 140–144.
- [12] H. Golpira and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol.*, Dec. 2009, pp. 31–36.
- [13] K. Zheng and X. Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms," in *Proc. Int. Conf. Comput. Intell. Security*, Dec. 2008, vol. 1, pp. 295–299.
- [14] D. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2006.
- [15] A. Poularikas, *Transforms and Applications Handbook*. Boca Raton, FL, USA: CRC Press, 2009.
- [16] 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.



Ayman Ibaida received the Master's degree in computer engineering from Baghdad University, Baghdad, Iraq, in 2005. He is currently working toward the Ph.D. degree in computer science at RMIT University, Melbourne, Australia.

He worked as a Lecturer in Computer College, Dubai, between 2006 and 2008. His research interests include biomedical signal processing, diagnoses, compression, and patient health records security in Health-care systems.



Ibrahim Khalil received the Ph.D. degree from the University of Berne, Berne, Switzerland, in 2003.

He is currently a Senior Lecturer in School of Computer Science & IT, RMIT University, Melbourne, Australia. He has several years of experience in Silicon Valley-based companies working on Large Network Provisioning and Management software. He also worked as an academic in several research universities. Before joining RMIT, he worked for EPFL and University of Berne in Switzerland and Osaka University in Japan. His research interests include scalable computing in distributed systems, m-health, e-health, wireless and body sensor networks, biomedical signal processing, network security, and remote health-care.