

# A Low Complexity High Capacity ECG Signal Watermark for Wearable Sensor-net Health Monitoring System

Ayman Ibaida<sup>1</sup>, Ibrahim Khalil<sup>1</sup>, Ron van Schyndel<sup>1</sup>

<sup>1</sup>Comuter Science and Information Technology, RMIT University, Melbourne, Australia

## Abstract

*In Wireless telecardiology applications, an ECG signal is often transmitted without any patient details which are often supplied separately as clear text. This allows the possibility of confusion of link between signal and identity (for example, with wireless signal collision attacks). ECG data transmission can be more robustly tied to either patient identity or other patient meta-data if this meta-data is embedded within the ECG signal itself when sent.*

*In this paper ECG signals are watermarked with patient biomedical information in order to confirm patient/ECG linkage integrity. Several cases have been tested with different degrees of signal modification due to watermarking. These show its effect on the diagnostic value of the signal (for example, the PRD as an error measure). It is found that a marginal amount of signal distortion that is sufficient to hold the patient information, will not affect the overall quality of the ECG. The proposed system will not increase the size of host signals, nor change its scaling nor bandwidth. In addition, its low complexity makes it suitable for power-limited wearable computing and sensor-net applications.*

## 1. Introduction

### 1.1. Data Watermarking

Data watermarking is a relatively old branch in the domain of steganography (data hiding). Its main purpose is to trace the watermarked data as that data is used.

Data watermarking can be used to protect data ownership priority, copyright assertions and securely sending data through unsecured communication channels such as the Internet or the wireless channels. Data watermarking is defined as the process by which a digital stream of data called the Watermark, is hidden inside another stream called the host signal, necessarily 'damaging' it. The amount of data which can be hidden and how it is hidden depends primarily on the host signal characteristics and the amount of damage to the host signal that can be

tolerated. This is necessarily a subjective and application-dependent measure.

For multimedia watermarking, where the primary consumer of the data is human perception, watermark detectability is described in terms of visual or auditory perceptibility. A strongly applied image watermark for example would be visible as noise, and would compromise the visual integrity of the host image. How much compromise is considered acceptable is subjective and application-dependent.

### 1.2. The Wireless Sensor-Net Context

In recent years, there has been much work in telemonitoring - typically involving transmission of data in a wireless form. Such medical data needs to be protected from changes - deliberate or otherwise - during its online transmission. The various image modalities (Xray, ECG, EKG, MRI, PET, ...) all having unique data properties and formats, need also to be watermarked in a wireless health care system. In our paper, we discuss one such modality: the ECG signal.

In a typical wireless telemonitoring scenario, a patient wears wireless sensors capable of reading samples of ECG, temperature, blood pressure, etc. In general, these data streams are sent separately to the hospital. In our scenario, different biomedical information will be watermarked inside the ECG signal in a patient's PDA device. then sent wirelessly to a central server, where the server can check the watermarked signal and extract the meta-information hidden within the signal. The server will then distribute the received de-assembled information to e-doctors (eg. doctors who are roaming around with mobile devices) that can take quick action according to its priority [1].

In this scenario, the watermarking algorithm must preserve the main features of the ECG signal as shown in figure 1 for a typical normal and abnormal ECG. Moreover, it must guarantee that diagnosing the ECG signal can be done directly without removing the watermark. The watermark must thus ideally be *invisible* on a trace.

For the purpose of watermarking, it was deemed best to retain the signal closest to its original sampled form and

not rely on absolute measures. Figure 1(b) shows this graphically. Observe the large overall dip in the normal signal close to the start.

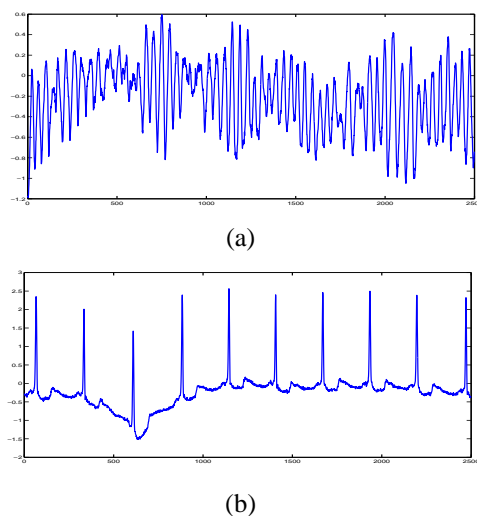


Figure 1. (a) VT ECG sample (b) Normal ECG sample

### 1.3. Other Work

There has some specific application of watermarks to ECG data. Kong and Feng [2] describe three watermarking techniques popular in 2001 applied to EEG signals: Bender's *Patchwork* [3], van Schyndel's *LSB* [4], and Chen's *QIM* [5] watermarking methods. Each was inserted using a pseudorandom scrambling key. The watermark was designed as a '1-bit' watermark: it was either detected, or not. Our method is a combination of the QIM and LSB methods, but the watermark contains a message, and there is no attempt at encryption, although its incorporation is straightforward.

In line with the sophisticated techniques introduced more recently, Engin, idam, and Zeki [6] implemented a wavelet based watermarking technique for ECG signals. In their work, they wavelet-decomposed the ECG signal up to level 3 to divide the ECG signal into 8 bands, then computed the average power for each scale and used the calculated power as threshold parameters to select sub-bands to add to the watermark, according to the threshold value. Finally they took an inverse DWT to reconstruct the watermarked ECG signal. While their algorithm is robust, its data-carrying capacity is limited. Similarly Kaur et al [7] described in 2010 a Chirp-signal based watermark which can self-synchronise, but again, its capacity is limited. In this case to a 15 digit numeric code.

By contrast, Nambakhsh and Ahmadian [8], used the ECG signal itself as an embedded watermark message, and injected it inside medical CT and MRI images. Anand and

Niranjan had attempted the same thing in 1998 [9] These might both facilitate fusion of the ECG data set with the patient data set, for example.

In all the above techniques. the algorithms involve high computation complexity. Since some data transformation must be performed, these operations requires high resources and will produce delay.

Our sensor-net applications may involve 'motes' with extremely limited resources and power (for example in wearable computing applications), so a simpler power- and bandwidth-preserving technique is required for the data-gathering and watermarking process.

In this paper we will use a variation on a Quantisation Index Modulation (QIM) watermarking technique developed by Brian Chen and Greg Wornell at MIT [5], to preserve bandwidth and decrease the size of transmitted information as much as possible. We analysed the ECG signal to find how many bits per sample that we can use for watermarking. To achieve this goal, we used a standard Percentage Residual Difference as an unbiased error measure between the original ECG and the watermarked ECG [10].

In order to establish a simple initial benchmark for diagnostic fidelity, we describe a simple model for the ECG fiducial points introduced by Sufi and Khalil [11].

This paper is organized as follows. In section 2 we discuss the basic system, Signal transformation and watermarking process. Next, in section 3 we show the results of PRDs for different number of embedded bits per sample. Finally, we conclude in section 4 with some application notes.

## 2. The Methodology

Our proposed model for ECG watermarking consists of 2 stages. as shown in figure 2. The first stage is responsible of signal pre-processing, which consists of a simple linear transform of the form

$$\bar{X} = \lfloor mX + c \rfloor \quad (1)$$

where  $X$  is a raw unscaled ECG vector,  $m$  and  $c$  are a scalar multiplier and offset and  $\bar{X}$  is the resultant scaled signal ECG signal, truncated to the nearest integer, if necessary. The selection of  $m, c$  are dependant on the ECG acquisition device (eg. the resolution of the analog to digital converter), and perhaps the data type of the incoming data stream (which may not need to be calibrated, but will need to be shape-preserving).

The second stage of the proposed model is the watermarking process, After the scaling, an LSB watermarking algorithm is selected, because of its simplicity in implementation inside the sensor nodes. It can be shown that through optimal selection of scaling and truncation, the

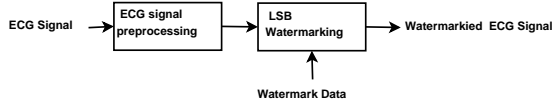


Figure 2. Block Diagram for the Proposed ECG detection system

LSB approach coincides with the QIM approach, but it is much simpler (and less flexible) than full QIM.

This LSB algorithm can be implemented as a series of OR and AND operations and its purely hardware implementation is feasible.

The least significant  $n$  bits of the scaled result are then watermarked with sequential bits in the watermark stream. Let  $X$  be the host signal, and  $b$  is the watermark bit extracted from the watermark bit stream. then the watermarking operation can be summarized as shown in eq 2

$$\hat{X} = \begin{cases} (X \wedge \bar{1}) \vee 1 & \text{if } b=1 \\ (X \wedge \bar{1}) \vee 0 & \text{if } b=0 \end{cases} \quad (2)$$

Comparison of the resulting watermarked signal with the original signal is performed using a simple Euclidean error-distance: the Percentage Residual Difference (PRD), in common use for ECG measurements, as shown in eq 3.

$$PRD = \sqrt{\frac{\sum_{i=1}^N (\bar{x}_i - \hat{x}_i)^2}{\sum_{i=1}^N \bar{x}_i^2}} \quad (3)$$

where  $\bar{x}$  represents the scaled ECG signal, and  $\hat{x}$  represents the watermarked signal.

### 3. Results

We collected 81 ECG segments from The Creighton University Ventricular Tachyarrhythmia Database [12]. Each ECG segment was 10 seconds long and had a sampling rate of 250Hz. Therefore, the total number of samples in each segment is 2500 samples.

Using the procedure discussed earlier, and by comparing the watermarked ECGs with the original ECGs for different number of bits, we get figure 3 which represents the average PRD calculated for up to 9-bits. The figures show the difference error increasing linearly with  $2^n$  for  $n$  bits of watermark. When the watermark is less than 5 bits the differences are negligible (less than 1%).

#### 3.1. Numerical Value

Table 1 and figure 3 shows the average PRDs, for different number of bits, for a normal ECG, one with

Table 1. Average PRD for 1-9 bits for 3 kinds of ECG

Numb Bits	Normal (%)	VT (%)	PVC (%)
1-bit	0.012073	0.002975	0.007178
2-bit	0.022476	0.025342	0.08287
3-bit	0.062345	0.053405	0.175318
4-bit	0.145895	0.108464	0.362422
5-bit	0.316965	0.217443	0.720631
6-bit	0.655582	0.432033	1.46666
7-bit	1.325998	0.842508	2.943103
8-bit	2.688043	1.700876	5.949832
9-bit	5.419369	3.374862	11.91365

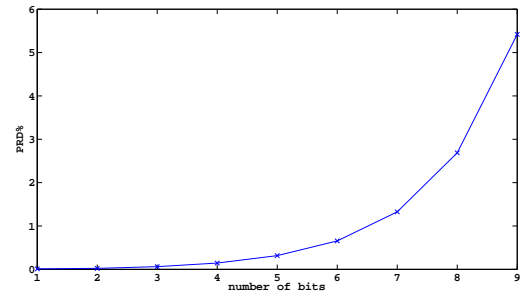


Figure 3. The relation of average PRD and number of bits

Ventricular Tachycardia, and one with PVC, all from the Creighton University database [12].

The source data was scaled such that the total distance represents full resolution for the sampling device used (-10V..10V = 12 bits nominal = -2047..2048 integer range)

For 12 bits, a maximum error in bit 4 (for example if  $x = 1023 \implies \bar{x} = 1008$ ) represents maximally  $15/4096 = -24dB$  intensity difference between signal and noise which is about the upper bound of detectability on a screen. Hence, for a 12 bit per sample signal, up to 4 bits can be used for watermarking.

For a 10 second sample at 250Hz, we can maximally store 10000 bits or 1250 bytes of data. In practice, we would need to include synch code, a convolutional code framework, and error control and correction, so a more typical capacity with good robustness would be around 200 bytes.

#### 3.2. Diagnostic Value

To address the diagnostic value of these samples, we need to remember that in a wearable computing sensor-net environment, we are unlikely to have precise control or calibrated data, so a pattern-matching approach to cardiac pathology would need to be employed.

As can be seen in figure 1, it is self-evident in the style of watermarking used, that any changes will not result in any sample timing changes, so the  $t$  coordinate of the

points PQRST are not altered. The sample value is altered according to the maximum bit level used.

Appendix 1 shows the three types of ECG for normal, VT and PVC types of ECG. As can be seen, the overall shape of the signal is not changed, even for up to 9 bits of watermark embedded data.

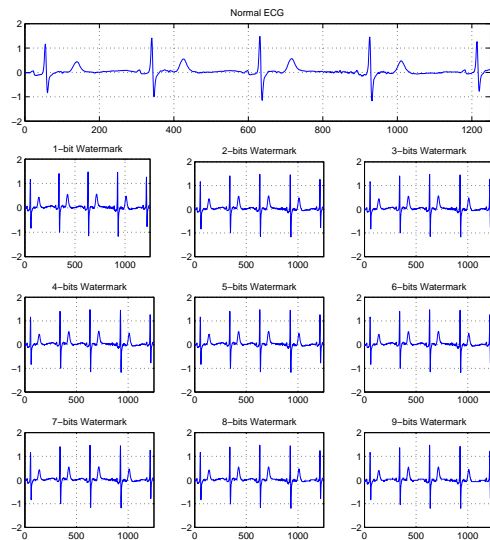


Figure 4. ECG watermarked signal for normal ECG

#### 4. Conclusion and Future Work

Because ECG signal dumps over long periods of time can be enormous in size [11], it can be used as a host to carry other biomedical information watermarked inside it, as the size of information needed to be transferred wirelessly increases in health care systems and patient monitoring system.

Therefore, a bandwidth preserving technique is presented in this paper, where we showed that changing some parts of the ECG signal will not affect the overall utility of the ECG signal. Also we used watermark to embed the information inside the ECG signal which can be implemented in real time monitoring systems and does not add to overall transmission bandwidth.

While we did not include any physical security layering that could be applied - instead relying on message encryption to perform the task, we presented some variations on our approach which can be used for a simple security through obfuscation.

Om future, we intend to extend the physical security aspect, with a rigorous security layer, bearing in mind the low-complexity requirement of our application domain.

#### References

- [1] Lo B, Thiemjarus S, King R, Yang G. Body sensor network – a wireless sensor platform for pervasive healthcare monitoring. In *The 3rd International Conference on Pervasive Computing*, 2005; .
- [2] Kong X, Feng R. Watermarking medical signals for telemedicine. *IEEE Transactions on Information Technology in Biomedicine* 2001;5(3):195–201. ISSN 1089-7771.
- [3] Bender W, Gruhl D, Morimoto N, A.Lu. Techniques for data hiding. *IBM Systems Journal* 1996;35(3&4). MIT Media Lab.
- [4] van Schyndel RG, Tirkel AZ, Osborne CF. A digital watermark. In *Proc. of the IEEE Int. Conf. on Image Processing (ICIP)*, volume 2. Austin, Texas, USA, November 1994; 86–90.
- [5] Chen B, Wornell G. Digital watermarking and information embedding using dither modulation. In *1998 IEEE Second Workshop on Multimedia Signal Processing*. Dec 1998; 273–278.
- [6] Engin M, Çıdam O, Engin E. Wavelet Transformation Based Watermarking Technique for Human Electrocardiogram (ECG). *Journal of Medical Systems* 2005;29(6):589–594.
- [7] Kaur S, Farooq O, Singhal R, Ahuja B. Digital watermarking of ecg data for secure wireless communication. In *International Conference on Recent Trends in Information, Telecommunication and Computing (ITC)*. Kochi, Kerala: IEEE. ISBN 978-1-4244-5956-8, March 2010; 140–144.
- [8] Nambakhsh M, Ahmadian A, Ghavami M, Dilmaghani R, Karimi-Fard S. A novel blind watermarking of ecg signals on medical images using ewz algorithm. In *Conference proceedings:... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference*, volume 1. 2006; 3274.
- [9] Anand D, Niranjana U. Watermarking medical images with patient information. In *Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*. Hong Kong, China. ISSN 0-7803-5164-9, Oct–Nov 1998; .
- [10] Lu Z, Kim D, Pearlman W. Wavelet compression of ECG signals by the set partitioning in hierarchical trees (SPIHT) algorithm. *IEEE Trans Biomed Eng* 2000;47(7):849–856.
- [11] Sufi F, Khalil I, Fang Q, Cosic I. A mobile web grid based physiological signal monitoring system. In *Technology and Applications in Biomedicine, 2008. ITAB 2008. International Conference on*. 2008; 252–255.
- [12] PhysioNet. The creighton university ventricular tachyarrhythmia database. URL <http://www.physionet.org/physiobank/database/cu>

Address for correspondence:

Ayman Ibaida  
 Department of CS & IT, RMIT University, Melbourne, Vic, Australia.  
 ayman.ibaida@student.rmit.edu.au