Hiding Data in Electrocardiogram Based on IWT Domain via Simple Coefficient Adjustment

Ching-Yu Yang[a*] and Kuang-Tsan Lin[b]

[a]Department of Computer Science and Information Engineering
National Penghu University of Science and Technology
300, Liu-Ho Rd., Magong, Penghu, 880 Taiwan

[b]Department of Mechanical and Computer-Aided Engineering
St. John's University 499, Sec. 4, Tam King Road,Tamsui District
New Taipei City, 25135 Taiwan

[*]*Corresponding author's email: chingyu [AT] gms.npu.edu.tw*

ABSTRACT---- ***The authors present a data hiding method for electrocardiogram (ECG) signal based on integer wavelet transform (IWT). By using a simple coefficient adjusting technique, data bits can be rapidly embedded in an ECG host signal, and be successfully extracted at the receiver site. Simulations confirmed that the perceived quality introduced by the proposed method is good, while hiding storage is greater than existing techniques. In addition, the method has a certain degree of robustness. Since the proposed method provides the advantage of low time complexity, it is feasible for use in real-time applications.***

Keywords--- Data Hiding, ECG Watermarking, ECG Steganography, IWT

1. INTRODUCTION

During the last two decades, many researchers have successfully designed data hiding techniques for digital media such as images, videos, and audio [1-3]. However, only few authors pay attention to hide patient privacy and diagnosis data in biometric media such as electrocardiogram (ECG) and electroencephalogram (EEG) signals. The study of hiding data in biometric is still in its infancy. Generally speaking, data hiding can be dived into two categories: steganography and digital watermarking. The main distinction between both categories is that the former tried to hide secret bits in media as large as possible while maintaining a good (or an acceptable) perceived quality, and the latter emphasizes robustness performance with a small to moderate volume of payload. In this article, we focus on the ECG data hiding.

At present, several data hiding techniques have been applied in ECG signal for securing patient information [4-8]. Ibaida et al. [4] designed a high-capacity ECG signal watermark for a wearable sensor-net health monitoring system. Simulations confirmed that the proposed method is suitable for real-time monitoring systems. Based on the IWT transform and a self-synchronization technology, He et al. [5] suggested a watermarking scheme for ECG signals. Simulations showed that the signal-to-noise ratio (SNR) is greater than 30 dB while the marked ECG signal is tolerant of noise-addition attacks. Based on discrete wavelet transform (DWT), Ibaida and Khalil [6] proposed an ECG steganography scheme in combination with encryption and scrambling techniques. Simulations indicated that the method protects patient information effectively. Additionally, the perceptual quality was good and the resultant ECG signal could be used for diagnosis after extracting the hidden data.

Tseng et al. [7] integrated watermarking and compression approach, and presented a data hiding technique for ECG signals based on discrete wavelet transform (DWT). Simulations showed that the proposed method is capable of protecting ECG transmission security while optimizing the ECG shape. Based on DWT and singular value transform (SVD) decomposition, Jero et al. [8] proposed an ECG steganography scheme for protecting confidential patient data. To embed data bits in the selected sub-band of decomposition, first a one-dimensional (1D) ECG is converted to a two-dimensional ECG image. Simulations indicated that the scheme has good performance in terms of percentage residual difference (PRD) and bit error rate (BER) when the high-high sub-band of IWT was used for hiding a secret message.

The remainder of this paper is organized as follows. Our proposed method which includes bit-embedding and bit-extraction techniques is described in Section 2. Experimental results are presented in Section 3, and our conclusions are summarized in Section 4.

2. PROPOSED METHOD

The block diagram of our proposed method is shown in Fig. 1. To provide a good perceived quality and robustness, the proposed method embeds data bits in ECG signal based on integer wavelet transform (IWT) domain [9]. More specifically, data bits are embedded in the low-subband and high-subband of IWT coefficients, respectively. The details of bit embedding and bit extraction for our methods are specified in the following sections.

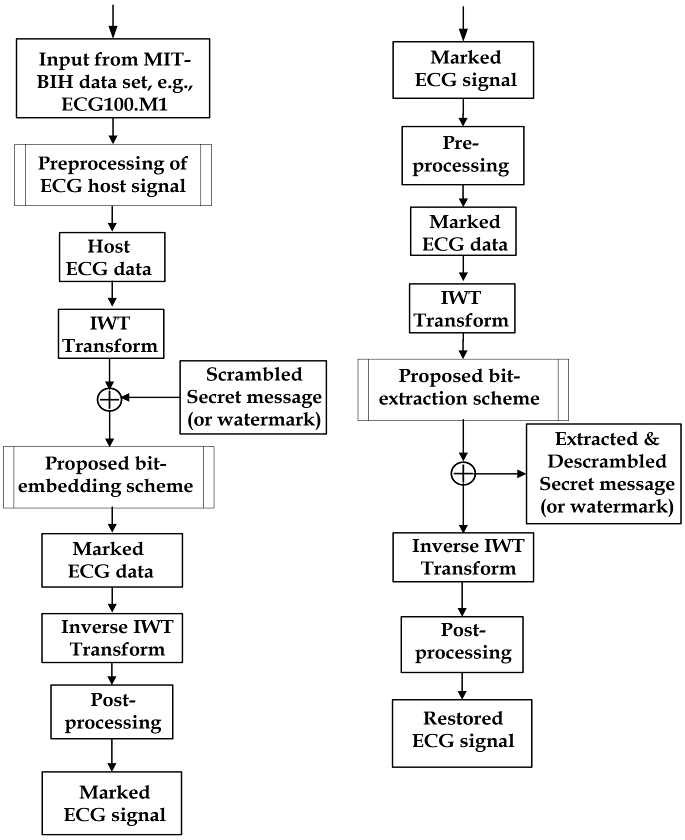

Input from MIT-BIH data set, e.g., ECG100.M1
Preprocessing of ECG host signal
Host ECG data
IWT Transform
Scrambled Secret message (or watermark)
Proposed bit-embedding scheme
Marked ECG data
Inverse IWT Transform
Post-processing
Marked ECG signal
Marked ECG signal
Pre-processing
Marked ECG data
IWT Transform
Proposed bit-extraction scheme
Extracted & Descrambled Secret message (or watermark)
Inverse IWT Transform
Post-processing
Restored ECG signal

Fig. 1 Block diagram of method. (a) Encoding part and (b) decoding part.

2.1 Bit-embedding

Let T_j be the *j*-th bundle of size *n* taken from the low-subband of IWT coefficients, where $T_j = \left\{t_{ji}\right\}_{i=0}^{n}$ and offset $d_j = t_{j0} - t_{j1}$ with *n* = 2.

The main procedure of bit embedding is described in the following algorithm.
Algorithm 1. Hiding a secret message in the low-subband of IWT coefficient.
Input: Low-subband of IWT $\Phi = \{s_k \mid k = 1,2,\ldots,|\Phi|\}$, secret message *W*, and control parameter τ.

Output: Marked ECG data Θ (and overhead bits).
Method:

Step 1. Input a bundle T_j derived from Φ. If the end of input is encountered, then proceed to Step 7.

Step 2. Compute offset $d_j = t_{j0} - t_{j1}$.

Step 3. Input a data bit b_l from *W*.

Step 4. If b_l = 0, then execute the following sub-steps:

Step 4.1 If the condition $0 \le d_j \le \tau$ is satisfied, then do nothing, which means the bundle "carries" data bit 0 without altering the value in T_j, and proceed to Step 1.

Step 4.2 If $d_j > \tau$ then reduce t_{j0} from 1 and increase t_{j1} by 1 repeatedly each time until either $0 \le d_j \le \tau$ or τ times is encountered. If $0 \le d_j \le \tau$ is true, then proceed to Step 1; otherwise, go to Step 6.

Step 4.3 Increase t_{j0} by 1 and reduce t_{j1} from 1 repeatedly each time until either $0 \le d_j \le \tau$ or τ times is encountered. If $0 \le d_j \le \tau$ is true, then proceed to Step 1; otherwise, go to Step 6.

Step 5. If b_l = 1, then execute the following sub-steps:

Step 5.1 If the condition $-\tau \le d_j < 0$ is satisfied, then do nothing, which means the bundle "carries" data bit 1 without altering the value in T_j, and proceed to Step 1.

Step 5.2 If $d_j < -\tau$ is satisfied, then increase t_{j0} by 1 and reduce t_{j1} from 1 repeatedly each time until either $-\tau \le d_j < 0$ or τ times is encountered. If $-\tau \le d_j < 0$ is true, then proceed to Step 1; otherwise, go to Step 6.

Step 5.3 Reduce t_{j0} from 1 and increase t_{j1} by 1 repeatedly each time until either $-\tau \le d_j < 0$ or τ times is encountered. If $-\tau \le d_j < 0$ is true, then proceed to Step 1.

Step 6. Undo alteration and mark T_j as a skipped block, and proceed to Step 1.

Step 7. Stop.

Note that Step 6 was rarely encountered in the proposed method. Our simulations revealed that all input bits were directly (or underwent successful coefficient adjusting and) embedded in the host bundles with null skipped blocks. Since the procedure of data hiding in the high-subband of IWT was similar with that of Algorithm 1, it was omitted here.

2.2 Bit-extraction

The bit extraction procedure of the proposed method is much simpler than its bit embedding procedure. Let $\hat{\Phi}$ and $\hat{\Psi}$ be the low-subband and high-subband of coefficients, which were generated by an IWT transform of marked ECG data Θ. Let $\hat{T}_j$ and $\hat{H}_j$ be the *j*-th bundle taken from the low-/high-subband of $\hat{\Phi}$, and the corresponding offset are $d_j = \hat{t}_{j0} - \hat{t}_{j1}$ and $d'_j = \hat{h}_{j0} - \hat{h}_{j1}$. The major steps of bit extraction are described here.

Step 1. Input a bundle $\hat{T}_j$ derived from $\hat{\Phi}$. If the end of input is encountered, then proceed to Step 4.

Step 2. Compute offset $d_j = \hat{t}_{j0} - \hat{t}_{j1}$.

Step 3. If the condition $-\tau \le d_j < 0$ is satisfied, then data bit "1" is extracted, otherwise, data bit "0" is extracted, proceed to Step 1.

Step 4. Input a bundle $\hat{H}_j$ derived from $\hat{\Psi}$. If the end of input is encountered, then proceed to Step 7.

Step 5. Compute offset $d'_j = \hat{h}_{j0} - \hat{h}_{j1}$.

Step 6. If the condition $-\tau \le d'_j < 0$ is satisfied, then data bit "1" is extracted, otherwise, data bit "0" is extracted, proceed to Step 4.

Step 7. Assemble all extracted bits and rebuild the secret message *W*.

Step 8. Stop.

3. EXPERIMENTAL RESULTS

The ECG host signal was obtained from the MIT-BIH arrhythmia database [10]. One set of 27-test-data was taken from Lead-1 in an ECG. The size of each host-data was 30,000, and each data was represented by a 12-bit signed integer. The size of an input gray-scale image (Baboon) was 43 × 43. In addition, the bundle size was 2 and each test-data used various τ-value. Since there are 15,000 coefficients for the low-subband and hig-subbnad of IWT, respectively, the optimal payload for the proposed method is 15,000 / 2 × 2 = 15,000 bits. Hiding performance in terms of SNR and PRD was first presented, and followed by the demonstration of robustness performance. The SNR and PRD are defined as follows:

$$SNR = 10\log_{10}\frac{\sum_i s_i^2}{\sum_i (s_i - \hat{s}_i)^2}, \qquad (1)$$

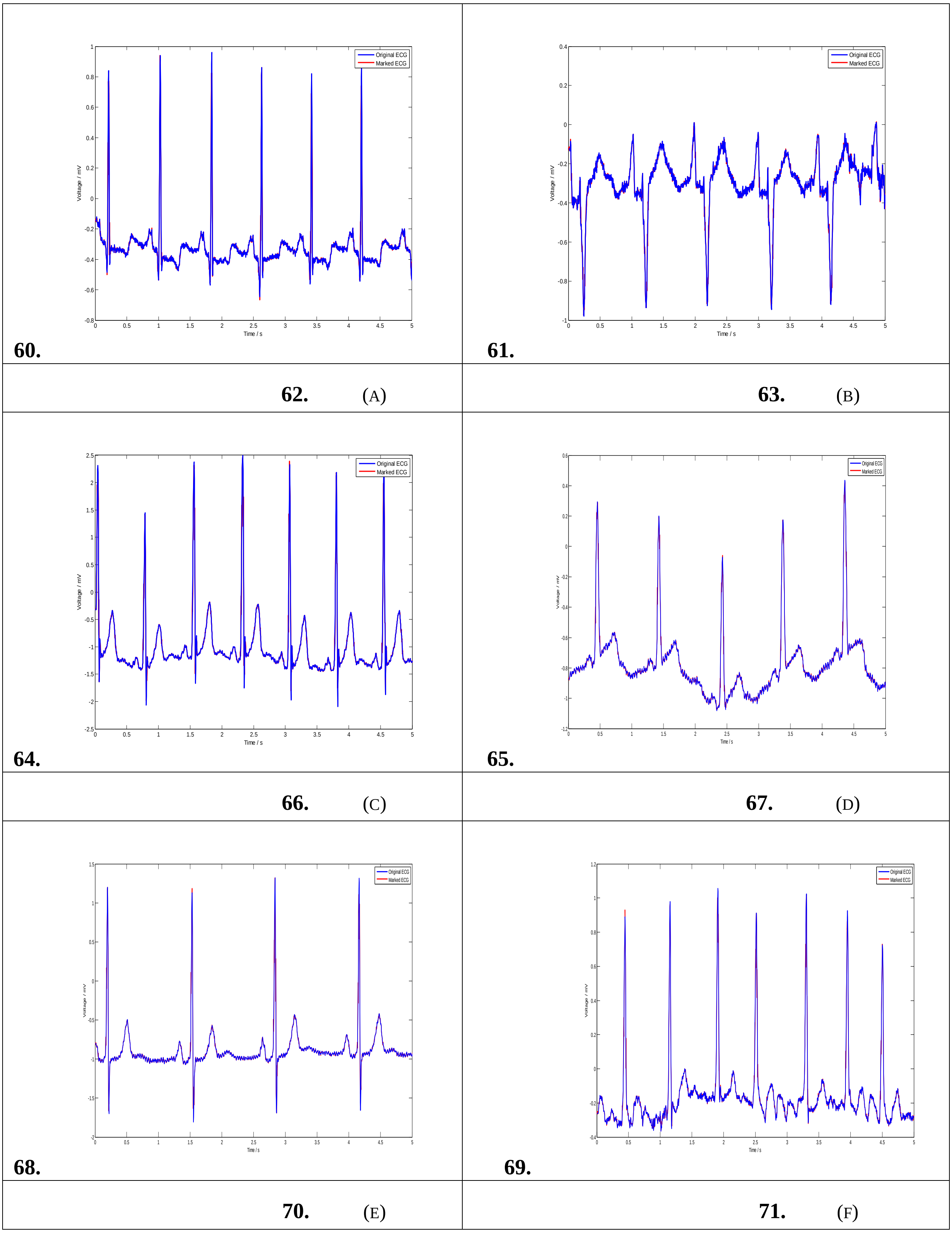
and

$$PRD = \sqrt{\frac{\sum_i (s_i - \hat{s}_i)^2}{\sum_i s_i^2}}, \qquad (2)$$

respectively, where s_i and $\hat{s}_i$ are the values of the coefficients in original ECG and marked ECG, respectively. Table 1 showed the SNR/PRD performance generated by the proposed method with various τ-value. The average SNR and PRD was 42.32 dB and 0.0084, respectively. In addition, the marked ECGs generated from ECG100, ECG108, ECG116, ECG121, ECG123 and ECG201 were depicted in Fig. 2. It is clear that the perceived quality is good. No apparent distortion existed in the marked ECGs. To demonstrate the robustness of the proposed method, examples of survived watermarks from the manipulations of marked ECG100 (using $\tau = 83$) was given in Table 2. A binary logo of size 120 × 120 was used as a test watermark. The value of PRD equals 0 if a marked ECG were not being manipulated. In spite of the PRD of the survived watermark which manipulated by "Inversion" was larger than 1, it was still recognized. From Table 2 we can see that all extracted marked were identified. Performance comparison between our method and He et al.'s technique [5] in terms of SNR/PRD/Payload was listed in Table 3. It is obvious that the performance of proposed method is superior to that of He et al.'s technique [5]. Moreover, the payload size of Tseng et al's techniques [7] was only 32 bits. Although the SNR for Jero et al.'s scheme [8] is around 50 dB, the scheme provided payload only 4,489 bits. Due to the above three methods [5, 7-8] provided a limited size of payload, it may confine their applications when a larger watermark (or secret message) being required.

Table 1. SNR/PRD performance of the proposed method with various τ.

1. ECG **2.** DATA SET	**3.** SNR/PRD/τ
4. 100	**5.** 42.37/0.0076/83
6. 101	**7.** 42.54/0.0075/73
8. 102	**9.** 44.44/0.0060/71
10.103	**11.**38.96/0.0113/121
12.104	**13.**42.06/0.0079/88
14.105	**15.**44.05/0.0063/59
16.106	**17.**40.03/0.0100/125
18.107	**19.**38.62/0.0117/128
20.108	**21.**49.14/0.0035/60
22.109	**23.**43.42/0.0067/55
24.111	**25.**46.76/0.0046/31
26.112	**27.**44.86/0.0057/45
28.113	**29.**38.49/0.0119/129
30.114	**31.**48.05/0.0040/40
32.115	**33.**37.99/0.0126/129
34.116	**35.**33.44/0.0213/129
36.117	**37.**43.87/0.0064/57
38.118	**39.**38.32/0.0121/111
40.119	**41.**38.63/0.0117/104
42.200	**43.**42.18/0.0078/84
44.201	**45.**46.14/0.0049/46
46.202	**47.**46.33/0.0048/47
48.203	**49.**40.64/0.0093/99
50.205	**51.**42.91/0.0072/62
52.207	**53.**47.80/0.0041/37
54.208	**55.**40.38/0.0096/96
56.209	**57.**40.28/0.0097/14
58.*AVERAGE*	**59.**42.32/0.0084/-



60.

61.

62. (A)

63. (B)

64.

65.

66. (C)

67. (D)

68.

69.

70. (E)

71. (F)

Fig. 2. The marked ECGs generated by the proposed method. (a) ECG100, (b) ECG108, (c) ECG116, (d) ECG121, (e) ECG123 and (f) ECG201.

Table 2. Examples of survived watermarks from the manipulations of marked ECG100.
† The last three bits of the marked data were truncated.

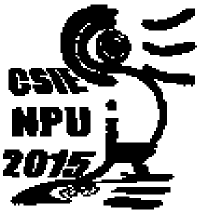
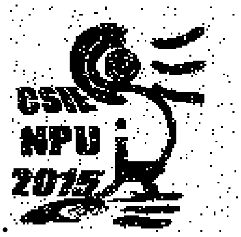
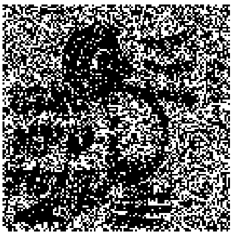
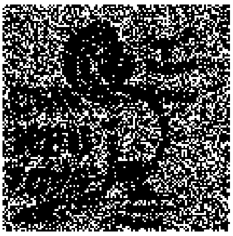
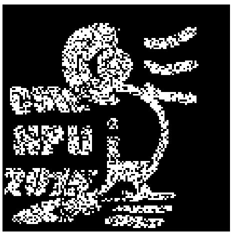
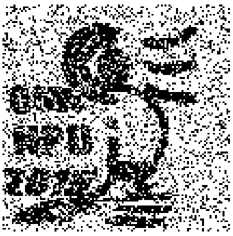
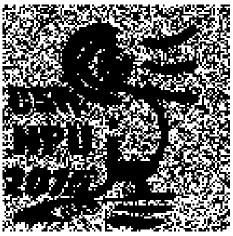
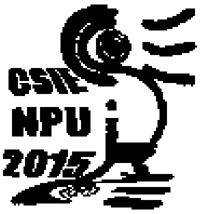
72. ATTACKS	**73.** SURVIVED WATERMARKS	**74.** ATTACKS	**75.** SURVIVED WATERMARKS
76. NULL-ATTACK **77.** PRD = 0	**78.** 	**79.** SCALING (×3) **80.** PRD = 0.1910	**81.** 
82. CROPPING (50%) **83.** PRD = 0.7531	**84.** 	**85.** TRUNCATION† **86.** PRD = 0.8015	**87.** 
88. INVERSION **89.** PRD = 1.1421	**90.** 	**91.** WHITE-GAUSSIAN NOISE (WITH SNR OF 1 DB) PRD = 0.5178	**92.** 
93. SMOOTH (1×2) **94.** PRD = 0.7059	**95.** 	**96.** TRANSLATION (+1000) **97.** PRD = 0	**98.** 

Table 3. SNR/PRD/Payload comparison with He et al. [5].

ECG Data	SNR/PRD/Payload	
	He et al. [5]	Our method
100	30.40/0.0299/32	42.37/0.0076/15,000
101	30.63/0.0354/32	42.54/0.0075/15,000
102	31.78/0.0327/32	44.44/0.0060/15,000
103	32.08/0.0269/32	42.06/0.0079/15,000
Average	31.22/0.0312/32	42.85/0.0072/15,000

4. CONCLUSION

In this work, we present an effective data hiding method for ECG signal based on IWT domain via a simple coefficient adjusting technique. Simulations indicated that the perceived quality in terms of SNR/PRD by the proposed method is good, while hiding capacity is superior to existing techniques. Moreover, the proposed method is tolerant of resisting several manipulations. Since the major operations of the proposed bit embedding procedure include only the computation of increment and decrement, it is feasible for the proposed method applied in real-time applications.

5. REFERENCES

[1] I. J. Cox, M. L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd Ed., Morgan Kaufmann., MA, 2008.

[2] E. Eielinska, W. Mazurczyk, and K. Szczypiorski, “Trends in steganography,” *Comm. of the ACM*, vol. 57, pp. 86-95, 2014.

[3] S. Wang, R. Miyauchi, M. Unoki, and N.S. Kim, “Tampering detection scheme for speech signals using formant enhancement based watermarking,” *J. of Inform. Hiding and Multim. Signal Process.*, vol. 6, pp. 1264-1283, 2015.

[4] A. Ibaida, I. Khalil, and R.V. Schynde, “A low complexity high capacity ECG signal watermark for wearable sensor-net health monitoring system,” *Comput. in Cardiology*, vol. 38, pp.393−396, 2011.

[5] X. He, K.K. Tseng, H.N. Huang, S.T. Chen, S.Y. Tu, F.F. Zeng, and J.S. Pan, “Wavelet-based quantization watermarking for ECG signals,” *Int. Conf. on Comp., Meas., Cont. and Sens. Net.*, pp. 233-236, 2012.

[6] A. Ibaida and I. Khalil, “Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems,” *IEEE T. Biomedical Eng.*, vol. 60, pp. 3322-3330, 2013.

[7] K.K. Tseng, X. He, W.M. Kung, S.T. Chen, M.H. Liao, and H.N. Huang, “Wavelet-based watermarking and compression for ECG signals with verification evaluation,” *Sensors*, vol. 14, pp. 3721-3736, 2014.

[8] S.E. Jero, P. Ramu, and S. Ramakrishnan, “Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission,” *J. of Medical Sys.*, 38:132, s10916-014-0132-z, 2014.

[9] A.R. Calderbank, I. Daubechies, W. Sweldens, and B.L. Yeo, “Wavelet transforms that map integers to integers,” *Applied & Computat. Harmonics Analysis*, vol. 5, pp. 332-369, 1998.

[10] G.B. Moody and R.G. Mark, “The impact of the MIT-BIH arrhythmia database,” *IEEE Eng. in Med. and Biol.*, vol. 20, pp. 45-50, 2001.