World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:12, No:7, 2018

# High Performance Electrocardiogram Steganography Based on Fast Discrete Cosine Transform

Liang-Ta Cheng, Ching-Yu Yang

***Abstract*—**Based on fast discrete cosine transform (FDCT), the authors present a high capacity and high perceived quality method for electrocardiogram (ECG) signal. By using a simple adjusting policy to the 1-dimentional (1-D) DCT coefficients, a large volume of secret message can be effectively embedded in an ECG host signal and be successfully extracted at the intended receiver. Simulations confirmed that the resulting perceived quality is good, while the hiding capability of the proposed method significantly outperforms that of existing techniques. In addition, our proposed method has a certain degree of robustness. Since the computational complexity is low, it is feasible for our method being employed in real-time applications.

***Keywords*—**Data hiding, ECG steganography, fast discrete cosine transform, 1-D DCT bundle, real-time applications.

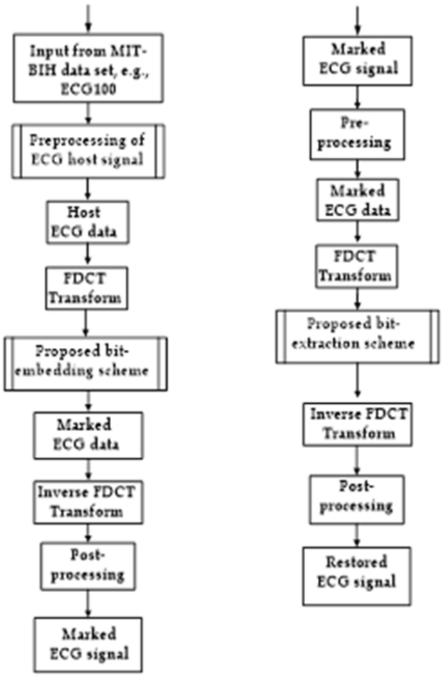
## I. INTRODUCTION

TO prevent a secret (or private) information from being eavesdropped or tampered with during transmission, many researchers have successfully designed data hiding techniques, namely, information steganography and digital watermarking, for multimedia such as images, videos, and audio [1], [2]. Generally speaking, the main goal of a steganographic method is to hide data bits in host media as large as possible while maintaining a good (or an acceptable) perceived quality, whereas the watermarking schemes focus on the achievement of robustness with a limited payload. To embed patient privacy and diagnosis data in biometric media such as ECG signals, several data hiding techniques have been employed in an ECG signal for securing patient information [3]-[6]. Ibaida and Khalil [3] presented a high capacity ECG watermarking technique for a wearable sensor-net health monitoring system based on wavelet transform domain. Simulations confirmed that their method is feasible for point-of-care monitoring systems. Based on discrete wavelet transform, Jero et al. [4] proposed an ECG steganography using encryption and scrambling techniques. Simulations indicated that the method protects patient information effectively while the perceptual quality is good. Based on integer wavelet transform, Yang and Lin [5] embedded secret bits in an ECG host signal via the coefficient adjusting technique. Simulations indicated that the perceived quality is good with a moderate hiding storage. Yang and Wang [6] designed two hiding methods: lossy and reversible ECG steganography for ECG signals. Simulations confirmed that the perceived quality generated by the lossy ECG steganography is good while hiding capability was acceptable. In this article, we present an effective ECG steganography based on FDCT domain.

The remainder of this paper is organized as follows. Section II describes the procedures of bit embedding and bit extraction. Section III presents the experimental results, and Section IV provides the conclusion.

## II. PROPOSED METHOD

To provide a high hiding storage with resistance against manipulations, the proposed method embeds a secrete message in 1-D DCT coefficients domain. Namely, an ECG host signal is first transformed into a series of non-overlapping DCT bundles with the size of 1 × $n$ via FDCT [7]-[9]. Then, data bits are embedded in the target coefficients of a DCT bundle. The block diagram of the proposed method is depicted in Fig. 1. The details of bit embedding and bit extraction for our methods are specified in the following sections.



(a) (b)

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

L. T. Cheng is with the National Penghu University of Science and Technology, 300, Liu-Ho Rd., Magong, Penghu, 880 Taiwan (e-mail: mk1043@mksh.phc.edu.tw).

C. Y. Yang is with the National Penghu University of Science and Technology, 300, Liu-Ho Rd., Magong, Penghu, 880 Taiwan (corresponding author, phone: 886-6-9267115; fax: 886-6-9260047; e-mail: chingyu@gms.npu.edu.tw).

### *A. Bit-Embedding*

Let $\Omega = \{A_j \mid j = 1,2,\ldots,|\Omega|\}$ be the host ECG data, where $A_j$ is the *j*th bundle of Ω with the size of 1 × *n*. Also let $\mathrm{I} = \{H_j \mid j = 1,2,\ldots,|\mathrm{I}|\}$ be the 1-D DCT coefficients, which obtained by performing forward FDCT from Ω with $H_j = round(10 \times A_j\mathbf{X})$ and **X** being a predetermined 8 × 8 matrix which defined as:

$$X = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \frac{3}{2} & \frac{5}{4} & \frac{3}{4} & \frac{3}{8} & -\frac{3}{8} & -\frac{3}{4} & -\frac{5}{4} & -\frac{3}{2} \\ 1 & \frac{1}{2} & -\frac{1}{2} & -1 & -1 & -\frac{1}{2} & \frac{1}{2} & 1 \\ \frac{5}{4} & -\frac{3}{8} & -\frac{3}{2} & -\frac{3}{4} & \frac{3}{4} & \frac{3}{2} & \frac{3}{8} & -\frac{5}{4} \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \frac{3}{4} & -\frac{3}{2} & \frac{3}{8} & \frac{5}{4} & -\frac{5}{4} & -\frac{3}{8} & \frac{3}{2} & -\frac{3}{4} \\ \frac{1}{2} & -1 & 1 & -\frac{1}{2} & -\frac{1}{2} & 1 & -1 & \frac{1}{2} \\ \frac{3}{8} & -\frac{3}{4} & \frac{5}{4} & -\frac{3}{2} & \frac{3}{2} & -\frac{5}{4} & \frac{3}{4} & -\frac{3}{8} \end{bmatrix}^{-1}. \qquad (1)$$

The *round*() is the round function. Without loss of generality, let $H_j = \{s_{ji}\}_{i=0}^{n-1}$ be the *j*-th bundle of size *n* taken from I, as shown in Fig. 2, with *n* = 8 and $\phi$ be the (desired) number of secret bits to be embedded in a host bundle $H_j$. The main procedure of bit embedding of the proposed method is described in the following algorithm.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $s_{j7}$ | $s_{j6}$ | $s_{j5}$ | $s_{j4}$ | $s_{j3}$ | $s_{j2}$ | $s_{j1}$ | $s_{j0}$ |

Fig. 2 Bundle of size 8

Algorithm 1. Hiding a secret message in host ECG data.

Input: Host ECG data Ω, secret message *W*, and a control integer $\phi$.

Output: Marked ECG data $\tilde{\Omega}$.

Method:

Step 0. Perform forward FDCT from Ω to obtain 1-D DCT bundles I.

Step 1. Input a bundle $H_j$ derived from I and let *k* = 1. If the end of input is encountered, then proceed to Step 6.

Step 2. If $k > \phi$, then repeat to Step 1.

Step 3. Input a data bit $b_i$ from *W*.

Step 4. If $b_i = 1$, then execute the following sub-steps:

Step 4.1. If $|s_{jk}| > \frac{\sum_{a=0}^{k-1}|s_{ja}|}{k}$, then do nothing; otherwise, compute $s_{jk} = \left\lfloor (\sum_{a=0}^{k-1}|s_{ja}|)/k \right\rfloor + 1$ if $s_{jk} \ge 0$; or $s_{jk} = -\left\lfloor (\sum_{a=0}^{k-1}|s_{ja}|)/k \right\rfloor - 1$ if $s_{jk} < 0$.

Step 4.2. Evaluate *k* = *k* + *1*, and go to Step 2.

Step 5. If $b_i = 0$, then execute the following sub-steps:

Step 5.1. If $|s_{jk}| \le \frac{\sum_{a=0}^{k-1}|s_{ja}|}{k}$, then do nothing; otherwise, compute $s_{jk} = \left\lfloor (\sum_{a=0}^{k-1}|s_{ja}|)/k \right\rfloor$ if $s_{jk} \ge 0$; or $s_{jk} = -\left\lfloor (\sum_{a=0}^{k-1}|s_{ja}|)/k \right\rfloor$ if $s_{jk} < 0$.

Step 5.2. Evaluate *k* = *k* + *1*, and go to Step 2.

Step 6. Perform inverse FDCT from the marked bundles and form marked ECG data.

Step 7. Stop.

Note that at the Step 6 the marked ECG data $\tilde{\Omega} = \{\tilde{A}_j \mid j = 1,2,\ldots,|\tilde{\Omega}|\}$ was obtained by conducting inverse FDCT from the marked DCT bundles $\hat{\mathrm{I}} = \{\hat{H}_j \mid j = 1,2,\ldots,|\hat{\mathrm{I}}|\}$, where $\tilde{A}_j = round(\hat{H}_j \times inv(\mathbf{X}))$.

### *B. Bit-Extraction*

The decoding part of the proposed method is much easier than its encoding part. The primary steps of the proposed bit extraction are specified here.

Algorithm 2. Extracting hidden message from mark ECG data.

Input: Marked ECG data $\tilde{\Omega}$, and a control integer $\phi$.

Output: A secret message *W* (and host ECG data)

Method:

Step 0. Perform forward FDCT from $\tilde{\Omega}$ to obtain 1-D DCT bundles $\hat{\mathrm{I}} = \{\hat{H}_t \mid t = 1,2,\ldots,|\hat{\mathrm{I}}|\}$, where $\hat{H}_t = \hat{H}_t / 10$.

Step 1. Input a bundle $\hat{H}_t$ derived from I and let *k* = 1. If the end of input is encountered, then proceed to Step 5.

Step 2. If $k > \phi$, then repeat to Step 1.

Step 3. If $|\hat{s}_{jk}| > \frac{\sum_{a=0}^{k-1}|\hat{s}_{ja}|}{k}$, then data bit "1" was collected, otherwise, data bit "0" was obtained.

Step 4. Compute *k* = *k* + *1*, and go to Step 2.

Step 5. Assemble all extracted bits and rebuild the secret message (and perform inverse FDCT from $\hat{\mathrm{I}}$ to obtain ECG data).

Step 6. Stop.

## III. EXPERIMENTAL RESULTS

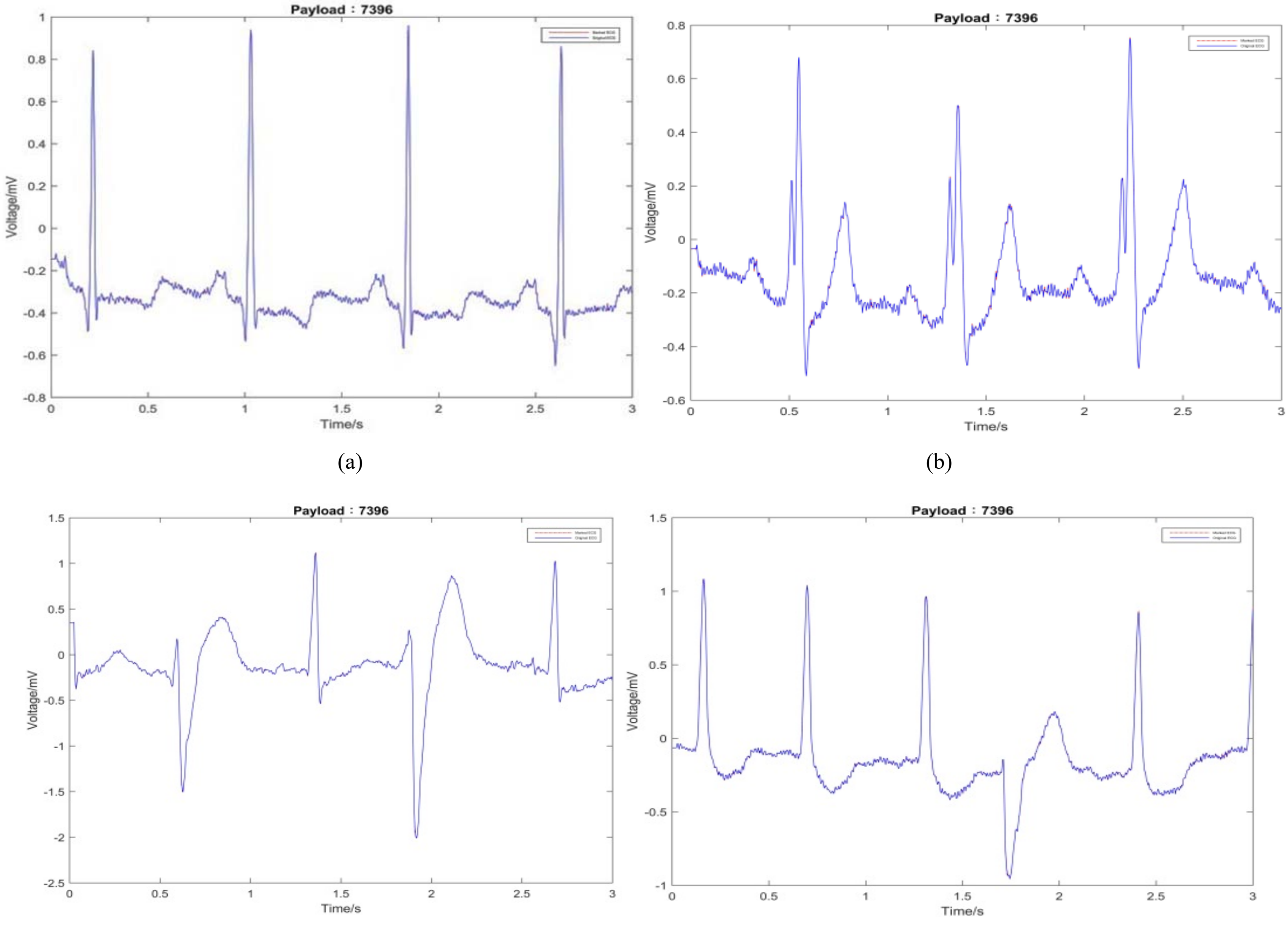
All simulations were performed in MATLAB (R2015b) programming language under the platform of Microsoft Windows 10 and an Intel Core (TM) i5-6300U 2.4 GHz Laptop with 8 GB RAM. The average execution time for the proposed algorithms was about 0.061 s. The ECG signal was obtained from the MIT-BIH arrhythmia database [10]. Several sets of host ECG data were employed in our experiments. The size of each host ECG data was 30,000. Besides, the size of a DCT bundle was 8. Namely, the optimal hiding capacity for the proposed method is (30,000 / 8) × 6 = 22,500 bits if the control integer $\phi$ was set 6. Table I indicated the SNR/PRD performance generated by the proposed method (using $\phi = 4$) with a payload of size 14,400 bits. The input watermark used here was an image of size 120 × 120. The average SNR and PRD was 54.63 dB and 0.0019. The SNR and PRD are defined as:

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

and

$$PRD = \sqrt{\frac{\sum_i (s_i - (\hat{s}_i/10))^2}{\sum_i s_i^2}}, \tag{3}$$

respectively, where $s_i$ and $\hat{s}_i$ are the data in original ECG and marked ECG, respectively. Moreover, close observation of the host and marked ECGs (at the beginning of 3-second) generated from ECG100, ECG111, ECG200, ECG210, ECG220 and ECG230 with two payloads in different size were depicted in Figs. 3 and 4, respectively. It is clear that the perceived quality is very good. No apparent distortion existed in the marked ECGs. Performance comparison between our method and existing techniques [5], [6] in terms of SNR/PRD/Payload was listed in Table II. It is clear that the hiding capability of the proposed method is the best among the compared methods while both the SNR and PRD are still superior to other two techniques [5], [6]. Notice that there are 5-bit embedded in each DCT bundle, the resulting payload for our method is (30,000 / 8) × 5 = 18,750 bits. Moreover, the robustness of the proposed method and examples of survived watermarks from the manipulations of marked ECG111 were given in Table III. The value of PRD equals 0 if a marked ECG were not attacked. Although the marked ECGs had been manipulated by noise addition, truncation, scaling, and translations, it can be seen from Table III that the extracted watermarks were identified. In spite of marked ECG manipulated by "Inversion" and "translation," the values of PRD for the survived watermarks were 0. This implies that the absolute operation at the Step 4 in Algorithm 1 is tolerant of both kinds of attacks. From Table III, we can conclude that our proposed method has a certain degree of robustness. In the other words, the proposed method has the merits of high capacity, high SNR with robustness. The features are rarely existed in the conventional ECG steganography.

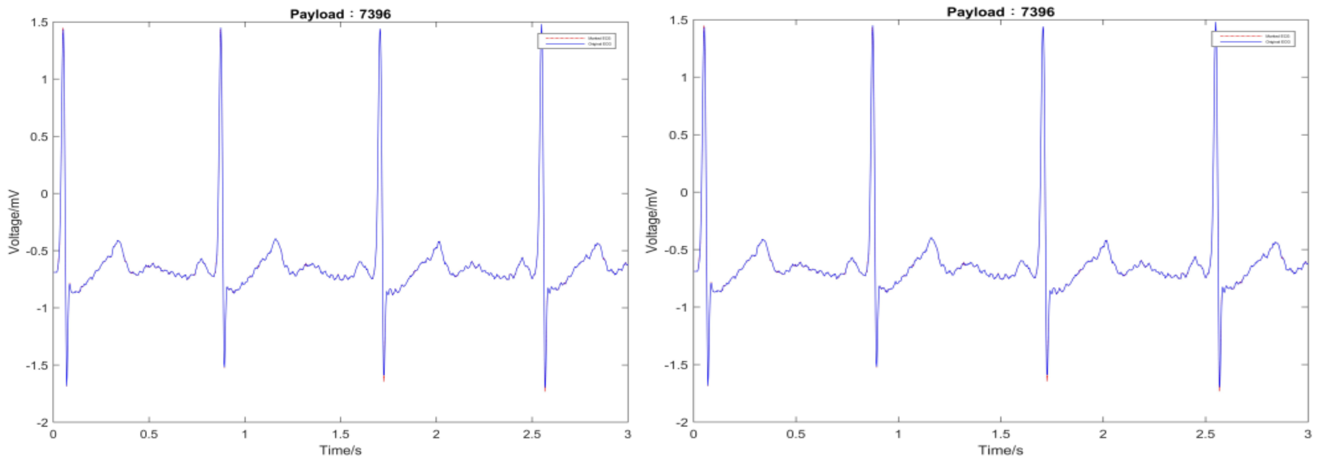


(a)

(b)

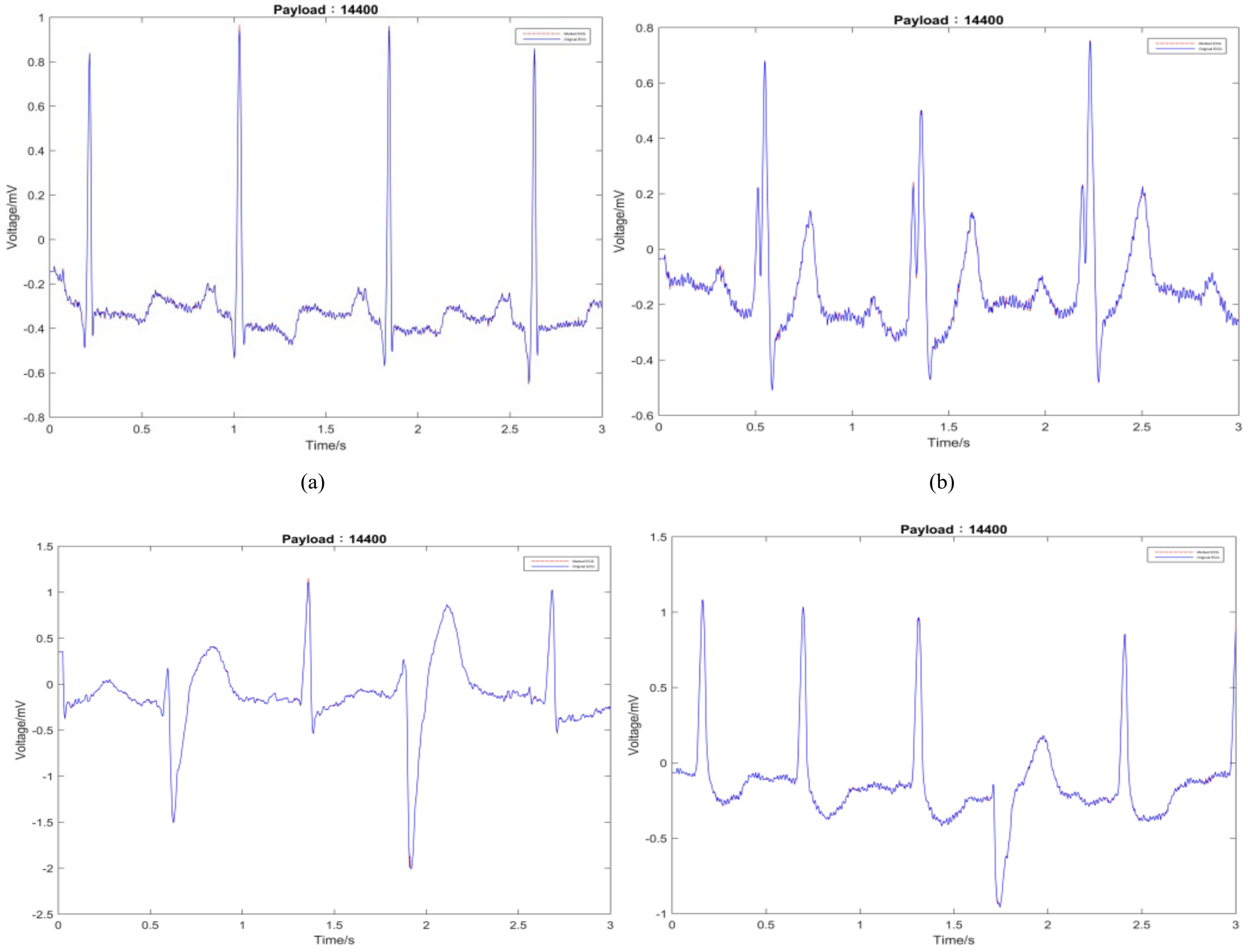
(c)

(d)



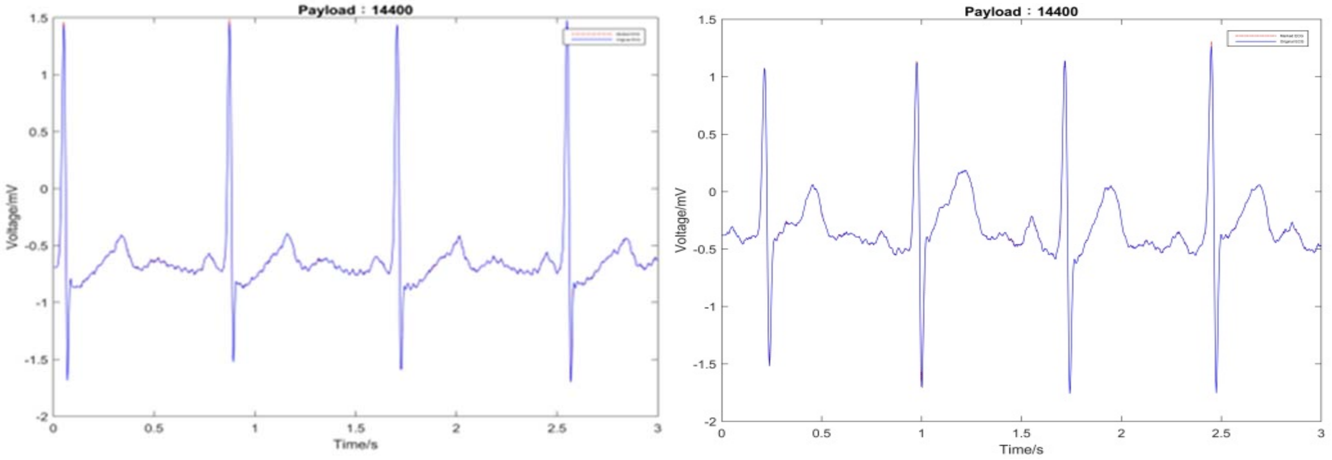
(e) (f)

Fig. 3 Close observation of the host and marked ECGs generated by the proposed method with payload size of 7,396 bits. (a) ECG100, (b) ECG111, (c) ECG200, (d) ECG210, (e) ECG220 and (f) ECG230



(a) (b)

(c) (d)



(e) (f)

Fig. 4 Close observation of the host and marked ECGs generated by the proposed method with payload size of 14,400 bits. (a) ECG100, (b) ECG111, (c) ECG200, (d) ECG210, (e) ECG220 and (f) ECG230

TABLE I
SNR/PRD PERFORMANCE OF THE PROPOSED METHOD

| ECG data set | SNR/PRD |
|---|---|
| 100 | 55.97/0.0016 |
| 101 | 54.91/0.0018 |
| 102 | 53.52/0.0021 |
| 103 | 52.72/0.0023 |
| 104 | 49.90/0.0032 |
| 111 | 57.95/0.0013 |
| 112 | 57.57/0.0013 |
| 113 | 52.01/0.0025 |
| 114 | 58.00/0.0013 |
| 115 | 52.99/0.0022 |
| 121 | 59.43/0.0011 |
| 122 | 53.44/0.0021 |
| 123 | 53.20/0.0022 |
| 124 | 54.72/0.0018 |
| 200 | 54.99/0.0018 |
| 201 | 58.32/0.0012 |
| 202 | 57.87/0.0013 |
| 203 | 50.94/0.0028 |
| 210 | 57.86/0.0013 |
| 212 | 53.58/0.0021 |
| 213 | 50.26/0.0030 |
| 214 | 54.68/0.0018 |
| 215 | 54.77/0.0018 |
| 220 | 49.64/0.0033 |
| 221 | 55.26/0.0017 |
| 222 | 58.01/0.0013 |
| 223 | 53.65/0.0021 |
| 230 | 53.36/0.0021 |
| *Average* | 54.67/0.0019 |

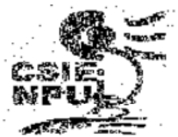
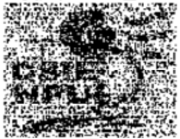
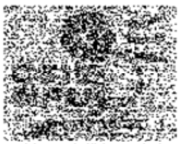
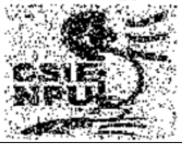
## IV. CONCLUSION

In this work, we present an effect data hiding method for ECG signal based on FDCT. Simulations confirmed that a large volume of secret bits can be embedded in an ECG host signal via simple offset adjustment to 1-D DCT coefficients. In additions, the hiding capacity, SNR, and PRD of the proposed method are superior to existing techniques. Moreover, the proposed method has a certain degree of robustness to against manipulations. Since the processing time of bit-embedding and bit-extraction is fast, it is suitable for the proposed method to implement in real-time applications.

TABLE II
SNR/PRD/PAYLOAD COMPARISON WITH VARIOUS METHODS

| ECG Data | SNR/PRD/Payload | | |
|---|---|---|---|
| | Yang & Lin [5] | Yang & Wang [6] | Our method |
| 100 | 42.37/0.0076/ 15,000 | 41.85/0.0081/ 14,806 | 48.25/0.0039/ 18,750 |
| 101 | 42.54/0.0075/ 15,000 | 41.94/0.0080 /14,794 | 47.57/0.0042/ 18,750 |
| 102 | 44.44/0.0060/ 15,000 | 44.04/0.0063/ 14,778 | 47.80/0.0041/ 18,750 |
| 103 | 38.96/0.0113/ 15,000 | 38.84/0.0114/ 14,858 | 45.60/0.0053/ 18,750 |
| 104 | 42.06/0.0079/ 15,000 | 41.17/0.0087/ 14,790 | 45.77/0.0051/ 18,750 |
| 200 | 42.18/0.0078/ 15,000 | 42.14/0.0078/ 14,826 | 49.10/0.0035/ 18,750 |
| 201 | 46.14/0.0049/ 15,000 | 45.72/0.0052/ 14,828 | 52.46/0.0024/ 18,750 |
| 202 | 46.33/0.0048/ 15,000 | 46.34/0.0048/ 14,760 | 53.02/0.0022/ 18,750 |
| 203 | 40.64/0.0093/ 15,000 | 40.05/0.0099/ 14,762 | 46.80/0.0046/ 18,750 |
| 230 | 38.93/0.0113/ 15,000 | 39.08/0.0111/ 14,902 | 44.50/0.0060/18,750 |
| 231 | 39.77/0.0103/ 15,000 | 39.92/0.0101/ 14,898 | 45.79/0.0051/ 18,750 |
| 232 | 46.96/0.0045/ 15,000 | 46.63/0.0045/ 14,860 | 52.71/0.0023/ 18,750 |
| 233 | 39.70/0.0104/ 15,000 | 39.52/0.0106/ 14,872 | 46.96/0.0045/ 18,750 |
| *Aver.* | 42.39/0.0080/ 15,000 | 42.10/0.0082/ 14,826 | 48.18/0.0041/ 18,750 |

TABLE III
EXAMPLES OF SURVIVED WATERMARKS FROM THE MANIPULATIONS OF MARKED ECG111

| Attacks | Survived Watermarks |
|---|---|
| Null-attack<br>PRD = 0 |  |
| Inversion<br>PRD = 0 |  |
| Scaling (×5)<br>PRD = 0.3320 |  |
| Scaling (×0.5)<br>PRD = 0.6126 |  |
| Translation (+1000)<br>PRD = 0 |  |
| Truncation†<br>PRD = 0.6406 |  |
| White-Gaussian noise<br>(with SNR of 3 dB)<br>PRD = 0.3621 |  |
| White-Gaussian noise<br>(with SNR of 1 dB)<br>PRD = 0.4357 |  |

† The last three bits of the marked data were truncated.

## 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] 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.
[4] 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., vol. 38, s10916-014-0132-z, 2014.
[5] C. Y. Yang and K. T. Lin, "Hiding data in electrocardiogram based on IWT domain via simple coefficient adjustment," The 4th Int. Conf. on Annual Conference on Engineering and Information Technology, March 29-31, Kyoto, Japan, 2016.
[6] C. Y. Yang and W. F. Wang, "Effective electrocardiogram steganography based on coefficient alignment," Journal of Medical Sys., vol. 40, s10916-015-0426-9, 2016.
[7] W. H. Chen, C. H. Smith, and S. C. Fralick, "A fast computational algorithm for the discrete cosine transform," IEEE T. Comm., vol. COM-25, pp. 1004-1009, 1977.
[8] E. Feig and S. Winograd, "Fast algorithm for the discrete cosine transform," IEEE T. Signal Proc., vol. 40, pp. 2174-2193, 1992.
[9] J. Liang and T. D. Tran, "Fast multiplierless approximations of the DCT with the lifting scheme," IEEE T. Signal Proc., vol. 49, pp. 3032-3044, 2001.
[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.