Adaptive Electrocardiogram Steganography Based on 2D Approach with Predetermined Rules

Ching Yu Yang*, Chi-Ming Lai, Hung-Chang Lin, Ting-Ying Lin, Ruei-Long Lu

Department of Computer Science and Information Engineering
National Penghu University of Science and Technology
Magong, Penghu, Taiwan

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

ABSTRACT— ***Based on two-dimensional (2D) bit-embedding/-extraction approach, we propose a simple data hiding for electrocardiogram (ECG) signal. The patient's sensitive (diagnostic) data can be efficiently hidden into 2D ECG host via the proposed decision rules. The performance of the proposed method using various sizes of the host bundles was demonstrated. Simulations have confirmed that the average SNR of the proposed method with a host bundle of size 3 × 3 is superior to that of existing techniques, while our payload is competitive to theirs. In addition, our method with a host bundle of size 2 × 2 generated the best SNR values, while that with a host bundle of size 4 × 4 provided the largest payload among the compared methods. Moreover, the proposed method provides robustness performance better than existing ECG steganography. Namely, our method provides high hiding capacity and robust against the attacks such as cropping, inversion, scaling, translation, truncation, and Gaussian noise-addition attacks. Since the proposed method is simple, it can be employed in real-time applications such as portable biometric devices.***

Keywords— Data Hiding, ECG Steganography, 2D Bit-embedding/-extraction Approach, Real-time Applications

1. INTRODUCTION

Due to ubiquitous and smart services provided from the Internet, many promising applications can be found in (cloud) computing networks and be usable in hosts and portable devices. It is obvious that a large volume of information (stream) goes through the Internet all the time around the world. The packet streams may contain vital data such as commercial transaction details of the companies, important documents of the organizations, personal sensitive message (or privacy), and so on. However, data could be eavesdropped and tampered with during transmission by third parties. Instead of using encryption and decryption systems, data hiding techniques provided an alternative and economic solution in data security [1-2]. Namely, an important data (or secret message) can be effectively hidden in multimedia such as documents, images, and video with no apparent distortion of the host media via steganography or digital watermarking. In general, the steganographic methods are employed to achieve the goal of providing a high hiding-capacity with imperceived quality, while a major purpose of digital watermarking is robustness performance with a limited payload [3-6]. Due to the necessity of embedding patient's diagnosis (and personal dada) in biometrics and the use of portable healthcare equipment, several researchers have developed data hiding algorithms in electrocardiogram (ECG), electroencephalogram (EEG), and electromyogram (EMG) signals. Some authors have proposed reversible data hiding in biometrics that not only can embed/extract secret bit in/from ECG host but also completely restore the original host without distortion [7-9]. To obtain robustness and secure authorized message, several scholars have presented ECG watermarking schemes to achieve the goal [10-11]. Most of the ECG steganographic methods are irreversible schemes [12-18], however, those methods often provide a high hiding capability and good resultant perceived quality with low error rate. Since our approach is an irreversible ECG steganography, only related topic is surveyed in this section.

Based on wavelet transform, Ibaida and Khalil [12] proposed an ECG steganography for protecting patient's diagnosis in point-of-care systems. To secure secret data, the method combined employed encryption and scrambling techniques. Simulations confirmed that the method provided high security protection with low bit error rate. Jero et al. [13] used discrete wavelet transform (DWT) to decompose signals and singular value decomposition (SVD) so as to

embed data bits into the decomposed ECG signal. The novelty of the method was using SVD technique to embed secret message in 2D ECG host. Demonstrations indicated that the high-high sub-band of SVD was an ideal one to hide data. In addition, the signal degradation was less than 0.6% even if the number of secret bits is larger than the size of the sub-band. Based on curvelet transform domain, Jero et al. [14] successfully embed watermark bits in an ECG host. By adaptive selection of watermark position with the control thresholds, data bits can be effectively embedded in the curvelet coefficients with less distortion. Simulations validated that coefficients around zero were feasible for hiding secret bit with the minimum degradation of perceived quality.

Yang and Wang [15] used a simple coefficient adjustment technique to embed secret message in ECG signals. Simulations confirmed that the perceived quality generated by the method was good, while hiding capability was not bad. In addition, the reversible ECG staganography can not only hide secret messages but also completely restore the original ECG signal after bit extraction. By preprocessing of 1D ECG signal via SVD and 2D DWT techniques, Jero et al. [16] utilized continuous ant colony optimization and developed an ECG steganography scheme. Experimental results indicated that 11% decrease in imperceptibility for 30% increase in data bits. In addition, the hidden message can be extracted in error free at receiver site. Yang and Wang [18] employed an absolute-value-decision policy and effectively promote the SNR performance of the Yang and Wang's scheme [17] without using overhead information. Furthermore, the number of data bits can be hidden elastically in the ECG hosts. Experimental results showed that the average SNR of the method was better than that of the Yang and Wang scheme [17] about 3.54 dB. To obtain a high perceived quality with robustness performance, we employ 2D ECG steganography with the predetermined rules to achieve the goal. The remainder of this study is organized as follows. Sec. 2 specifies the process of bit embedding and bit extraction of our proposed method. Sec. 3 demonstrates the simulation results, and Sec. 4 gives brief conclusion.

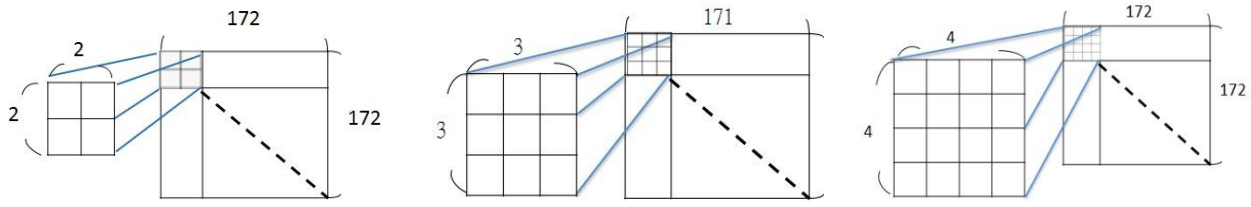
2. PROPOSED METHOD

First, an input one-dimensional (1D) ECG data H was converted into 2D form H′. Then, a series of host bundles of size $n \times n$ were derived from H′, data bits can be sequentially embedded in the host bundles. To obtain a good perceived quality, at most $(n\text{-}1) \times n$ secret bits can be embedded in a host bundle at a time. The host bundles with various size, namely, 2×2, 3×3, and 4×4 that obtained from 2D ECG data is illustrated in Figs. 1(a)-1(c). For example, if the size of the jth host bundle $H'_j = \{s_{ji}\}_{i=0}^{n^2-1}$ is $n \times n$, as shown in Fig. 1(d) with $n = 3$. Assuming that an input 1D ECG consists of K samples, the size of H′ is $N \times N$ with $N = \left\lfloor 10^{\frac{\log K}{2}} \right\rfloor$, where N is divisible by n. As a result, the number of the host bundles is $N/n \times N/n$. The optimal payload of the proposed method would be $(N/n) \times (N/n) \times (n-1) \times n = \frac{(n-1)N^2}{n}$ bits. The embedding procedure of the proposed method consists of two stages. At the first stage, one data bit can be hidden into each row of a host bundle according to the decision rule 1, namely,

$$\left| s_{j0} - s_{j1} \right| \le \tau. \tag{1}$$

At the second stage, the next input bit is tries to be embedded in the same row of the bundle according to the decision rule 2, namely,

$$\left| \frac{s_{j0}+s_{j1}}{2} - s_{j2} \right| \le \tau. \tag{2}$$



(a) (b) (c)

s_{j0}	s_{j1}	s_{j2}
s_{j3}	s_{j4}	s_{j5}
s_{j6}	s_{j7}	s_{j8}

(d)

Figure 1: The host bundles with various size that obtained from the 2D ECG. (a) 2 × 2, (b) 3 × 3, (c) 4 × 4, and (d) the jth host bundle of size 3×3

An offset alignment may be employed in the host bundles so as to solve the issue of violation. Here τ is a control integer. It is clear that two data bits can be embedded in the host bundle as the above two decision rules were satisfied. If either rule 1 or rule 2 is satisfied, then only one data bit can be hidden in the bundle. However, if none of criterion is satisfied, then the bundle carries no data bit. A bundle with no data bit is referred to as a skipped bundle. Note that there is no need to write down the corresponding position of a skipped bundle. Because, the skipped bundles were easily determined from the receiver via the above two rules. The major steps of bit embedding and bit extraction of the proposed method are summarized in the following sections.

2.1 Data Embedding Scheme

The main steps of bit embedding are described in the following algorithm.

Algorithm 1. Hiding secret bit in an ECG host.

Input: Host 1D ECG data $H = \{s_k\}_{k=0}^{|H-1|}$, the size of the host bundle n, an integer τ, and a secret message W.

Output: Marked ECG data $\widetilde{H}$.

Method:

Step 0. Convert H into 2D ECG form H' with $H' = \{H_j \mid j = 1,2,\ldots,(N \times N)\}$.

Step 1. Set parameter $m = 0$ and input a bundle, say $H_j = \{s_{ji}\}_{i=0}^{n^2-1}$ from H'. If the end of input is encountered, then go to Step 9.

Step 2. If the condition of $m < n$, then set index $p = m \times n$, otherwise, return to Step 1.

Step 3. Compute the offset $\mu = s_{jp} - s_{j(p+1)}$, if $|\mu| > \tau$ is satisfied, then go to Step 6, otherwise, input a data bit b_1 from W.

Step 4. If both conditions of $b_1 = 1$ and $-\tau \le \mu < 0$ are satisfied, then go to Step 6, namely, the bundle carries data bit "1." Otherwise, if $b_1 = 1$, then repeatedly adjust the value of μ by increasing $s_{j(p+1)}$ by 1 and decreasing s_{jp} from 1 simultaneously until $-\tau \le \mu < 0$ being reached, go to Step 6.

Step 5. If both conditions of $b_1 = 0$ and $0 \le \mu \le \tau$ are satisfied, then go to the next step, namely, the bundle carries data bit "0." Otherwise, if $b_1 = 0$, then repeatedly adjust the value of μ by increasing s_{jp} by 1 and decreasing $s_{j(p+1)}$ from 1 simultaneously until $0 \le \mu \le \tau$ being reached**.**

Step 6. Compute the offset $\upsilon = \frac{s_{jp} + s_{j(p+1)}}{2} - s_{j(p+2)}$, if $|\upsilon| > \tau$ is satisfied, then set $m = m + 1$, $p = m \times n$, and go to Step 2; otherwise, input a data bit b_2 from W.

Step 7. If both conditions of $b_2 = 1$ and $-\tau \le \upsilon < 0$ are satisfied, then set $m = m + 1$, $p = m \times n$, and go to Step 2, namely, the bundle carries data bit "1." Otherwise, if $b_2 = 1$, then repeatedly adjust the value of υ by increasing $s_{j(p+2)}$ by 1 and decreasing both s_{jp} and $s_{j(p+1)}$ from 1 simultaneously until $-\tau \le \upsilon < 0$ being reached. Set $m = m + 1$, $p = m \times n$, and go to Step 2.

Step 8. If both conditions of $b_2 = 0$ and $0 \le \upsilon \le \tau$ are satisfied, then set $m = m + 1$, $p = m \times n$, and go to Step 1, namely, the bundle carries data bit "0." Otherwise, if $b_2 = 0$, then repeatedly adjust the value of υ by increasing both s_{jp} and $s_{j(p+1)}$ by 1 and decreasing $s_{j(p+2)}$ from 1 simultaneously until $0 \le \upsilon \le \tau$ being reached. Set $m = m + 1$, $p = m \times n$, and go to Step 2.

Step 9. Restore marked 1D ECG data $\widetilde{H}$ from the marked 2D ECG H'.

Step 10. Stop.

2.2 Data Extraction Scheme

The process of bit extraction is much simpler than that of bit embedding. The major steps of bit extraction are given in the following algorithm.

Algorithm 2. Extracting hidden message from marked ECG.

Input: Marked ECG data $\tilde{H}$, the size of the host bundle *n*, and an integer τ.

Output: A secret message *W*.

Method:

Step 0. Convert $\tilde{H}$ into 2D ECG form $\hat{H}$ with $\hat{H} = \{H_j \mid j = 1,2,...,(N \times N)\}$.

Step 1. Set parameter $m = 0$ and input a bundle, say $H_j = \{\hat{s}_{ji}\}_{i=0}^{n^2-1}$ from $\hat{H}$. If the end of input is encountered, then go to Step 7.

Step 2. If the condition of $m < n$, then set index $p = m \times n$, otherwise, return to Step 1.

Step 3. Compute the offset $\mu = \hat{s}_{jp} - \hat{s}_{j(p+1)}$, if $|\mu| > \tau$ is satisfied, then go to Step 5.

Step 4. If $-\tau \le \mu < 0$ is satisfied, then data bit "1" can be identified, otherwise, data bit "0" is recognized.

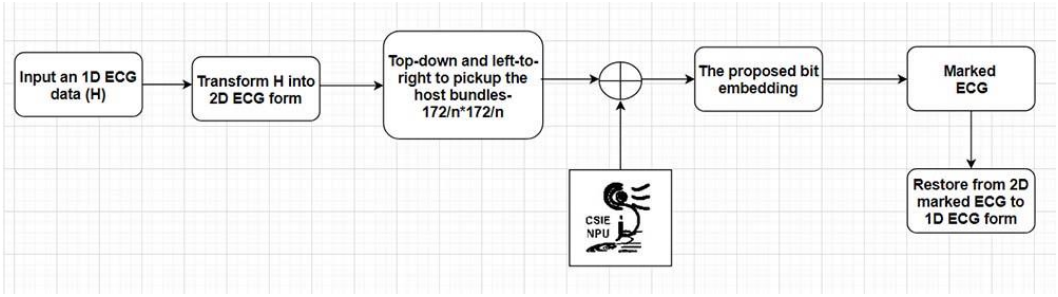
Step 5. Compute the offset $\upsilon = \frac{\hat{s}_{jp} + \hat{s}_{j(p+1)}}{2} - \hat{s}_{j(p+2)}$ if $|\upsilon| > \tau$ is satisfied, then set $m = m + 1$, $p = m \times n$, go to Step 2.

Step 6. If $-\tau \le \upsilon < 0$ is satisfied, then data bit "1" can be recognized, otherwise, data bit "0" is identified. Set $m = m + 1$, $p = m \times n$, and go to Step 2.

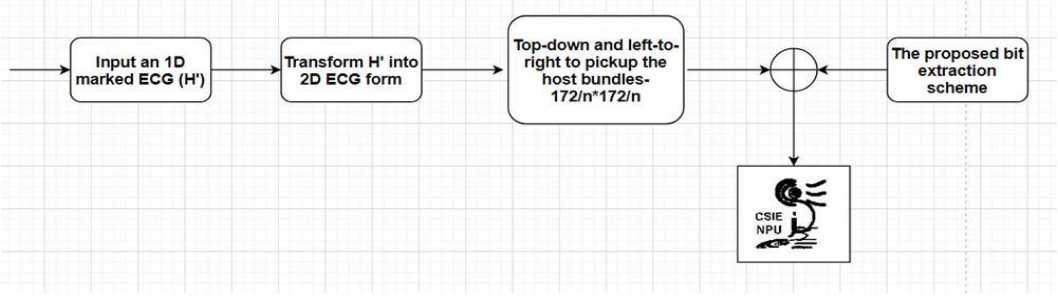
Step 7. Assemble all extracted bits and rebuild the secret message *W*.

Step 8. Stop.

As described previously, the optimal payload of the proposed method with no skipped bundles is $\frac{(n-1)N^2}{n}$ (or approximated to N^2 as $n >> 1$). In other words, the maximum payload for our method using the host bundles of size 2, 3 and 4 are $\frac{172}{2} \times \frac{172}{2} \times 2 = 14{,}792$, $\frac{171}{3} \times \frac{171}{3} \times 6 = 19{,}494$, and $\frac{172}{4} \times \frac{172}{4} \times 12 = 22{,}188$ bits, respectively, as an input ECG host consists of 30,000 samples. In addition, the value of τ is not necessarily a fixed value. The less the value of τ, the larger the SNR value, and vice versa. However, the proposed method with the larger τ provide better robustness performance than that with the smaller τ. A block diagram of the proposed method with the size of host bundle is *n* is depicted in Fig. 2.



(a)



(b)

Figure 2: Block diagram of the proposed method with the bundle of size *n*. (a) Encoder and (b) decoder

3. EXPERIMENTAL RESULTS

Demonstrations of our method have been implemented on an Intel(R) Core™i5-6300HQ Laptop with 8 GB RAM. The average CPU time for the proposed method (including I/O) was less than 0.12 s. The test ECG signals were obtained from the MIT-BIH arrhythmia database [19]. Each input ECG host consists of 30,000 samples. The size of a bundle was set to 3. Two objective measurements signal-to-noise-ratio (SNR) and percentage residual difference (PRD) are used for performance evaluation. They are defined as follows:

$$SNR = 10\log_{10}\frac{\sum_i s_i^2}{\sum_i (s_i - \hat{s}_i)^2} \tag{3}$$

and

$$PRD = \sqrt{\frac{\sum_i (s_i - \hat{s}_i)^2}{\sum_i s_i^2}}, \tag{4}$$

where s_i and $\hat{s}_i$ are the coefficients in original ECG and marked ECG. The performance of the proposed method in terms of SNR, PRD, and payload was listed in Table 1. Their average SNR, PRD, and payload are 50.35 dB, 0.0031, and 2.28k bytes, respectively.

Table 1: SNR/PRD/payload performance of the proposed method using $\tau = 30$

ECG data	SNR/PRD/payload
100	52.43/0.0024/18,824
101	52.18/0.0025/18,791
102	52.05/0.0025/19,113
103	51.69/0.0026/18,648
104	50.03/0.0032/18,781
105	50.28/0.0031/18,694
106	51.20/0.0028/18,797
107	47.00/0.0045/18,065
108	50.28/0.0031/19,446
109	48.49/0.0038/18,514
111	49.50/0.0034/19,218
112	49.45/0.0034/18,983
113	50.86/0.0029/18,869
114	50.90/0.0029/19,274
115	52.68/0.0023/18,536
116	49.21/0.0035/17,997
201	50.38/0.0030/18,971
202	51.04/0.0028/19,026
203	47.14/0.0044/18,065
205	52.40/0.0024/18,674
207	50.02/0.0032/19,346
210	50.35/0.0030/19,014
212	49.28/0.0034/18,594
213	47.79/0.0041/17,638
214	48.87/0.0036/18,401
220	51.67/0.0026/18,443
221	50.20/0.0031/18,680
222	52.13/0.0025/19,093
223	49.92/0.0032/18,514
230	51.00/0.0028/18,234
Average	50.35/0.0031/18,708

Relationship between SNR and payload for the proposed method by using six pieces of ECG data were shown in Fig. 3. From the figure we can see that the SNR value of ECG116 and ECG 213 were around 40 dB as the size of payload was approximately to 2.20k bytes, and the average SNR of other four ECGs was about 46 dB with payload about 2.38k bytes. In addition, close observation (in the first ten seconds interval) randomly selected from the marked ECGs were shown in Fig. 4. It is clear that the marked signal introduced by the proposed method (red line) was approximately similar to the original one (blue line).

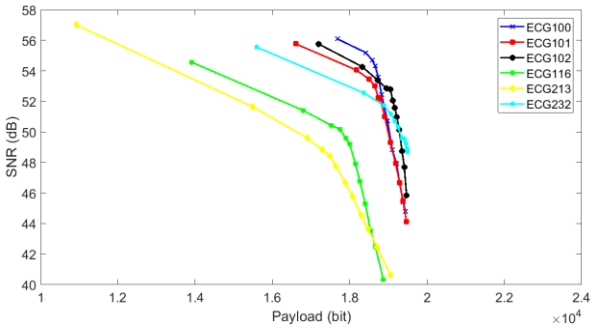
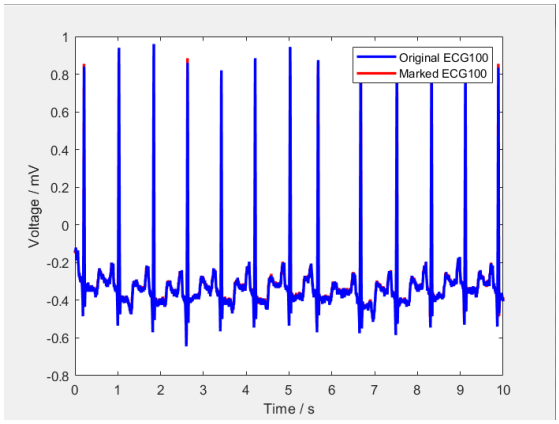
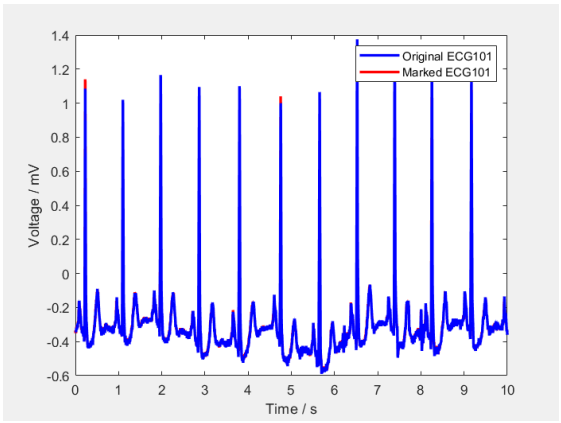


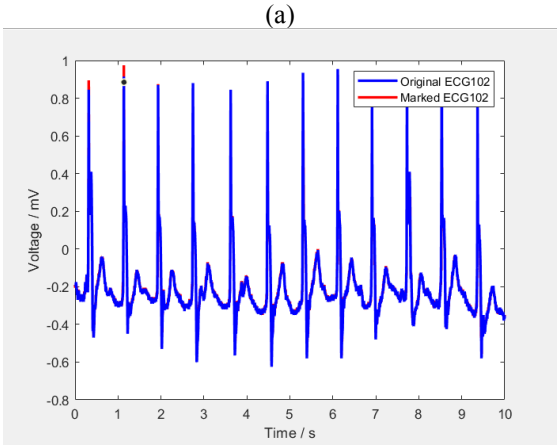
Figure 3: Trade-off between SNR and payload of the proposed method



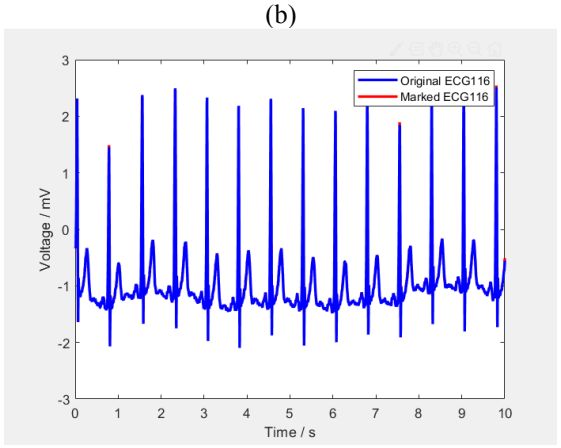
(a)



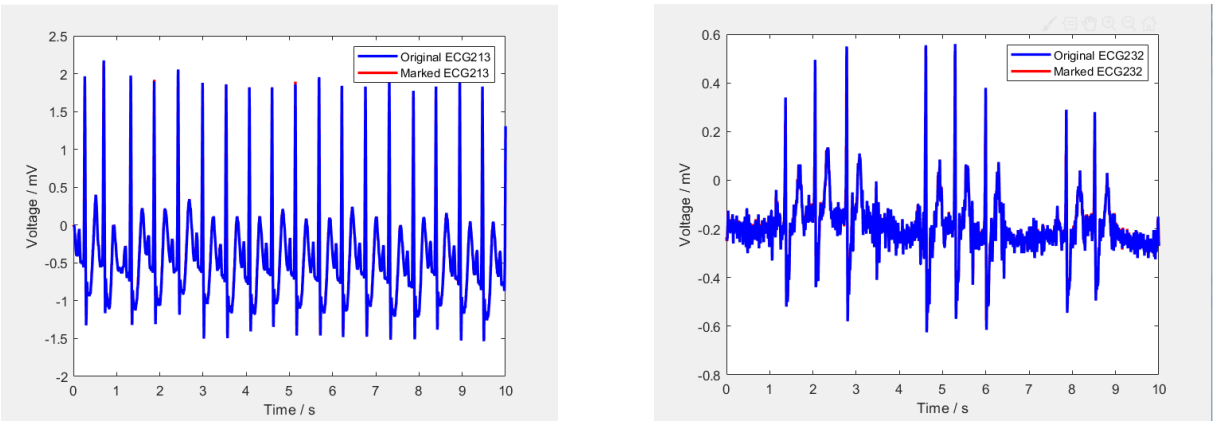
(b)



(c)



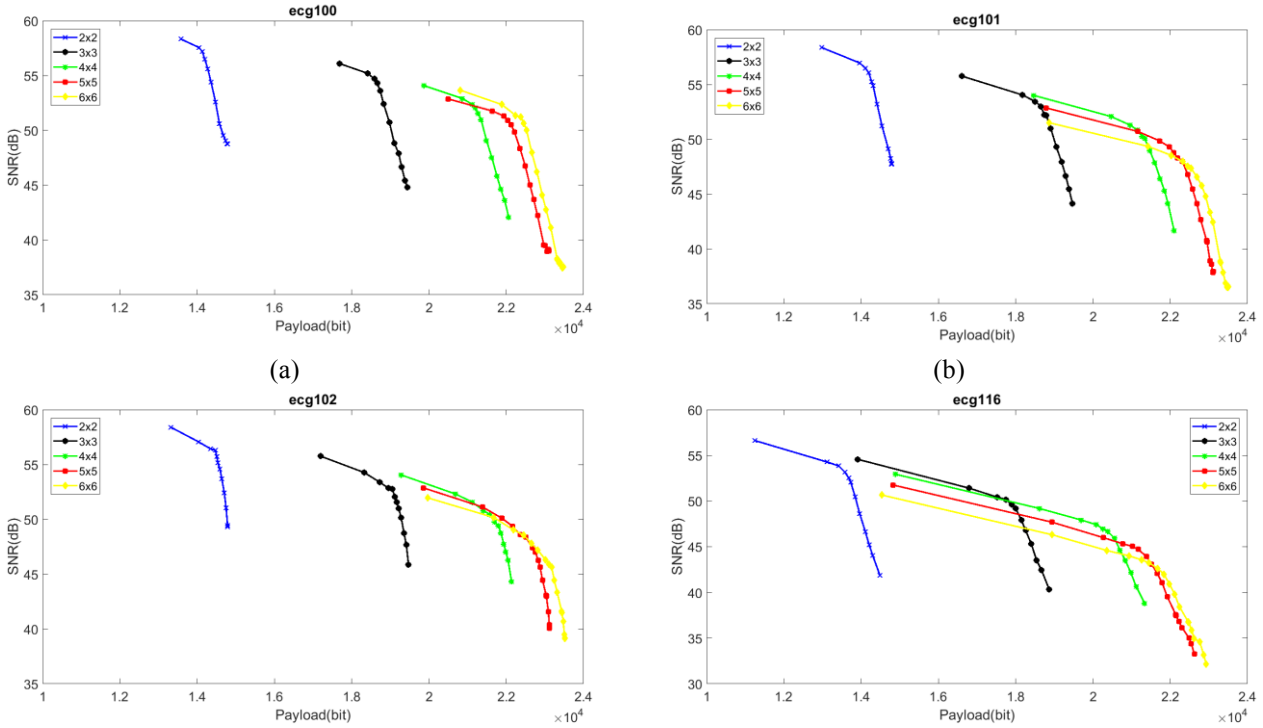
(d)



(e) (f)

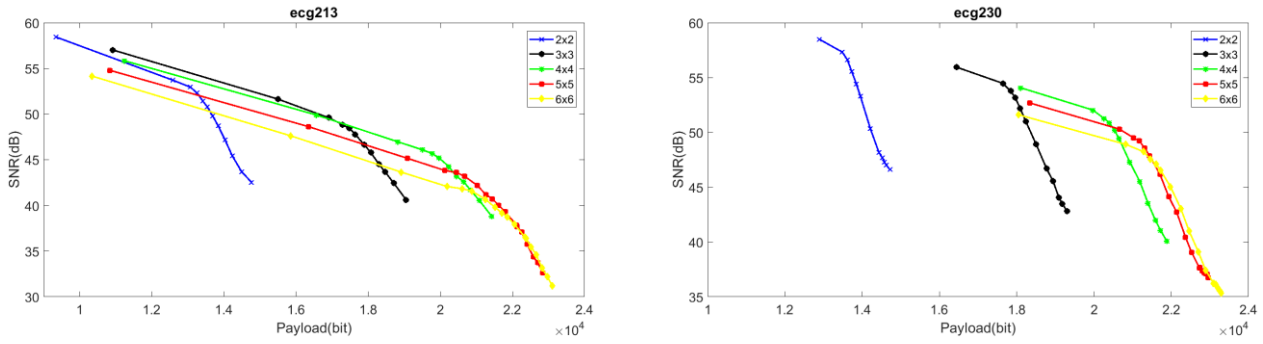
Figure 4: Close observations of the marked ECG generated by the proposed method using $\tau = 30$. (a) ECG100, (b) ECG101, (c) ECG102, (d) ECG116, (e) ECG213, and (f) ECG232

Furthermore, trade-off between SNR and payload of our method using host bundles in various size, namely, 2 × 2, 3 × 3, 4 × 4, 5 × 5, and 6 × 6, was depicted in Fig. 5. It is obvious that the larger the size of host bundles used by the proposed method, the larger the payload was obtained, and the lower the resultant SNR. As described in Sec. 2.2, the hiding capacity of the proposed method is bounded by N^2 when the size of a host bundle $n >> 1$. It can be observed from Fig. 5 that the payload of our method would be increased slowly as the larger size of the host bundles being employed. Conversely, a smaller host bundle provides higher SNR than a larger one does. Performance comparison between various methods was given in Table 2. The average SNR of the proposed method with the size of bundles 3 × 3 is superior to that of both Yang and Wang scheme [17] and Yang and Wang technique [18], while our payload is competitive to that of two compared methods [17-18]. Notice that our method with a host bundle of size 2 × 2 generated the best SNR values, while that with a host bundle of size 4 × 4 provided the largest payload among the compared methods.



(a) (b)

(c) (d)



(e) (f)

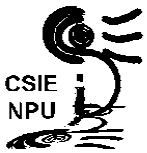
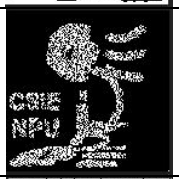
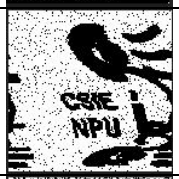
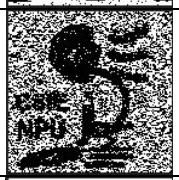
Figure 5: Relationship between SNR and payload of the proposed method using host bundles in various size. (a) ECG100, (b) ECG101, (c) ECG102, (d) ECG116, (e) ECG213, (f) ECG230

Table 2. SNR/payload (bits) performance comparison between various methods

ECG data set	Yang and Wang [17]	Yang and Wang [18]	Our method (2 × 2)	Our method (3 × 3)	Our method (4 × 4)
100	44.15/20,000	48.19/19,604	54.42/14,357	52.44/18,824	50.96/21,349
101	44.09/20,000	47.39/19,610	54.89/14,309	52.18/18,791	50.07/21,341
102	45.44/20,000	51.60/19,602	55.15/14,309	52.05/19,113	49.74/21,702
103	40.86/20,000	44.92/19,600	54.47/14,216	51.69/18,648	49.53/21,171
104	42.74/20,000	46.84/19,602	53.02/14,335	50.03/18,781	47.61/21,265
111	48.22/20,000	49.43/19,630	52.16/14,771	49.50/19,218	47.49/21,638
112	46.59/20,000	48.32/19,658	51.41/14,615	49.45/18,983	47.55/21,451
114	49.09/20,000	51.59/19,604	53.49/14,709	50.90/19,274	49.26/21,840
121	49.91/20,000	51.97/19,602	52.86/14,790	50.32/19,391	48.17/21,911
122	42.30/20,000	44.69/19,602	51.35/14,103	49.20/18,384	47.53/20,808
123	40.79/20,000	46.49/19,602	53.38/14,278	50.93/18,735	48.89/21,242
124	43.54/20,000	46.36/19,602	53.66/14,186	50.68/18,586	48.75/21,019
200	43.98/20,000	47.36/19,608	50.76/14,466	47.96/18,819	45.94/21,153
201	47.62/20,000	50.13/19,612	52.59/14,581	50.38/18,971	49.01/21,407
202	47.82/20,000	50.16/19,632	52.93/14,604	51.04/19,026	49.60/21,538
231	41.67/20,000	45.82/19,618	53.95/14,325	50.64/18,773	48.52/21,249
232	41.67/20,000	51.58/19,620	53.65/14,662	50.31/19,249	47.67/21,846
Average	44.73/20,000	48.40/19,612	53.18/14,448	50.57/18,915	48.61/21,407

Examples of survived watermarks from the manipulations of the marked ECG100, which generated by the proposed method using $\tau = 30$, were given in Table 3. A binary image of size 135 × 135 was used as an input watermark. The resultant SNR of the marked ECG100 was around 48 dB. Notice that the value of PRD equals 0 if a marked ECG were not being manipulated. The 5th row of the table indicated that the watermark which extracted from the mark ECG attacked by "Cropping (with 25% off)" was identified. In addition, the extracted watermark was still identified as the last three bits of the marked samples were truncated. Although the PRD value of the survived watermarks which manipulated by "Inversion" and "Scaling" were around 1.0, they were recognized. The marked ECG data under AWGN (additive white Gaussian noise) attack of signal strengths with 0.1 and 1 dB, respectively, the extracted watermarks were recognizable. Furthermore, our method has good performance in against "Translation (-1800)" attack. We can conclude from Table 3 that the proposed method is robust against manipulations.

Table 3: Examples of survived watermarks (WMs) from the manipulations of marked ECG100

Attacks	Survived WMs
Null-attack PRD = 0.0000	
AWGN (with SNR 0.1 dB) PRD = 0.5790	
AWGN (with SNR 1 dB) PRD = 0.5344	
Cropping (25% off) PRD = 0.8149	
Inversion PRD = 1.0440	
Scaling (*0.88) PRD = 0.6767	
Truncation† PRD = 0.6861	
Translation (-1800) PRD = 0.3535	

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

4. CONCLUSION

In this paper, we presented a simple ECG steganography for hiding patient's personal information and measurement data based on 2D bit-embedding/-extraction approach. Namely, according to the predetermined decision rules, data bits were effectively embedded in the host bundles of 2D ECG host. To show the hiding efficiency of the proposed method, several different sizes of the host bundles were implemented in simulations. Experimental results have revealed that the average SNR of the proposed method with a host bundle of size 3 × 3 is superior to that of existing techniques, while the payload is competitive to theirs. Additionally, our method with a host bundle of size 2 × 2 generated the best SNR values, while that with a host bundle of size 4 × 4 provided the largest payload among the compared methods. Furthermore, the proposed method has the merits of high hiding capacity and is tolerant of the attacks such as cropping, inversion, scaling, translation, truncation, and Gaussian noise-addition attacks. Since the computation speed is fast, the applications of our method can be employed in mobile biometric devices.

5. REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," 2nd Ed., Morgan Kaufmann, USA, 2007.

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

[3] S. Liu, Z. Pan, and H. Song, "Digital image watermarking method based on DCT and fractal encoding," *IET Image Proc.*, vol. 11, pp. 815-821, 2017.

[4] K.M. Hosny and M.M. Darwish, "Invariant image watermarking using accurate Polar harmonic transform," Computer and Electrical Engineering, vol. 62, pp. 429-447, 2017.

[5] C.Y. Hsiao, M.F. Tsai, and C.Y. Yang, "Simple and robust watermarking scheme based on square-root-modulus technique," Multimedia Tools and Applications, vol. 77, pp. 30419-30435, 2018.

[6] Hedieh Sajedi, "Applications of data hiding techniques in medical and healthcare systems: a survey," Network Modeling Analysis in Health Informatics and Bioinformatics, doi: 10.1007/s13721-018-0169-x, 2018.

[7] H.J. Shiu, B.S. Lin, C.H. Huang, P.Y. Chiang, and C.L. Lei, "Preserving privacy of online digital physiological signals using blind and reversible steganography," Computer Method and Programs in Biomedicine, vol. 151, pp. 159-170, 2017.

[8] L.T. Cheng and C.Y. Yang, "High-performance Reversible Electrocardiogram Steganography Based on Fast Discrete Cosine Transform with Coefficients Offset," 2019 Global Conference on Engineering and Applied Science (GCEAS 2019), July 16-18, Sapporo, Japan, 2019.

[9] S. Bhalerao, I.A. Ansari, A. Kumar, D. Kumar, and D.K. Jain, "A reversible and multipurpose ECG data hiding technique for telmedicine applications," Pattern Recogition Letter, vol. 125, pp. 463-473, 2019.

[10] A. Swierkosz and P. Augustyniak, "Optimizing wavelet ECG watermarking to maintain measurement performance according to industrial standard," Sensors, vol. 18, doi: 10.3390/s18103401, 2018.

[11] S.T. Chen, Y.J. Guo, H.N. Huang, W.M. Kung, K.K. Tseng, and S.Y. Tu, "Hiding patients confidential data in the ECG signal via transform-domain quantization," Journal of Medical Systems, vol. 38, doi: 10.1007/s10916-014-0054-9, 2014.

[12] 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.

[13] S.E. Jero, P. Ramu, and S. Ramakrishnan, "Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission," Journal of Medical Systems, vol. 38:132, doi: 10.1007/s10916-014-0132-z, 2014.

[14] S.E. Jero, P. Ramu, and S. Ramakrishnan, "ECG steganography using curvelet transform," Biomedical Signal Processing and Control, vol. 22, pp. 161-169, 2015.

[15] C.Y. Yang and W.F. Wang, "Effective electrocardiogram steganography based on coefficient alignment," Journal of Medical Systems, vol. 40, DOI: 10.1007/s10916-015-0426-9, 2016.

[16] S.E. Jero, P. Ramu, and S. Ramakrishnan, "Imperceptability-robustness tradeoff studies for ECG steganography using continuous ant colony optimization," Expert Systems With Applications, vol. 49, pp. 123-135, 2016.

[17] C.Y. Yang and W.F. Wang, "High-capacity ECG steganography with smart offset coefficients," The 13th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2017), Aug. 12-15, Matsue, Japan, 2017.

[18] C.Y. Yang and W.F. Wang, "An improved high-capacity ECG steganography with smart offset coefficients," The 14th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2018), Nov. 26-28, Sendai, Japan, 2018.

[19] G.B. Moody and R.G. Mark, "The impact of the MIT-BIH arrhythmia database," IEEE Eng. in Medical and Biol., vol. 20, pp. 45-50, 2001.