

Hiding Secrets in Electrocardiogram Based on Integer Wavelet Transform with Coefficient Adjustment and LSB Substitution

Ching-Yu Yang¹ & Wen-Fong Wang²

¹ Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Taiwan

² Department of Computer Science and Information Engineering, National Yunlin University of Science and Technology, Taiwan

Correspondence: Ching-Yu Yang, Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, No. 300, Liu-Ho Rd., Magong, Penghu, 880 Taiwan. Tel: 886-6-9264115. E-mail: chingyu@gms.npu.edu.tw

Received: June 8, 2022 Accepted: July 5, 2022 Online Published: July 19, 2022

doi:10.5539/nct.v7n1p27

URL: <https://doi.org/10.5539/nct.v7n1p27>

Abstract

In this paper, we present an efficient data hiding for electrocardiogram (ECG) hosts to solve the issues of existing ECG steganographic methods, which have less hiding capacity and insufficient signal-to-noise ratio (SNR)/ peak SNR (PSNR). Based on the integer wavelet transform (IWT), private (or sensitive) data such as patients' diagnosis and personal information can be embedded in an ECG host via the IWT coefficient adjustment and the least significant bit (LSB) technique. Simulations indicated that the SNR (or PSNR), and payload of the proposed method outperform those of existing techniques. In addition, the proposed method is capable of resisting attacks, such as cropping, Gaussian noise-addition inversion, scaling, translation, and truncation attacks from third parties (or adversaries). Since the proposed method has low computational complexity, our method can be employed in portable biometric devices or wearable electronics.

Keywords: coefficient adjustment, data privacy, ECG steganography, integer wavelet transform, LSB technique

1. Introduction

Recently, the COVID-19 pandemic has caused organizations and individuals to stay at home and work via the Internet. One of the important services provided by the Internet is the medical treatment of the elderly care and personal health maintenance. For example, elders who need help from families or individuals can evaluate their own biometric status, such as electrocardiogram (ECG), glucose, and blood pressure, and transmit the sensitive measurement data to community hospitals (medical centers) through intelligent networks. Because data packets are prone to be eavesdropped and tampered during transmissions between senders and receivers via public networks, care must be taken to ensure the security (or privacy) of the sensitive data. Typically, data hiding techniques provide an economic and easy way to achieve this goal. Data hiding can be classified into steganography and digital watermarking (Cox et al., 2008; Eielinska et al., 2014). One main goal of steganography (Hussain et al., 2018; Kadhim et al., 2019) is to embed a large volume of data in host multimedia, such as text, images, or video, while maintaining a good (or acceptable) perceived quality. Generally, a good perceived quality attracts no attention of third parties (or adversaries). By contrast, robust performance is one of the major aims of (robust) digital watermarking (Liu et al., 2017; Hsiao et al., 2018). The watermarked multimedia generated by a robust watermarking scheme often has good performance in resisting attacks. Thus, most watermarks extracted from the watermarked multimedia, which have undergone manipulation, can still be recognized. However, they often provide a limited payload size. Furthermore, some authors have proposed reversible (or lossless) data hiding techniques to completely restore the original content of (valuable) host media, such as medical or satellite images, after data extraction (Wu et al., 2020; Li & Huang 2020). Because the proposed ECG steganography is a lossy data hiding approach, only the related articles are surveyed in the following subsection.

Recently, several data hiding methods have been developed for the protection (or privacy) of sensitive information in ECG signals. Swierkosz and Augustyniak (2018) proposed an ECG watermarking scheme based on the discrete wavelet transform (DWT) domain. With the use of a continuous noise measurement and adaptive coding bit depth, the watermarked ECGs generated by the approach were capable of resisting noise attacks. The values of

percentage residual difference (PRD) ranged from 0.06 to 0.51 with a bit depth from 2 to 5, and was capable of introducing an optimal payload of approximately 6.5 Kb. Using the DWT with QR image decomposition, Sanivarapu et al. (2020) successfully embedded patient information in an ECG host. An input ECG was first converted to a two-dimensional (2D) ECG image using the Pan–Tompkins algorithm. The 2D image was subsequently decomposed by DWT. Then, data bits can be effectively hidden into the target coefficients via DWT and QR decomposition techniques. Simulations indicated that the method was tolerant of additive white Gaussian noise (AWGN) noise attacks. In addition, the average PRD and SNR were 0.0020 and 53.81 dB with a payload size of 4 Kb.

Based on curvelet transforms, Jero and Ramu (2016) developed a data hiding technique for ECG signals. Demonstrations showed that the PRD was 0.11 with a payload size of 4 Kb, and the bit error rate (BER) was 31.84%. In addition, the BER linearly increased as the payload increased. Yang and Wang (2016) employed the coefficient adjustment technique and proposed two types of ECG steganography, namely, a high-perceived quality and a high-capacity ECG steganography. Simulations indicated that the average SNR and payload for the high-perceived quality and high-capacity ECG steganography were 54 and 43 dB with payload sizes of 7 and 14 Kb, respectively. Based on the DWT and singular value decomposition, Jero et al. (2016) presented a continuous ant colony optimization skill to embed patient information in a 2D ECG signal. Simulations indicated that the PRD and PSNR were 0.0018 and 62.87 dB with a payload size of 0.89 Kbytes. In addition, the method was resistant from cropping and noise (or high-frequency) attacks. To design a suitable ECG steganography for wireless transmission, Pandey et al. (2017) employed a chaotic map and sample inversion technique to accomplish the goal. Experimental results revealed that the average PRD and PSNR were 0.26 and 55.49 dB with a payload size of 21 Kbytes (the input of all datasets took 20 min).

Without the use of auxiliary information, Yang and Wang (2018) utilized the absolute-value decision policy and proposed an ECG steganography. The number of input bits can be designed on-demand using host bundles in various sizes. Simulations indicated that the average payload and SNR of the method was approximately 19 Kb and 48 dB, respectively. In addition, the average SNR of 58 dB can be obtained with a payload size of 10 Kb. To further obtain a lower distortion and security, Pandey et al. (2019) used a fused coupled chaotic map with the LSB technique and presented an upgraded ECG steganography. Simulations confirmed that the average PRD and PSNR were 0.21 and 56.83 dB with a payload size of 21 Kbytes (the input of all datasets took 30 min). Furthermore, a good perceptual quality with a PSNR value of approximately 70 dB and payload size of 2.4 Kbytes can be achieved by the method. Christian et al. (2019) presented an ECG steganography based on the discrete cosine transform (DCT) domain. The method embedded secret bits in the second decimal place of the DCT coefficients and generated a very high perceptual quality. Although a high SNR with high payload can be obtained by their method, the size of the resultant ECG signal is increased by about two times larger than that of the original one, which may lead to the storage burden of the mobile measurement devices.

Based on a 2D bit-embedding and bit-extraction approach, Yang et al. (2020) proposed an effective ECG steganography, where a patient's data can be hidden into the host blocks of an ECG. The performance of the method was demonstrated with host blocks in various sizes. Compared with existing techniques, the method with a 2×2 block generated the best SNR and payload values, that is, 53 dB and 14 Kb, respectively, whereas the 4×4 block provided the largest payload (21 Kb) among the compared methods. The method has a merit of resisting manipulations because it embedded data bits in the blocks of a 2D ECG host. To obtain high hiding capacity and robustness performance, Yang and Wang (2020) embedded data bits in the low sub-band (LB) and high sub-band (HB) coefficients of the integer wavelet transform (IWT) domain. First, an input ECG host was decomposed into the LB and HB using level 1 IWT. Then, the predetermined criteria for bit embedding/ extraction were employed to hide a secret message into both sub-bands. Simulations indicated that their average SNRs were 50 and 40 dB with payload sizes of size 21 and 25 Kb, respectively, when the control parameters $\tau = 9$ and $\tau = 55$ were used. From the above survey we can see that the major issues of existing steganographic methods for ECG hosts have less hiding capacity and insufficient SNR (or PSNR). Thus, the motivation of this study is to propose an improved ECG steganography for the protection of patients' data and personal privacy.

The major contributions of the study include: 1) The proposed method has merits of good perceived quality, high hiding capacity, and the support of robustness, which is rarely seen in conventional ECG steganography methods. 2) The hiding storage and SNR (or PSNR) provided by the proposed method are superior to those provided by existing techniques. 3) Due to the fast computation time, the proposed method can be employed in portable biometric devices or wearable electronics.

The remainder of the paper is organized as follows. Section 2 describes the proposed bit embedding and bit extraction technique and the capacity analysis. Section 3 presents the experimental results. Section 4 makes a

discussion, and Section 5 concludes this work.

2. Method

To achieve high hiding capacity, good perceived quality, and robustness, an input ECG host was first decomposed into low sub-band coefficients (I_L) and high sub-band coefficients (I_H) via 1D IWT (Calderbank et al., 1998). Then, a series of host blocks with a size of $n \times n$ were sequentially derived from the I_L and I_H . The number of $(n - 1) \times (n - 1)$ bits can be virtually embedded in the IWT coefficients of the first $(n - 1)$ rows of a host block according to the coefficient adjustment. In addition, the number of $(2 \times n)$ bits can be hidden into the IWT coefficients at the last row of the host block via the LSB technique. If a sub-block of the first (or the second) row of host block failed to be used for hiding bit after the adjustment, it is referred to as a skipped sub-block. Moreover, the skipped sub-blocks carry no data bits. Because a skipped sub-block can be easily detected by the receiver using the above criteria, no auxiliary information is required to record their positions. The major steps of bit embedding and bit extraction for our proposed method are summarized in the following sections.

2.1 Bit Embedding

The main procedure of bit embedding is described in the following algorithm.

Algorithm 1. Hiding data bits in the ECG host.

Input: Host ECG Ω , size of a host block n , a control integer τ , and a secret message W .

Output: Marked ECG Ω' .

Method:

Step 0. Perform 1D forward IWT from Ω to obtain two sets of host blocks $I_L = \{E_j | j = 1, 2, \dots, |I_L|\}$ and $I_H = \{E_j | j = 1, 2, \dots, |I_H|\}$.

Step 1. Set parameter $m = 0$ and input a block $E_j = \{s_{ji}\}_{i=0}^{n-1}$ from I_L (or I_H). If the end of input is encountered, then go to Step 10.

Step 2. If $m < (n - 1)$, then set index $r = m \times n$ and go to the next step; otherwise, go to Step 9.

Step 3. Compute the offset $\alpha = s_{jr} - s_{j(r+1)}$, if the condition $|\alpha| > \tau$ is satisfied, which means that the sub-block carries no data bit, and then go to Step 6; otherwise, input a data bit b_p from W .

Step 4. If both conditions of $b_p = 1$ and $-\tau \leq \alpha < 0$ are satisfied, which means that the sub-block carries data bit "1," and then go to Step 6. Otherwise, if $b_p = 1$ is satisfied, which implies the occurrence of a violation, then repeatedly adjust the value of α by increasing $s_{j(r+1)}$ by 1 and decreasing s_{jr} from 1 simultaneously until $-\tau \leq \alpha < 0$ is achieved, and go to Step 6.

Step 5. If both conditions of $b_p = 0$ and $0 \leq \alpha \leq \tau$ are satisfied, which means that the sub-block carries data bit "0," and then go to Step 6. If $b_p = 0$ is satisfied, which implies the occurrence of a violation, and then repeatedly adjust the value of α by increasing s_{jr} by 1 and decreasing $s_{j(r+1)}$ from 1 simultaneously until the condition $0 \leq \alpha \leq \tau$ is satisfied.

Step 6. Compute the offset $\beta = (s_{jr} + s_{j(r+1)})/2 - s_{j(r+2)}$, and if the condition $|\beta| > \tau$ is satisfied, then set $m = m + 1$ and go to Step 2; otherwise, input next bit b_q from W .

Step 7. If both conditions of $b_q = 1$ and $-\tau \leq \beta < 0$ are satisfied, which means that the sub-block carries data bit "1," then set $m = m + 1$ and go to Step 2. Otherwise, if $b_q = 1$ is satisfied, then repeatedly adjust the value of β by increasing $s_{j(r+2)}$ by 1 and decreasing both s_{jr} and $s_{j(r+1)}$ from 1 simultaneously until the condition $-\tau \leq \beta < 0$ is satisfied. Set $m = m + 1$ and go to Step 2.

Step 8. If both conditions of $b_q = 0$ and $0 \leq \beta \leq \tau$ are satisfied, which means that the sub-block carries data bit "0," then set $m = m + 1$ and go to Step 2. Otherwise, if $b_q = 0$ is satisfied, then repeatedly adjust the value of β by increasing s_{jr} and $s_{j(r+1)}$ by 1 and decreasing $s_{j(r+2)}$ from 1 simultaneously, until the condition $0 \leq \beta \leq \tau$ is met. Set $m = m + 1$ and go to Step 2.

Step 9. Embed $(2 \times n)$ bits in the three coefficients at the last row of E_j via the LSB, and return to Step 1.

Step 10. Perform 1D inverse IWT from I_L and I_H to obtain mark ECG.

2.2 Bit Extraction

Bit extraction is considerably simpler than the proposed bit embedding. The major steps of bit extraction are listed in the following algorithm.

Algorithm 2. Extracting hidden bits from marked ECG.

Input: Marked ECG Ω' , size of a host block n , and an integer τ .

Output: Secret message W .

Method:

Step 0. Perform 1D forward IWT from Ω' to obtain two sets of marked bundles $I'_L = \{E_j | j = 1, 2, \dots, |I_L|\}$ and $I'_H = \{E_j | j = 1, 2, \dots, |I_H|\}$.

Step 1. Set $m = 0$ and input a block $E_j = \{s'_{ji}\}_{i=0}^{n^2-1}$. If the end of input is encountered, then go to Step 8.

Step 2. If $m < (n - 1)$, then set index $r = m \times n$ and go to the next step; otherwise, proceed to Step 7.

Step 3. Compute the offset $\alpha = s'_{jr} - s'_{j(r+1)}$, if $|\alpha| > \tau$ is true, then go to Step 5; otherwise, go to the next step.

Step 4. If the condition $-\tau \leq \alpha < 0$ is satisfied, then data bit "1" is recognized, otherwise, data bit "0" is identified.

Step 5. Compute the offset $\beta = (s'_{jr} + s'_{j(r+1)})/2 - s'_{j(r+2)}$, if the condition $|\beta| > \tau$ is satisfied, then set $m = m + 1$, and return to Step 2; otherwise, proceed to the next step.

Step 6. If the condition $-\tau \leq \beta < 0$ is satisfied, then data bit "1" is recognized, otherwise, data bit "0" is identified. Set $m = m + 1$ and return to Step 2.

Step 7. Extract $(2 \times n)$ bits from the three coefficients of E_j via the LSB technique, and return to Step 1.

Step 8. Assemble all extracted bits and rebuild the secret message W .

Notably, the value of the control parameter τ was not necessarily constant. When τ was small, SNR increased, and the PRD and payload size decreased. Moreover, the proposed method with a large τ provides more a robust performance than with any smaller τ . The block diagram of the bit embedding and bit extraction of the proposed method is summarized in Figure 1.

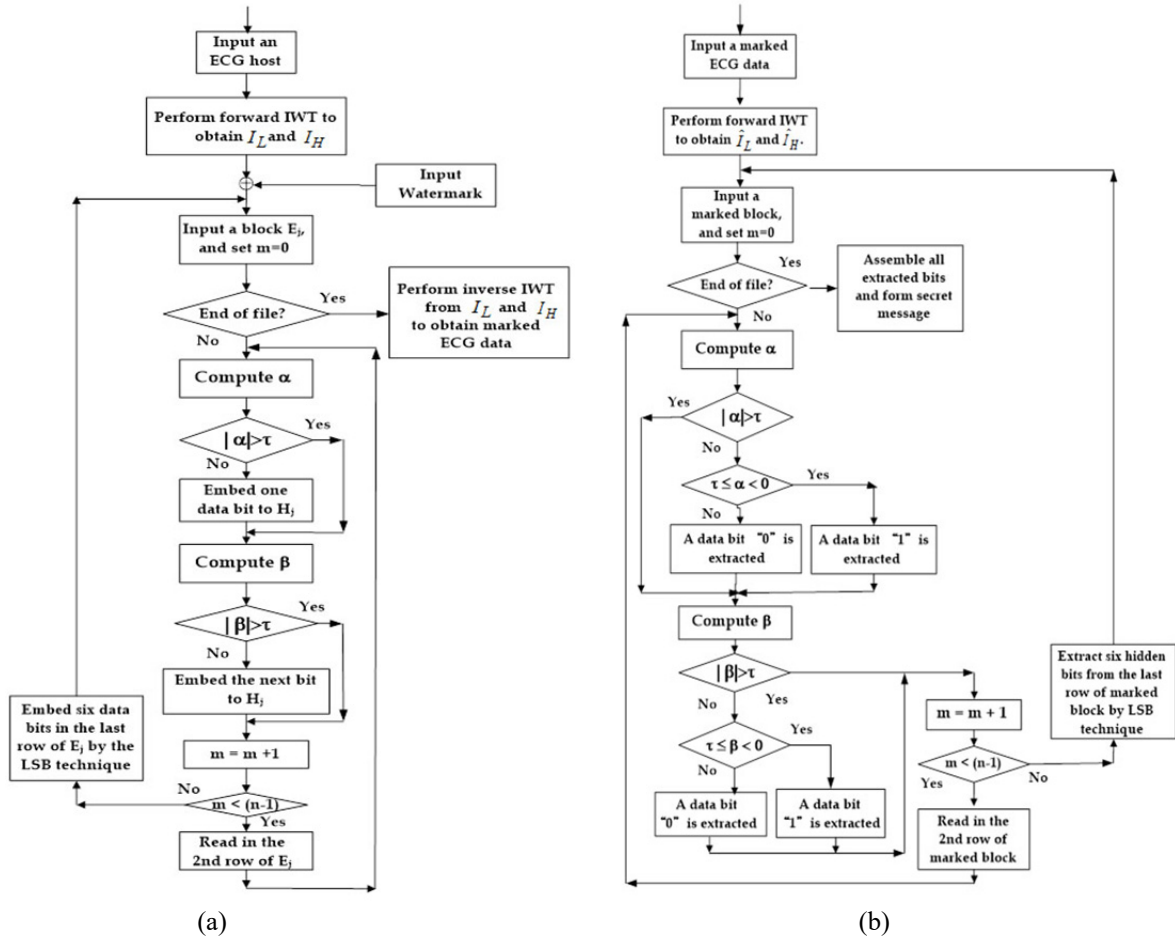


Figure 1. Block diagram of the proposed method. (a) Bit embedding and (b) bit extraction

2.3 Capacity Analysis

If the number of skipped sub-blocks is null and an input ECG consists of K samples, then the optimal payload size of the proposed method is $[(n-1) \times (n-1) + (2 \times n)] \times \left\lfloor \frac{K}{n \times n} \right\rfloor = (n^2 + 1) \times \left\lfloor \frac{K}{n \times n} \right\rfloor$ bits, where $\left\lfloor \frac{K}{n \times n} \right\rfloor$ stands for the number of host blocks. However, if we choose to embed n bits in the last row of a host block via the LSB technique, then the optimal payload of the proposed method would be $[(n-1) \times (n-1) + n] \times \left\lfloor \frac{K}{n \times n} \right\rfloor = (n^2 - n - 1) \times \left\lfloor \frac{K}{n \times n} \right\rfloor$. In addition, our simulations have revealed that the distortion caused by embedding secret bits in I_H was considerably less than that caused by embedding secret bits in I_L . To further pursue high-perceived quality (or high SNR value), data bits can only be embedded in the I_H sub-band with the constraint of embedding n bits in the last row of a host block via the LSB technique. However, in this case, the optimal payload (with no skipped sub-blocks) would be $(n^2 - n - 1) \times \left\lfloor \frac{|I_H|}{n^2} \right\rfloor = (n^2 - n - 1) \times \left\lfloor \frac{K}{2n^2} \right\rfloor$. As compared with the aforementioned payload, the hiding capability of this version is no more than 50% of the original payload size. Actually, this version with a host block of size 3×3 introduced approximately 30% to 45% size of the aforementioned (optimal) payload when $\tau < 9$ was used. Furthermore, data bits can be forcedly hidden into the skipped sub-blocks via the LSB technique. Although the payload size can be slightly promoted, the resultant SNR and robustness performance would be significantly degraded. The authors did not employ this methodology in the proposed method.

3. Results

To evaluate the performance of our method, simulations were implemented on an Intel® Core™ i5 1.7 GHz laptop with 12 GB RAM. The average central processing unit (CPU) time for the proposed method, including I/O, was approximately 0.025 s. A total of 48 ECG host signals obtained from the MIT-BIH Arrhythmia Database (Moody & Mark 2001) were used as test data. After the preprocessing of an ECG signal, each ECG host consists of $K = 30,000$ samples. The size of a host block is 3×3 . Several measurements, such as SNR, mean absolute error (MAE), PRD, and PSNR are used for performance evaluation and are defined as follows:

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

$$MAE = \frac{1}{K} \sum_{i=1}^K |s_i - \hat{s}_i|, \quad (2)$$

$$PRD = \sqrt{\frac{\sum_i (s_i - \hat{s}_i)^2}{\sum_i s_i^2}} \times 100\%, \quad (3)$$

and

$$PSNR = 10 \log_{10} \frac{Max(s_i)^2}{\frac{1}{K} \sum_i (s_i - \hat{s}_i)^2}, \quad (4)$$

where s_i , \hat{s}_i , and $Max(s_i)$ stand for the coefficients in the original ECG, marked ECG, and maximum value of s_i , respectively. The trade-off between the SNR and payload for our method in six pieces of ECG is depicted in Figure 2. The figure shows that the average SNR values of ECG116 and ECG213 at around 45 dB with a payload of 32 Kb was less than those of the other four ECGs. That is, the average SNR of the four ECGs was approximately 48 dB with a similar payload size.

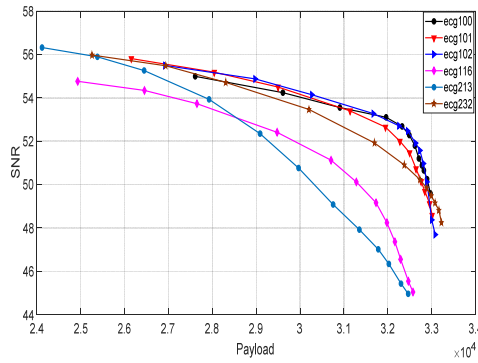


Figure 2. Trade-off between the SNR and payload of the proposed method

The SNR and payload generated by the proposed method used various τ , and the number of corresponding skipped blocks are shown in Figures 3(a) and 3(b). The larger the value of τ , the lower the number of skipped blocks, and the lower the SNR values, which means that a larger payload can be obtained by the proposed method, vice versa. Moreover, the distortions in terms of PRD and MAE are given in Figures 3(c) and 3(d). The average PRD and MAE for ECG116 and ECG213 were slightly higher than those of the other four ECGs. From Fig. 3 we can conclude that the proposed method embeds data bits in ECG100, ECG101, ECG102, and ECG232 with better efficiency than in ECG116 and ECG 213.

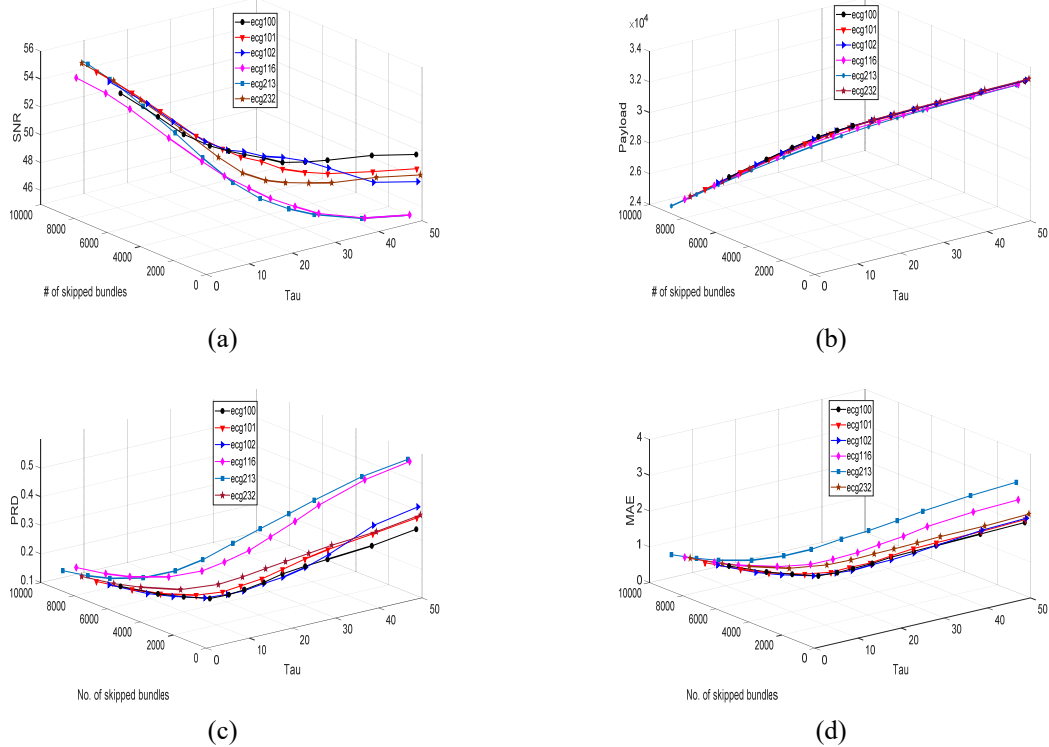


Figure 3. Performance generated by the proposed method using various τ and the number of corresponding skipped blocks. (a) SNR, (b) payload, (c) PRD, and (d) MAE

To further examine the hiding capability of each ECG host by the proposed method, the resulting payloads of these ECGs with a lower and larger value of τ are illustrated in Fig. 4. The x-axis in both figures numbered from 1 to 48 stands for the 48 sets of ECG inputs. The corresponding name of the ECG input of the serial number is listed in Table 1. Figure 4(a) shows that the average hiding capacity provided by serial numbers of 1 (or ECG100), 20 (or ECG121), and 28 (or ECG205) with lower values of $\tau (\leq 8)$ was higher than that of other ECGs. On the contrary, the average hiding capacity provided by serial numbers of 8 (or ECG107), 27 (or ECG203), 30 (or ECG208), and

34 (or ECG213) was less than that of other ECGs. Figure 4(b) presents that the average hiding storage provided by serial numbers of 9 (or ECG108), 20 (or ECG121), 29 (or ECG207), and 46 (or ECG232) with larger values of τ (≥ 20) was higher than that of other ECGs, and the average hiding storage provided by serial numbers of 8 (or ECG107), 27 (or ECG203), and 34 (or ECG213) was less than that of other ECGs.

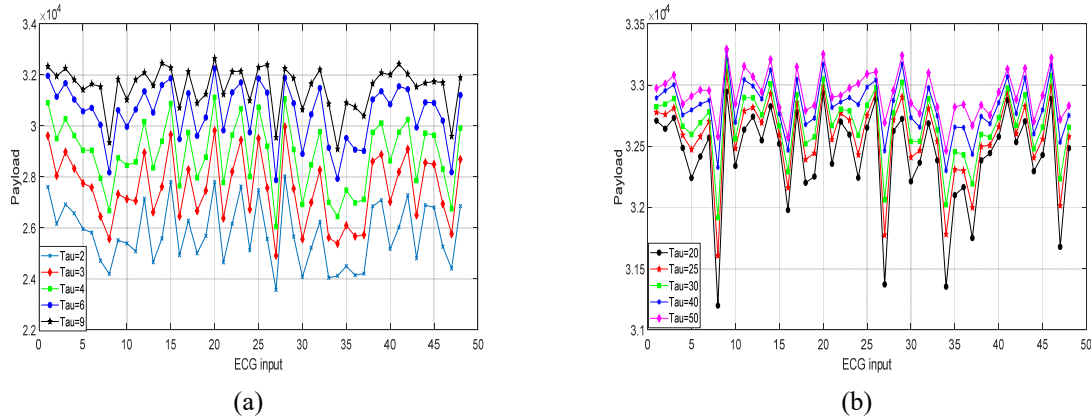


Figure 4. Payload of the proposed method using various values of τ . (a) $\tau \leq 8$ and (b) $\tau \geq 20$

Table 1. Corresponding ECG names to the labels of the x-axis in Figure 4

No.	ECG input	No.	ECG input	No.	ECG input	No.	ECG input
1	ECG100	13	ECG113	25	ECG201	37	ECG217
2	ECG101	14	ECG114	26	ECG202	38	ECG219
3	ECG102	15	ECG115	27	ECG203	39	ECG220
4	ECG103	16	ECG116	28	ECG205	40	ECG221
5	ECG104	17	ECG117	29	ECG207	41	ECG222
6	ECG105	18	ECG118	30	ECG208	42	ECG223
7	ECG106	19	ECG119	31	ECG209	43	ECG228
8	ECG107	20	ECG121	32	ECG210	44	ECG230
9	ECG108	21	ECG122	33	ECG212	45	ECG231
10	ECG109	22	ECG123	34	ECG213	46	ECG232
11	ECG111	23	ECG124	35	ECG214	47	ECG233
12	ECG112	24	ECG200	36	ECG215	48	ECG234

For a clear examination of the ECG hosts, their full waveforms and standard deviation (SD) and entropy values are given in Figure 5. The figure shows that the SD and entropy of ECG107, ECG203, and ECG213 were significantly larger than those of other ECGs. Moreover, the value of the y-axis in these figures ranges either between -2 and 1.2 or between -4 and 3 . Generally, the larger the SD/entropy, the more drastic the variation of the waves, and the less the hiding capability obtained by the proposed method, and vice versa. The SD and entropy are defined as follows:

$$SD = \sqrt{\frac{1}{K} \sum_i (s_i - \mu)^2} \quad (5)$$

and

$$H = -\sum_i p(s_i) \log_2 p(s_i), \quad (6)$$

where μ and $p(s_i)$ denote the mean and possibility of the coefficients in the ECG host.

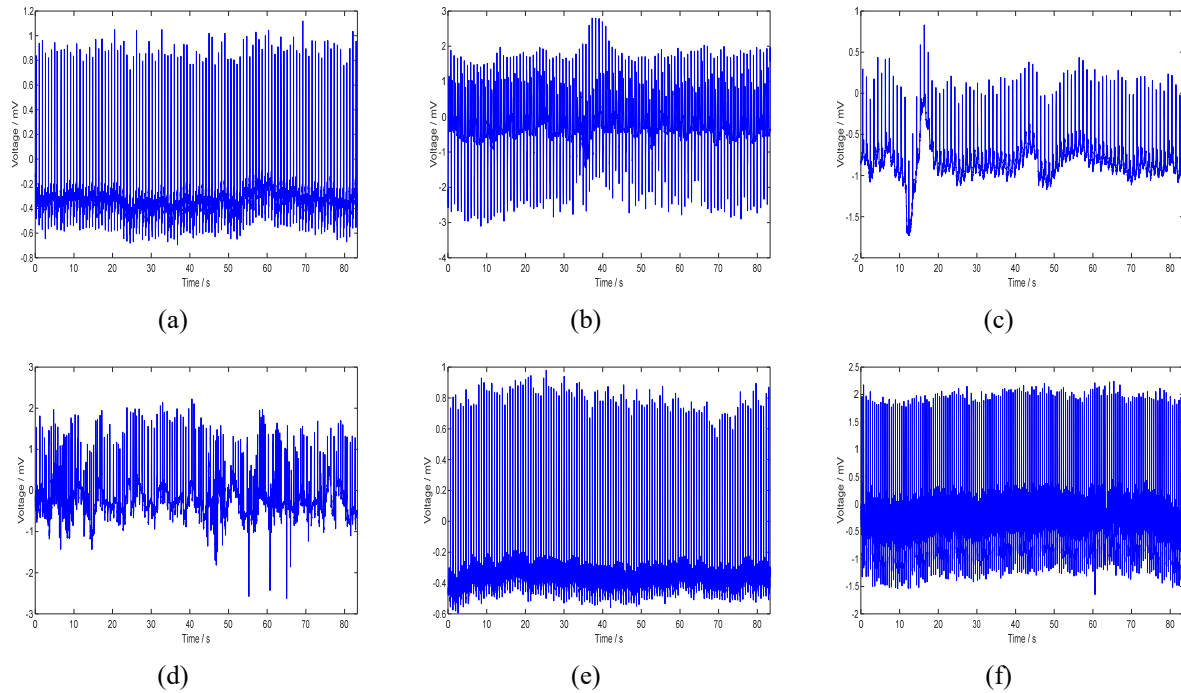


Figure 5. Waveforms of the ECG host with their SD/ entropy values. (a) ECG100 (35/6.23), (b) ECG107 (164/9.16), (c) ECG121 (53/7.34), (d) ECG203 (102/8.64), (e) ECG205 (36/5.82), (f) ECG213 (113/8.55)

The distortions generated by the proposed method (in the first 5-s interval) from the marked ECG100 and ECG231 with various τ are shown in Figure 6. The marked signal introduced by our methods (red line) was approximately similar to the original one (blue line).

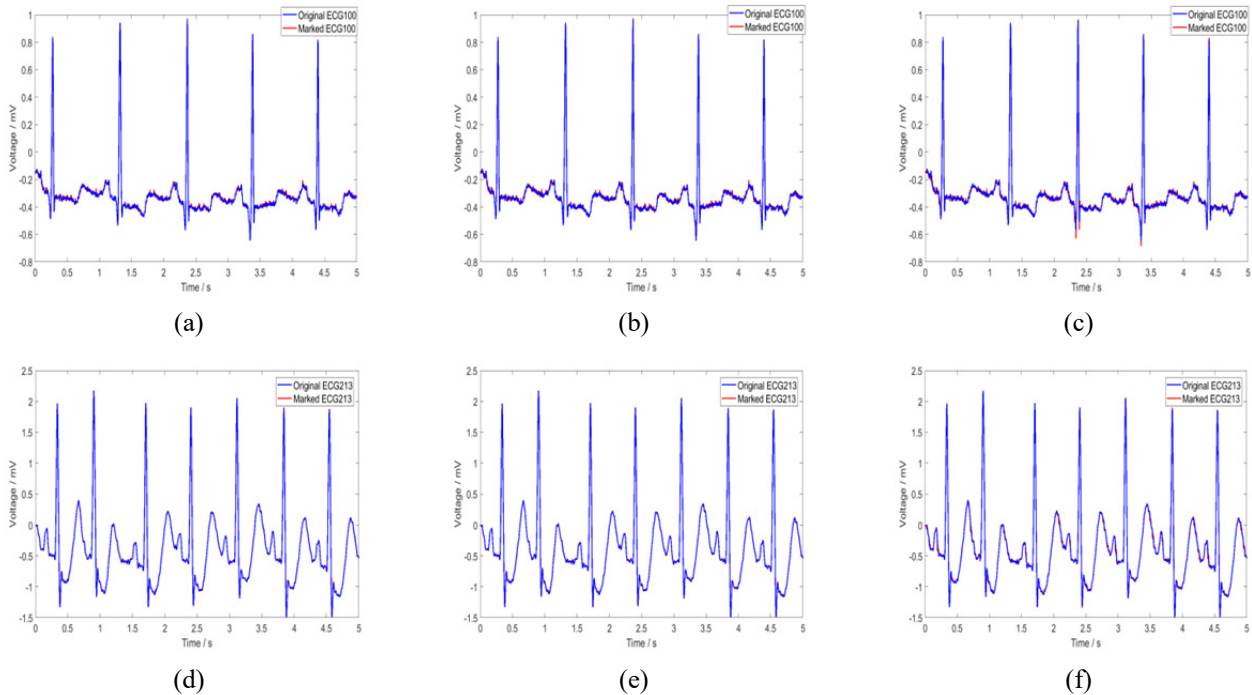


Figure 6. Close observations of the marked ECGs generated by the proposed method. (a) ECG100 with $\tau = 2$, (b) $\tau = 4$, (c) $\tau = 30$; (d) ECG213 with $\tau = 2$, (e) $\tau = 4$, and (f) $\tau = 30$

3.1 Performance Comparison

Performance comparison between various methods is illustrated in Figure 7. The (original version of the) proposed method (represented as OurLSB2) provided the largest payload among the compared methods, and the SNR of value 55.63 dB (with a payload size of around 25 Kb) is still better than that of Yang & Wang's technique (2020). In addition, the second version of the proposed method (represented as OurLSB) provided the best SNR performance in the payload between 15 Kb and 22 Kb among the various techniques. The other three methods (Yang & Wang, 2018; Yang et al., 2020; Yang & Wang, 2020) provided similar SNR values when the payload size is less than 15 Kb. The second version of the proposed method embedded only three data bits in the last row of a host block. The main difference between the proposed two versions is that the former method can be implemented in situations that require a payload greater than 25 Kb, whereas the latter method can be applied to environments where a good perceived quality (or high SNR) is an important indicator (or a concern factor). As specified in Section 2.3, in the third version of the proposed method, to further obtain good perceived quality (or high SNR value), data bits can only be embedded in the I_H sub-band with the constraint of embedding n data bits in the last row of a host block via the LSB technique. Our experiments indicated that the average payload of 9 Kb with an average SNR of 64 dB was acquired by this approach. Compared with other existing schemes, the average payload and SNR provided by Yang & Wang's technique (2020) was 9 Kb and 60 dB, and those provided by Yang et al.'s approach (2020) was 8 Kb and 62 dB, respectively. Furthermore, Jero et al.'s (2016) and Pandey et al.'s scheme (2019) used the PSNR as their perceived quality measurement, and the performance comparison in terms of the payload size and PSNR is given in Table 2. Evidently, the PSNR value of the proposed method (with our three versions) is the best among the methods, and our payload is still larger than that of the other two techniques. Figure 7 and Table 2 shows that the proposed method generates better perceived quality and higher payload than existing techniques.

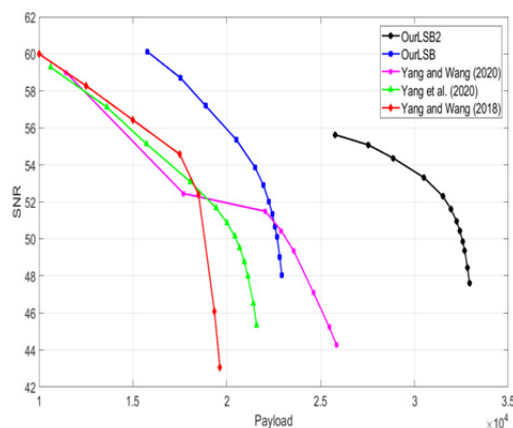


Figure 7. Performance comparison of various methods

Table 2. Payload (bits) and PSNR performance comparison of various methods

Jero et al. (2016)	Pandey et al. (2019)	Proposed method
7,290/62.87	7,290/61.54	8,237/ 67.88 ¹
10,650/54.75	10,650/58.01	11,101/ 63.15 ¹
14,450/51.13	14,450/55.55	14,733/ 63.51 ²
18,022/45.12	18,022/53.62	18,876/ 60.20 ²
21,873/39.52	21,873/51.98	21,951/ 55.90 ²
25,149/34.46	25,149/50.79	25,764/ 58.51 ³

¹The third version of our method.





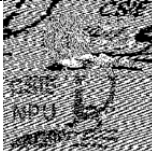




²The second version of our method.

³The original version of our method.

3.2 Extra Functions

Several examples of survived watermarks from the manipulations of the marked ECG100 (with $\tau = 16$) are given in Table 3. A binary image of size 180×180 was used as an input watermark. The resultant SNR of the marked ECG100 was approximately 52 dB. Table 3 indicates that both the values of PRD and bit error rate (BER) equal 0 for a “Null-attack,” which meaning a marked ECG was not manipulated. The BER is the number of (the extracted) bit errors divided by the total number of input watermark bits. In general, the lower the BER, the better the perceived quality of the extracted watermarks. The fourth and sixth columns on the second row of the table indicated that the watermark extracted from the marked ECG and attacked by AWGN attacks of signal strengths 0.001 and 1 dB, respectively, were recognizable. Although the PRD of the survived watermarked (at the second column on the third row of the table) from the “cropping” attack was 0.8246 with BER = 0.5317, it was identified. Moreover, at the same row of the table, the survived watermarks manipulated by “Inversion” and “Scaling” were still recognized. In spite of the PRD and BER for the extracted watermark (at the second column on the last row of the table) were 0.8190 and 0.5244, respectively, it can be identified by squinting eyes. Besides, the last row of the table shows that our method has good performance against the “translation (with scale of +1500 and -1500)” attack. Table 3 shows that our method is capable of resisting several kinds of attacks.

Table 3. Examples of survived watermarks from the manipulations of the marked ECG100

Attacks	Survived Watermarks	Attacks	Survived Watermarks	Attacks	Survived Watermarks
Null-attack PRD = 0.0000 BER = 0.0000		AWGN (with SNR 0.01 dB) PRD = 0.6810 BER = 0.3626		AWGN (with SNR 3 dB) PRD = 0.6347 BER = 0.3149	
Cropping (50% off) PRD = 0.8246 BER = 0.5317		Inversion PRD = 0.7648 BER = 0.4573		Scaling (*2.0) PRD = 0.7056 BER = 0.3892	
Truncation [†] PRD = 0.8190 BER = 0.5244		Translation (+1500) PRD = 0.0000 BER = 0.0000		Translation (-1500) PRD = 0.4228 BER = 0.1389	

[†]The last two bits of the marked data were truncated.

4. Discussion

As described in Section 2.3, the payload of our method was limited by $(n^2 + 1) \times \lfloor K / n^2 \rfloor$ with null skipped block. Although the optimal payload can be obtained by the proposed method with host block of size 2×2 , the robustness performance was not better than that the method uses host block whose size being larger than 2×2 . In addition, one can use the coefficient adjustment and the LSB technique to embed data bits in the IWT coefficients of the first row and the second-/third-row the host blocks, respectively. It certainly enlarges hiding capacity. However, it increases the proportion of the LSB usage, and undermines the robustness of the proposed method. The study discovers that if we embed data bits in the first two rows and the last row of the host blocks of size 3×3 via the coefficient adjustment and the LSB technique, respectively, a high hiding capacity, good perceived quality, and robustness can be achieved by the proposed method. Moreover, the hiding performance of the method can be improved by analyzing the characteristic of each host block before bit embedding. Theoretically, a smooth block which encoded by the coefficient adjustment introduces less distortion, while a non-smooth block generates the larger payload by the LSB technique.

To evaluate hiding performance, several objective assessments such as SNR, PSNR, MAE, and PRD have been commonly used in ECG steganography (Yang & Wang, 2018; Yang et al., 2020; Yang & Wang, 2020; Jero et al., 2016; Pandey et al., 2019). Simulations have indicated that the less value of τ , the lower the MAE, the larger the SNR/PSNR, implying that a good perceived quality can be obtained by the proposed method, and vice versa. In

addition, the average payload and SNR/PSNR of the proposed method outperforms existing techniques. Moreover, the proposed method has an extra characteristic of robustness, which is rarely existed in conventional ECG steganography.

In this article, we proposed an improved ECG steganography for the protection of the sensitive personal information of patients. Based on the IWT domain with coefficient offset and LSB technique, data bits can be effectively embedded in the host blocks of an ECG signal. Experiments confirmed that the average SNR (or PSNR) and payload of the proposed method are superior to those of the existing ECG steganography. Moreover, our method equipped with robustness performance was rarely seen in existing ECG steganography techniques. That is, the proposed method is tolerant of attacks, such as cropping, inversion, scaling, translation, truncation, and Gaussian noise-addition attacks. Because the processing time is fast, our method can be applied in mobile biometric devices or wearable electronics. To further promote hiding capacity and robustness, our future work will focus on an a priori analysis and statistics of each ECG input and performed steganography in other transform domain.

Compliance with Ethical Standards

- Conflicts of interest/ Competing Interests: The authors declare that they have no conflict of interest/ competing interests.
- Ethical approval: This article does not contain any studies with human participants performed by any of the authors.
- Informed consent: Not applicable.

References

- Calderbank, A. R., Daubechies, I., Sweldens, W., & Yeo, B. L. (1998). Wavelet transforms that map integers to integers. *Applied & Computat Harmonics Analysis*, 5(3), 332-369. <https://doi.org/10.1006/acha.1997.0238>
- Christian, M., Yang, C. Y., Xie, Y. Z., & Yang, C. Y. (2019) Hiding secret message in electrocardiogram based on discrete cosine transform. *Int. Conf. on Innovative Computing and Management Science (ICMS 2019)*, July 19-22, Osaka, Japan. <https://doi.org/10.5281/zenodo.1317262>
- Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). *Digital watermarking and steganography* (2nd ed.). Morgan: Kaufmann, MA.
- Eielinska, E., Mazurczyk, W., & Szczypiorski, K. (2014). Trends in steganography. *Communications of the ACM*, 57(3), 86-95. <https://doi.org/10.1145/2566590.2566610>
- Hsiao, C. Y., Tsai, M. F., & Yang, C. Y. (2018). Simple and robust watermarking scheme based on square-root-modulus technique. *Multimedia Tools and Applications*, 77(23), 30419-30435. <https://doi.org/10.1007/s11042-018-6121-3>
- Hussain, M., Wahab, A. W. A., BinIdris, Y. I., Ho, A. T. S., & Jung, K. H. (2018). Image steganography in spatial domain: a survey. *Signal Processing: Image Communications*, 65, 46-66. <https://doi.org/10.1016/j.image.2018.03.012>
- Jero, S. E., & Ramu, P. (2016). Curvelets-based ecg steganography for data security. *Electronics Letters*, 52(4), 283-285. <https://doi.org/10.1049/el.2015.3218>
- Jero, S. E., Ramu, P., & Ramakrishnan, S. (2016) Imperceptability-robustness tradeoff studies for ecg steganography using continuous ant colony optimization. *Expert Systems with Applications*, 49, 123-135. <https://doi.org/10.1016/j.eswa.2015.12.010>
- Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. *Neurocomputing*, 335, 299-326. <https://doi.org/10.1016/j.neucom.2018.06.075>
- Li, N., & Huang, F. (2020). Reversible data hiding for JPEG images based on pairwise nonzero ac coefficient expansion. *Signal Processing*, 171, 107476. <https://doi.org/10.1016/j.sigpro.2020.107476>
- Liu, S., Pan, Z., & Song, H. (2017). Digital image watermarking method based on dct and fractal encoding. *IET Image Proc.*, 11, 815-821. <https://doi.org/10.1049/iet-ipr.2016.0862>
- Moody, G. B., & Mark, R. G. (2001). The impact of the MIT-BIH arrhythmia database. *IEEE Engineering in Medicine and Biology Magazine*, 20(3), 45-50. <https://doi.org/10.1109/51.932724>

- Pandey, A., Saini, B. S., & Sood, N. (2017). An integrated approach using chaotic map & sample value difference method for electrocardiogram steganography and OFDM based secured patient information transmission. *J. Medical Systems*, 41(12), 29043502. <https://doi.org/10.1007/s10916-017-0830-4>
- Pandey, A., Singh, B., Saini, B. S., & Sood, N. (2019). A novel fused coupled chaotic map based confidential data embedding-then-encryption of electrocardiogram signal. *Biocybernetics and Biomedical Engineering*, 39(2), 282-300. <https://doi.org/10.1016/j.bbe.2018.11.012>
- Sanivarapu, P. V., Rajesh, K. N. V. P. S., Reddy, N. V. R., & Reddy, N. C. S. (2020). Patient data hiding into ecg signal using watermarking in transform domain. *Physical and Engineering Sciences in Medicine*, 43, 213-226. <https://doi.org/10.1007/s13246-019-00838-2>
- Swierkosz, A., & Augustyniak, P. (2018). Optimizing wavelet ecg watermarking to maintain measurement performance according to industrial standard. *Sensors*, 18(10). <https://doi.org/10.3390/s18103401>
- Wu, X., Yang, C. N., & Liu, Y. W. (2020). A general framework for partial reversible data hiding using hamming code. *Signal Processing*, 175, 107657. <https://doi.org/10.1016/j.sigpro.2020.107657>
- Yang, C. Y. & Wang, W. F. (2016). Effective electrocardiogram steganography based on coefficient alignment. *J. Medical Systems*, 40(3), 1-15. <https://doi.org/10.1007/s10916-015-0426-9>
- Yang, C. Y., & Wang, W. F. (2018). An improved high-capacity ecg steganography with smart offset coefficients. *The 14th Int. Conf. on Intell. Inform. Hiding and Multim. Sig. Proc. (IIH-MSP 2018)*, Nov. 26-28, Sendai, Japan.
- Yang, C. Y., & Wang, W. F. (2020). Progressive data hiding in integer wavelet transform of electrocardiogram by using simple decision rule and coefficient calibration. *Revue d'Intelligence Artificielle*, 2, 11-20. <https://doi.org/10.18280/ria.340102>
- Yang, C. Y., Lai, C. M., Lin, H. C., Lin, T. Y., & Lu, R. L. (2020). Adaptive electrocardiogram steganography based on 2D approach with predetermined rules. *Asian J Computer and Information Systems*, 8(1), 1-10. <https://doi.org/10.24203/ajcis.v8i1.6059>

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).