Transactions on Machine Learning and Artificial Intelligence - Vol. 9, No. 6
Publication Date: December, 25, 2021
DOI:10.14738/tmlai.96.11177.
Yang, C., & Huang, C. (2021). Nearly Reversible ECG Steganography based on Polar Coordinate System with Digital Replacement Technique. Transactions on Machine Learning and Artificial Intelligence, 9(6). 09-19.

Nearly Reversible ECG Steganography based on Polar Coordinate System with Digital Replacement Technique

Ching-Yu Yang
Dept. of Computer Science and Information Engineering

Chi-Kai Huang
National Penghu University of Science and Technology, Taiwan

ABSTRACT

In this paper, we present a nearly reversible data hiding for electrocardiogram (ECG) hosts. Based on the polar coordinate system domain, medical diagnosis and personal data can be embedded in an ECG signal by the simple digital replacement technique. Simulations revealed that the restored ECG with near lossless quality can be obtained by the proposed method at receiver site. In addition, the perceived quality of the marked ECG is very good with a high payload size. Moreover, the resultant signal-to-noise ratio (SNR), peak SNR, and payload of the proposed method outperforms those of existing techniques. Since the computation cost is low, the proposed method can be used in portable biometrics or ECG measuring instruments.

Keywords: Data Hiding; ECG Steganography; Polar Coordinate System; Digital Replacement.

INTRODUCTION

Recently, the artificial intelligence, data analytics, the fifth generation cellular, and internet of things have been widely applied in the Internet. The companies (and individuals) are capable of sharing their resources and important (or private) data such as business transaction and personal information around the world. A practical example is the medical treatment of the elderly care in a family. The elders helped by the families or individuals can use portable biometric devices to evaluate their physical health such as ECG, glucose, and blood pressure, and send the measurements with sensitive information to community hospital (medical center) through the Internet. However, data are prone to be eavesdropped and tampered with during transmission. Data hiding provides an economic and simple way to protect data from being compromised by third parties (or adversaries). General, data hiding techniques are classified into steganography and digital watermarking. The main goal of steganography [1-3] is to embed data bits in host multimedia such as images or videos as large as possible while maintaining a good (or acceptable) perceptual quality. By contrast, robustness is a major function required by digital watermarking [4-6]. A watermarked multimedia generated from the robust watermarking schemes often has an acceptable quality with good performance in resisting from manipulations. But, they usually provide a limited payload size. Due to the proposed method is used to protect personal sensitive data and patients' diagnosis, only the related articles are surveyed in the following sub-section.

Yang and Wang [7] used coefficient alignment technique and proposed two types of data hiding for ECG signals, namely, lossy and reversible ECG steganography. The average SNR of the lossy high-perceived quality/high-capacity methods were about 55 and 44 dB with the payload of size 7,500 and 14,642 bits, respectively. By contrast, the reversible version can not only successfully extract hidden bits but also completely recover original ECG host. Based on jointly using discrete wavelet transform, singular value decomposition, and quantization techniques, Jero et al. [8] presented a continuous ant colony optimization (CACO) algorithm to embed patient's diagnosis in an ECG signal. The main function of CACO is to promote the robustness with less distortion in the marked ECG. Simulations revealed that the percentage residual difference (PRD) and PSNR were 0.0018 and 62.87 dB with the payload of size 0.89 Kb. In addition, the method was resisting from noise, cropping and high frequency attacks. Pandey et al. [9] employed a fused coupled chaotic map and LSB technique, and proposed an ECG steganography. Experimental results revealed 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).

Based on the discrete cosine transform (DCT) domain and digital replacement technique, Christian et al. [10] developed an ECG steganography, which is capable of hiding a number of data bits in the second decimal place of the DCT coefficients, and the quality is quite good. However, the storage of the marked ECG required by the method is twice larger than that required by traditional ECG method. Since our method shares similar digital replacement technique, a detailed review of the method was presented in Section 2. Based on two-dimensional (2D) bit-embedding/-extraction approach, Yang et al. [11] proposed an effective 2D ECG steganography. Simulations showed that the average SNR of the method with the block size of 2×2 was about 53 dB with the payload size 14 Kb, while 4×4 provided the average payload of size 18 Kb with the SNR of value 50 dB. In addition, the proposed 2D approaches have a merit of resisting from manipulations. To further improve payload size and robustness, Yang et al. [12] embedded data bits adaptively in a host block of the integer wavelet transform domain, which obtained from an ECG signal. Simulations revealed that the average payload of the method is approximately 19 dB but the SNR is less than that of Yang et al.'s scheme [11]. In addition, the method was tolerant of several different types of attacks.

The major issues of most existing ECG steganography were lossy methods with less hiding capability, SNR and PSNR. To improve the hiding performance of existing methods, we embed data bits in the PCS via the digital replacement technique. Basically, the contribution of the work is to present a nearly reversible ECG steganography with high hiding-capacity and the perceived quality of the marked ECG is very good.

The remainder of the paper is organized as follows. Section 2 describes the related work. Section 3 specifies the proposed bit embedding and bit extraction. Sec. 4 presents the experimental results. Section 5 makes a discussion, and Section 6 concludes this work.

RELATED WORK

Generally, there are two major merits of hiding data bits in the digitals after the decimal point of the coefficients in the transform domain, such as discrete cosine transform (DCT) domain or polar and polar coordinate system (PCS). Namely, a steganography with high hiding capacity and good perceived quality can be obtained via the digital replacement based on transform domain. Therefore, Christian et a. [10] presented an ECG steganography, which is capable of

hiding a number of data bits in the second decimal place of the DCT coefficients. The idea of that method is described below subsection.

An ECG host is first divided into a series of non-overlapping blocks. Then, the host blocks are performed by DCT operation. A set of input bit *l* of length *k* was convert into a decimal value *d*. Subsequently, the 2nd coefficient after decimal point in a DCT block was replaced with *d*. The procedure is repeated until all of the host blocks have been processed. Finally, a marked ECG can be obtained by performing inverse DCT from the marked DCT blocks. At the receiver, the marked ECG was first converted into a series of DCT blocks. Then, we can extract the decimal value *d'* from the 2nd coefficient after decimal point in a DCT block and convert it into binary bits *l'* in length *k*. The procedure is repeated until all of the hidden bits have been extracted. Eventually, assemble the data bits, rebuild the secret message, and perform inverse FDCT to obtain ECG data.

Simulations revealed that the SNR value of the method was large with the size of payload 86,400 bits. In addition, the resultant perceived quality was good and robust against manipulations. An illustration of the Christian et al.'s technique [10] was depicted in Fig. 1. The size of a DCT block is 1 × 8 and the number of input bit is two for each DCT coefficient. It results in 16 bits can be hidden in a DCT block.

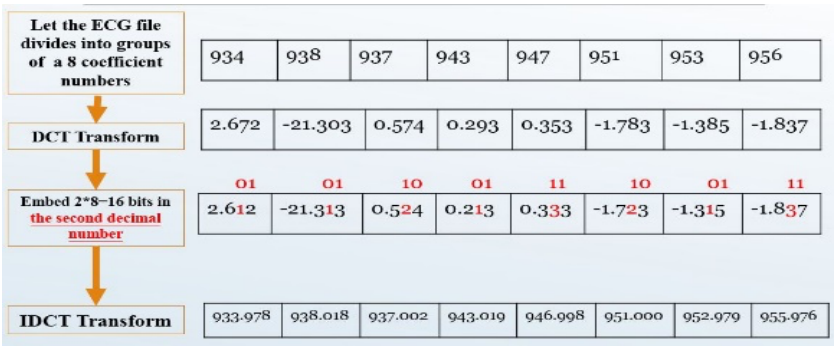


Fig. 1. Illustration of the Christian et al.'s technique [10]. (a) Bit-embedding and (b) bit-extraction.

PROPOSED METHOD

To obtain a nearly distortion-free perceived quality and high hiding capacity, the proposed method embeds secret bits in ECG signals based on the PCS. Namely, an ECG host is first

converted into polar coordinate system from the Cartesian coordinate system (CCS). Data bits are then embedded in the radial coordinate coefficients of the PCS. The block diagram of the proposed method is depicted in Fig. 2. The details of bit embedding and bit extraction for our method are specified in the following sections.

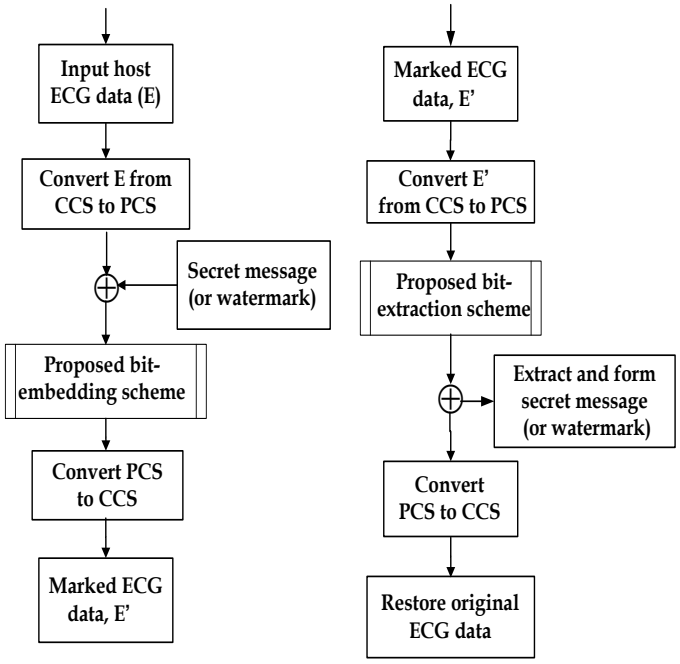


Fig. 2. Block diagram of the proposed method. (a) Encoding part and (b) decoding part.

Bit Embedding

Without loss of generality, let $E = \{x_j \mid j = 1,2,..., \mathrm{L}\}$ be the input ECG host with the size of L. Also, let *P* be the PCS of *E*, where $P = \{(r_i, \theta_i) \mid i = 1,2,..., \mathrm{L}/2\}$ with

$$r_i = \sqrt{x_j^2 + x_{j+1}^2} \tag{1}$$

and

$$\theta_i = \arctan\frac{x_j}{x_{j+1}}. \tag{2}$$

The polar coordinates r_i and θ_i can be converted to the Cartesian coordinates x_j and x_{j+1} by the following two equations:

$$x_j = r\cos\theta_i \tag{3}$$

and

$$x_{j+1} = r\cos\theta_i \tag{4}$$

To alleviate distortion, data bits are hidden into the first and second digits after the decimal point of r_i. The main procedure of bit embedding of the proposed method is described in the following algorithm.

Algorithm 1. Hiding a secret message in host ECG data.
Input: Host ECG data *E* and secret message *W*.
Output: Marked ECG data *E'*.

Method:
Step 0. Convert *E* to PCS, namely, *P*.
Step 1. Input *i*th target coefficient r_i from *P*. If the end of input is encountered, then go to Step 5.
Step 2. Let $d_m = (b_3 b_2 b_1)_2$ and $d_{m+1} = (b_6 b_5 b_4)_2$ be the two sets of bit-stream containing six consecutive input bits obtained from the *m*th set of *W*. Also, let r_i^{d1}, r_i^{d2}, r_i^{d3} and, r_i^{d4} be the first, second, third, and fourth digits after the decimal point of r_i.
Step 3. Replace r_i^{d3} and r_i^{d4} with r_i^{d1} and r_i^{d2}, respectively.
Step 4. Substitute d_m and d_{m+1} for r_i^{d1} and r_i^{d2}, respectively. Proceed to Step 1.
Step 5. Convert *P* to CCS and form marked ECG.
Step 6. Stop.

Bit Extraction
The major steps of bit extraction are described here.

Algorithm 2. Extracting hidden message from mark ECG data.
Input: Marked ECG data *E'*.
Output: A secret message *W* (and host ECG data)

Method:
Step 0. Convert *E'* to PCS, namely, *P'*.
Step 1. Input an *i*th marked coefficient $\tilde{r}_i$ from *P'*. If the end of input is encountered, then proceed to Step 4.
Step 2. Extract six hidden bits from $\tilde{r}_i^{d1}$ and $\tilde{r}_i^{d2}$.
Step 3. Replace $\tilde{r}_i^{d1}$ and $\tilde{r}_i^{d2}$ with $\tilde{r}_i^{d3}$ and $\tilde{r}_i^{d4}$, respectively. Proceed to Step 1.
Step 4. Convert *P'* to CCS, assemble all the extracted bits, and restored ECG host.
Step 5. Stop.

Due to the original radial coordinates $\tilde{r}_i^{d3}$ and $\tilde{r}_i^{d4}$ were omitted during bit embedding, it is not possible for the decoding part to fully restore the original ECG data. Since the coding error computed between the original ECG and the restored one was small, a nearly reversible ECG steganography can be obtained by the proposed method. The maximum payload of the proposed method is [3 × 2 × (L/2)] = 3L bits. If we only embed data bits in the first digit after the decimal point of r_i, then the optimal payload size would be [3 × (L/2)] = 1.5L bits. By contrast, if the first four digits after the decimal point of r_i were used to hide secret bits, then the total number of hidden bits would be [3 × 4 × (L/2)] = 6L bits. As we know, the larger the payload size, the less the SNR value, vice versa.

Notice that the marked ECGs are transmitted to the receiver site as floating-point data type. If transmission time and saving space are a big concern of a marked ECG, an alternative simplified version of the proposed method is suggested to employ here. Instead of transmitting each polar angle of the polar coordinates, only the average polar angle which computed from all the angular coordinates was send to the receiver. It is apparently that both the transmission time

and memory storage can be reduced to half of the size of the original one. It is inevitable that the reduction of SNR performance and the degradation of perceived quality. An extra usage of the simplified approach is that it can be used as in the preliminary stage of progressive transmission of the proposed method from source host to destination host.

EXPERIMENTAL RESULTS

Based on the platform of Microsoft Windows 10 and an Intel Core (TM) i5-6300U 2.4 GHz personal computer with 8 GB RAM, all simulations were performed in Matlab (R2015b) programming language. The average execution time for the proposed algorithms was about 0.061 s. The 96 sets of ECG hosts, namely, Lead I and Lead II, were obtained from the MIT-BIH arrhythmia database [13]. The size of each host set was 30,000. The SNR and PSNR are defined as follows:

$$SNR = 10\log_{10}\frac{\sum_i s_i^2}{\sum_i (s_i - \hat{s}_i)^2} \quad (5)$$

and

$$PSNR = 10\log_{10}\frac{Max(s_i)^2}{\frac{1}{K}\sum_i (s_i - \hat{s}_i)^2}, \quad (6)$$

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. First, several ECG hosts, namely, ECG100, ECG107, ECG116, ECG203, ECG213, and ECG233 were employed in our experiments. A binary image of size 300 × 300 was used as the test data. Trade-off between the SNR and payload generated by the proposed method was depicted in Fig. 3. The average SNR is approximately 68 and 75 dB as the optimal payload size reaches 90,000 and 20,000 bits, respectively. Moreover, close observation of the host and restored ECGs (at the beginning of 10-second) from these ECGs were depicted in Fig. 4. It is clear that the perceived quality is quite good. No apparent distortion existed in the restored ECGs. In other words, a nearly reversible ECG steganography can be achieved by the proposed method. To show the hiding performance of the proposed method, all the 96 sets of ECG inputs (from Lead I and Lead II) were implemented and illustrated in Fig. 5. The label of x-axis in the figure with number from 1 to 48 stands for the name of each ECG input. The corresponding name of the ECG input of the serial number was listed in Table 1. Figure 5 indicates that the SNR values of the ECG inputs from Lead I and Lead II lies between 67-69 dB and 69-71 dB, respectively. The maximum payload provided by all these inputs is 90,000 bits.

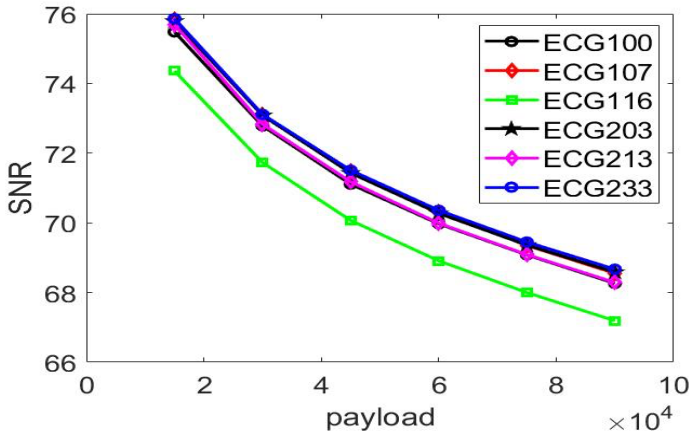
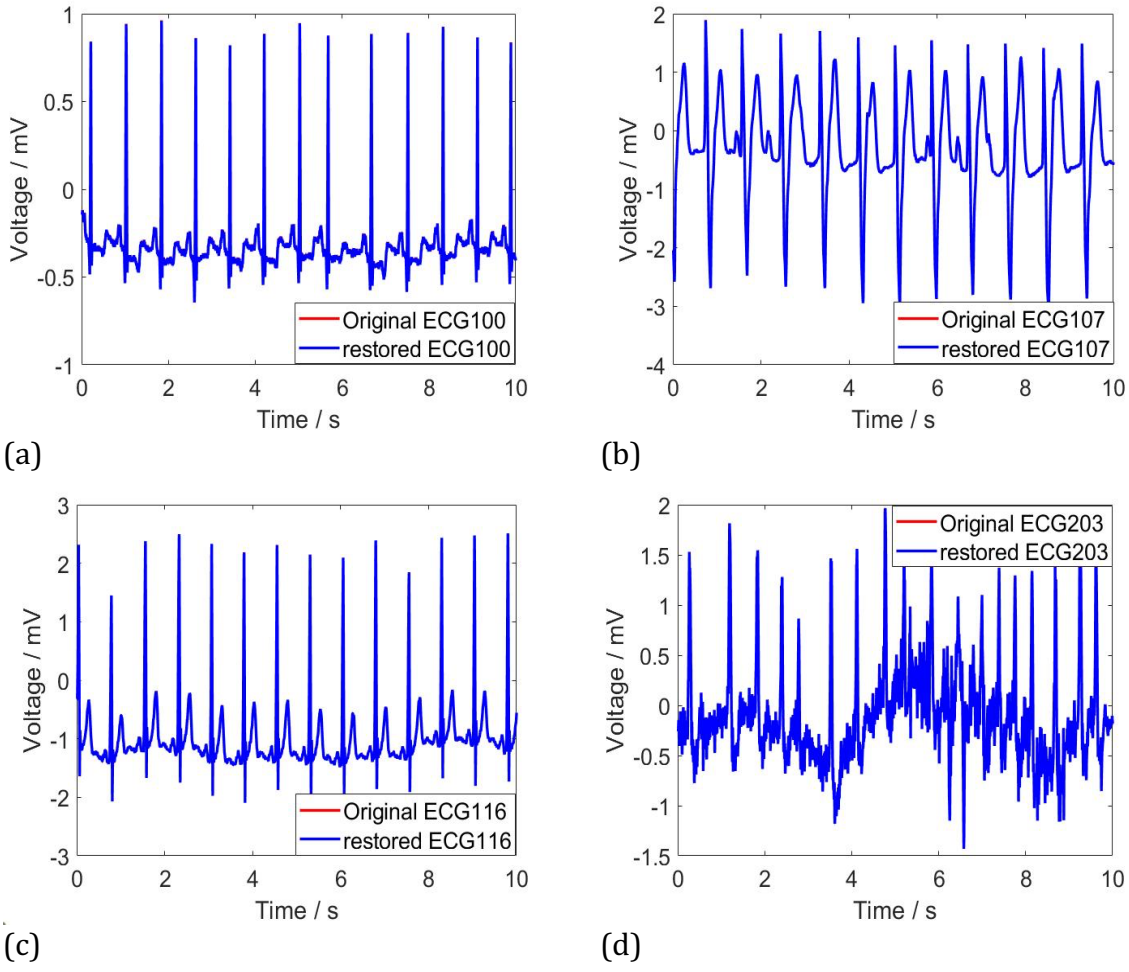
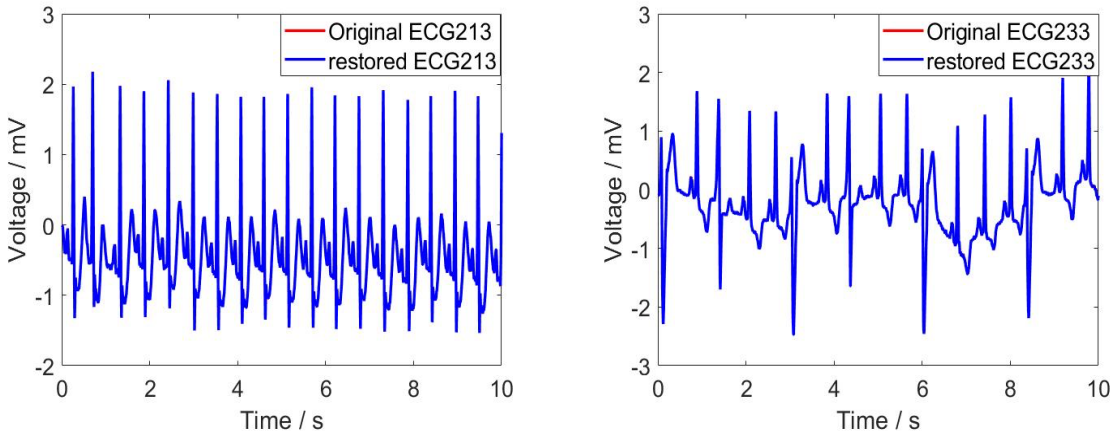


Fig. 3. Trade-off between the SNR and payload via the proposed method.





(e) (f)

Fig. 4. Close observation of the host and restored ECGs. (a) ECG100, (b) ECG107, (c) ECG116, (d) ECG203, (e) ECG213, and (f) ECG233.

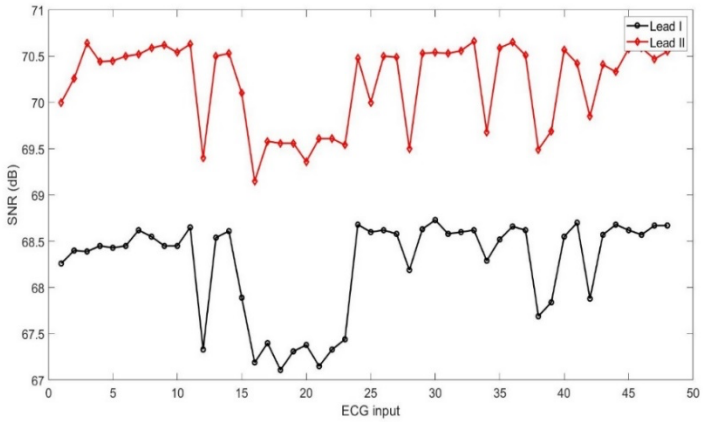


Fig. 5. The SNR of the proposed method uses two Leads as input sources.

Table 1. Corresponding ECG name to the legends in Figure 5

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

Performance comparison between the proposed method and its simplified version with existing techniques in terms of SNR, PSNR, and payload were listed in Tables 2 and 3. Table 2 reveals that the poposed method and its simplified version provided the largest payload among the compared methods. Christian et al. [10] has the best SNR performance. Generally, it is hard for human to tell the distinction of perceived quality between the marked and host ECGs when the resultant SNR is larger than 60 dB. Although the SNR of the simplified approach was the least, the payload size was much greater than the other two compared techniques [11,12]. Furthermore, Table 3 indicates that the PSNR of the proposed method was much larger than other two methods under similar payload size. In addition, the PSNR of the simplified approach was better than that of Jero et al. [8], and was slighly less than that of Pandey et al. [9].

Table 2. SNR/payload performance of the proposed methods

ECG data	Christian et al. [10]	Yang et al. [11]	Yang et al. [12]	Proposed method	Simplified approach
100	88.00/86,400	52.44/18,824	48.23/19,556	68.26/90,000	42.45/90,000
101	88.14/86,400	52.18/18,791	47.11/19,600	68.40/90,000	42.45/90,000
102	88.10/86,400	52.05/19,113	51.70/19,193	68.39/90,000	43.21/90,000
103	88.24/86,400	51.69/18,648	47.09/19,153	68.45/90,000	40.46/90,000
104	88.16/86,400	50.03/18,781	46.95/19,602	68.43/90,000	41.94/90,000
107	-	46.91/18,065	40.41/19,156	68.55/90,000	40.38/90,000
111	-	49.50/19,218	47.01/19,600	68.55/90,000	44.08/90,000
112	-	49.45/18,983	46.22/19,600	67.33/90,000	43.47/90,000
113	-	50.73/18,869	45.89/19,600	68.54/90,000	40.14/90,000
116	-	46.09/17,997	43.18/18,979	67.19/90,000	36.36/90,000
201	88.26/86,400	50.38/18,971	47.15/19,600	68.68/90,000	43.85/90,000
202	88.33/86,400	51.04/19,026	49.47/19,600	68.60/90,000	43.93/90,000
203	-	46.98/18,065	43.55/19,020	68.62/90,000	41.40/90,000
221	-	50.19/18,680	46.74/19,551	68.55/90,000	42.40/90,000
222	-	52.15/19,030	47.44/19,791	68.70/90,000	43.86/90,000
223	-	49.65/18,514	46.47/19,434	67.88/90,000	41.25/90,000
230	88.29/86,400	51.25/18,234	47.35/19,236	68.68/90,000	40.54/90,000
Average	88.19/86,400	50.16/18,695	46.59/19,428	68.34/90,000	41.89/90,000

Table 3. Payload/PSNR performance of the proposed methods

Jero et al. [8]	Pandey et al. [9]	Proposed method	Simplified approach
7,290/62.87	7,290/61.54	7,200/83.79	8,004/55.32
10,650/54.75	10,650/58.01	10,200/82.29	12,000/53.42
14,450/51.13	14,450/55.55	15,000/80.31	16,002/52.27
18,022/45.12	18,022/53.62	18,000/79.38	20,002/51.27
21,873/39.52	21,873/51.98	21,000/78.70	24,000/50.42
25,149/34.46	25,149/50.79	25,140/77.81	28,002/49.77

DISCUSSION

As specified in Section 4, the proposed method has a good performance in terms of SNR, PSNR and payload, while the perceived quality is good. Since the coefficients of the PCS are floating-point numbers, it takes four bytes to store each coefficient. Namely, the memory storage for saving a marked ECG is two times larger than that for conventional methods do. This shortcoming of the proposed method can be solved by using a lossless coding technique to compress the marked ECG before transmission.

The alternative simplified version shares the same payload size as the proposed method but with less SNR (or PSNR) and less memory storage. Namely, only a predetermined θ value has to be sent to the receiver, the size of memory storage required by the simplified version is only a half size of the proposed method. In addition, the proposed method and its simplified version can be jointly employed in an ECG steganography for the use of progressive transmission.

CONCLUSION

In this article, the authors proposed a nearly reversible ECG steganography for protecting personal information of the patients. Based on the polar coordinate system with the digital replacement technique, a secret message can be effective hidden into an ECG signal. Experiments confirmed that the stored ECG is near lossless and the perceived quality of the marked ECG is quite good. In addition, the SNR, PSNR and payload of the proposed method are superior to those of existing ECG steganography. The simplified version has an extra merit of reducing the memory storage. Since the processing time is fast, the proposed method (and its simplified version) can be applied in the mobile biometric devices or ECG measuring electronics. Our future work will be focus on the fully restored the content of the original ECG host, the promotion of hiding-capacity, and the characteristic of robustness of the proposed method.

References

Shehzad, D., et al., *LSB image steganography based on blocks matrix determinant method*. Internet and Information Systems, KSII Transactions on, 2019. 13(7): p. 3778-3793.

Alhomoud, A.M., *Image steganography in spatial domain: current status, techniques, and trends*. Intelligent Automation and Soft Compting, 2021. 27(1): p.69-88.

Liu, Y., et al. *Video steganography: a review*. Neurocomputing, 2019. 335(3): p.238-250.

Zheng, P.J., et al., *A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks*. Multimedia Tools and Applications, 2020. 79(3): p.18343-18365.

Kadian, P., et al., *Robust digital watermarking techniques for copyright protection of digital data: a survey*," Wireless Personal Communications, 2021. 118(2): p.3225-3249.

Agarwal, N., et al., *Survey of robust and imperceptible watermarking*. Multimedia Tools and Applications, 2019. 78(8): p. 8603-8633

Yang, C.Y. and W.F. Wang, *Effective electrocardiogram steganography based on coefficient alignment*. Journal of Medical System, 2016. 40(3), DOI: 10.1007/s10916-015-0426-9.

Jero, S.E., et al., *Imperceptability-robustness tradeoff studies for ECG steganography using continuous ant colony optimization*. Expert Systems with Applications, 2016. 49(1): p. 123-135.

Pandey, A., et al., *A novel fused coupled chaotic map based confidential data embedding-then-encryption of electrocardiogram signal*. Biocybernetics and Biomedical Engineering, 2019. 39(2): p. 282-300.

Christian, M., et al., *Hiding secret message in electrocardiogram based on discrete cosine transform*. Int. Conf. on Innovative Computing and Management Science, July 19-22, 2019, Osaka, Japan.

Yang, C.Y., et al., *Adaptive electrocardiogram steganography based on 2D approach with predetermined rules.* Asian Journal of Computer and Information Science, 2020. 8(1): p. 1-10.

Yang, C.Y., et al., *Adaptive data-hiding in electrocardiogram based on integer wavelet transform domain and incremental approach*. 2020 9th Int. Conf. on Industrial Technology and Management (ICITM 2020), Feb. 11-13, London, UK (2020).

Moody, G.B and R.G. Mark, *The impact of the MIT-BIH arrhythmia database*. IEEE Engineering in Medicine and Biology Magazine, 2001. 20(3): p. 45-50.