Multimed Tools Appl (2016) 75:13733–13747
DOI 10.1007/s11042-015-2706-2

Protecting patient confidential information based on ECG reversible data hiding

Hui Wang[1] · Weiming Zhang[1] · Nenghai Yu[1]

Received: 30 January 2015 / Revised: 9 May 2015 / Accepted: 20 May 2015 /
Published online: 10 June 2015

Abstract Nowadays telecardiology is widely popular due to the fact that an increasing number of people are suffering from cardiac disease in the world. Therefore huge amount of ECG signal as well as patient confidential information will be transmitted via the Internet. Ibaida's wavelet-based data hiding technique aims to protect patient confidential data utilizing ECG signal as a host media. But it cannot completely reconstruct the original ECG signal. Any alteration of the ECG may lead to an inaccurate diagnosis conclusion drawn by the doctor, which cannot be accepted by patients. In this paper, our elemental standpoint requires that both patient information and ECG signal must be perfectly restored at the extraction side. Firstly a method is proposed to embed patient confidential data into ECG signal, while keeping its high visual quality. Then we use a unified embedding-scrambling method to guarantee the security of patient privacy as well as the ECG signal itself. The structure of watermarked ECG signal is severely deconstructed. Both of the experimental results demonstrate that our proposed methods are reversible. Moreover the latter scheme can achieve high information payload.

Keywords Telecardiology · Confidentiality · ECG · Reversible data hiding · Unified · Scrambling

This work was supported in part by the Natural Science Foundation of China under Grant 61170234 and Grant 60803155 and by the Strategic and Piloted Project of CAS under Grant XDA06030601.

✉ Weiming Zhang
zhangwm@ustc.edu.cn

Hui Wang
whglory@mail.ustc.edu.cn

Nenghai Yu
ynh@ustc.edu.cn

[1] Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China

1 Introduction

With the booming of the world population a significant rise in chronic diseases are threatening people's life security. An advanced telecommunication technology called telemedicine has become popular with the rapid development of innovative high-tech industries like mobile communication [6]. Telemedicine is the application of for diagnostic, monitoring and therapeutic purposes, which enables real-time data transmission from patients' whereabouts to a specialized medical care center [1]. The advantage of this technology consists of reducing the overall cost at hospitals and enabling doctors to adopt measures without delay to save life in emergence situation.

When using Internet as a key communication channel, it is of great significance for patients to control who can gain access to their privacy (name, age and address) and biological signals. If the information is available by unauthorized person, it will easily suffer from malicious attack. Any alteration of ECG signal and any leak of private information shall not be accepted by patients and doctors. To ensure the safety and integrity of patients' privacy as well as ECG signal, recently several researchers have applied data hiding technique to embed patient confidential information into ECG signal. Ibaida [5] introduced a wavelet-based data hiding technique but the ECG signal has suffered permanent destructions after extracting secret data. The result is prohibited because the unrecoverable distortion of ECG signal may leads to wrong diagnosis report for doctors. Ibaida's method is named as irreversible data hiding, a subcategory of data hiding, which places more emphasis only on correctly extracting the secret information regardless of the completely restore of the host cover media. Another technique named as reversible data hiding (RDH) is able to completely recover the original media. Because of its outstanding attribution of reversibility, it has been widely used in those applications like medical and military images' protection in which region data is confidential, sensitive and crucial.

RDH technique of images in the spatial domain can be further classified into three subcategories, compress-and-append, difference expansion (DE) and histogram shifting (HS).

The main idea of RDH based on compress-and-append technique is to find a compressible region to get redundancy space [3]. Then the data can be inserted into the space but the payload is always limited. Introduced by Tian [14], DE transforms the host image into a low-pass image containing the integer averages and a high-pass image containing the pixel differences. Then it expands two times the difference and embeds one bit of data by adding it to the expanded difference. In fact because of the expansion the resulting pixels may be out of the range. Thus it is necessary to use a location map to record these pixels which severely reduces the effective payload. To increase the effective payload, Thodi [12] proposed an improved DE called prediction-error expansion (PPE) embedding message into the prediction errors which better exploits the correlation inherent in the neighborhood of a pixel than the DE scheme. Ni's HS [8] method has higher visual quality than DE, but its performance is closely relied on the distribution of the host image. Combining PPE and HS, Thodi gains large payload as well as significantly improving image quality [13]. In essence to improve the performance of RDH, it consists of two steps, first to construct an accurate prediction template to get a sharp histogram, and then to embed message by modifying the histogram. Based on such point of view, Qin et al. [9] propose an adaptive strategy for choosing reference pixels according to the distribution characteristics of image content and then uses an image inpainting prediction template. Zhang et al. [15] proposed a coding method which recursively utilizes the decompression and compression process of an entropy coder. In this way their method improves the performance of previous RDH based on DE and HS.

In this paper, seeing that ECG signal is of vital importance to provide the diagnosis results of heart diseases, our elemental standpoint requires that both patient information and ECG signal must be perfectly reconstructed at the extraction side. Two RDH methods are proposed. The first one is to keep ECG signal's high visual quality after embedding data following conventional principle of RDH. The experiment results demonstrate that our method is reversible but the embedding capacity is low.

Ibaida et al. and the first RDH proposed in this paper only embed message into ECG signal to protect patient privacy. However ECG signal itself as a host is also patient's privacy whose security also needs to be guaranteed at the same time. To accomplish this goal, we further propose a new technique which combines data embedding and scrambling method. This method deliberately degrades ECG signal visual quality to a desirable level of distortion, quite different from conventional RDH. Results shows that it can gain large embedding capacity and keep ECG signal's reversibility.

The rest of the paper is organized as follows. In Section 2 the scheme of traditional ECG RDH will be proposed. Then Section 3 introduces a novel embedding and scrambling algorithm. Finally conclusion will be presented in Section 4.

2 ECG reversible data hiding

Although RDH has been flourished in 2-D images, few researchers use it on medical signal such as ECG. Due to its large size compared to other biological signals, it is suitable for ECG to be a host to embed privacy. The key point of PPE-HS RDH scheme is to find an accurate predictor to construct a sharp histogram. In this section a predictor called LLP [2] will be implemented in ECG signal.

2.1 Local liner prediction

Compared to fixed predictors like mean predictor, in which all weight coefficients are the same, we shall focus on liner predictors, which can adaptively make use of every term's distinction. Assume that ECG signal is $\mathbf{A} = (x_1, x_2, \cdots, x_N)$, where N is the total number of ECG sample points, and let x_i be the current point. For liner prediction, we should consider an indexing of prediction context to estimate x_i. By several experiment tests, a segment of points centered on x_i provides the most accurate prediction results. Thus the prediction context for x_i is $\{x_{i-k}, x_{i-k+1}, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{i+k-1}, x_{i+k}\}$, where $2k$ is the order of the liner predictor. Liner prediction can be written in form as:

$$\hat{x}_i = \sum_{\substack{p=-k,\\ p\neq 0}}^{k} \nu_p x_{i+p} \tag{1}$$

where $\nu = [\nu_1, \ldots, \nu_{2k}]'$ is the column vector with the coefficients of the predictor and can be derived by applying the least square (LS) approach. The LS predictor is denoted as follows which minimizes the sum of the squares of the prediction error:

$$\min \sum_i {e_i}^2 \tag{2}$$

in which $e_i = x_i - \hat{x}_i$.

Since the statistics of the ECG signal change from a region to another, it is impossible that a global liner predictor which contains all sample points will have a good performance. By dividing the signal into segments and by computing a distinct predictor for each segment, it can be expected that the predictor called local liner predictor (LLP) will provide better results.

Suppose the segment length is L, LLP computes a distinct column vector ν_i for each segment. Let y_i be the column vector obtained by scanning the current segment centered on x_i, which has $L - 2k$ points. And let X_i be the matrix whose rows are the corresponding context vectors, each of which contains $2k$ points. Then the local prediction error vector is $y_i - X_i\nu_i$. Equation (2) can be represented as

$$(y_i - X_i\nu_i)'(y_i - X_i\nu_i) \tag{3}$$

which has $2k$ unknown variables. Next we need to calculate the partial derivatives of every variable and set them to zero to get $X_i'^{X_i\nu_i} = X_i'^{y_i}$. Thus for the current segment ν_i is computed by as follows:

$$\nu_i = \left(X_i'X_i\right)^{-1}X_i'y_i \tag{4}$$

Next we consider if our predictor is reversible, a key concern in this work. To avoid sending all coefficients to the decoder, which can significantly reduces the amount of payload, we implement the prediction on segments containing both original and modified points not all original points. The detail is as follows. Let *start* be first local liner prediction points and *end* the last. Data is embedded from *start* to *end* but decoded in a reverse order. If one compares the segment taken at detection before the decoding of current points x_i, with the same segment, but taken at embedding before the embedding of x_i, it is immediately found that only x_i is different. Since the decoding proceeds from *end*, all the points following x_i have already been decoded to original value.

On the other hand, it is the character of reversibility of the algorithm that requires us not to take x_i into account for its prediction, whose prediction effect is not very good as a result. To further improve predictor accuracy, we add a point value close to x_i as a sample data for the computation of the current predictor. The estimation of approximate x_i(denoted as $\tilde{x}_i$) is as follows:

$$\tilde{x}_i = \frac{x_{i-2} + x_{i-1} + x_{i+1} + x_{i+2}}{4} \tag{5}$$

It should be noted that in (5) two out of four points, x_{i-2}, x_{i-1} are not original values, but already embedded ones. Experiment results show that it is more accuracy than that without the term $\tilde{x}_i$.

Take an example to further explain LLP, where segment length $L = 7$ and order $2k = 4$. At first we use (5) to get the approximate value $\tilde{x}_i$ in which the four points in are the red points in Fig. 1 including embedded value and original ones. By scanning the current

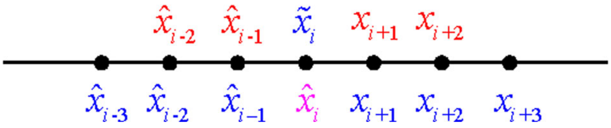


Fig. 1 Estimation of the current point x_i

segment centered on x_i, one will get $L - 2k = 3$ points, $y_i = \left[\hat{x}_{i-1}, \tilde{x}_i, x_{i+1}\right]'$ (blue points in Fig. 1) and the matrix $X_i = \begin{bmatrix} \hat{x}_{i-3} & \hat{x}_{i-2} & \tilde{x}_i & x_{i+1} \\ \hat{x}_{i-2} & \hat{x}_{i-1} & x_{i+1} & x_{i+2} \\ \hat{x}_{i-1} & \tilde{x}_i & x_{i+2} & x_{i+3} \end{bmatrix}$ (blue points), each row vector of which is centered on the corresponding point in y_i and made up of $2k = 4$ points. Then according to (4) we can obtain v_i and finally use (1) to get the estimated value $\hat{x}_i$ (magenta points in Fig. 1).

2.2 Prediction error expansion

By LLP we get the estimated value $\hat{x}_i$ of the original value x_i, then the prediction error is:

$$e_i = x_i - \hat{x}_i \tag{6}$$

Let $T > 0$ be the threshold, which controls the ECG distortion introduced by the watermark. Then the prediction error is modified as follows:

$$e_i' = \begin{cases} 2e_i + b, & \text{if } |e_i| < T \\ e_i + T, & \text{if } e_i \geqslant T \\ e_i - (T - 1), & \text{if } e_i \leqslant -T \end{cases} \tag{7}$$

where b is the message bit and e_i' is the modified prediction error. Then the modified point value x_i' is:

$$x_i' = \hat{x}_i + e_i' \tag{8}$$

At extraction, the decoder firstly gets the same prediction value $\hat{x}_i$, then computes following equation:

$$e_i' = x_i' - \hat{x}_i \tag{9}$$

If $-2T+1 < e_i' < 2T$, the decoder gets an expanded point. Then the secret bit b is extracted from e_i''s LSB and the original ECG sample value is restored as:

$$x_i = \frac{x_i' + \hat{x}_i - b}{2} \tag{10}$$

For the shifted points, the original value x_i can be recovered as follows:

$$x_i = \begin{cases} x_i' - T, & \text{if } e_i' \geqslant 2T \\ x_i' + T - 1, & \text{if } e_i' \leqslant -2T + 1 \end{cases} \tag{11}$$

As the amount of patients' confidential information is small, embedding capacity is not our major concern. The most important goal in our PEE-HS based ECG RDH is low distortion. Threshold T controls the embedding capacity and watermarked ECG distortion. Obviously the larger it is, the higher the distortion will be.

2.3 Data embedding

It proceeds data embedding in this section. To achieve the reversible goal, the encoder must transmit three variables (segment length L, the order of the predictor k and the threshold T) in a header file to the decoder.

Firstly we should divide the ECG signal into 3 parts, each of which uses different predictors. In Fig. 2, it needs to compute $a\_start = k + \left\lceil \frac{L-2k}{2} \right\rceil$, $a\_end = N - k - \left\lfloor \frac{L-2k}{2} \right\rfloor$, $b1\_start = 3, b1\_end = a\_start - 1$ and $b2\_start = a\_end + 1, b2\_end = N - 2$. Then follow steps:

1. Points in Part a compute estimated value by LLP as follows:
   (a) Extract centered points x_i in the current segment;
   (b) Replace x_i with $\tilde{x}_i$ computing (5);
   (c) Get X_i and y_i by scanning the segment;
   (d) Compute the local predictor coefficients with (4);
   (e) Compute $\hat{x}_i$ rounding the result of (1).
2. Points in Part $b1$ and Part $b2$ of ECG signal create exceptions to the predictor, which do not have a sufficient number of neighboring points that compose X_i andy_i. For such points, we will use a fixed predictor like (5) to predict their values, in which case $\hat{x}_i = round\left(\tilde{x}_i\right)$.
3. For other points in Part c, keep their original values unchanged and do not embed data into their locations.

The embedding proceeds from the first ECG points as follows, for the current x_i,

1. Compute $\hat{x}_i$ by different predictors;
2. Compute the prediction error e_i with (6);
3. Compute the modified prediction error e_i' using (7);
4. Use (8) to calculate the modified prediction value x_i';
5. Data underflow/overflow problem should be solved. Expansion embedding and histogram shifting of some points will result in over range of the modified points value $x_i{}'$. In our experiment every ECG data is formed of 12 bits. Thus if $x_i{}' \in [0, 4095]$, replace x_i by $x_i{}'$ and if $x_i{}' \in [0, \mathrm{T} - 1] \cup [4095 - \mathrm{T}, 4095]$, insert the flag bit $b = 1$ into the next embeddable point; otherwise if $x_i{}' \notin [0, 4095]$, keep x_i unchanged and insert the flag bit $b = 0$ into the next embeddable point.

Take an example to further explain data embedding process mentioned above. Consider a segment of five points as shown in Table 1. The five points are intended to display different cases possible at embedding. Suppose that the original value, predicted value and prediction error are shown in the first three rows of Table 1. Let the threshold T is 4 and the secret bit stream is $S = 01011011....$

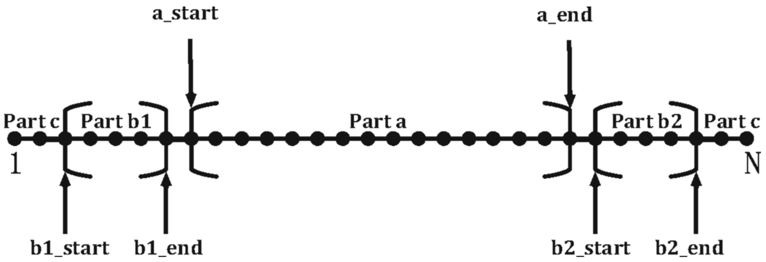


Fig. 2 Dividing ECG signal into 3 parts

Table 1 An example of data embedding process

Original value	Predicted value	Prediction error	Modified value
3872	3879	−7	3869
4094	4092	+2	4094
4091	4088	+3	4094
4085	4085	0	4086
4075	4076	−1	4074

Since the first prediction error e_i is -7, whose absolute magnitude is greater than T, the histogram shifts to the left by $T - 1 = 3$. As a result the modified value $x_i{}'$ is 3870 and S is unchanged. The second point value x_i is 4094 and e_i is $+2$, which is smaller than T. But expanding the prediction error, one will get $e_i' = 4$ and $x_i{}' \notin [0, 4095]$, causing overflow problem. Thus keep x_i unchanged and insert flag bit 0 into the first location of S. Now bit stream $S = 001011011....$ Next x_i is 4091 and e_i is also $+2$, which is smaller than T and can be embeddable. After expanding e_i and embedding bit b = 0, the first bit of S, $x_i{}'$ will be 4094, which belongs to [0, T − 1] ∪ [4095 − T, 4095]. Therefore a flag bit 1 should be added to S in the first place. Now bit stream $S = 101011011....$ The next two points are both embeddable and $x_i{}' \notin$ [0, T − 1] ∪ [4095 − T, 4095], so just embed the first two bits of S into the two points and the modified value is shown as Table 1. Then bit stream S is 1011011. . ..

2.4 Exaction and restoration

The decoder just proceeds in a reverse order from the last point. The process is defined below.

1. First one should get three parameters L, k and T in a header file, then partition the ECG signal into 3 parts as said in Section 2.3.
2. Next one should select the corresponding predictor to obtain the estimated value $\hat{x}_i$.
3. Compute the modified prediction error e_i' using (9). The process of extraction and restoration is as follows.
   (a) If e_i' lies outside the range $(-2T + 1, 2T)$ and the point value $x_i{}'$ lies outside the range [0, T − 1] ∪ [4095 − T, 4095], the point has been shifted. Just shift it back to get its original value according to (11).
   (b) If e_i' lies in the range $(-2T + 1, 2T)$ and $x_i{}'$ lies outside the range [0, T − 1] ∪ [4095 − T, 4095], the point has been expanded. Then the secret bit b is extracted from the LSB of e_i' and the original ECG sample value is restored as (10).
   (c) If x_i' lies in the range [0, T − 1] ∪ [4095 − T, 4095], one should tell apart whether x_i has been embedded or unchanged. Since the encoder has embedded flag bits in the next embeddable points and the decoding is done in the reverse order, the flag bit is firstly decoded then it determines if the current point has been embedded or unchanged. The flag bit will be dropped from the secret bit stream. If the flag bit is 0, it means x_i unchanged, that is to say $x_i{}' = x_i$. If the flag bit is 1 and e_i' lies in the range $(-2T + 1, 2T)$, the point has been expanded, in which case it is decoded in the same way as case (b). Otherwise it is decoded as case (a).

2.5 Experiment results

In this paper we evaluate our scheme based on MIT-BIH format ECG signal, an important universal format standard easily stored and transported, which comes from MIT-BIH Arrhythmia Database [7, 11]. Each sample is 10 s long with 360-Hz sampling frequency.

We use two metrics to evaluate the proposed reversible watermarking model. One is used to measure the embedding capacity named BPS (bits per sample point) calculated as:

$$BPS = \frac{Bit}{SP} \tag{12}$$

where Bit denotes the total amount of message embedded and SP denotes the number of sample points. The other is PRD (percentage residual difference) computed to judge the distortion between original ECG host signal and the watermarked ECG signal as

$$PRD = \sqrt{\frac{\sum\limits_{i=1}^{N}(x_i - y_i)^2}{\sum\limits_{i=1}^{N}{x_i}^2}} \times 100\ \% \tag{13}$$

where x represents the original ECG value and y is the watermarked signal value, both of which are the true ECG signal values in the time domain.

Table 2 Proposed method: *BPS* and *PRD* results for 20 ECG samples

No.	*BPS*	0.05	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45
	PRD									
1		0.370	0.504	0.616	0.718	1.058	1.162	1.255	1.344	1.423
2		0.361	0.500	0.609	0.698	1.060	1.116	1.214	1.318	1.416
3		0.344	0.474	0.565	0.664	0.958	1.065	1.134	1.213	1.283
4		0.151	0.214	0.258	0.298	0.445	0.491	0.525	0.564	0.596
5		0.252	0.352	0.432	0.492	0.740	0.818	0.885	0.947	0.996
6		0.132	0.185	0.224	0.265	0.400	0.435	0.471	0.499	0.528
7		0.302	0.418	0.508	0.597	0.878	0.961	1.029	1.098	1.175
8		0.224	0.311	0.381	0.434	0.655	0.726	0.781	0.832	0.887
9		0.130	0.179	0.217	0.263	0.383	0.416	0.449	0.480	0.508
10		0.164	0.224	0.275	0.319	0.474	0.521	0.558	0.597	0.640
11		0.143	0.197	0.246	0.289	0.417	0.465	0.501	0.539	0.576
12		0.158	0.216	0.262	0.308	0.455	0.500	0.537	0.572	0.607
13		0.466	0.632	0.769	0.894	1.309	1.438	1.555	1.666	1.747
14		0.484	0.709	0.885	1.129	1.489	1.619	1.770	1.896	2.020
15		0.380	0.548	0.668	0.775	1.149	1.252	1.357	1.447	1.533
16		0.248	0.344	0.413	0.483	0.734	0.799	0.858	0.916	0.972
17		0.432	0.626	0.767	0.846	1.279	1.414	1.519	1.636	1.709
18		0.182	0.257	0.309	0.361	0.535	0.586	0.634	0.678	0.725
19		0.432	0.581	0.706	0.828	1.231	1.352	1.446	1.548	1.649
20		0.187	0.264	0.327	0.380	0.565	0.618	0.669	0.719	0.763
Average		0.277	0.386	0.471	0.552	0.810	0.887	0.957	1.025	1.087

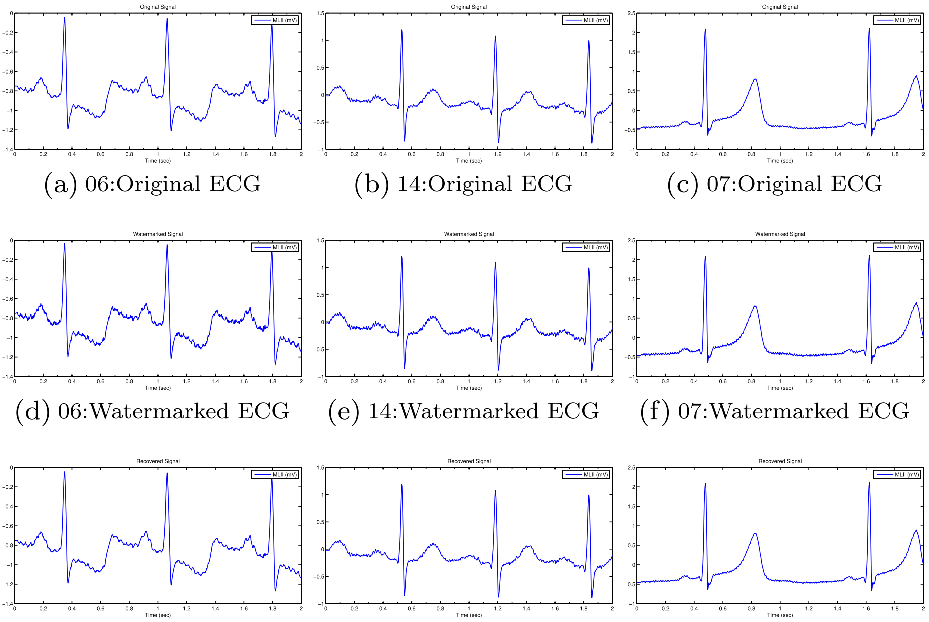
It is easily inferred that as threshold increases, both of above metrics will become larger. So we firstly investigate how segment length and order exert an influence on both metrics when the threshold remains 1 unchanged. It is noticed that the optimal segment length and order depend on the test ECG sample. Considering the true fact that the efficiency of proposed algorithm will reduce as both factors increase, we use a fixed segment of length $L = 15$ and the fixed order is $2k = 6$. Luckily compared to the optimum values determined for each sample we conclude that the loss of BPS and PRD is very small. The maximum BPS loss, 0.024 bit, appears in ECG sample No. 20. And the maximum PRD loss, 0.009 %, appears in ECG sample No. 17.

Tables 2 and 3 shows the results of proposed method and Ibaida [5] obtained for 20 MIT-BIH arrhythmia ECG samples. Due to the reason that Ibaida et al. do not measure their embedding capacity, we just put emphasis on the distortion. It can be seen that PRD turns larger as BPS increases for all samples in our method. Accordingly, when the embedding capacity is 0.45 bit per sample point the average distortion between watermarked signal and original is very small, just only 1.087 %. By contrast the average PRD in [5] is 0.659 %, smaller than ours. However their method is nor reversible. Pay attention to the PRD extracted it is 0.902 % which may cause wrong result of diagnosis for doctors.

Moreover Fig. 3 shows three ECG original samples, and the resultant signals after watermark and extraction process, in which ECG sample $No.06$ has the best result. However $No.14$ is the worst result and $No.07$ is approximate to the average. Although the

Table 3 Ibaida [5]: *PRD* and *PRD extracted* results for 20 ECG samples

Sample no	PRD	PRD extracted
01	0.651	0.900
02	0.584	0.794
03	0.542	0.744
04	0.400	0.552
05	0.303	0.410
06	0.384	0.528
07	0.479	0.663
08	0.488	0.663
09	0.451	0.600
10	0.667	0.920
11	0.797	1.073
12	0.843	1.161
13	1.051	1.429
14	0.711	0.966
15	1.073	1.454
16	0.660	0.916
17	0.619	0.855
18	0.799	1.113
19	0.925	1.298
20	0.762	0.993
Average	0.659	0.902



(a) 06:Original ECG (b) 14:Original ECG (c) 07:Original ECG

(d) 06:Watermarked ECG (e) 14:Watermarked ECG (f) 07:Watermarked ECG

(g) 06:Recovered ECG (h) 14:Recovered ECG (i) 07:Recovered ECG

Fig. 3 ECG signal before embedding patient confidential information, after embedding and after extracting

PRD of ECG $No.14$ is large, it is difficult to notice the distortion for naked eyes. All of the samples are well restored after data extraction. The obtained experimental results further prove that our proposed scheme is reversible, no distortion to ECG signal after extraction.

3 Unified ECG embedding-scrambling reversible data hiding

Traditional RDH aims to keep the visual quality of watermarked ECG, but it exposes the patient ECG itself. Since ECG can reflect a lot of aspects of physical status, it should be well protected. To meet such vital demand we propose a unified ECG embedding and scrambling method called UES [10], which deliberately degrades ECG structure. Instead of changing the least significant bit, we will embed external information in a direct replacement. Although severely destroying the perceptual quality of the host ECG, it can still perfectly restore the original ECG signal at the decoder. Moreover UES can significantly increase embedding capacity.

3.1 Proposed scheme

We also use LLP as a predictor, but there is a little difference. On one hand, since the locations of the predicted points are vacated to insert information by direct replacement, it will result in larger prediction error if doing like Section 2.1 in which case we embed data right after finishing the prediction for the current point. Instead we will firstly predict all the points and then implement data embedding. On the other hand, considering the basic target of our scheme is reversible, we need to select a segment of points ended on x_i instead of centered on it as Section 2.1. Therefore (5) is changed as follows,

$$\tilde{x}_i = x_{i-1} + \frac{\Delta x_{i-1} + \Delta x_{i-2}}{2} \tag{14}$$

where $\Delta x_{i-1} = x_{i-1} - x_{i-2}$, $\Delta x_{i-2} = x_{i-3} - x_{i-4}$, all of the four points are original values.

The proposed scheme consists of LLP tailored for Huffman coding. In order to be reversible at detection the segment length, the order of the predictor, Huffman compression dictionary $dict$ and compressed prediction error code stream EB should be stored in a header. The embedding proceeds from the last ECG points as follows, for the current x_i,

1. Compute $\hat{x}_i$ by different predictors as Section 2.3, but replace (5) by (14);
2. Compute the prediction error e_i with (6);
3. Get all points' prediction error E repeating step 1 and 2;
4. Create prediction error code stream EB and Huffman compression dictionary $dict$ by Huffman coding;
5. Directly insert the header file and secret information into the predicted locations.

The decoder needs to extract information and recover signal in an order contrary to the encoder. One should extract $dict$ and decoder EB to obtain E in the first place then extract the secret information. The extraction procedure is simple, just directly carrying on. Next according to point position, select the appropriate predictor as Section 2.3. Finally one just needs to compute (15) for every sample point to obtain original value x_i:

$$x_i = \hat{x}_i + e_i \tag{15}$$

Thus ECG signal will be perfectly recovered.

Table 4 *BPS* and *PRD* results for 20 ECG samples

Sample no	BPS	PRD
01	7.9733	2.1179e+03
02	7.9336	2.1252e+03
03	7.4358	878.4971
04	7.8717	1.4528e+03
05	8.3300	893.4514
06	7.8097	1.5603e+03
07	8.2858	1.3850e+03
08	7.4636	721.6234
09	8.0242	930.2058
10	7.7792	826.8294
11	8.0742	898.3971
12	8.3192	2.8444e+03
13	7.6375	2.7891e+03
14	7.5361	2.0601e+03
15	7.4342	1.2769e+03
16	7.8972	2.2624e+03
17	8.1528	1.1646e+03
18	7.9161	2.0106e+03
19	8.0250	2.5370e+03
20	8.0256	1.2044e+03

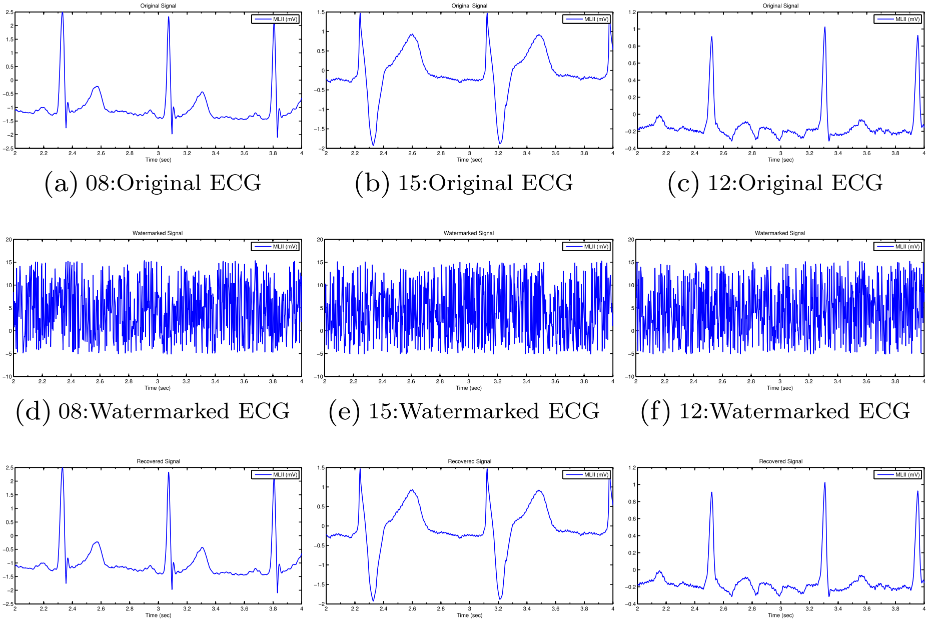
3.2 Experiment results

In this experiment we let the segment length is 17 and the order of the predictor is 4. It is noticed from Table 4 that the proposed scheme can achieve very high information embedding capacity for each ECG sample. The average capacity is computed as follows,

$$BPS_{average} = \frac{\sum_{i=1}^{20} BPS_i}{20} = 7.8962 \tag{16}$$

which means that it can be embedded 7.8962 bits per sample point on average. Since every point in MIT-BIH format ECG signal is formed of 12 bits, it can be inferred that the embedding rate is high, approximate to 65.8 %. Although scheme proposed by Ibaida et al. does not introduce embedding capacity, the maximum value will not be larger than 1 bit per sample. Compared to ECG RDH based on wavelet transform [16] in which embedding payload is larger than 56 Kb, approximate to 0.2 bit per sample point, our capacity is much larger.

For each ECG sample, the distortion of watermarked signal are considered objectively using PRD and subjectively by visual inspection. It is observed from Fig. 4 all of samples' perceptual quality is severely degraded, giving rise to hardly telling apart whether it is an ECG signal. Although the huge number of modifications in the structure of the original signal, the reconstruction process is perfectly successful. The results further demonstrate and verify that our approach is fully reversible, which not only protects patients' secret information but also ensures ECG signal's own security.



(a) 08:Original ECG (b) 15:Original ECG (c) 12:Original ECG

(d) 08:Watermarked ECG (e) 15:Watermarked ECG (f) 12:Watermarked ECG

(g) 08:Recovered ECG (h) 15:Recovered ECG (i) 12:Recovered ECG

Fig. 4 ECG signal before embedding patient confidential information, after embedding and after extracting

Table 5 The average running time for 20 ECG samples

Code language	Running time(s)
Matlab	14.852
C++	0.336

3.3 UES complexity analysis

Next we investigate the computation complexity of UES method. Generally the computation is mainly made up of two parts, one is the local liner prediction (LLP), and the other is Huffman compress algorithm. As above, let N, L, $2k$ be the length of the ECG sinal, the segment length and the order of the predictor, respectively. It should be noticed that, for common length ECG signals, one has $N \gg L$.

At first, we figure out the computation of Huffman coding [4]. As a kind of greedy algorithms, it aims to minimize the average code length. If the frequency of a character is high, the dictionary will be short. On the contrary the dictionary will be long. The main idea of Huffman coding is to construct a Huffamn tree. And the computation complexity is $\mathrm{O}\left(N \log\left(N\right)\right)$.

Next we discuss the computation of LLP, which calculates a distinct predictor for each sample points. One should solve approximate to N systems extracted from the local L segment length. In one system one just should consider the computation of $v_i = \left(X_i' X_i\right)^{-1} X_i' y_i$. The size of matrix X_i and the corresponding vector y_i is $(L-2k) \times 2k$ and $2k$ respectively. Since multiplications are more expensive than the additions, we take into account only on the multiplications for simplicity. The product of matrices for a single system demands $8k^3(L-2k)^2$. The total cost of all systems become $8k^3(L-2k)^2N$. In the light of the results we experimented, we has $N \gg 8k^3$ and $N \gg (L-2k)^2$ and they can be viewed as a constant. So the computation complexity is $\mathrm{O}\left(N\right)$.

Combine the complexity of Huffman coding and LLP, the final computation complexity of UES is $\mathrm{O}\left(N \log\left(N\right)\right)$. The average execution time of the proposed unified ECG embedding-scrambling RDH on a standard 10 s long with 360 Hz sampling frequency for 20 MIT-BIH arrhythmia ECG samples is 14.852 s for the Matlab code and 0.336 s for the C++ code (using GCC 4.8 of the GNU complier collection). These results are obtained on a common computer with Intel Core(TM)2 Duo E7500 processor at 2.93 GHz, 2 GB of RAM and a 32-bit Windows 7 Ultimate operation system. The average running time is present in Table 5. Since the cost of UES is too small, which is much less than the ECG acquisition time, they can be processed in a parallel way at the same time. So UES is suitable for real-time processing and it will not bring additional overhead.

4 Conclusion

In this work, our elementary demand is that ECG signal must be completed restored after extraction in order to diagnose illness precisely for doctors. We proposed two RDH methods based on ECG to protect patient confidential information. One is to keep ECG signal's structure following the conventional principle of reversible data hiding. We tested 20 ECG samples from MIT-BIH Arrhythmia Database. Experimental results show that the average distortion between the watermarked ECG and the original one is approximately 1 %. The other scheme integrated data embedding with scrambling to protect ECG signal and patient privacy, in which output ECG quality is no longer a concern. It obtained high embedding capacity about 7.8962 bits per sample point on average. Experimental results demonstrate that both methods are reversible, which is vital. Both of methods is suitable for real-time processing.

References

1. Birati E, Roth A (2011) Telecardiology. Isr Med Assoc J 13:498–503
2. Dragoi I (2014) Local-prediction-based difference expansion reversible watermarking. IEEE Trans Image Process 23(4):1779–1790
3. Fridrich J, Goljan M (2002) Lossless data embedding for all image formats. In: SPIE proceedings of photonics west, electron. imaging, security and watermarking of multimedia contents, vol 4675, pp 572–583
4. Huffman DA (1952) A method for the construction of minimun-redundancy codes. Proc IRE 1098–1102
5. Ibaida A, Khalil I (2013) Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. IEEE Trans Biomed Eng 60(12):3322–3330
6. Lin Y, Jan I, Ko P, Chen Y, Wong J, Jan G (2004) A wireless PDA-based physiological monitoring system for patient transport. IEEE Trans Inf Technol Biomed 8(4):439–447
7. Moody CB, Mark RG (2002) The impact of the MIT-BIH arrhythmia database. IEEE Eng Med Biol Mag 3(20):45–50
8. Ni Zh, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circ Syst Video Technol 16(3):354–362
9. Qin C, Chang C, Huang Y, Liao L (2013) An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism. IEEE Trans Circ Syst Video Technol 23(7):1109–1108
10. Rad RM, Wong K, Guo J (2014) An unified data embedding and scrambling method. IEEE Trans Image Process 23(4):1463–1475
11. Song XG, Deng QK (2004) On the format of MIT-BIH arrhythmia database. Chin J Med Phys 21(4): 230–232
12. Thodi D, Rodriguez J (2004) Reversible watermarking by prediction-error expansion. In: Proceedings of IEEE, southwest symposium on image analysis and interpretation, pp 21–25
13. Thodi DM, Rodriguez JJ (2007) Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16(3):721–730
14. Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circ Syst Video Technol 13(8):890–896
15. Zhang W, Hu X, Li X, Yu N (2013) Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression. IEEE Trans Image Process 22(7):2775–2785
16. Zheng K, Qian X (2008) Reversible data hiding for electrocardiogram signal based on wavelet transforms. Computat Intell Secur 1:295–299

Hui Wang received his B.S. degree in electronic engineering from Hefei University of Technology in 2014. He is currently pursuing the M.S. degree in electronic engineering in University of Science and Technology of China. His research interests include information hiding.

Weiming Zhang received his M.S. degree and Ph.D. degree in 2002 and 2005 respectively from the Zhengzhou Information Science and Technology Institute, Zhengzhou, China. Currently, he is an associate professor with the School of Information Science and Technology, University of Science and Technology of China. His research interests include information hiding and cryptography.

Nenghai Yu received his B.S. degree in 1987 from Nanjing University of Posts and Telecommunications, M.E. degree in 1992 from Tsinghua University and Ph.D. degree in 2004 from University of Science and Technology of China, where he is currently a professor. His research interests include multimedia security, multimedia information retrieval, video processing and information hiding.