Reversible data hiding in ECG Signals Based on Histogram Shifting and Thresholding

WenchaoWu, Bin Liu, Weiming Zhang
Key Laboratory of Electromagnetic Space Information,
Chinese Academy of Sciences, P. R. China,
School of Information Science and Technology,
University of Science and Technology of China,
Hefei, Anhui, 230027, P.R.China

Changwen Chen
University at Buffalo,
the State University of New York
Buffalo, NY, 14260-2000 USA

***Abstract*—With the development of communication and networking technologies, the telemedicine system has become more and more popular due to its distance unawareness, low cost to the patients, long-term physiological data recording and real-time diagnosis. In order to protect the private information of patients when transmiting data in the telemedicine system, data hiding technique is used by hiding the patient confidential information in the ECG signals. In this paper, a reversible data hiding scheme for patient privacy protection is proposed. An integer-to-integer Harr wavelet transform for the integer ECG signal is adopted to guarantee the reversibility. A histogram shifting and thresholding scheme is carefully designed to adaptively embed private data according to the given capacity and recover both the private data and the original ECG signal without any distortion. Simulation results show that the proposed method outperforms the existing method.**

Keywords*—*ECG, reversible data hiding, wavelet transform, histogram shifting

I. Introduction

With the increasingly global aging trend, a significant rise of chronic diseases among the elderly has made it important to design a more reliable, real-time and convenient health-care system. During the recent years, with the development of sensor technologies as well as networking and mobile communication technologies, the widely use of remote health-care monitoring system, usually called telemedicine [1], has become more and more popular. Monitoring patients at their home can reduce the cost for patients to visit hospitals and also the traffic around the hospitals. It can also provide more reliable and real-time diagnose service as patients' medical information can be sent immediately to doctors and responses can be timely sent back.

In the telemedicine system, it is important to protect patient privacy and data security. An easy way to achieve it is encryption[2], [3], [4], i.e., patients' private data are encrypted by the sender and decrypted on the receiver side. Besides encryption, another technique is adopted by more and more researchers, namely data hiding. By hiding patients' sensitive information, e.g., name, age, identification number, etc, inside patients' insensitive data, e.g., ECG signals, EEG signals, etc, we could not only protect patient privacy from invasion, but also make the data management more convenient. We only need to manage the embedded host signals instead of both the host and the private data, thus the mismatch between patient name and patient physiological data would never happen. It will not incur any increment in the host size either. Furthermore, we can build an authorized channel between patient and doctor if we embed authentication information in the host data. In the telemedicine system, researchers usually use the ECG signal as the host signal to carry the patient private information as well as readings from other sensors. The ECG signal is selected because most health-care systems will collect ECG information and the size of ECG signal is large enough to hide private data.

Engin, *et al.* [5] implemented a wavelet based watermarking/data hiding technique for ECG signal by computing the average power for each sub-band and using the power as threshold parameters to select which sub-band to embed data. Kaur, *et al.* [6] developed an embedding way by using low frequency chirp signal to embed watermark data. Ibaida, et al. [7] described a low complexity way of embedding watermark by combining the Quantisation Index Modulation (QIM) and Least Significant Bit (LSB) substitution method. The watermark data is embedded by using LSB substitution watermarking method after linear transform of the original signal. In [8], they also proposed a method to embed watermark data into a position called special range numbers. By this way, it could achieve the minimum distortion to the original signal and make it hard for attacker to recognize where the private data is embedded. In [9] , Ibaida *et al.* proposed a wavelet-based watermarking technique which combines encryption and scrambling technique to protect patient's confidential data. It uses the shared key to encrypt the secret data and apply scrambling technique to determine which sub-band of wavelet transform coefficients to embed the confidential data. The common disadvantage of technique mentioned above is that they can not recover the original ECG signals without any distortion after extracting the watermark data from the embedded signals. This may cause the doctor getting wrong diagnosis and bring great harm to the patient. Zheng *et al.* [10] proposed a reversible watermarking algorithm based on ECG signals by applying wavelet transform. The private data are hiden in the non-QRS coefficients of ECG signals to achieve the least distortion of QRS complex waves. However, this method has low embedding capacity and limited performance because only one-level wavelet transform is used and at most one bit could be embedded in each high frequency coefficient of non-QRS waves. Furthermore, the algorithm only performs well for normal ECG signals since it is difficult to detect QRS complex for abnormal signals.

Seeing that undistorted ECG signals is of great importance to provide the proper diagnosis of heart diseases, we propose a reversible data hiding method for ECG signals to protect the patient confidential information and also guarantee the perfect recovery of original ECG signals. To achieve the reversibility, multi-level integer-to-integer Harr wavelet transform is used. The private data is embedded into the multi-level high-frequency wavelet coefficients of ECG signals to achieve least distortion after embedding as well as high embedding capacity. A histogram shifting and thresholding scheme is designed for data embedding to guarantee the undistorted recovery of original ECG signals after extracting the private data. To achieve the inperceptibility of the signal, we select coefficients between the threshold range to hide private data according to the given embedding capacity. By applying the proposed data hiding scheme, we can finally achieve high capacity as well as high quality after embedding.

The paper is organized as follows. In Section II, the proposed reversible data hiding scheme is illustrated in details. The experimental results are given and analyzed in Section III. Finally, we conclude the paper in Section IV.

II. Proposed Algorithm

Here we propose a reversible data hiding scheme in ECG signals for patient privacy protection. In order to recover both the private data and original ECG signals without distortion, we apply histogram shifting and thresholding technique based on integer-to-integer Harr discrete wavelet transform (DWT). Firstly, we divide the original ECG signals into non-overlapping segments and then apply multi-level integer-to-integer Harr wavelet transform to them. The signal segmentation process is applied since the data hiding process may cause overflow (above the upper bound) or underflow (blow the lower bound) problem after embedding. Those segments with overflow or underflow problem will be ignored and only trouble-free segments are used for data hiding. We use a location map to register whether a segment can embed data or not. Secondly, we embed the payload into the high frequency coefficients of ECG segments by a well-designed histogram shifting and thresholding scheme whose parameters can be adaptively adjusted to meet the capacity requirement. In order to recognize which segments have data embedded at the receiver end, we embed the location map and other side information in the low frequency coefficients of ECG segments by using LSB substitution method.

A. Invertible Integer-to-Integer Harr Wavelet Transforms

We try to embed the main payload in the high-frequency coefficients of wavelet transform such that low difference is induced after embedding. However, as ECG signals are stored as integers after preprocessing by the A/D converter, conventional floating-point wavelet transform cannot achieve the reversible watermarking scheme, which will result in distortion. To avoid this problem, we adopt the invertible integer-to-integer based lifting wavelet transform scheme [11], [12], [13], which could map integer ECG signals to integers and does not cause any distortion after inverse transforms.

The lifting based Harr wavelet transform consists of 3 steps named as split, predict and update. In the split step, the data set are divided into odd index and even index elements. Then the next odd element is set to be the difference between the current odd and even element in the prediction step.

$$odd_{j+1} = odd_j - even_j \tag{1}$$

In the update step, the next even element is replaced with the floor of the average of the previous even/odd pair. By this way, we can achieve the reversibility of the wavelet transform.

$$even_{j+1} = \lfloor \frac{even_j + odd_j}{2} \rfloor \tag{2}$$

B. Histogram Shifting and Thresholding Scheme

In order to avoid the overlapping problem, i.e., the value after embedding overlaps with the non-embedded value, caused by embedding and make it possible to be reversible, a histogram shifting and thresholding scheme is proposed. In the proposed scheme, two threshold values T_l and T_h are used, where T_l is the negative low threshold and T_h is the positive high threshold. The histogram shifting encoding algorithm modifies the high-frequency coefficients d_i as follows,

$$D_i = \begin{cases} 2d_i + b, & \text{if} \quad d_i \in [T_l, T_h] \\ d_i + T_h + 1, & \text{if} \quad d_i > T_h \geq 0 \\ d_i + T_l, & \text{if} \quad d_i < T_l < 0. \end{cases} \tag{3}$$

The decoder recovers the original coefficients and embedded bit b from D_i according the following equation,

$$d_i = \begin{cases} \lfloor \frac{D_l}{2} \rfloor, & \text{if} \quad D_i \in [2T_l, 2T_h + 1] \\ D_i - T_h - 1, & \text{if} \quad D_i > 2T_h + 1 \text{ and } T_h > 0 \\ D_i - T_l, & \text{if} \quad D_i < 2T_l \text{ and } T_l < 0, \end{cases} \tag{4}$$

$$b = D_i \bmod 2, \quad D_i \in [2T_l, 2T_h + 1]. \tag{5}$$

By using the technique above, we can avoid the overlapping problem after embedding. The value of T_l and T_h is adjusted according to the capacity requirement and the distortion depends on the histogram shape and the thresholds. In order to decrease the distortion as low as possible after embedding, it is important to select proper high frequency coefficients to embed data. According to equation (3) , the smaller the coefficient is, the less distortion will be caused after embedding. Therefore, the high frequency coefficients are selected from low-level sub-band to high-level sub-band and from zero to larger absolute value by properly setting the initial values of T_l and T_h.

C. Overflow and Underflow Detection

In the proposed scheme, the original ECG signals are divided into non-overlapping segments before DWT to solve overflow/underflow problem. A location map L is used to describe the status of segments. The size of L equals to the number of segments and each element of L contains 1 bit information indicating the status of the corresponding segment.

The values of ECG signals usually lie in a specific range according to the sampling voltage. For example, the ECG signals from MIT-BIH Arrhythmia Database [14] lie in the range of [0, 2048). The histogram shifting of the high-frequency coefficients may cause the overflow/underflow problem, i.e., the value exceeding the specific range. For the segments with overflow/underflow problem, the proposed data hiding scheme is no longer reversible, thus it is necessary to detect these segments and not to use them as watermarking host.

Since we embed the data in the coefficients after lifting Harr wavelet transform, it is hard to judge whether the overflow/underflow problem happens according to the coefficients after embedding. To detect the overflow/underflow segments exactly, we apply the inverse wavelet transform first, and then detect if any value is out of range. If no value is out of range, a bit with value 1 is set to the corresponding element of location map L, otherwise the value 0 is set and the corresponding segment will not be used to embed data.

When decoding the watermarked signal, we should have the location map L in hand to get the knowledge about which segments containing hidden data. In order to achieve this, we embed the location map in low-frequency coefficients of ECG signals by using LSB substitution technique. It only changes a little to the relatively large low-frequency coefficients and will not cause overflow/underflow problem.

In summary, the data to be embedded consists of two parts, the side information embedded in the low frequency and the main payload embedded in the high frequency coefficients. The side information includes the location map L, the value T_l, T_h and the size of the payload $|P|$. To achieve the reversible performance, we also need to record the original LSBs into an array LL which has the same size as all the side information mentioned above. Thus the total data to embed into the high-frequency coefficients is

$$B = LL \cup P \tag{6}$$

We embed the data into the high-frequency coefficients of effective segments by using the histogram shifting and thresholding scheme introduced in subsection B.

D. Reversible Encoding and Decoding Algorithm

The process of the reversible encoding scheme is shown in Fig. 2. The sender firstly splits the original signal into segments and then apply multi-level Harr DWT to get original low frequency and high frequency coefficients. According to the given capacity of data B, we embed the data into the high frequency coefficients from small to large value by changing the threshold T_l and T_h. Finally, LSB substitution method is used to embed the side information and then apply the inverse Harr DWT to get the embedded signals. The whole process is summarized in Algorithm 1.

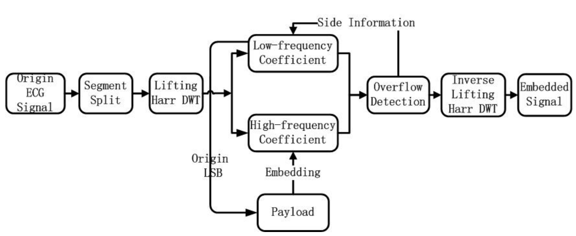

Fig.2 The encoding process of reversible data hiding

The decoding algorithm is almost the inverse process of the encoding algorithm. After receiving the embedded signals, the receiver firstly split the signals according the segment size and then apply multi-level Harr DWT to get the low frequency and high frequency coefficients. The side information is extract from the low frequency coefficients and used to extract the payload and LL from the high frequency coefficients according to equation (4) and (5). Finally, the inverse Harr DWT is applied to recover the original signals. The corresponding decoding process is shown in Fig. 3.

Algorithm 1 The Embedding Process

Input Origin ECG signal $\boldsymbol{E}$, segment size s, embedded data $\boldsymbol{P}$
Output The embedded ECG signal $\hat{\boldsymbol{E}}$

```
initialize T_l = -1, T_h = 0, T = 0;
Divide E according to s into segments E[n], n is the number of segments;
Set LL = 0, the length of LL is M = n + 7bit (the size of T_l) + 7bit (the size of T_h) + 21bit (the size of |P|) ;
for i=1:n do
    COEF = multi-level HarrDWT(E[i]);
    LOW = low frequency LSBs of COEF;
    Insert LOW into LL until LL is full;
end for
B = LL ∪ P, set R = |B|, length of B,indicate remain data to embed;
while (TRUE) do
    for i=1:n do
        COEF = multi-level HarrDWT(E[i]);
        Embed B according equation (3);
        if Overflow or Underflow then
            set Location map L;
            continue;
        end if
        Reduce R;
        if R == 0 then
            break;
        end if
    end for
    if R == 0 then
        break;
    else
        T_h += 1 or T_l -= 1 (change in turn);
        R = |B|;
    end if
end while
Embed side information using LSB substitution;
Applying inverse Harr discrete wavelet transform;
```

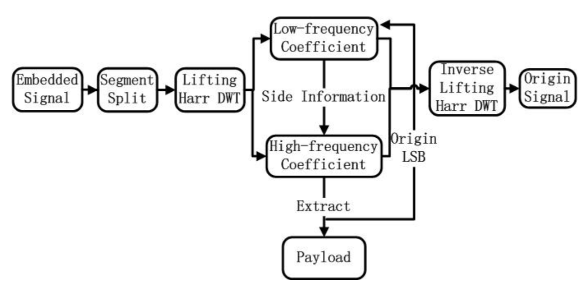

Fig.3 The decoding process of reversible data hiding

III. SIMULATION RESULTS

In this section, we evaluate the proposed scheme based on the MIT-BIH format ECG signal, an important universal

TABLE I. THE NRMSE COMPARISON OF THE PROPOSED METHOD AND THE METHOD IN [10]

Signal	Capacity	[10](%)	Our(%)	Capacity	Our(%)
100.dat	74.6kb	0.1196	0.0710	324.3kb	0.1928
121.dat	71.6kb	0.1286	0.0756	324.3kb	0.2135
122.dat	68.9kb	0.1922	0.1186	324.3kb	0.3076
205.dat	68.1kb	0.1036	0.0690	324.3kb	0.1835
207.dat	67.9kb	0.1222	0.0793	324.3kb	0.2241

TABLE II. THE NRMSE OF THE PROPOSED METHOD FOR THE ABNORMAL SIGNAL

Signal	Capacity	Our(%)
615.dat	74.6kb	0.1130
425.dat	74.6kb	0.0981
428.dat	74.6kb	0.1113
429.dat	74.6kb	0.1551
418.dat	74.6kb	0.1507

format standard easily stored and transported from the MIT-BIH Arrhythmia Database. The sampling frequency is 360 Hz and the length of the ECG signal is 30 min. We choose the segment size as 256 which is close to the RR interval of the ECG signal. In order to embed more payload data and have enough space to hide side information, we select a 4-level lifting Harr discrete wavelet transform.

To evaluate the proposed model, The normalized root-mean-square error (NRMSE) is used to measure the distortion caused by data hiding, which is calculated as

$$\mathbf{NRMSE} = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N} x_i^2}} \times 100\% \tag{7}$$

where x represents the original ECG signal and y is the watermarked signal. We compare the performance of the proposed method with that of another reversible data hiding method introduced in [10] and the simulation results are shown in Table 1.

From Table 1 we can see that with the same embedding capacity, the proposed method has around half NRMSE of the method in [10]. This is due to the fact that the histogram shifting and thresholding scheme is designed to adaptively choose proper high frequency coefficients for data hiding, which alleviates the distortion effect of embedding. Furthermore, high embedding capacity requirement could be easily handled with the proposed scheme. As shown in Table 1, even if the capacity is enlarged to more than 300kb, the NRMSE still keeps as low as far less than 1% and the visual impact also changes little, especially in the QRS part.

The algorithm in [10] only performs well for normal ECG signals because it is difficult to detect QRS complex for abnormal signals. However, our proposed algorithm performs well even for the abnormal signal. The simulation results of the proposed algorithm for abnormal signals are shown in Table 2. From the table, we can see that the NRMSE of the proposed algorithm is near to the NRMSE of normal signals in [10] as shown in Table 1. The NRMSE is still far less than 1% and the visual impact still changes little.

In Fig. 4 and Fig. 5, we show the visual impact of part of the normal signal (100.dat) before and after embedding with capacity of 74.6kb and 324.3kb, respectively. And in Fig.6, we show the visual impact of part of the abnormal signal (425.dat) before and after embedding with capacity of 74.6kb.

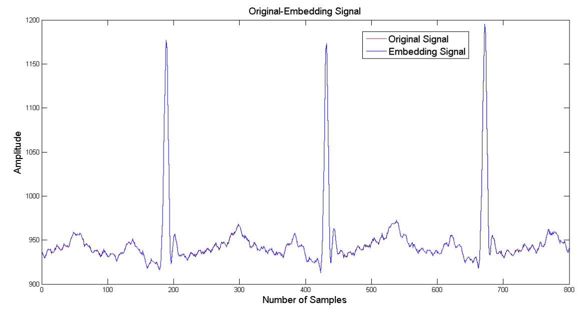

Fig.4 The visual impact with capacity 74.6kb of 100.dat

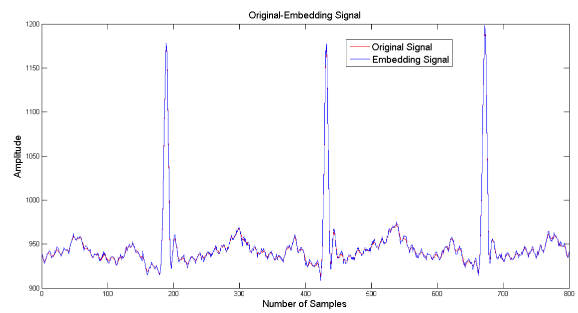

Fig.5 The visual impact with capacity 324.3kb of 100.dat

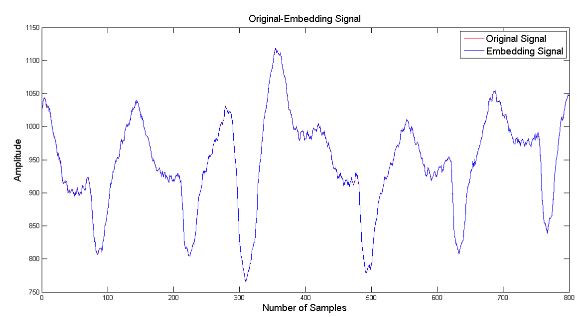

Fig.6 The visual impact with capacity 74.6kb of 425.dat

IV. CONCLUSION

In this paper, a novel reversible data hiding technique to embed patient private information into the host ECG signal is proposed. By adopting reversible multi-level Harr DWT, a histogram sifting and thresholding scheme is proposed to achieve high embedding capacity, low distortion and guarantee the recovery of the original ECG signal without any loss. Experiment results demonstrate the effectiveness of the proposed scheme.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China(Grant No.61202406) and the USTC Grand Master Professor Funds(ZC9850290097).

References

[1] Y.-H. Lin, I.-C. Jan, P.-I. Ko, Y.-Y. Chen, J.-M. Wong, and G.-J. Jan, "A wireless pda-based physiological monitoring system for patient transport," *IEEE Trans. Information Technology in Biomedicine*, vol. 8, no. 4, pp. 439–447, 2004.

[2] F. Hu, M. Jiang, M. Wagner, and D.-C. Dong, "Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/software codesign," *IEEE Trans. Information Technology in Biomedicine*, vol. 11, no. 6, pp. 619–627, 2007.

[3] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," *IEEE Trans. Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34–41, 2008.

[4] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," *IEEE Trans. Information Technology in Biomedicine*, vol. 13, no. 6, pp. 946–954, 2009.

[5] M. Engin, O. Çıdam, and E. Z. Engin, "Wavelet transformation based watermarking technique for human electrocardiogram (ecg)," *Journal of medical systems*, vol. 29, no. 6, pp. 589–594, 2005.

[6] S. Kaur, O. Farooq, R. Singhal, and B. S. Ahuja, "Digital watermarking of ecg data for secure wireless commuication," in *Recent Trends in Information, Telecommunication and Computing (ITC), 2010 International Conference on*. IEEE, 2010, pp. 140–144.

[7] A. Ibaida, I. Khalil, and R. Van Schyndel, "A low complexity high capacity ecg signal watermark for wearable sensor-net health monitoring system," in *Computing in Cardiology, 2011*. IEEE, 2011, pp. 393–396.

[8] A. Ibaida, I. Khalil, and D. Al-Shammary, "Embedding patients confidential data in ecg signal for healthcare information systems," in *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*. IEEE, 2010, pp. 3891–3894.

[9] A. Ibaida and I. Khalil, "Wavelet based ecg steganography for protecting patient confidential information in point-of-care systems," *IEEE Trans. Biomedical Engineering*, vol. 60, no. 12, 2013.

[10] K.-m. Zheng and X. Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms," in *Computational Intelligence and Security, 2008. CIS'08. International Conference on*, vol. 1. IEEE, 2008, pp. 295–299.

[11] A. Calderbank, I. Daubechies, W. Sweldens, and B.-L. Yeo, "Wavelet transforms that map integers to integers," *Applied and computational harmonic analysis*, vol. 5, no. 3, pp. 332–369, 1998.

[12] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," *Journal of Fourier analysis and applications*, vol. 4, no. 3, pp. 247–269, 1998.

[13] W. Sweldens, "The lifting scheme: A construction of second generation wavelets," *SIAM Journal on Mathematical Analysis*, vol. 29, no. 2, pp. 511–546, 1998.

[14] G. B. Moody and R. Mark, "Mit-bih arrhythmia database directory," *MITBIH Database Distribution, Harvard–MIT Division of Health Sciences and Technology, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA. Available on the World Wide Web at:(http://www. physionet. org/physiobank/database/html/mitdbdir/mitdbdir. htm)(last date visited: Jul. 23, 2008)*, 1992.