ECG Steganography to secure patient data in an E-Healthcare System

Dolly Meghani
VIT University, Chennai
+91 9176191031
dollymeghani14@gmail.com

S.Geetha
VIT University, Chennai
+91 9842550862
geethabaalan@gmail.com

ABSTRACT

E-healthcare systems are rapidly gaining importance with the evolution of remote monitoring devices for patient diagnosis. While transmitting patient classified information, it is essential to ensure that patient confidentiality is maintained. ECG signals are used as a medium to mask the patient’s confidential data. ECG steganography is achieved by using Discrete Wavelet Transform along with Singular Value Decomposition. To assure that minimal distortion is reported after embedding the data, two distortion metrics namely, Percentage Residual Difference and Bit Error Rate are used. The proposal is implemented on MIT-BIH database and it has been observed that the proposed approach offers minimum distortion hence retaining the authenticity of the original signal.

Keywords

ECG Steganography; Discrete Wavelet Transform; Singular Value Decomposition

1. INTRODUCTION

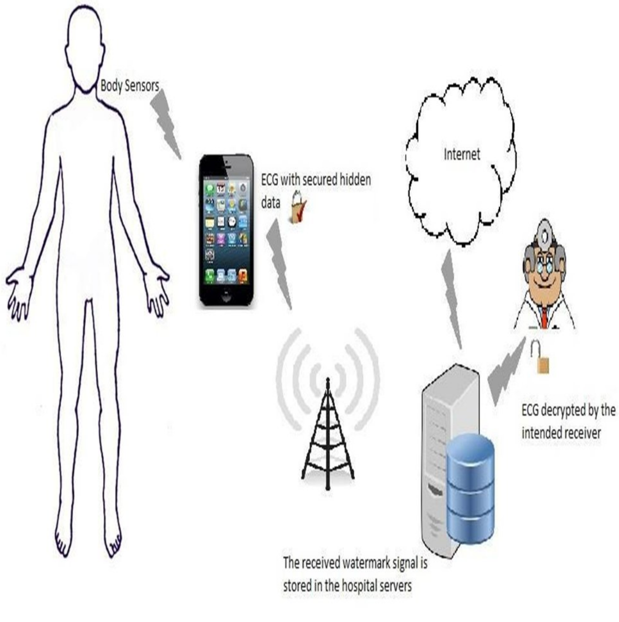
There has been a swift advancement in the use of point-of-care technologies. The patient can easily be monitored from a remote place by transmitting essential health coordinates such as blood pressure, temperature, glucose level; by the means of internet. These amelioration not only saves the hassles of visiting a health care unit, but also prove to be of immediate assistance in case of emergencies. The programmed sensors collect the required information and transmit it over the dedicated channels to the requested servers. Figure 1 shows an ideal health care monitoring system. As internet is used as a mode of transmission of data, it involves threat to patient privacy. The information may be misused or received by unintended receiver. Hence, it is fundamental to safeguard the data so that it meets the patient confidentiality laws as laid by the government. The federal law enforced Health Insurance Portability and Accountability Act (HIPAA), to ensure that electronic health information is secured in all the electronic forms. HIPAA mandates the Electronic Health Records (EHR) manager to consider the following laws:

i) Patient’s confidentiality: It is imperative to ensure that that the patient has the rights to authorize the access to her/his confidential data such as name, date of birth, medical history and MediClaim number as given in Figure 2.

ii) Security: The EHR issuing authorities has to assure that the patient data is transmitted through secure means. They are liable to inform the patient about the use and distribution of the patients to the concerned circles such as insurance authorities and medical pharmacies. Hence, the patient has the sole right over the medical data and can choose the audience and the means of sharing his/her medical data. This also suggests that the means chosen to transmit the data must be secure and must not be vulnerable to the attacks by unintended receivers.

Hence the patient is to be provided with improved and efficient an monitoring system which provides convenience. The measures to build a secure EHR include having access controls such as passwords, so that the information is accessible only to limited audience; encrypting the information and having audit trails to monitor the user of the information as laid down by HIPAA.

However, these measures might not prove to be sufficient as encrypted data can be viewed and decrypted by expert hackers. Also, encryption includes large computational overheads and storage capacities. The encrypted based techniques [1], [2] are not suggestable for PDAs where there might be limited storage space. Steganography technique is proposed where data is hidden in other insensitive data without increasing the size of the cover.



Body Sensors
ECG with secured hidden data
Internet
ECG decrypted by the intended receiver
The received watermark signal is stored in the hospital servers

Figure 1. ECG Steganography illustration in E-Healthcare systems.

DOI: 10.1145/2909067.2909078

Patient Confidential Information

Name:	Dolly
Date of Birth:	01/04/1993
Address:	VIT University
Medicare number:	0123456789
Telephone number:	0123456789

Patient Diagnosis Information

Blood pressure

Glucose level

Temperature

Location

Patient Biometric Information

Figure 2. Patient Data containing patient information and sensor readings

ECG signals are used as a cover as they are large in size so the extended of the sensitive information can be varied used without much consideration of the size

The proposed technique first converts the patient related data to ASCII values which is further converted to binary stream. The obtained result is termed as watermark which is used to embed in the Signal. The Signal is primary converted into a 2D ECG image where the watermark is hidden. The data is hidden using Discrete Wavelet Transform (DWT) on the data obtained from MIT-BIH database [3]. Singular Value Decomposition (SVD) is applied on the image to embed the secret data. To obtain the original image and data after transmission, Inverse DWT is applied and the image is reconstructed into its original form. By implementing this technique, it is aimed to abide by HIPAA standards for secure transmission and storage of electronic medical data.

The further sections of this paper are arranged asper the following sequence: Section 2 gives a gist of the related work that has been done in the proposed field. Next, Section 3 deals with the proposed methods where suggested modules are explained in detail. Section 4 explains the evaluation methods and the results obtained. Finally, concluding remarks are shared in section 5.

2. RELATED WORK

Significant advancement has been observed in the field of data hiding for medical datasets. However the challenging task is to define the efficiency of methods proposed and how productive are they in generating secure algorithms for data transmission. When ECG is used as a cover, it is essential to ensure that the significance of the signal remains the same after watermarking and extraction. Hence, minimal distortion should be achievable after reverse transform is applied. Also, each data hiding technique faces the limitation on the amount data that can be hidden for a given cover size. Various studies have been conducted which use ECG as a cover image. ECG steganography is done on ECG signals [4] using DWT and Least Significant Bit algorithm. In addition, encryption and scrambling approaches are used on the secret data to enhance security. A curvelet based steganography has been proposed where the ECG signal is decomposed using Fast Discrete Curvelet Transform [5]. The proposed method uses quantization to embed the data along with threshold algorithm to choose the coefficients for embedding. A reversible data hiding technique is proposed using B- spline waves to identify the QRS complex [6]. After detecting the R waves, Haar wavelet transform is enforced to decompose the signals. The non-QRS wavelet coefficients are selected and shifted to 1 bit towards the left, where the watermark is embedded. However this limits the size of the watermark where only 1 bit can be embedded per ECG sample. A study was conducted to measure the efficiency of the wavelet decomposition techniques used for Signal decomposition. [9] It was observed that Discrete Cosine Transform and DWT perform better than Discrete Fourier Transform.

A reversible blind watermarking technique is proposed using medical images such as MRI for hosting the data. [8]. 2- D wavelet transform is applied to detect the sub bands and two thresholds are selected based on the positions of the sub bands. A zero point is created by shifting the high and the low sub band towards the left and right respectively to embed the watermark. However, this algorithm works well only for MRI images and not for ECG signals.

Quantization is used as one of the most commonly used technique for watermarking. In SVD, quantization factor determines the distortion of the original cover signal. [7] A lower single scaling factor provides better efficiency where as a higher single scaling factor provides better shield against external attacks. However, it is easy to determine a uniform single scaling factor in case of an attack is attempted.

3. PROPOSED SYSTEM

3.1 Pre-processing of ECG Signal and Patient data

The ECG signals used are from MIT-BIT database [3]. The ECG signals consist of waves from which QRS Complex is considered to be the most crucial part in the given waves. The obtained signals have the frequency of 128 Hz and a gain of 200. The 1D ECG signals are converted into 2D ECG signal image for the purpose of embedding using Tompkins algorithm for each fiducial mark of the QRS complex. The patient data is first converted into its equivalent ASCII values. These ASCII values are further converted into their respective binary streams. Hence the data now obtained is in the streams of 1’s and 0’s. Further security is added by converting these bits using XOR encryption as it is reversible and cannot be easily detected. Hence this adds an additional layer of security.

3.2 Embedding and Extraction

DWT is used against Discrete Fourier Transform as it has the advantage of measuring time against frequency. Hence, it proves to be ideal for ECG. When DWT is applied on the 2D ECG Signal Image, various sub bands are obtained. It is observed that the most imperative parts of the signal such as QRS complex lie in the lower levels of the sub bands.

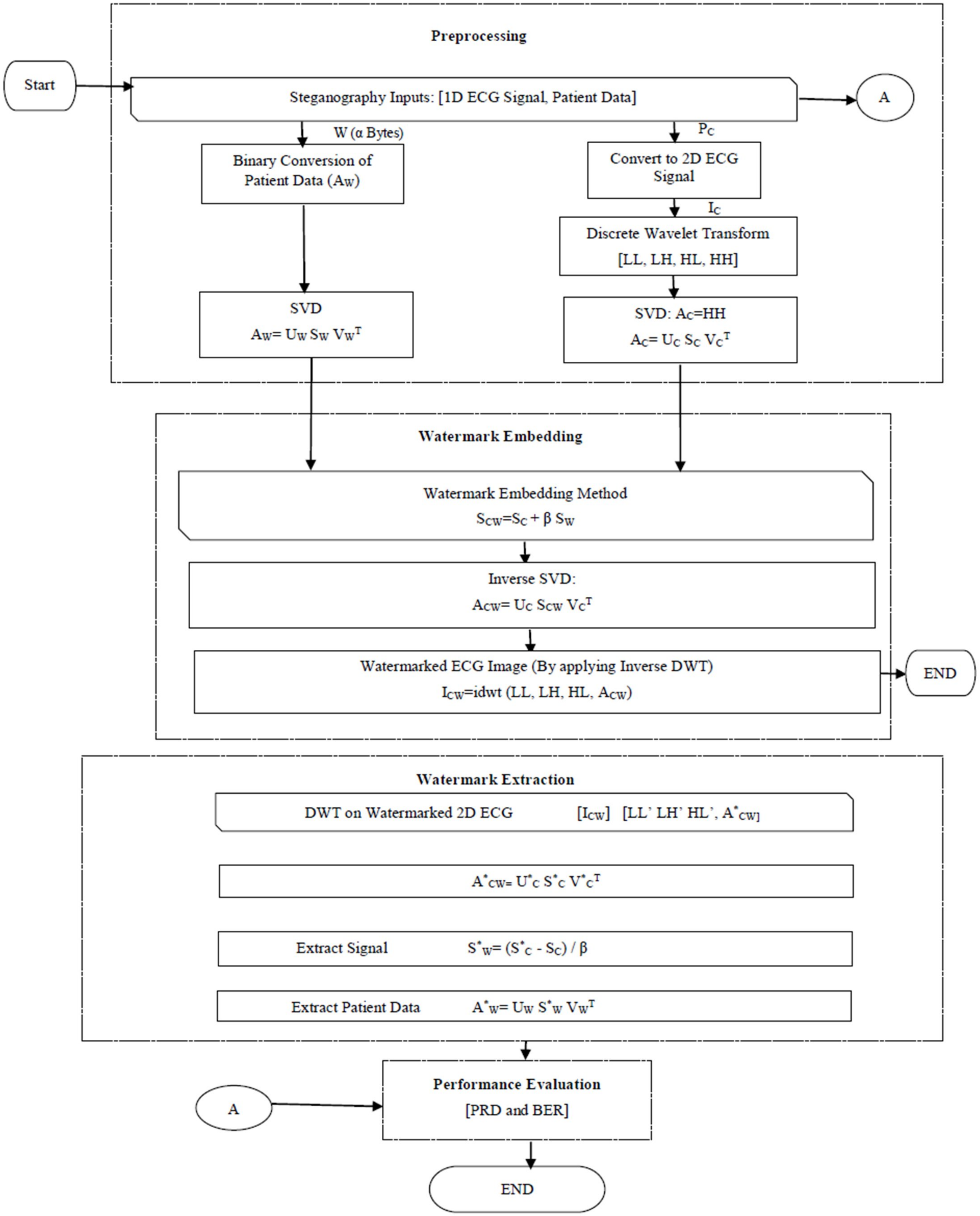

Preprocessing
Start
Steganography Inputs: [1D ECG Signal, Patient Data]
A
W (α Bytes)
P_C
Binary Conversion of Patient Data (A_W)
Convert to 2D ECG Signal
I_C
Discrete Wavelet Transform [LL, LH, HL, HH]
SVD
$A_W= U_W S_W V_W^T$
SVD: A_C=HH
$A_C= U_C S_C V_C^T$
Watermark Embedding
Watermark Embedding Method
$S_{CW}=S_C + \beta S_W$
Inverse SVD:
$A_{CW}= U_C S_{CW} V_C^T$
Watermarked ECG Image (By applying Inverse DWT)
I_{CW}=idwt (LL, LH, HL, A_{CW})
END
Watermark Extraction
DWT on Watermarked 2D ECG [I_{CW}] [LL' LH' HL', A^*_{CW}]
$A^*_{CW}= U^*_C S^*_C V^*_C{}^T$
Extract Signal $S^*_W= (S^*_C - S_C) / \beta$
Extract Patient Data $A^*_W= U_W S^*_W V_W^T$
Performance Evaluation [PRD and BER]
A
END

Figure 3. Wavelet Transform based ECG Steganography architecture

Hence, out of the four levels that are obtained LL, LH, HL, and HH; HH proves to be the most ideal sub band to embed the data. DWT is also used an optimal choice as the inverse transform can be applied on the sub bands to obtain the original image. Furthermore, SVD is used as a factorization technique which is widely used in reducing the dimensions. The algorithm for the proposed technique is demonstrated in Figure 3.

3.2.1 Watermark Embedding Algorithm

Step 1: The 2D ECG signal with is obtained from the original signal is decomposed into sub bands of four different level using the equation (1). Hence, four sub bands are obtained namely LL, LH, HL, and HH using Haar 4 wavelet.

$$[LL, LH, HL, HH] = dwt\ (I_C) \qquad (1)$$

Step 2: The coefficient matrix (Ac) of the sub band is then subjected to SVD.

$$[U_C\ S_C\ V_C^T] = SVD\ (A_C) \qquad (2)$$

Step 3: The watermark A_W is then subjected to SVD.

$$[U_W\ S_W\ V_W^T] = SVD\ (A_W) \qquad (3)$$

Step 4: Addictive quantization is applied to embed the values of the watermark (S_W) into the cover signal (S_C). Here, β is used as the scaling factor.

$$S_{CW} = S_C + \beta\ S_W \qquad (4)$$

Step 5: To reconstruct the coefficients after embedding, apply the inverse SVD to the modified coefficients A_{CW} of the high frequency band HH.

$$A_{CW} = [U_C\ S_{CW}\ V_C^T] \qquad (5)$$

Step 6: Inverse DWT is applied to build the watermarked image which now consist of the secret data. As given in equation (6)

$$I_{CW} = idwt\ (LL, LH, HL, A_{WT}) \qquad (6)$$

3.2.2 Watermark Extraction Algorithm

Step 1: Apply the DWT on the watermarked image I $_{CW}$ to obtain [LL_{CW}, LH_{CW}, HL_{CW}, HH_{CW}]

Step 2: SVD is then applied to the coefficient matrix of A^*_{CW} of the high frequency band HH_{CW} to obtain singular values of the watermarked images.

Step 3: Evaluate the singular values of the extracted watermark from S*C as given below

$$S^*_W = (S^*_C - S_C) / \beta \qquad (7)$$

Step 4: From Eq. 3 which consist of UC and VCT values, retrieve the watermark A^*_W using inverse SVD.

$$A^*_W = [U_C\ S^*_W\ V_C^T]$$

4. EVALUATION AND RESULTS

To measure the rate of distortion caused in the original signal and the watermarked signal, Percentage Residual Difference (PRD) is proposed as given in equation 8.

$$PRD = \sqrt{\frac{\Sigma \quad ((\; - \;)^2)}{\Sigma \quad ^2}} \qquad (8)$$

Where p represents the ECG signal and q represents the watermarked signal.
The results obtained from the PRD are given in table 1.

Table 1: Performance metrics for Bit Error Rate

Sample No	PRD %	PRD extracted %
1	0.44336	0.54661
2	0.57813	0.78582
3	0.58836	0.80713
4	0.52756	0.77654
5	0.54341	0.72231
6	0.58613	0.80903
7	0.57654	0.69987
8	0.28971	0.32212
9	0.45129	0.63465
10	0.50559	0.71287
11	0.43549	0.6123
12	0.44126	0.59062

Alternatively, BER is also used to calculate the bit shift error that is caused when the image is watermarked. The equation to calculate the Bit Error Rate is given as follows:

$$BER = \frac{}{} * 100\% \qquad (9)$$

It has been observed that as the length of the watermark increases, the bit error rate also increases. This can be seen from the figure 4 where α is the watermark metrics.

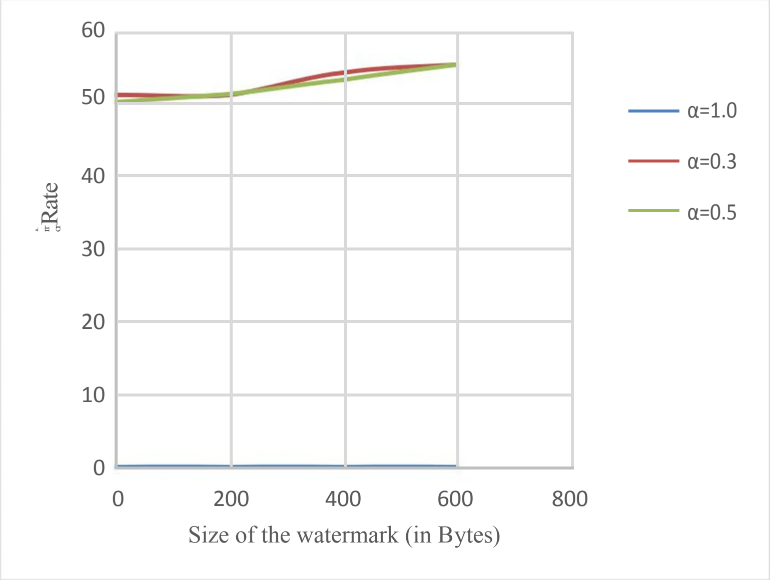


Figure 4. The performance of BER upon the chance of α values.

5. CONCLUSION

We observe that a novel ECG steganography algorithm is obtained where the distortion is minimal and does not largely affect the ECG readings. This approach can be further used in studying and transmitting EEG signals. Also, with the emergence of IoT, the technique can be embedded along with remote sensors that are available in wearables such as smart watches, ECG bands and other remote monitoring devices.

6. REFERENCES

[1] F. Hu, M. Jiang, M. Wagner, and D. Dong. 2007. Privacy-preserving tele cardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign. IEEE Trans. Inf. Technol. Biomed.11, 6 (Nov.2007), 619–627.

[2] W. Lee and C. Lee. 2008. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Trans. Inf. Technol. Biomed.12, 1 (Jan.2008), 34–41.

[3] Goldberger AL, Amaral LAN, Glass L, Hausdorff JM, Ivanov PCh, Mark RG, Mietus JE, Moody GB, Peng C-K, Stanley HE. PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals. Circulation 101(23):e215-e220; 2000 (June 13).

[4] Ayman Ibaida and Ibrahim Khalil. 2013. Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems. In IEEE Transactions on biomedical engineering.60, 12 (DEC 2013), 3322-3330.

[5] S. Edward Jero, Palaniappan Ramu, S. Ramakrishnan. 2015. ECG steganography using curvelet transform. Biomedical Signal Processing and Control. 22 (Aug 2015),161–169

[6] K. Zheng and X. Qian.2008.Reversible data hiding for electrocardiogram signal based on wavelet transforms.In Proc. Int. Conf. Comput. Intell. Security. 1, (Dec. 2008), 295–299.

[7] Mishra,A., Agarwal,C., Sharma,A. and Bedi,P. (2014).Optimized gray scale image water marking using DWT–SVD and Firefly Algorithm. Expert Systems with Appli-cations, 41, 17, (2014), 7858–7867.

[8] H. Golpira and H. Danyali. (2009).Reversible blind watermarking for medical images based on wavelet histogram shifting. In Proc. IEEE Int. Symp. Signal Process. Inf. Technol. (Dec.2009), 31–36.

[9] S.T. Chen, Y.J. Guo, H.N. Huang, W.M. Kung, K.K. Tseng, S.Y. Tu. (2014)Hiding patients confidential data in the ECG signal via transform-domain quantization scheme, J. Med. Syst.38,6. (June 2014), 1-8.