J Med Syst (2014) 38:132
DOI 10.1007/s10916-014-0132-z

PATIENT FACING SYSTEMS

Discrete Wavelet Transform and Singular Value Decomposition Based ECG Steganography for Secured Patient Information Transmission

S Edward Jero · Palaniappan Ramu · S Ramakrishnan

Received: 28 May 2014 / Accepted: 21 August 2014

Abstract ECG Steganography provides secured transmission of secret information such as patient personal information through ECG signals. This paper proposes an approach that uses discrete wavelet transform to decompose signals and singular value decomposition (SVD) to embed the secret information into the decomposed ECG signal. The novelty of the proposed method is to embed the watermark using SVD into the two dimensional (2D) ECG image. The embedding of secret information in a selected sub band of the decomposed ECG is achieved by replacing the singular values of the decomposed cover image by the singular values of the secret data. The performance assessment of the proposed approach allows understanding the suitable sub-band to hide secret data and the signal degradation that will affect diagnosability. Performance is measured using metrics like Kullback–Leibler divergence (KL), percentage residual difference (PRD), peak signal to noise ratio (PSNR) and bit error rate (BER). A dynamic location selection approach for embedding the singular values is also discussed. The proposed approach is demonstrated on a MIT-BIH database and the observations validate that HH is the ideal sub-band to hide data. It is also observed that the signal degradation (less than 0.6 %) is very less in the proposed approach even with the secret data being as large as the sub band size. So, it does not affect the diagnosability and is reliable to transmit patient information.

Keywords ECG steganography · DWT-SVD watermarking · KL performance metric · ECG image

This article is part of the Topical Collection on *Patient Facing Systems*

S. Edward Jero (✉) · P. Ramu
Department of Engineering Design, Indian Institute of Technology Madras, Chennai, India
e-mail: edwardjero@gmail.com

S. Ramakrishnan
Department of Applied Mechanics, Indian Institute of Technology Madras, Chennai, India

Introduction

Advances in medical domain have lead to the development of various electronic medical devices for the purpose of diagnosis and treatment of diseases. Developments in data transmission allow for remote access of these diagnosis data through wired or wireless networks. Often times, patient personal information is transmitted with the medical diagnosis data. Irrespective of the transmission medium, the personal information is subjected to hack threat [1]. To prevent the personal information theft, Department of Health and Human Services under US government even introduced an act: Health Insurance Portability and Accountability (HIPPA). HIPPA gives rights for privacy to individuals [2]. Under circumstances where the patient diagnosis information needs to be transmitted [3], Steganography is a useful technique that hides personal information inside medical information. Examples for the personal information include: name, age, gender, location etc. Examples for the medical information include Magnetic Resonance Imaging (MRI), Electrocardiogram (ECG), Electro encephalogram (EEG). These form the cover signal and owing to embedding of the secret data, they degrade and affect diagnosability. A good Steganography technique should not compromise the diagnosability and should be robust under external attacks.

Steganography is achieved by embedding the secret data into the cover signal using a watermarking algorithm. This results in modifying the cover signal. It is to be noted that not all parts of a cover signal carries crucial information about diagnosis. So, the art of steganography lies in identifying the points that don't contribute much to the diagnosability and embed the information there so that even degradation to the original cover signal do not affect diagnosability. Therefore, it is desirable to develop a Steganography algorithm that can selectively identify the frequency bands of signal where the secret data can be embedded so that there is less compromise

Published online: 04 September 2014

on the diagnosability while the patient information is also secure. Here, ECG is the cover signal and personal information is the watermark. The performance of a Steganography procedure can be assessed by the measure of distortion in cover data and amount of secret data retrieved correctly.

Typically, Steganography has been practiced in images [4–10], network communication [11, 12], audio signals mostly directed towards [13, 14] multimedia application. Steganography hides secret information inside base information, whereas in cryptography the secret information is encrypted and less secure than Steganography [15]. Steganography techniques are classified into substitution system, transform domain, spread spectrum method, statistical methods and distortion techniques [16]. In substitution system, locations of redundant data of cover signal are identified to embed the secret information. In transform domain the cover signal is transformed using any one of the transforms like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Slantlet Transform (SLT) and its coefficients carries the secret data [4, 5, 10]. Statistical methods use the statistical characteristics of cover signal to identify the location for secret data [17]. The locations where the secret data is embedded in the cover signal can also be formulated as a hypothesis testing problem [18]. In [19], Hilbert filling curve maps the cover image into 1D pixels and by using an adaptive pixel pair matching approach, they hide the data in the pixel value difference of three pixels leading to secured transmission of patient information.

Transform domain is widely used in Steganography in conjunction with various watermarking techniques to embed the secret data into cover signal. Three watermarking techniques: patchwork, least significant bit and quantization methods are evaluated for their performance on EEG cover signal in[20]. They observed that patchwork method performs better. In [21], the performance of ECG steganography using quantization watermarking scheme with various transforms like DWT, DCT and DFT are evaluated and it is observed that DCT and DWT provide better results than DFT. [22] Investigates DWT based ECG steganography using threshold watermarking algorithm and two wavelet functions namely: daubechies 2 and biorthogonal. They show that daubechies 2 performs better than biorthogonal wavelet function. When medical image is used as cover signal, LSB watermarking and error correcting code techniques are used to embed the watermark in [23]. The DWT based watermarking for signal integrity verification is investigated in [24] for ECG signal. However, this is not very secure against external threats. Wavelet based ECG Steganography is achieved by using the combination of encryption and scrambling technique in [25]. [26] Uses DWT to perform ECG steganography and as well achieve data compression. Private metadata is embedded and retrieved in [27] using ECG. [28] Hides the patient information in retinal fundus image where patient information is encrypted using error control coding techniques. In medical image watermarking, in order to enhance data security, the region to which watermark need to be embedded is analyzed and categorized in [29].

The performance of a Steganography approach depends on the watermarking algorithm. The watermarking algorithm should allow for easy embedding and retrieval of the secret data while being robust against external attacks or unauthenticated access. Researchers [24] use techniques like scrambling matrix to shuffle the secret data information embedded in the cover signal. Here, we use Singular Value Decomposition (SVD) technique. Researchers used SVD technique for digital image watermarking [4, 29]. Watermarking scheme in [8, 9] uses combined DWT and SVD for watermarking of digital images. SVD watermarking technique in [13] is applied for audio cover signal. The advantage of using SVD technique is to achieve blind detection of watermark. That is, the receiver does not require the cover image to retrieve the secret data.

The effectiveness of a Steganography algorithm is qualified using metrics like Peak Signal to Noise Ratio (PSNR), Percentage Residual Difference (PRD), Kullback–Leibler Divergence (KL), which are used to analyze the watermarked signal in terms of imperceptibility, fidelity and robustness. Bit Error Rate (BER) is used to qualify the loss in the retrieved secret data.

The rest of the paper is organized as follows: Preliminaries presents discussion on DWT and SVD. Proposed methodology is discussed next followed by a discussion on Performance evaluation metrics. Finally, the summary is presented in Results and discussion.

Preliminaries

Discrete wavelet transform

The wavelet transforms are one of the widely used techniques to understand signals in a joint time- frequency domain. A wavelet is a simple oscillating wave that exists only in a finite domain and is zero elsewhere. The finite domain is typically a window in a large signal. The transform is about convolving the signal with the wavelet at different time instances and is expressed as [30]:

$$x(t) = \frac{1}{\sqrt{M}} \sum_{x} W_{\varphi}(j_0, k)\varphi_{j_0,k}(t) + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} \sum_{k} W_{\psi}(j, k)\psi_{j,k}(t) \quad (1)$$

$$W_{\varphi}(j_0,k)=\frac{1}{\sqrt{M}}\sum_{t}x(t)\varphi_{j_0,k}(t) \tag{2}$$

$$W_{\psi}(j,k)=\frac{1}{\sqrt{M}}\sum_{t}x(t)\psi_{j,k}(t) \tag{3}$$

The discrete wavelet transform decomposes a signal $x(t)$ into wavelet coefficients where W_{φ} are the approximation coefficients W_{ψ}, the detailed coefficients. The scaling function is $\varphi_{j_0,k}(t)$; j_0 is an arbitrary starting scale and $j \geq j_0$. The wavelet function $\psi_{j,k}(t)$ is defined as follows:

$$\psi_{j,k}(t)=2^{-i/2}\psi\left(2^{-i}t-j\right) \tag{4}$$

Where ψ is the wavelet and the transforming function, j and k are the scale and position parameters of the wavelet. $1/\sqrt{M}$ is a normalizing factor. In many applications, the signals are discrete and DWT is achieved by passing the time domain signal through a high pass and low pass filter which filters out the high and low frequency components of the signal. The filtering of the signal into low and high frequency components is called decomposition and each pass is denoted as a level [31, 32]. This decomposition can be repeated at multiple levels to decompose the signals further. The total number of levels are generally user defined and are governed by the application.

Singular value decomposition

SVD is a matrix factorization technique that finds wide application in many areas. Often times, SVD is used as dimension reduction technique [33, 34]. That is, SVD allows for identification and ordering the dimensions along which the data points feature most variation. Essentially, it is expressing the original data in another co-ordinate system where the covariance matrix is diagonal. SVD is mathematically stated as [34]:

$$A = U\,S\,V^{T} \tag{5}$$

In our context, A denotes an mxn matrix which consists of wavelet coefficients for the selected frequency sub-band of the given ECG image; $UU^T=I$ and $V^TV=I$. I is the identity matrix. The columns of U are the orthogonal eigenvectors of AA^T, the columns of V are orthogonal eigen vectors of A^TA, S is the diagonal matrix containing the square roots of eigen values from U or V in descending order and is expressed as:

$$S=\begin{bmatrix}\lambda_1 & & & & & & \\ & \lambda_2 & & & & & \\ & & \lambda_3 & & & & \\ & & & \vdots & & & \\ & & & & \lambda_r & & \\ & & & & & \vdots & \\ & & & & & & 0\end{bmatrix} \tag{6}$$

where $\lambda_r=\sqrt{\sigma_r};\quad r=1,2,3\ldots$; σ_r are the eigen values. $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_r \geq \lambda_{r+1} \geq 0$; r is the order of singular values.

In the case of ECG data, SVD represent the energy distribution. Here, we propose to replace the S of the actual signal with the S matrix of the secret data which is elaborated in the next section. Researchers have used SVD for data compression. Though this is not of interest to us in this work, it provides an additional motivation because for transmission of medical data, one needs to anyways use data compression techniques. From that perspective, this approach can adapt itself directly.

Proposed methodology

The basic idea of Steganography lies in hiding information in cover signals. Usually, the data hiding happens through a watermarking algorithm. The success of the method lies in the watermarked signal being robust to external attacks and not deteriorate too much from the cover signal. Deterioration is generally measured as the difference between the original and the watermarked signal using different metrics which are discussed later.

Conversion of 1D ECG signal to 2D ECG image

This work uses an ECG signal of MIT/BIH arrhythmia database [35] which is down sampled to 128 Hz [36]. We propose to use DWT for the decomposition of the signal and SVD for watermarking. In order to apply SVD, one needs 2D data and ECG signal is 1D information. 2D ECG image can be constructed based on the QRS complexes and RR intervals of 1D ECG. In [37, 38], the cover ECG signal is filtered through the band pass filters. The filtered ECG signal undergoes the processes of differentiation, squaring, and moving window integration. Information about the slope of QRS complex is obtained from the derivatives. The squaring prevents the false identification of T wave as QRS complex. Moving window integrator provides the slope and width of QRS complex. The fiducial mark for the temporal location of QRS complex is the maximum slope of QRS complex or peak of R wave. The

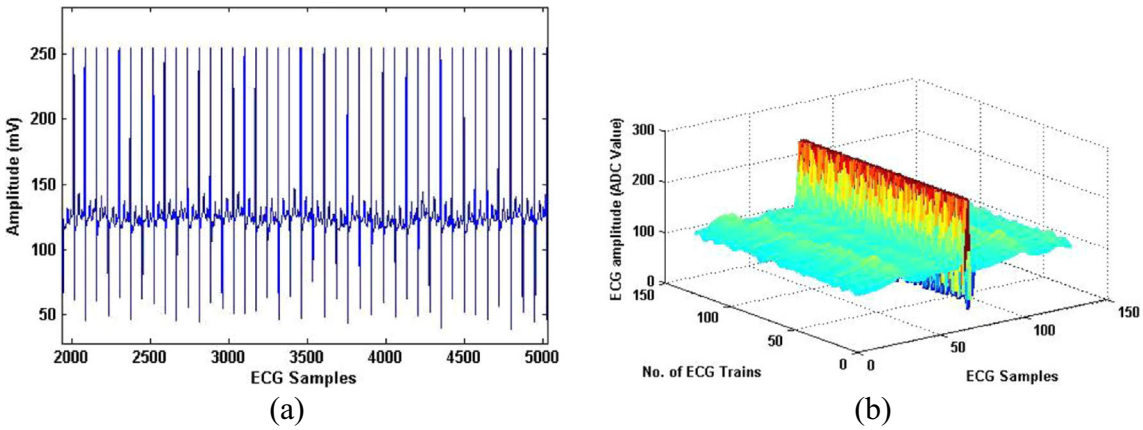

Fig 1 **a** 1D ECG signal **b** 2D ECG Image

cover ECG is sampled with the frequency of 128 Hz, and 64 points are taken from both sides of a fiducial point for each ECG train. The size of the original ECG determines the number of ECG trains in the 2D ECG. The fiducial data is provided during the reconstruction of 1D ECG signal. The above technique is used for conversion of 1D ECG signal to 2D image. When this approach is followed, there is negligible data loss in the conversion process. Using the above method, a 2D image produced from a 1D ECG signal is presented in Fig. 1.

Embedding secret data and obtaining watermarked signal

The proposed approach is presented in Fig. 2. Upon conversion from 1D data to 2D image, DWT is applied to decompose the image into sub-bands: LL, LH, HL, and HH. Here we have used Daubechies 4 wavelet [25]. The decomposed images are presented in Fig. 3. For the signals on a particular sub-band, SVD is applied and the singular values S_c are obtained. The secret data is also subjected to SVD and the singular values S_w are obtained. The proposed approach replaces S_c with S_w. This modifies the cover signal of the sub-band from A_c to $A_.$ Upon inverse DWT on the sub-bands, one can obtain the watermarked ECG signal. The performance of the algorithm is assessed based on the deterioration of the watermarked ECG signal compared to the cover ECG signal. The deterioration can be captured by metrics discussed in the next section. In this work we have attempted embedding in all the sub-bands, one at a time and studied the performance in terms of signal deterioration.

Watermark extraction algorithm

The watermarked signal is transmitted through a network. Once it reaches the authenticated care givers (or health provider), they need to extract the patient information which is embedded in the watermarked signal. In order to retrieve the data, one will need the orthogonal matrices U_w and V_w. This can typically be transmitted with a protected key. The extraction algorithm works as follows:

i. Daubechies 4 wavelet is used to decompose watermarked ECG image.
ii. The coefficients of the selected sub-band are subjected to SVD resulting in singular matrix, S_{we}
iii. Next, S_{we} is used with U_w and V_w to retrieve secret data A_{we}.

The efficiency of a watermarking algorithm is measured by the amount of data retrieved correctly which is measured by bit error rate.

Performance evaluation metrics

ECG Steganography introduces degradation in cover ECG signal. The amount of degradation is based on the type of watermarking algorithms. To evaluate the performance of the algorithm, one needs to compare the cover signal and the watermarked signal. The classical metrics [8, 25, 39] that are used to compare include: PSNR, PRD and BER

The metrics are defined by:

PSNR is the ratio of maximum amplitude of the cover ECG signal to the mean squared deviation between the two signals. Higher the value of PSNR, better is the quality [40]. PSNR represents a measure of peak error and expressed in terms of the logarithmic decibel units as follows:

$$\mathrm{PSNR} = 20\log_{10}\frac{\max[x_c]}{\sqrt{\frac{1}{N}\sum_{n=1}^{N}[x_c - x_w]^2}} \quad (7)$$

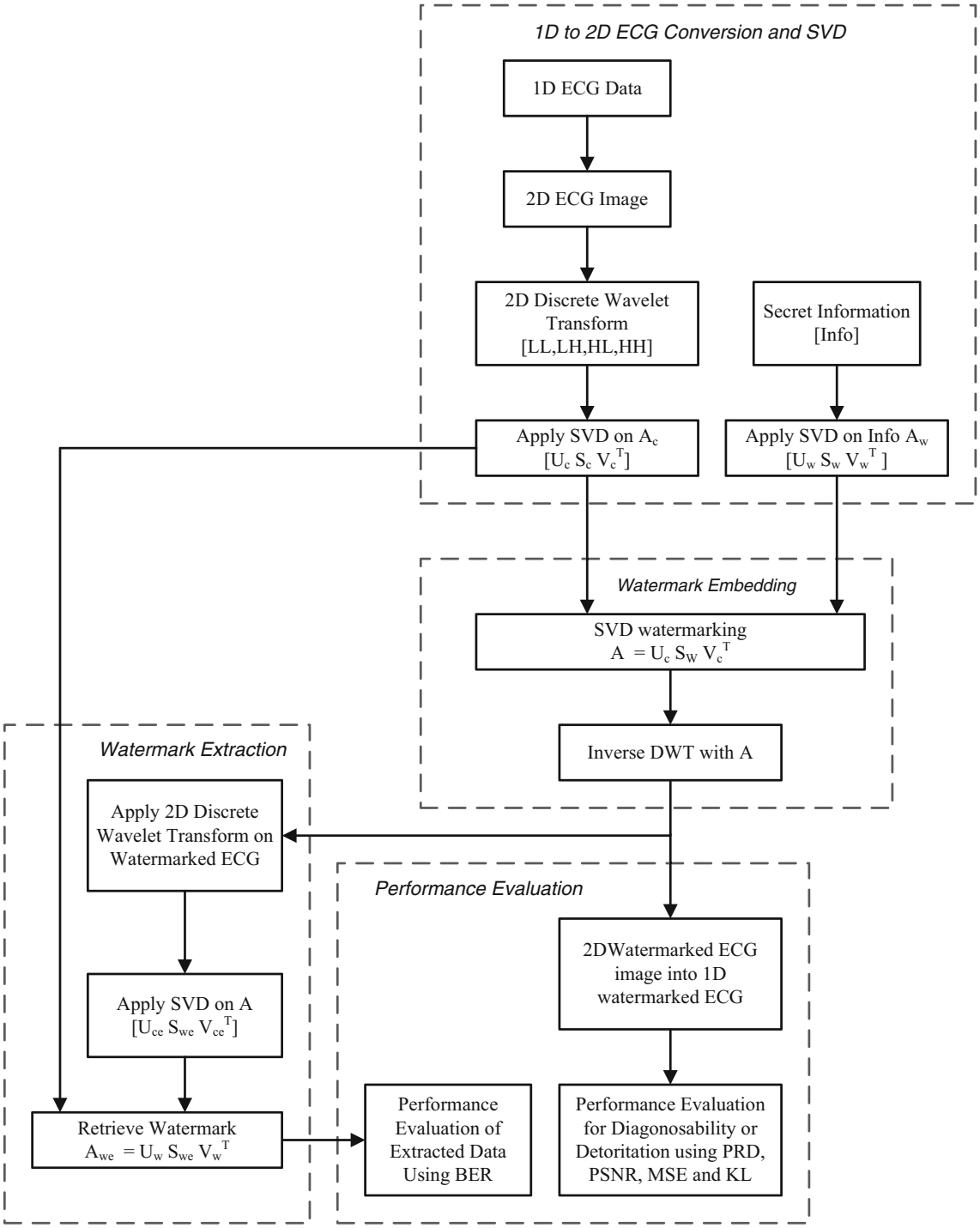

Fig 2 Flow chart of DWT-SVD based ECG Steganography

Where N is the total number of samples. $x_c(.)$ is the amplitude of the cover signal and $x_w(.)$ is the amplitude of the watermarked signal

PRD is a relative squared difference between the two signals. PRD increases linearly with increase of difference between the cover ECG and watermarked ECG and is expressed as follows [41]:

$$\mathrm{PRD}\,\% = \sqrt{\frac{\sum_{i=1}^{N}(x_c - x_w)^2}{\sum_{i=1}^{N}(x_c)^2}} \times 100 \tag{8}$$

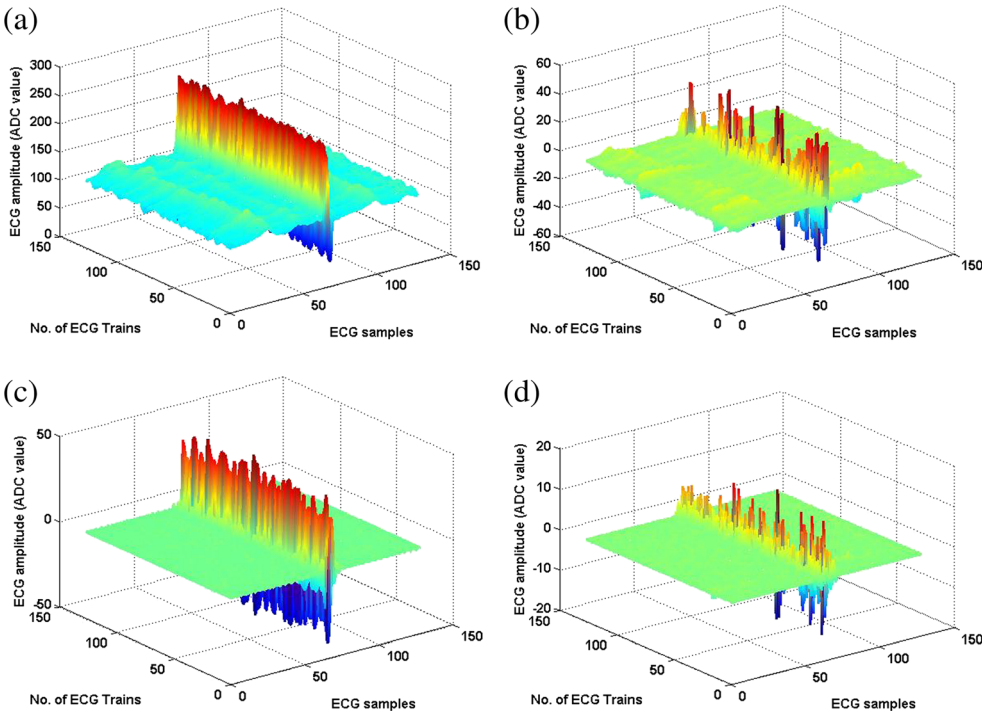

Fig 3 2D ECG Images of frequency sub-bands

BER is the ratio between the extracted secret information and the original secret information which gives the measure of data loss [25]. BER increases with increase in data loss.

$$\mathrm{BER} = \frac{\text{Bits retrieved correctly}}{\text{Total Bits}} \times 100 \tag{9}$$

The idea of a robust algorithm lies in hiding the secret data in the cover signal in such a way that the diagnosability is not lost and there is minimal degradation to the overall signal. Therefore, the logical choice is the high frequency bands which don't play a crucial role in the diagnoses of a rhythmic ECG. However, due to data embedding, the peaks like QRS

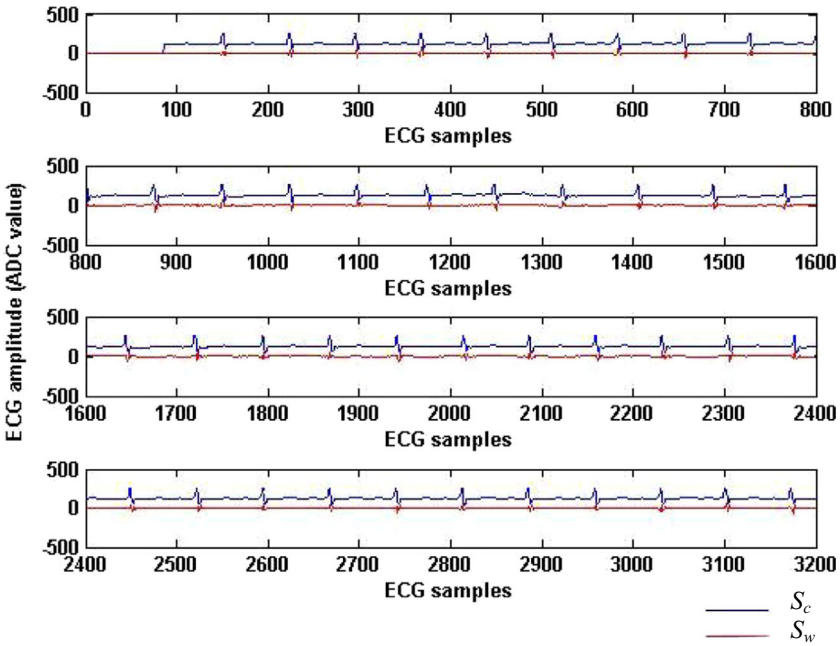

Fig 4 Cover ECG Vs Watermarked ECG of Frequency Sub-band LL

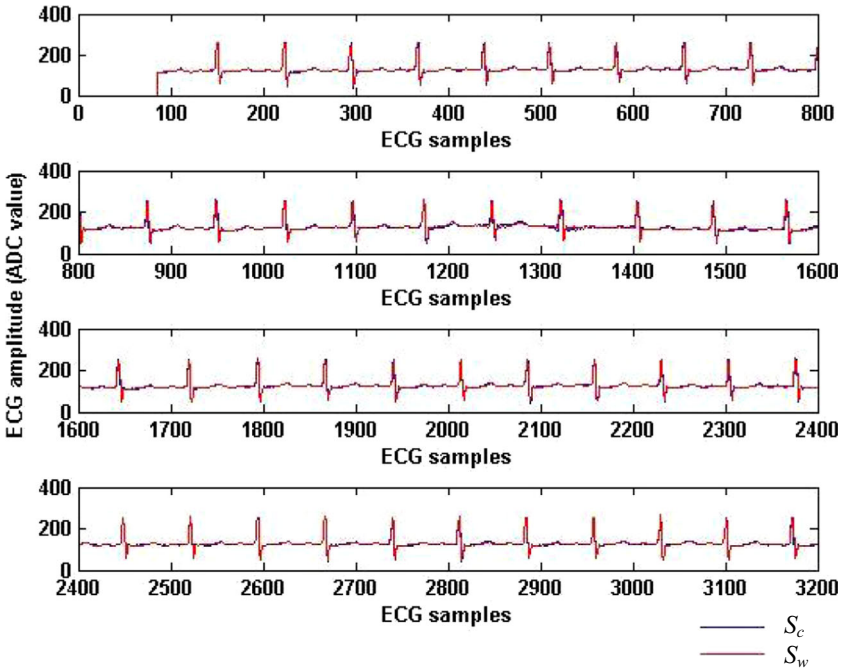

Fig 5 Cover ECG Vs Watermarked ECG of Frequency Sub-band HL

complexes might get affected and they will influence the diagnoses heavily. Therefore, while assessing the performance of embedding algorithms, changes to the peak amplitudes of the cover signal need to be penalized more than the ones at other positions. Ibaida and Khalil [25] achieve this by using a weighted PRD for which the weights are obtained from previous work done by Al-Fahoum [41]. However the approach is not extendable to all types of decomposition techniques. Here, we propose a statistical measure called the Kullback–Leibler divergence (KL) which essentially measures the distance between histograms of the cover and watermarked signals and is expressed as [42, 43]:

$$D(p_c, p_w) = \int p_c(x) \log \frac{p_w(x)}{p_c(x)} dx \tag{10}$$

Where D is KL divergence, p_c is the probability of the cover signal and p_w is the probability of the watermarked signal. The advantage of using KL is that it works in the frequency domain while the other metrics presented are in

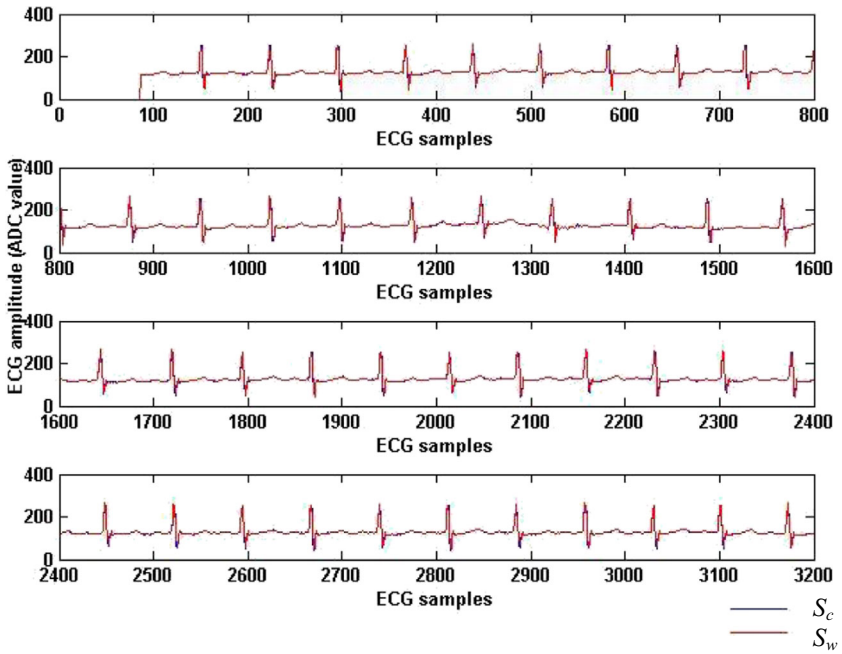

Fig 6 Cover ECG Vs Watermarked ECG of Frequency Sub-band LH

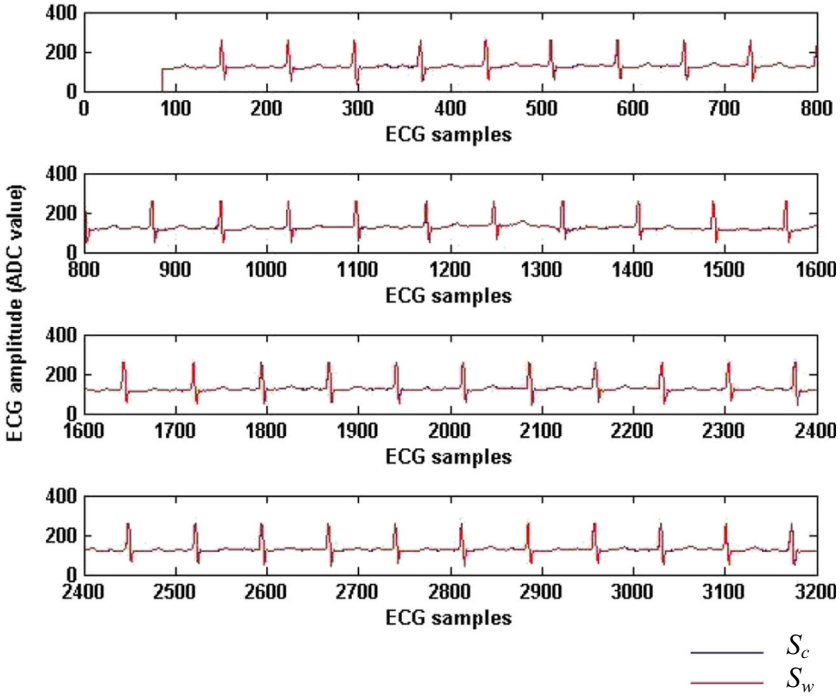

Fig 7 Cover ECG Vs Watermarked ECG of Frequency Sub-band HH

the time domain. Therefore, this can be used in conjunction with the other metrics. In addition, based on the threshold values, the penalization can be easily assigned. Often times, it's not clear which watermarking algorithm might work better on what signal. Even if that categorization is available, while watermarking real time, one might not be able to classify the ECG signal as belonging to a particular category. In such situations, the robust algorithm can be selected by minimizing the KL. Sometimes, owing to watermarking if a peak is affected by the same units as a point in high frequency band, the error is masked in a relative sense but will degrade the cover signal affecting the diagnosability. However, KL will capture this as a change in the histogram and based on threshold it can be penalized appropriately [42–45]. A similar metric called the area metric can also be used. Area metric actually measures the difference between the CDFs of the two signals [46]

Results and discussion

1D normal ECG signal of size 76,800 samples, the cover signal from the MIT arrhythmia database is subjected to DWT and SVD as discussed in the previous section. The size of 2D image is 128×128 and the decomposed sub-bands are of size 67×67. Here, we are embedding a secret data of size 67×67 in different sub-bands and study the deterioration. The perceptual difference between cover and watermarked ECGs are shown in Figs. 4, 5, 6 and 7 for the frequency sub-bands of LL, HL, LH and HH. Different windows of the sub-bands are presented in the Figures. Since important features like QRS complex lie in low frequency sub-band LL, watermark embedding in LL frequency components highly distorts the cover ECG as shown in Fig. 4. In Figs. 5, 6, 7, the watermarked signals are very similar to the cover signal and the differences are not evident to naked eye. Metrics discussed in the previous sections are presented in Table 1 and will be used to assess the distortion of the watermarked signal. The PDFs of the signals are provided in Fig. 8. This information is essentially captured by KL

From Table 1, it can be readily observed that watermarked ECGs of HL, LH and HH frequency sub-bands show less difference. It is to be noted that the KL metric is lowest in the HH band. Similarly, all other metrics also indicate that watermarked signal in HH band has less distortion compared to the cover signal. Hence HH is the ideal band to hide data.

The error is dependent on the watermarking approach and the size of the secret data. In the first case, we have used a 67×

Table 1 Performance metrics for different sub-bands

Metric	LL	HL	LH	HH
PSNR (dB)	5.92	35.82	32.12	50.44
PRD %	99.41	3.18	4.87	0.59
BER %	0.05	0.02	0	0
KL	0.85	0.53	0.42	0.15

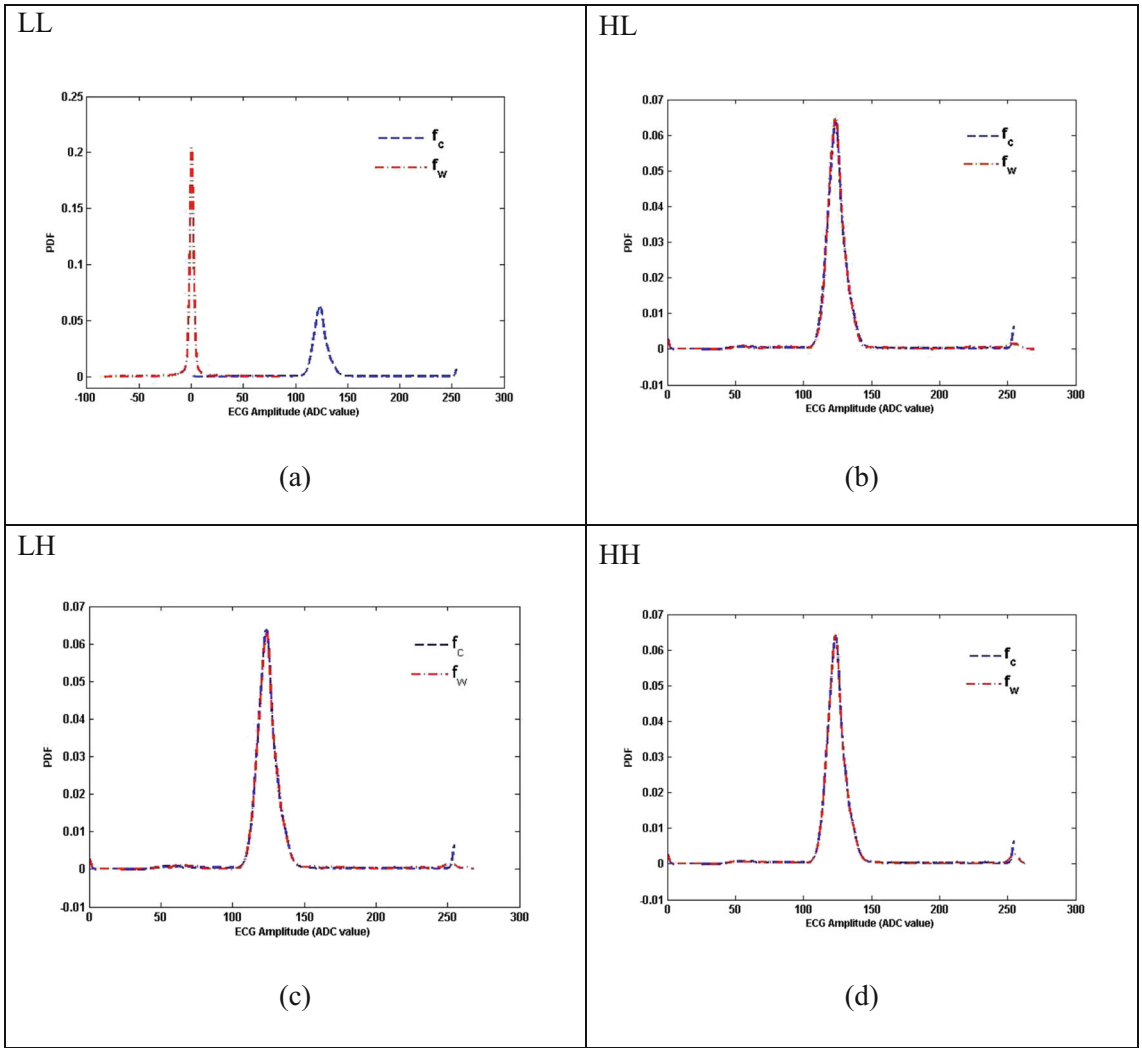

Fig 8 PDFs of Cover and Watermarked ECG of Frequency Sub-bands

67 data which is large compared to the usual size of patient information which typically consists of patient name, age, location etc., In order to understand the effect of secret data size on the performance of the algorithm, we use a 50×7 size secret data embedded in the HH sub-band. In this case the S_w is a different size than the S_c and a choice is to be made on which locations to embed in S_w. Similar to [8] we identify the index of the S_c that is less than the maximum of S_w and replace the S_w from the identified index of S_c. In this approach, there could be few left out singular values in S_c that are typically of very low values. So, we replace them with zeros. The results are presented in Table 2. It can be noted that the diagnosability might not be lost as all the metrics are very good. However, the BER is high. That is, the patient information is not retrieved properly. The reason is that we modify the left out singular values. Therefore, it is desirable that an approach is developed which allows for dynamic selection of location to embed the secret data. In the current context, it boils down to selecting the indices in S_c that are close to the values in S_w.

In order not to deliberately change the left out singular values, we propose dynamic location selection approach. Here, we select the location dynamically (index of S_c) for embedding, based on each value of the S_w. That is, the algorithm searches for the indices of S_c whose values are

Table 2 Performance metrics for direct replacement and dynamic location selection approaches

Metric	Direct replacement	Dynamic location selection
PSNR (dB)	69.13	96.03
PRD%	0.0687	0.0031
BER%	4.29	0
KL	6.84e-5	2.89e-7

closer to the values in S_w. Then, the corresponding S_c's are replaced with S_w. By doing this, we are managing to maintain the energy of the singular values of the watermark match the energy of the singular values in the HH band that they are displacing. The results for this approach are presented in Table 2. It can be observed that this approach gives extremely negligible error and 100 % data retrieval. The index mapping of S_c will be provided during watermark extraction.

Summary

This paper proposed a Steganography approach based on DWT and SVD to hide patient confidential information along with the ECG data. The approach aims at less distortion to the watermarked signal so that the diagnosability is not lost and also at maximum retrieval of the patient information. Daubechies 4 wavelets are used to decompose the 2D ECG image. SVD is used on both the cover signal and the secret data. Watermarking is achieved by replacing the singular values of the secret data over the singular values of the cover signal. The patient information can be retrieved by performing an inverse DWT and using the orthonormal matrices from the initial secret data information. Different metrics are used to measure the performance of the proposed approach with respect to deterioration to the cover signal and ability to retrieve patient information. Firstly, it is observed that the method is capable of hiding secret data into ECG signal with error rates less than 0.6 % even for large secret data. It is observed that the HH band is the ideal band to hide secret data. Performance assessment was done for a slightly smaller secret data size and dynamic location selection approach was proposed which produced good results both in terms of signal deterioration as well as secret data retrieval. Therefore, the proposed approach can be used reliably for patient information transmission without much loss in the diagnosability of the ECG cover signal.

References

1. Ameen M, Liu J, Kwak K (2012) Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 36(1):93–101. doi: 10.1007/s10916-010-9449-4
2. Act, A. (1996) Health insurance portability and accountability act of 1996. Public Law, 104, 191. doi:10.4135/9781452234243.n359
3. Sufi F, Khalil I (2009) A new feature detection mechanism and its application in secured ECG transmission with noise masking. J Med Syst 33(2):121–132. doi: 10.1007/s10916-008-9172-6
4. Cheddad A et al. (2010) Digital image steganography: Survey and analysis of current methods, Signal Process, 90(3):727–752. doi:10.1016/j.sigpro.2009.08.010
5. Hernandez J R, Amado M, Perez-Gonzalez F (2000) DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure. IEEE Trans. Image Process. 9(1): 55–68. doi: 10.1109/83.817598
6. Dogan S, Tuncer T, Avci E, Gulten A (2012) A New Watermarking System Based on Discrete Cosine Transform in Color Biometric Images. J Med Syst 36(4):2379–2385. doi:10.1007/s10916-011-9705-2
7. Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin (2005) SVD-based digital image watermarking scheme, Pattern Recognit. Lett. 26(10): 1577–1586. doi:10.1016/j.patrec.2005.01.004
8. Gupta A K, Raval M S (2012) A robust and secure watermarking scheme based on singular values replacement. Sadhana 37(4):425–440. doi:10.1007/s12046-012-0089-x
9. Ganic E, Eskicioglu A M (2004) Robust DWT-SVD domain image watermarking: embedding data in all frequencies. Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and Security - MM&Sec'04.166-174. doi:10.1145/1022431.1022461
10. Thabit R, Khoo B E (2014) Robust reversible watermarking scheme using Slantlet transform matrix. J Syst Software 88:74–86. doi:10.1016/j.jss.2013.09.033
11. Martins D, Guyennet H et al. (2010) Steganography in MAC Layers of 802.15.4 Protocol for Securing Wireless Sensor Networks. 2010 International Conference on Multimedia Information Networking and Security. 4(6):824–828. doi:10.1109/mines.2010.175
12. Zielińska E, Mazurczyk W, Szczypiorski K (2014) Trends in steganography. Commun ACM 57(3):86–95. doi:10.1145/2566590.2566610
13. Bhat K V, Sengupta I, Das A (2010) An adaptive audio watermarking based on the singular value decomposition in the wavelet domain. Digit Signal Process 20(6):1547–1558. doi:10.1016/j.dsp.2010.02.006
14. Natgunanathan I, Xiang Y, Rong Y, Peng D (2013) Robust patchwork-based watermarking method for stereo audio signals. Multimed Tools Appl 1–24. doi:10.1007/s11042-013-1454-4
15. Marvel L M, Boncelet C G, Retter C T (1999) Spread spectrum image steganography. IEEE Trans. Image Process. 8(8):1075–1083. doi:10.1109/83.777088
16. Zaidoon Kh. Al-Ani et al. (2010) Overview: Main fundamentals for steganography. Journal of Computing 2(3):158–165
17. Bender et al. (1996) Techniques for data hiding. IBM Syst. J. 35(3.4): 313–336. doi:10.1147/sj.353.0313
18. Christian Cachin (2004) An information-theoretic model for steganography. Inform Comput 192(1):41–56. doi:10.1016/j.ic.2004.02.003
19. Liu J, Tang G, Sun Y (2013) A secure steganography for privacy protection in healthcare system. J Med Syst, 37(2). doi:10.1007/s10916-012-9918-z
20. Xuan Kong, Rui Feng (2001) Watermarking medical signals for telemedicine. IEEE T Inf Technol B 5(3):195–201. doi:10.1109/4233.945290
21. Chen S T, Guo Y J, Huang, H N, Kung W M, Tseng K K, Tu S Y (2014) Hiding Patients Confidential Data in the ECG Signal via a Transform-Domain Quantization Scheme. J Med Syst 38(6). doi:10.1007/s10916-014-0054-9
22. Engin M, Çidam O, Engin E Z (2005) Wavelet transformation based watermarking technique for human electrocardiogram (ECG). J Med Syst 29(6):589–594. doi:10.1007/s10916-005-6126-0
23. Nergui M, Acharya U S, Acharya U R, Yu W (2010) Reliable and Robust Transmission and Storage Techniques for Medical Images with Patient Information. J Med Syst 34(6):1129–1139. doi:10.1007/s10916-009-9332-3
24. Mehmet Engin, Oğuz Çıdam, Erkan Zeki Engin (2005) Wavelet Transformation Based Watermarking Technique for Human Electrocardiogram (ECG). J Med Syst 29(6):589–594. doi:10.1007/s10916-005-6126-0

25. 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. doi:10.1109/tbme.2013.2264539
26. Tseng K K, He X, Kung W M, Chen S T, Liao M, Huang H N (2014) Wavelet-Based Watermarking and Compression for ECG Signals with Verification Evaluation. Sensors 14(2):3721–3736. doi:10.3390/s140203721
27. Kozat Suleyman S et al. (2009) Embedding and retrieving private metadata in electrocardiograms. J Med Syst 33(4):241–259. doi:10.1007/s10916-008-9185-1
28. Nayak J, Subbanna Bhat P, Acharya U R, Sathish Kumar M (2009) Efficient Storage and Transmission of Digital Fundus Images with Patient Information Using Reversible Watermarking Technique and Error Control Codes. J Med Syst 33(3):163–171. doi:10.1007/s10916-008-9176-2
29. Planitz B M, Maeder A J (2005) A study of block-based medical image watermarking using a perceptual similarity metric. DICTA'05. Proceedings Digital Image Computing: Techniques and Applications 2005. doi:10.1109/dicta.2005.1578168
30. Gonzalez R C, Woods R E (2002) Digital image processing. 2nd SL, Prentice Hall.
31. Shensa M J (1992) The discrete wavelet transform: wedding the a trous and Mallat algorithms. IEEE T Signal Proces 40(10):2464–2482. doi:10.1109/78.157290
32. Heil C E, Walnut D F (1989) Continuous and discrete wavelet transforms. SIAM Review 31(4):628–666. doi:10.1137/1031129
33. Henry E R, Hofrichter J (2010) Singular value decomposition: application to analysis of experimental data. Method ENZYMOL 210:81–138. doi:10.1016/0076-6879(92)10010-b
34. Wall M E, Rechtsteiner A, Rocha L M (2003) Singular value decomposition and principal component analysis. A practical approach to microarray data analysis 91–109. doi:10.1007/0-306-47815-3_5
35. Moody G B, Mark R (1992) MIT-BIH arrhythmia database directory. MITBIH Database Distribution, Harvard–MIT Division of Health Sciences and Technology, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA. http://www.physionet.org/physiobank/database/html/mitdbdir/mitdbdir.htm. Accessed 23 May 2014
36. Gari D. Clifford (2002) Signal Processing Methods for Heart Rate Variability. Dissertation, University of Oxford
37. Pan J, Tompkins W J (1985) A Real-Time QRS Detection Algorithm. IEEE Trans. Biomed. Eng. 32(3):230–236. doi:10.1109/tbme.1985.325532
38. Gari D. Clifford (2010) MIT website. www.mit.edu/%7Egari/CODE/ECGtools/ecgBag/. Accessed 23 May 2014
39. Sankur B (2002) Statistical evaluation of image quality measures. J. Electron. Imaging 11(2):206–223. doi:10.1117/1.1455011
40. Huynh-Thu Q, Ghanbari M (2008) Scope of validity of PSNR in image/video quality assessment. Electron Lett 44(13):800. doi:10.1049/el:20080522
41. Al-Fahoum (2006) Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure. IEEE Trans. Inf. Technol. Biomed. 10(1):182–191. doi:10.1109/titb.2005.855554
42. Cihan Varol, Coskun Bayrak (2011) Estimation of quality of service in spelling correction using Kullback–Leibler divergence. Expert Syst. Appl. 38(5):6307–6312. doi:10.1016/j.eswa.2010.11.112
43. Sung-Hyuk Cha (2007) Comprehensive survey on distance/similarity measures between probability density functions. International Journal of Mathematical Models and Methods in Applied Sciences 1:300–307
44. Couceiro R, Carvalho P et al. (2008) Detection of Atrial Fibrillation using model-based ECG analysis. 2008 19th International Conference on Pattern Recognition. doi:10.1109/icpr.2008.4761755
45. Gacek, Adam, Witold, Pedrycz (2012) ECG Signal Processing, Classification and Interpretation. Springer
46. Oberkampf, Roy (2010) Verification and validation in scientific computing. Cambridge University Press, Cambridge