Multimedia Tools and Applications (2021) 80:8505–8540
https://doi.org/10.1007/s11042-020-09856-9

An integer wavelet transform and pixel value differencing based feature specific hybrid technique for 2D ECG steganography with high payload capacity

Neetika Soni[1,2] · Indu Saini[1] · Butta Singh[2]

Received: 9 April 2019 / Revised: 30 November 2019 / Accepted: 9 September 2020 /
Published online: 4 November 2020

Abstract

Electrocardiogram (ECG) is essentially a significant physiological signal required in the diagnosis of cardiac disorders. For remote healthcare assistance, ECG signal along with patient's meta-data is communicated over the public network. During communication, security and privacy of patient's sensitive information is a major issue. Presently, a common steganography technique is being applied on the entire ECG signal. Since ECG signal consists of clinically more significant QRS regions as well as less significant non-QRS regions and employing same steganography approach on both the regions is not admissible. In this work, a hybrid approach is proposed for concealing the sensitive information in 2-dimensional (2D) ECG. A fusion of integer wavelet transform and modified least significant bit (IWT-mLSB) approach is applied in the pivotal QRS complex region; while pixel inverted pixel value differencing (PI-PVD) technique is implemented in the non-QRS region to hide the confidential data. The performance of the proposed algorithm is evaluated on standard as well as self-recorded database in terms of statistical parameters, clinically critical metrics, heart rate variability (HRV) analysis, embedding capacity (EC) and bit error rate (BER). The security of the proposed algorithm is further evaluated in terms of key space and key sensitivity. A comparative analysis with other state-of-the-art techniques exhibits the competency of the proposed technique.

Keywords ECG steganography · Chaotic map · Integer wavelet transform · Pixel inverted pixel value differencing · Key space · Key sensitivity

✉ Butta Singh
bsl.khanna@gmail.com

[1] Department of Electronics and Communication Engineering, Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, 144011, India

[2] Department of Electronics and Communication Engineering, Guru Nanak Dev University, Regional Campus, Jalandhar, 144007, India

1 Introduction

Telemedicine is a significant tool in remote healthcare systems and is rapidly changing the dynamics of conventional healthcare systems. The patient centric approaches provide reliable emergency solutions to homebound patients and obtain expert opinions from globally available experienced healthcare providers. Biomedical signals such as electrocardiogram (ECG), electroencephalogram (EEG), electromyogram (EMG) etc. are the commonly used signals in tele-health services. To make this system more symptomatic, these signals are complimented by annotations, patient's medical biography and history. It raises the concern of security and authentication of the sensitive information during its transmission and storage. Legal regulations like U.S. health insurance portability and accountability act (HIPAA) [8], the personal information protection and electronic document act, 2000 (PIPEDA) [42] and digital signature laws in many countries also demanded security and confidentiality of the personal information.

This paper addresses these security related issues through information hiding technique named steganography. In steganography, the confidential data is secured by concealing it inside the host media without loss of its intelligent information [15]. Additionally, it provides efficient memory utilization and also cuts the risk of mismatching between the patient's physiological signal and his personal details. Various medical images [1, 24, 29] and physiological signals [27, 32, 37, 40] are observed in literature that were used as effective hosts to conceal confidential information. ECG signal is the widely considered tool in diagnosing cardiovascular diseases (CVD) as well as detecting and analysing issues related to autonomic nervous system [3, 4, 38, 43]. In this work time-series ECG signal is used as the host signal for concealing the patient's confidential information.

1.1 Related work

Research has been carried out to perform steganography in multimedia applications, but its implementation in biomedical applications particularly in ECG signal is still in its infancy. The ECG data contains valuable diagnostic information and any alteration due to payload embedding reduces the signal fidelity which may lead to wrong diagnosis. Hence it has to be taken care that the diagnosability should not be lost while concealing data in these signals. Different approaches of steganography in ECG signal are discussed in the literature. Most of these techniques perform steganography in spatial domain [27, 28, 40, 45] and transform domain [13, 14] however few researchers introduced hybrid approaches to conceal the secret data [11, 12, 19]. Pandey et al. [27] presented chaotic maps and sample value differencing (CMSaVD) based spatial domain steganography. It has been found that embedding 21 kb in ECG signal of 20 mins duration results in percentage root mean square difference (PRD) of 0.26. In another spatial domain approach, Soni et al. [40], adopted an optimum location selection (OLS) algorithm based ECG steganography to select the embedding locations on the basis of thresholded RR peak amplitude. The method achieved embedding capacity (EC) of 0.45 at low PRD of 0.004. Yang [45] proposed lossy and lossless steganography techniques in spatial domain using coefficient alignment. The approaches achieved EC of 0.25 and 0.49 at signal to noise ratio (SNR) of 56.34 and 46.31 for lossless and lossy approaches respectively. In [11], Ibaida et al. performed discrete wavelet transform (DWT) and least significant bit (LSB) substitution based ECG steganography to embed encrypted secret bits in the selected subbands of wavelet coefficients. The performance was evaluated on normal and abnormal (ventricular tachycardia and ventricular fibrillation) ECG datasets. The author claimed the embedding of nearly 14 k bits in ECG segments of 10s and attained the average PRD of 0.47129, 0.2759 and 0.5671 in case of normal, ventricular tachycardia and ventricular fibrillation datasets respectively. However, the amount of bit error rate (BER) occurred during extraction of secret information was not discussed. In [12–14], numerous researchers explored inter and intra beat correlations to formulate two-dimensional (2D) ECG arrays for steganography. In [12] Jero et al. presented 2D hybrid approach using DWT and singular value decomposition (SVD) to embed the secret information in the selected subband. The approach generates PRD of 0.0059 at very low EC of 0.0365 only. In [13], the same research group presented discrete curvelet transform based 2D ECG steganography in which selected curvelet co-efficients are modified according to 0 and 1 of secret bits. The PRD 0.0132 is achieved after embedding 350 bytes in test signal of 128 trains from normal sinus rhythm (NSR) database. Further they proposed continuous ant colony optimization (CACO) based 2D ECG steganography technique [14] and identify multiple scaling factors that improves the trade-off between peak signal to noise ratio (PSNR) and robustness. Kozat et al. [19] applied a blend of discrete Fourier transform with spread spectrum approach to embed robust watermark and used least significant bit (LSB) substitution to embed fragile watermark in an ECG signal. The method is robust against any signal deformations but has very low embedding power of 0.04 at SNR of 20 dB.

Spatial domain techniques have high embedding capacity and good visual quality but are prone to stego attacks whereas transform domain techniques are robust with limited EC [10]. In the above discussed methods, single steganography approach (either spatial or transform) is applied on the entire ECG signal [13, 14, 27, 28, 40, 45]. Although in few cases hybrid (both spatial and transform) approaches are formulated [11, 12, 19], but that too on the whole signal. Since ECG signal consists of crucial QRS regions as well as less significant non-QRS regions [34] and employing same steganography approach on both the regions is not admissible. The proposed hybrid technique encourages feature specific integrated approach to hide information in ECG signal. It has been observed in literature that DCT and DWT based steganography methods are robust but show high PRD at low EC. The common reason for high PRD is the reconstruction error that occurs due to the filter coefficients [21]. The analysis filters used to decompose the signal into subbands generate floating point coefficients and synthesis filters truncate these coefficients during reconstruction. Truncation of floating point numbers at any level results in potential loss of information. One of the solutions to this problem is the use of lifting scheme based integer wavelet transform (IWT) which decomposes the signal in integer coefficients [5, 7, 20, 31]. It solves the problem of rounding error hence reduces PRD. Besides PRD, it is also required to improve the EC while maintaining the perceptibility of the ECG signal. Pixel value differencing (PVD) is a promising technique that ensures high EC in high frequency regions [17, 36, 44]. Although the non-QRS region of ECG signal has nearly flat surface but inverting adjacent sample in each pair converts the low frequency non-QRS region into high frequency region and makes the region suitable to implement PVD scheme [27]. Thus according to the morphological features of the host ECG signal, IWT based modified LSB (IWT-mLSB) steganography is applied in the sensitive QRS region of an ECG beat while pixel inverted PVD (PI-PVD) based spatial domain steganography is performed in the non-QRS region. The proposed hybrid approach recuperates the EC without distorting its visual as well as clinical quality. Further, to intensify the security of the confidential information, chaotic maps are employed. Chaotic maps are the non-linear equations used to generate random sequences with very attractive properties of unpredictability, ergodicity and sensitivity to initial conditions that makes them suitable for designing steganographic applications [9, 23, 46]. The steganography in medical data acutely demands minimum deterioration in its morphological features while accomplishing its other traits viz. EC and robustness. The proposed technique is competent to accomplish all these attributes of steganography.

The rest of the paper includes: Section 2 discusses the preliminaries used in proposed method. The proposed methodology describing the embedding and extraction processes is detailed in section 3. Section 4 includes results and discussion. The proposed work is concluded in section 5.

2 Preliminaries and materials

ECG signal is a quasi-periodic, non-stationary signal that can be characterized in terms of both time and frequency. Wavelet transform is a mathematical tool that performs translation and dilation of basic shapes (e.g. Fourier transformation) to build space–frequency relations in such signals. In this work, lifting scheme based IWT is employed to exploit the correlation between the neighbouring samples and frequencies to build a sparse approximation [5, 7].

2.1 Lifting scheme based integer wavelet transform

Lifting scheme is a flexible technique used to design wavelets through an iterative process of predicting and updating a set of samples (subband) from an appropriate linear combination of the other set (subband). The output of IWT consists of detailed coefficients (D) and approximate coefficients (A). IWT can be expressed in three steps; split, predict and update as shown in Fig. 1.

Split: The input signal $S = (S_k)_{k\in z}$, $S_k \in \mathbf{R}$, is split up into two disjoint sets; even (S_e) and odd (S_o) indexed samples [7].

$$S_e = (S_{2k})_{k\in z}$$
$$S_o = (S_{2k+1})_{k\in z}$$

Predict: Since the two sets are closely correlated, therefore it is possible to build a predictor (Pr) for one set from the other set. As the predictor does not give the exact value, the difference between the original value and predicted value is recorded. This difference forms the detailed coefficients (D) and is calculated as.

$$\mathrm{D} = S_e - Pr(S_o)$$

From D and the odd samples, even samples can be recovered as.

$$S_e = Pr(S_o) + \mathrm{D}$$

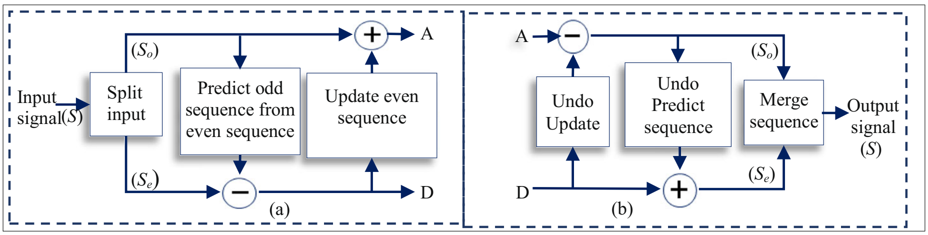


Fig. 1 Lifting scheme for level 1 in (**a**) Integer Wavelet Transform (**b**) Inverse Integer Wavelet Transform

The simplest predictor (*Pr*) considered for an odd sample S_{2k+1} is the average of its two even neighbours, hence D is written as.

$$D_k = S_{2k+1} - (S_{2k} + S_{2k+2})/2$$

A good predictor generates negligible values of D. This process of computing predictor and recording the difference is called as lifting.

Update: The lifting stage transforms the even and odd samples (S_e, S_o) into (S_e, D). Since S_e is obtained by subsampling the signal, it causes serious aliasing problem. Therefore a second lifting stage is required to replace the even samples with smoothed values by applying update operator (U) to the detailed coefficients as [7].

$$A = S_e + U\ (D)$$

The updated coefficients are called approximate coefficients. Given A and D, S_e can be recovered as.

$$S_e = A - U(D)$$

The update operator restores the correct running average and reduces aliasing. Daubechies et al. proposed that one-quarter of the wavelet coefficient ($D_k/4$) has to be added to the even samples as updated operation [7].

$$A_k = S_{2k} + (D_{k-1} + D_k)/4$$

2.2 LSB steganography

LSB steganography is one of the simplest technique to hide secret data in the LSBs of the signal samples [16]. Since, the human eye is imperceptible to the minor changes at LSB level, hence it is an effective method of steganography. But embedding the secret bits directly at the LSB positions are prone to stego attacks. In the proposed method, the secret data is embedded in the LSBs of the transformed ECG coefficients that makes it invulnerable to stego attacks as well as reduce the distortion to many folds.

2.3 Pixel value differencing (PVD)

PVD is a steganography technique originally implemented in images where the absolute difference between the two consecutive pixels is explored to store the secret bits [17, 36, 44]. Higher the difference, more will be the payload capacity and vice versa. For instance, higher number of data bits can be concealed at edges (high frequency) as compared to smoother (low frequency) regions. Further, the number of bits embedded is calculated by mapping the difference with the sub-range in the pre-defined range table. The table consists of non-overlapping dyadic-ranges W_j, $j = 1, 2....\ .$ n such that each sub-range (W_j) has a lower bound (l_j), upper bound (u_j) and the width (w_j) [36] i.e.

$$W_j = [l_j, u_j],\ \ j = 1, 2.....n$$

where

$$l_j = \begin{cases} 1, & j = 1 \\ 2^{j-1}, & j > 1 \end{cases} \quad (1)$$

$$u_j = 2^j - 1 \quad (2)$$

$$w_j = u_j - l_j + 1 \quad (3)$$

The procedure to embed long stream of secret bits using PVD approach is explained as:

Step 1. Partition the signal samples into non-overlapping pixel pairs.

If $P_{2p(i)}$is the i^{th} even sample, the pixel pair will be.

$$P_{2p(i)} \text{and } P_{2p(i)+1} \quad (4)$$

Step 2. Calculate absolute difference between sample values.

$$d_i = |P_{2p(i)} - P_{2p(i)+1}| \quad (5)$$

Step 3. The number of secret bits that can be embedded in each pair varies and is decided by the width of the sub-range to which d_i belongs. For that, compute range $W_j = [l_j, u_j]$ such that.

$l_j \le d_i$ && $d_i \ge u_j$ and hence calculate w_j (using (3)).

Step 4. Compute the hiding capacity of the pixel pair as [17].

$$r_i = \lfloor log_2 w_j \rfloor \text{ and } k_i = \lfloor log_2 r_i^2 \rfloor \text{where } k_i \text{ is the number of secret bits to be concealed in } W_j \quad (6)$$

[36]

$\lfloor \rfloor$ represents the greatest integer factor.

Step 5. Select next k_i bits from the secret bit stream and convert them into decimal value m_i.

Step 6. Compute the extraction function F such that its value lies between $(0, r_i^2 - 1)$ [17, 36]

$$F(P_{2p(i)}, P_{2p(i)+1}) = (P_{2p(i)} * (r_i - 1) + P_{2p(i)+1} * r_i) mod\ r_i^2 \quad (7)$$

Step 7. Based on the decimal value m_i,the selected pixel pair of the cover media is modified to form the stego-pixel pair ($P'_{2p(i)}$, $P'_{2p(i)+1}$). The secret data is embedded in the pixel pair such that the overflow and underflow conditions are to be avoided. For that, the absolute difference (d_i') between the stego pixel pair ($P'_{2p(i)}$, $P'_{2p(i)+1}$) must lie in the same sub-range (W_j) as that of the original pixel pair($P_{2p(i)}$, $P_{2p(i)+1}$). The embedding is done according to the following criteria:

if $m_i = F$ then the modified sample pairs

$(P'_{2p(i)}, P'_{2p(i)+1}) = (P_{2p(i)}, P_{2p(i)+1})$

elseif $m_i > F$

$P'_{2p(i)} = P_{2p(i)} - (m_i - F) mod\ r_i$

$P'_{2p(i)+1} = P_{2p(i)+1} + \left\lfloor \frac{m_i - F}{r_i} \right\rfloor + (m_i - F) mod\ r_i$

else $m_i < F$

$P'_{2p(i)} = P_{2p(i)} + (F - m_i) mod\ r_i$

$P'_{2p(i)+1} = P_{2p(i)+1} - \left\lfloor \frac{F - m_i}{r_i} \right\rfloor - (F - m_i)\ mod\ r_i$

end

To extract the embedded information from the stego pixel pair ($P'_{2p(i)}$, $P'_{2p(i)+1}$), compute d_i, w_j, r_i, k_i *and* F in the similar way as computed during embedding. The value of F is the extracted secret information from the stego-pair. The process of concealing and extraction of secret information using PVD method is explained below with the help of an example.

$$\text{Assume } P_{2p(i)}, P_{2p(i)+1} = (945, -944)$$
$$d_i = |P_{2p(i)} - P_{2p(i)+1}| = 945-(-944) = 1889$$

Sub-range to which difference d_i belongs is

$$W_j = [l_j, u_j] = (1024, 2047)$$

Width of the sub-range $w_j = u_j - l_j + 1 = (2047 - 1024 + 1) = 1024$

The number of secret bits to be selected for embedding is

$$r_i = \lfloor log_2 w_j \rfloor = \lfloor log_2 1024 \rfloor = 10$$

$$k_i = \lfloor log_2 r_i^2 \rfloor = \lfloor log_2 10^2 \rfloor = 6$$

Let the first six secret data bits are

$$m_i = (110110)_2$$

And its decimal equivalent is 54_{10}

The extraction function F is calculated as

$$F(P_{2p(i)}, P_{2p(i)+1}) = (P_{2p(i)} * (r_i - 1) + P_{2p(i)+1} * r_i) mod\ r_i^2$$
$$= mod((945 * 9 + (-944) * 10), 100) = 65$$

Because $m_\mathrm{i} < F$

$$P'_{2p(i)} = P_{2p(i)} + (F - m_i) mod\ r_i = 945 + \mathrm{mod}((65-54), 10) = 946$$

$$P'_{2p(i)+1} = P_{2p(i)+1} - \left\lfloor \frac{F - m_i}{r_i} \right\rfloor - (F - m_i)\ mod\ r_i = (-944) - \left\lfloor \frac{65-54}{10} \right\rfloor - mod((65-54), 10) = -946$$

Hence pixel pair (945,-944) is modified to (946,-946) after embedding.

During extraction of secret bits from the pixel pair (946, −946)

Compute d_i=946-(−946) = 1892

Sub-range to which d_i belongs to is

$$W_j = [l_j, u_j] = (1024, 2047)$$

And hence $w_j = u_j - l_j + 1 = (2047-1024+1) = 1024$

$$r_i = \lfloor log_2 w_j \rfloor = 10$$

$$k_i = \lfloor log_2 r_i^2 \rfloor = 6$$

$$m_i = \quad F(P_{2p(i)}, P_{2p(i)+1}) = (P_{2p(i)} * (r_i - 1) + P_{2p(i)+1} * r_i) mod\ r_i^2$$

$$= mod(\ 946*9 + (-946)*10), 10^2\Big) = 54$$

This 54 is converted into binary format to obtain the secret message bits.

2.4 Chaotic maps

In an effort to provide intense security to patient's confidential information, chaos theory is introduced. The chaotic systems produce random yet deterministic signals that are much suitable for steganographic applications [23, 27, 40]. Various algorithms have been developed to produce N-dimensional chaotic sequences however, in this work the focus is on 1D combined logistic-sine (CLS) chaotic map. Individually logistic and sine maps exhibits chaotic properties in limited range only [9, 23, 46]. To overcome this drawback, these seed maps are combined linearly to generate a new 1D chaotic sequence that displays excellent behaviour over the entire range within (0,4] as illustrated through the bifurcation diagram in Fig. 2. The mathematical expression to generate CLS based chaotic sequence [40] is given as:

$$H\left(x_{o,}\, y_{o,}\, l\right) : x_{n+1} = \left(y_o x_n(1-x_n) + (4-y_o)\sin\left(\frac{\pi x_n}{4}\right)\right) mod 1 \quad (8)$$

where y_o is the control parameter that lies within (0, 4] and x_{n+1} *and* x_n are the $(n+1)th$ and nth states of chaotic sequence respectively. In order to generate random integer values from the sequence H, it is sorted and the original indices of the sorted sequence are preserved and used as chaotic sequence (X) with integer values as [40]

$$(V, X) = int\_sort(H) \quad (9)$$

where array V contains the sorted magnitudes of H while array X contains the original positions of these magnitudes. The random sequence X consists of integer values and is used to conceal secret bits in ECG signal.

2.5 ECG database

Standard databases available online [25] are used to evaluate and compare the performance of the proposed algorithm with the existing ECG steganography techniques. The databases used have the following specifications:

1. Massachusetts Institute of Technology-Beth Israel Hospital (MIT-BIH) Arrhythmia database: The two-channel ambulatory ECG recordings of 47 subjects (both normal and

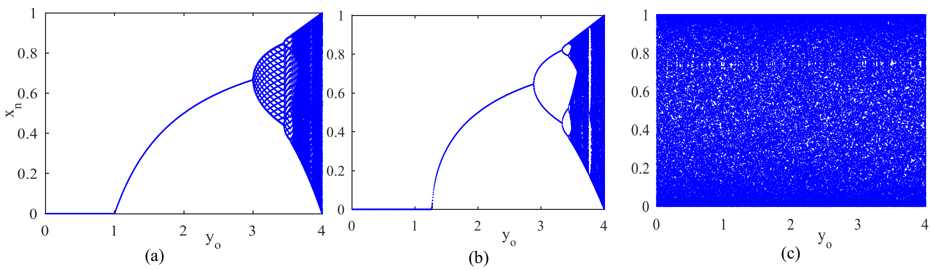


Fig. 2 The bifurcation diagrams of (**a**) logistic (**b**) sine and (**c**) CLS maps

abnormal) are approximately 30 min long. Each ECG signal is recorded at sampling frequency of 360 Hz per channel with 11-bit resolution over 10 mV range. The results are evaluated on the first channel of all the 48 records of 5 min duration.

2. MIT-BIH Normal Sinus Rhythm (MIT-BIH NSR) database: This database includes 18 long term recordings of 5 males aged 26 to 45 and 13 females aged 20 to 50 that have no significant arrhythmias. The performance is evaluated on all 18 records of 5 min duration.
3. Beth Israel Deaconess Medical Centre Congestive Heart Failure (BIDMC-CHF) database is used to test the proposed algorithm on recordings with acute abnormality. The database comprises of 15 ECG recordings that includes 11 men aged 22 to 71 and 4 women aged 54 to 63 suffered with stern cardiac failure. The recordings contain two ECG signals; each of about 20 h long duration and sampled at 250 Hz, 12-bit resolution over a range of ±10 mV. Results are evaluated on all 15 recordings of duration 1.5 min.
4. Self-recorded database: This database consists of ECG signals recorded in the Biomedical Signal Processing laboratory at Department of Electronics and Communication Engineering, Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, India on lead II using BIOPAC® MP150. The signals were recorded from the local population under standard conditions in a quiet room, at comfortable light and temperature levels and sampled at 500 Hz, 12-bit resolution. The written consent from 20 different subjects was taken prior to the recording.

3 Proposed methodology

The steganography technique proposed in this work explores both transform and spatial domain approaches to embed confidential information in 2D ECG (*Im*). The 2D ECG is divided into three non-overlapping fragments such that the side fragments occupies the pivotal QRS region while the intermediate part comprises relatively less significant non-QRS region of ECG signal. Different embedding algorithms are designed to conceal information in these fragments. The secret bits are embedded in the order of first, second and then third block respectively as per their maximum embedding capacities. The proposed methodology involves the following steps 1) Pre-processing of ECG signal 2) Conversion of 1D ECG signal into 2D ECG matrix (*Im*) 3) Generation of chaotic sequences 4) Encryption of patient's personal information. 5) Embedding process 6) Reconvert 2D stego-ECG (*sIm*) back to 1D stego-ECG (*sECG*) signal which is then transmitted over the channel. The embedded information is extracted at the receiver following the reverse procedure. The detailed diagram to demonstrate the process of embedding and retrieving the secret information is shown in Fig. 3.

3.1 Pre-processing of input ECG signal

The ECG signals available at standard databases are already processed to filter the noises and artefacts induced during acquisition whereas the self-recorded ECG signals are corrupted with different noises like; baseline drift, electrode contact noise, powerline interference muscle contractions, electrosurgical noise, instrumentation noise

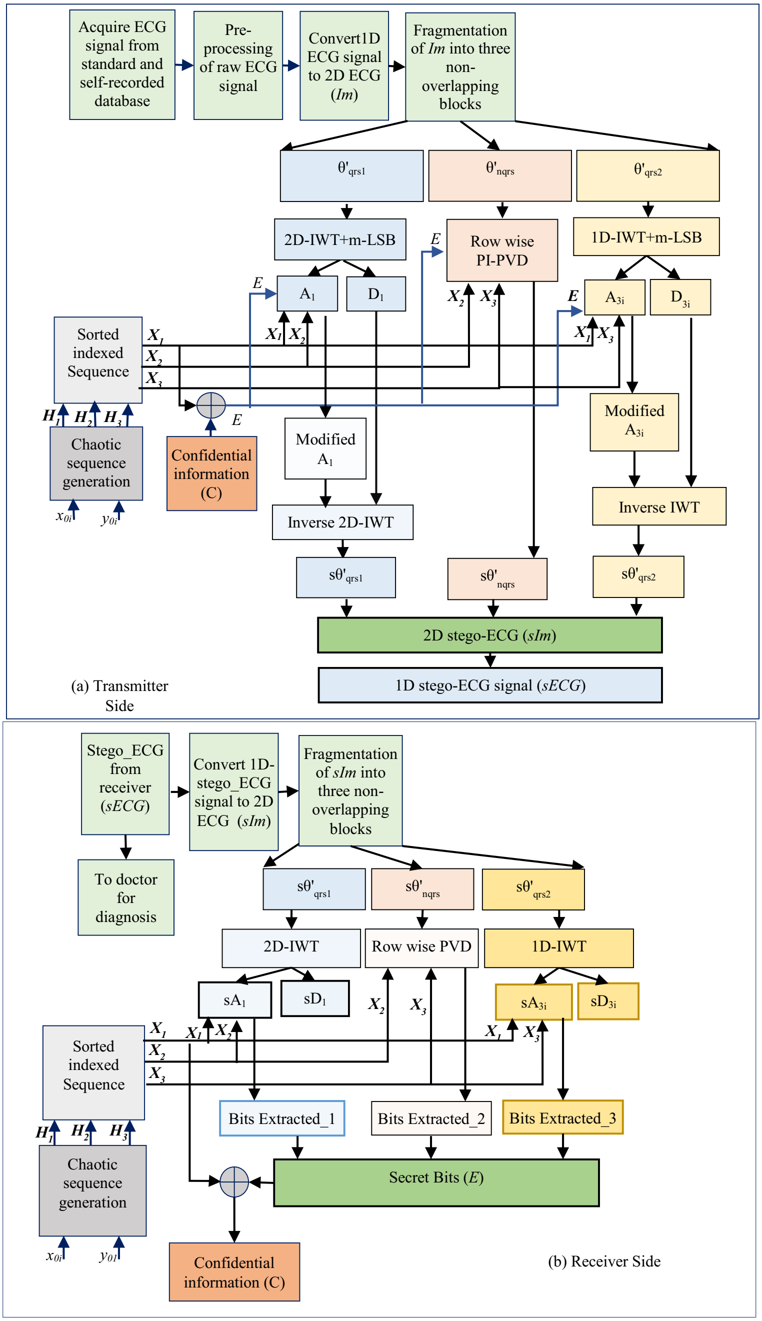


Fig. 3 (**a**) Embedding process (**b**) Extraction process involved in proposed methodology

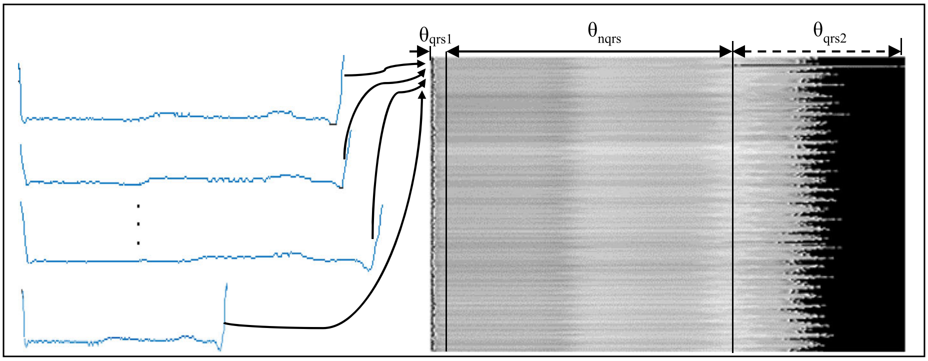


Fig. 4 Illustration of vertical stacking of beats to form 2D ECG matrix of 1 min duration of record 100 from MIT-BIH database

etc. These noises are attenuated from the ECG signal using different filters prior to embedding the secret information [4].

3.2 Conversion of 1D ECG signal into 2D ECG matrix

ECG signal has both inter-beat and intra-beat correlation properties and based on these properties 1D ECG signal is converted into 2D ECG matrix. The samples between two consecutive R-peaks of ECG are considered as one segment and all such segments are cut and aligned vertically to form 2D ECG (*Im*). Among several methods reported in the literature to detect R-peaks [26, 33, 39], k-NN method of QRS detection is used to remove noises and to identify R-peaks [33]. The length of each segment is normalised with zero padding [6]. The resultant 2D ECG formed with 1 min of ECG record 100 of MIT-BIH database is illustrated in Fig. 4.

3.3 Generation of chaotic sequences

Chaotic sequences are employed in the proposed steganography approach for two reasons; (i) to cipher the confidential information and (ii) to generate randomness in the selection process of ciphered bits embedding. For this, three sets of initial conditions (x_{01}, y_{01}), (x_{02}, y_{02}) and (x_{03}, y_{03}) are used to generate chaotic sequences H_1, H_2 and H_3 respectively using (8). Further these sequences are sorted to generate random sequences with integer values using (9). The initialization values and control parameters used to generate different chaotic sequences are mentioned in Table 1.

Table 1 List of initialization values and control parameters used to generate chaotic sequences

Chaotic Sequence	Sorted chaotic sequence	Initial value (x_o)	Control parameter (y_o)
$H_1(x_{01}, y_{01})$	$X_1 = int\_sort(H_1)$	$x_{01} = 0.897655762990$	$y_{01} = 3.9953461356011$
$H_2(x_{02}, y_{02})$	$X_2 = int\_sort(H_2)$	$x_{02} = 0.933453564978$	$y_{02} = 3.886954532619$
$H_3(x_{03}, y_{03})$	$X_3 = int\_sort(H_3)$	$x_{03} = 0.994357334262$	$y_{03} = 3.973256778521$

3.4 Encryption of confidential information into ciphertext

Though steganography secures patient's personal information from illegitimate access but to strengthen the security of the information, the confidential information (C) is initially converted into cipher text (*E*) before entrenching into ECG signal. The encryption process involves the XOR operation between chaotic sequence (X_1) and C. The process of converting confidential information into cipher text is explained in algorithm 1

Algorithm 1: Conversion of confidential information into ciphertext

L_c: Length of confidential information

Input: confidential information (C), initialization values of x_{01} and y_{01} as mentioned in Table 1
Output: Cipher text (*E*)

Generate $H_1\,(x_{01,}\,y_{01,}\,L_c)$ using (8)
$X_1 \leftarrow int\_sort\ (H_1)$
$l = \lceil log_2 L_c \rceil$
$bts \leftarrow 1$
for n=1:L_c
    $E(bts{:}bts+(l\text{-}1)) \leftarrow binary(X_1(n), l) \oplus binary(\mathrm{C}(X_1(n)), l)$
    $bts \leftarrow bts+l$
end for

3.5 Embedding process

The focus of the proposed technique is to improve the payload capacity without disturbing the diagnosability of an ECG signal. To accomplish this aim, QRS and non-QRS regions of 2D ECG are segregated into three non-overlapping blocks and specific steganography technique is applied in each block. The embedding is performed in two steps:

i) Disintegration of 2D ECG in three non-overlapping blocks

2D ECG (*Im*) is partitioned into three fragments; θ_{qrs1}, θ_{nqrs} and θ_{qrs2} where θ_{qrs1} and θ_{qrs2} comprises of R-peaks of crucial QRS complex region while θ_{nqrs} holds the non-QRS region of *Im* as shown in Fig. 5. The number of samples embodying QRS region (S_{qrs}) depends on the sampling frequency (f_s) of the signal and duration of QRS complex (t_{qrs}) which is calculated as

$$\mathrm{S_{qrs}} = \left\lceil f_s * t_{qrs} \right\rceil$$

Samples occupied by R-peaks each in blocks θ_{qrs1} and θ_{qrs2} are

$S_R = \lceil S_{qrs}/2 \rceil$ // QRS complex region is divided in two equal parts

The duration of normal QRS complex lies in range of 0.08 s to 0.12 s [34], but in case of pathological disorders it can be widened or narrowed. For experimentation, QRS complex of 0.15 s is considered in this work. This duration is wide enough to include cases of abnormal ECGs. The proposed approach has been analysed on both normal (MIT-BIH NSR) and abnormal (MIT-BIH arrhythmia, BIDMC-CHF) databases. None of the evaluated signals have QRS complex wider than 0.15 s. But if any abnormal case with QRS complex wider than 0.15 s is observed, then that QRS complex can be excluded from data embedding.

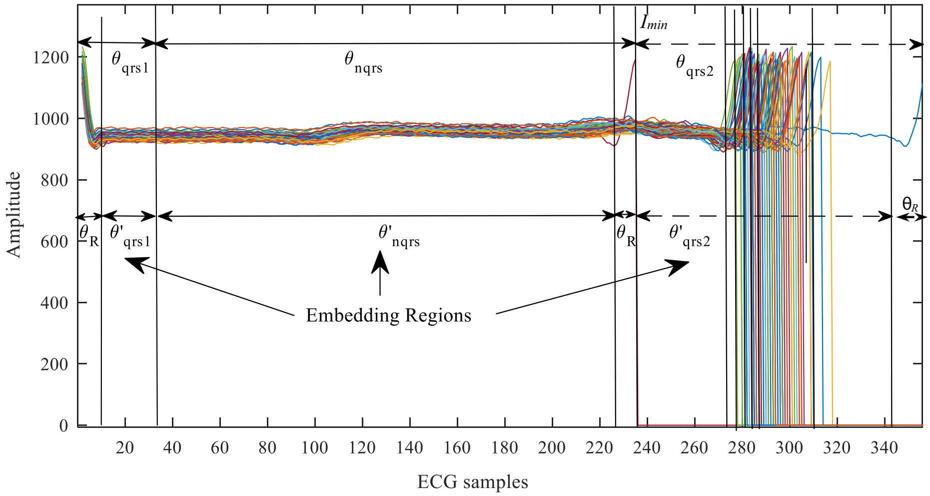


Fig. 5 Illustration of embedding regions in three fragments of an ECG image formed from 1 min of samples of record 100 of MIT-BIH arrhythmia database

Further to avoid any deviation in amplitude of R-peaks, θ_R samples ($\lceil 2\,\%\,of\,f_s \rceil$) that includes these peaks are excluded from the embedding portions. Finally, the fragments in 2D ECG used for hiding the ciphered bits are organised as:

Fragment I (θ'_{qrs1}): $\theta_R + 1$ to S_R

II(θ'_{nqrs}): $S_R + 1$ to $I_{min} - \theta_R$ // I_{min} is the index of the shortest beat in *Im.*

III(θ'_{qrs2}): $I_{min} + 1$ to (end' - θ_R) // end' depicts that each row has variable number of ECG samples and θ'_{qrs2} varies according to the length of individual beat.

$\lceil\ \rceil$ represents the least integer function

Figure 5 displays the embedding regions (θ'_{qrs1}, θ'_{nqrs} and θ'_{qrs2}) of 2D ECG formed from record 100 of MIT-BIH arrhythmia database of 1 min duration. The ECG record is sampled at f_s of 360 Hz, accordingly S_R is calculated as (360*0.15/2) i.e. 27. θ_R is 8 and the shortest peak (I_{min}) determined in *Im* lies at 236. Hence the first two fragments; θ'_{qrs1} and θ'_{nqrs} suitable for embedding the secret bits lies from 9 to 27 and 28 to 229 respectively whereas in third fragment i.e. θ'_{qrs2}, the embedding region varies from beat to beat depending upon number of ECG samples left in each beat after excluding θ_R.

ii) Blockwise embedding of encrypted data and side information

As displayed in Fig. 5 the image is fragmented on the basis of morphological features of an ECG signal and hence assorted approaches are applied in these fragments to embed secret data.

Case 1: IWT based modified-LSB (m-LSB) steganography in θ'_{qrs1}

This segment of *Im* consists of subtle information and afford minimal deviation only. Hence LSB based IWT steganography is pragmatic in this section. The approximate coefficients (*A*) are obtained by applying first level 2D-IWT on θ'_{qrs1} with db4 as the mother wavelet. The LSBs of the chaotically selected approximate coefficients are replaced with the ciphered bits using *m-LSB* steganography approach as discussed in algorithm 2.

Algorithm 2: Embedding process in θ'qrs1 region
Z_1: Maximum number of binary bits required to represent the largest coefficient in A_1
r_1: shifting factor, where $1 < r_1 < Z_1$ initialize $r_1 = 5$;
b: number of bits embedded in each coefficient; initialize $b = 2$,
E: Ciphered bits
N: length of ciphered bits
n_1: n_1th value of E; initialize $n_1=1$;
sA_1: approximate coefficients with stego values
Initialize $x_{01}, y_{01}, x_{02}, y_{02}$ with values mentioned in Table 1

Input: θ'_{qrs1}, Ciphered bits (E), r_1, b, x_{01}, y_{01}, x_{02}, y_{02}
Output: stego-θ'_{qrs1} ($s\theta'_{qrs1}$)
$[A_1\ D_1]$= IWT2 (θ'_{qrs1}, db4)
u_1, v_1: number of rows and columns in A_1
largest_App_coeff= maximum (A_1)
Z_1 = length (*binary* (*largest_App_coeff*)) // find maximum number of bits required to convert largest approximate coefficient into binary
$M_1 = Z_1 - r_1$
Using (8), generate two chaotic sequences $H_1(x_{01}, y_{01}, u_1)$ and $H_2(x_{02}, y_{02}, v_2)$
$X_1 = int\_sort(H_1)$
$X_2 = int\_sort(H_2)$
for $i = 1$ to u_1
  for $j = 1$ to v_1
    Selected_coff = $A_1(X_1(i), X_2(j))$
    Bin_ Selected_coff = binary (*Selected_coff*)
    Bin_ Selected_coff $(LSB_0 : LSB_{(b-1)}) \leftarrow$ *Bin_Selected_coff*$(M_1-(b-1)):M_1) \oplus E(n_1: n_1+(b-1))$
    $Stego\_A_1$ = *decimal* (*Bin_ Selected_coff*)
    $sA_1(X_1(i), X_2(j))$= $Stego\_A_1$
    if $n_1 < N$
      $n_1 = n_1 + b$;
    end if
  end for
end for
Take inverse IWT to generate $s\theta'_{qrs1}$
$s\theta'_{qrs1}$= *i*IWT(sA_1, D_1, db4)

Case 2: Embedding in θ'_{nqrs} *using pixel inverted-PVD (PI-PVD) technique*

As discussed in section 2, PVD is suitable in high frequency regions where the difference between the pixel pair is large enough to proliferate the EC. In the proposed method, this approach is applied on less sensitive non-QRS (θ'_{nqrs}) section of ECG beats. This section is like a flat terrain that consists of low frequencies only. To apply PVD in this region, high frequency region is created by inverting the amplitude of every alternate ECG pixel in this fragment. It increases the difference between adjacent samples and hence improves embedding capacity [27]. The secret bits are stored at chaotically chosen even pixel pairs (S_{2p}) in order to fully utilize the EC. PI-PVD is applied row-wise in θ'_{nqrs} and to generate randomness, both rows as well as sample pairs are selected chaotically. The implementation process is explained in algorithm 3 that follows the same procedure as discussed in section 2 The table consists of 12 dyadic-ranges varying between 2^0 and 2^{12} with lower ($l_j = 2^{j-1}$) and upper ($u_j = 2^j-1$) bounds for the sub ranges are given as

$$W_j = [l_j, u_j]; j = 0, 1, 2.....12$$

The width w_j for range W_j is same as l_j [27, 36]. The procedure to embed secret information (E) using PI-PVD approach is explained in algorithm 3.

Algorithm 3: To embed secret bits in θ'$_{nqrs}$ using PI-PVD technique

Initialize $x_{02}, y_{02}, x_{03}, y_{03}$ with values mentioned in Table 1

S: sample pairs (S_1, S_2)

d: absolute difference between sample values

n_2: $(n_1+1)^{th}$ value of N ciphered bits (E) // first n_1 values are stored in θ'$_{qrs1}$ region

u_2, v_2: rows and columns of θ'$_{nqrs}$ respectively

Input: ECG samples in θ'$_{nqrs}$, $n_2, x_{02}, y_{02}, x_{03}, y_{03}$

Output: stego-θ'$_{nqrs}$: (sθ'$_{nqrs}$)

Generate two chaotic sequences; $H_2(x_{02}, y_{02}, u_2)$ and $H_3(x_{03}, y_{03}, v_2)$ using (8)

```
X_2 = int_sort (H_2)
X_3 = int_sort(H_3)
for i=1:u_2
 for j=1:v_2
   S=[S_1 S_2]; S_1= θ'_nqrs (X_2(i), X_3(j)) , S_2= θ'_nqrs(X_2(i), X_3(j) +1)
   if S_1 * S_2 = +ve
      S_2 = -S_2
   end if
   d =|S_1 - S_2|
   W_j = [l_j, u_j] if l_j ≤ d && d ≥ u_j
   w_j = l_j
   s = ⌊log_2 w_j⌋
   k = ⌊log_2 s^2⌋
   m= decimal(E(n_2 to n_2 + k))
   F = (S_1 * (s - 1) + S_2 * s)mod s^2
      if m = F
          (stegoS_1, stegoS_2) = (S_1, S_2)
        elseif m > F
          stego S_1 = S_1 - (m - F)mod s
          stego S_2 = S_2 + ⌊(m- F)/s⌋+ (m - F)mod s
        elseif m < F
          stego S_1 = S_1 + (F - m) mod s
          stego S_2 = S_2 - ⌊(F-m)/s⌋ - (F - m) mod s
      end if
  Verify the underflow and overflow condition
      if l_j< (stego S_1)> u_j || l_j< ( stego S_2) > u_j

           stegoS = [stego S_1  stego S_2 ]
           n_2=n_2+k
      end if
  end for
        θ'_nqrs (X_2(i), X_3(j))= stego S_1
        θ'_nqrs(X_2(i), X_3(j) +1)= stegoS_2
end for
sθ'_nqrs = θ'_nqrs
```

⌊ ⌋ represents the greatest integer function || signifies the logical OR operation

Case 3: m-LSB based embedding in θ'_{qrs2}

ECG signal being quasi periodic, the duration is different for every heart beat and so are the number of ECG samples. Therefore in fragment θ'_{qrs2} of *Im*, 1D IWT embedding is performed row-wise on the chaotically selected row and *m-LSB* based embedding is done at the LSBs of randomly chosen approximate coefficients. The embedding process is explained in algorithm 4

Algorithm 4: Row wise embedding in θ'_{qrs2} using *m-LSB* method

```
Z_2i: Maximum number of binary bits required to convert the largest coefficient in A_3i
r_2: shifting factor  where 1< r_2 <Z_2, r_2=5;
n_3: (n_2+1)^th value of N ciphered bits   (First n_2 bits of E are embedded in fragments θ'_qrs1 and
θ'_nqrs
b: number of bits embedded in each coefficient; b =2;
R: vector contains count of the number of ECG samples in each row of θ'_qrs2
Initialize x_03, y_03, x_01, y_01 with values mentioned in Table 1
Input: θ'_qrs2, Ciphered bits E(n_3 to N), x_03, y_03, x_01, y_01, r_2
Output: stego-θ'_qrs2: (sθ'_qrs2)
u_3: number of rows in θ'_qrs2
Generate chaotic sequence H_3(x_03, y_03, u_3) using (8)
X_3 = int_sort(H_3)
for  i = 1 to u_3
        no_samples= R(X_3(i))
        M_2i= Z_2i – r_2
        row_selected= θ'_qrs2 (X_3(i), 1: no_samples)
        [A_3i D_3i]= IWT (row_selected, db4)          // apply 1D IWT on each row separately
        v_3i: number of columns in A_3i
     Generate chaotic sequence H_1 (x_01, y_01, v_3i) using (8)
        X_1 = int_sort(H_1)
   for j= 1 to v_3i
       Selected_coff = A_3i(X_1(j))
      Bin_ Selected_coff = binary (Selected_coff)
  Bin_ Selected_coff (LSB_0: LSB_b-1) ← Bin_Selected_coff (M_2i:M_2i+(b-1)) ⊕ E(n_3: n_3+(b-1))
        A_3i(X_1(j)) = decimal (Bin_ Selected_coff)
      if n_3 < N
          n_3= n_3+b;
        end if
   end for
   sθ'_qrs2 (row_selected)= iIWT(sA_3i, D_3i, db4)
end for
```

3.6 Reconstruction of stego-image and stego-ECG

The stego-blocks ($s\theta'_{qrs1}$, $s\theta'_{nqrs}$ and $s\theta'_{qrs2}$) are arranged back to their locations to obtain the complete 2D stego-ECG (*sIm*) which is further converted into 1D stego-ECG (*sECG*) and finally transmitted over the channel.

$$sIm = \left[s\theta_{qrs1}\ s\theta_{nqrs}\ s\theta_{qrs2}\right]$$

3.7 Receiver side

At receiver, the stego-ECG signal is received and forwarded to the concerned doctor for diagnosis while the administrative personnel who has the key (section 4.4.1), extracts the hidden information. The extraction process at receiver follows the reverse procedure as demonstrated in Fig. 3(b). Following steps are used to extract the hidden information:

Step 1: Convert *sECG* into 2D stego ECG (*sIm*).
Step 2: Divide *sIm* into blocks $s\theta_{qrs1}$, $s\theta_{nqrs}$ and $s\theta_{qrs2}$ as was done on transmitter side.
Step 3: Apply similar methodology on $s\theta'_{qrs1}$, $s\theta'_{nqrs}$ and $s\theta'_{qrs2}$ to extract the hidden information from respective fragments as implemented at transmitter but in reverse order. The complete procedures followed to obtain secret bits are well explained in algorithms 5, 6 and 7.

Algorithm 5: Extraction of embedded bits from $s\theta'_{qrs1}$

Z_1: Maximum number of *binary* bits required to represent the largest coefficient in sA_1
r_1: shifting factor where $1< r_1 <Z_1$ initialize $r_1 =5$;
b: number of bits embedded in each coefficient; initialize $b =2$,
Initialize $x_{01}, y_{01}, x_{02}, y_{02}$ with values mentioned in Table 1

Input: $s\theta'_{qrs1}, r_1, b, x_{01}, y_{01}, x_{02}, y_{02},$
Output: Extracted bits1 (*Ex_1*)

Using (8), generate two chaotic sequences $H_1(x_{01}, y_{01}, u_1)$ and $H_2(x_{02}, y_{02}, v_1)$
$X_1 = int\_sort(H_1)$
$X_2 = int\_sort(H_2)$
$[sA_1\ sD_1]$= IWT2 ($s\theta'_{qrs1}$, db4)
u_1, v_1: number of rows and columns in sA_1
M_1: Z_1-r_1
B←1
for $i = 1$ to u_1
  for $j = 1$ to v_1
    $Selected\_coff = sA_1(X_1(i), X_2(j))$
    $Bin\_Selected\_coff = binary(Selected\_coff)$
    $Ex\_1(B:B+(b-1)) \leftarrow Bin\_Selected\_coff(M_1-(b-1):M_1) \oplus Bin\_Selected\_coff(LSB:LSB+(b-1))$
      $B=B+b$
  end for
end for

Algorithm 6: Extraction of embedded bits from $s\theta'_{nqrs}$
Initialize $x_{02}, y_{02}, x_{03}, y_{03}$ with values mentioned in Table 1
Input: $s\theta'_{nqrs}, x_{02}, y_{02}, x_{03}, y_{03}$

Output: Extracted bits2 (*Ex_2*)
u_2, v_2: rows and columns of $s\theta'_{nqrs}$ respectively
Generate two chaotic sequences; $H_2(x_{02}, y_{02}, u_2)$ and $H_3(x_{03}, y_{03}, v_2)$ using (8)
$X_2 = int\_sort(H_2)$
$X_3 = int\_sort(H_3)$
C←1
for $i = 1$ to u_2
    Follow algorithm 3 to find S, *d, s, k and F*
    $Ex\_2(C:(C+k)-1) = binary(F, k)$
    $C=C+k$
end for

Algorithm 7: Extraction of embedded bits from sθ'$_{qrs2}$

Z_{2i}: Maximum number of binary bits required to convert the largest coefficient *in* A_{3i}
R: vector containing count of number of ECG samples in each row of sθ'$_{qrs2}$
Initialize $x_{03}, y_{03}, x_{01}, y_{01}$ with values mentioned in Table 1.
r_2: shifting factor where $1< r_2 <Z_1$ initialize r_2 =5;
b: number of bits embedded in each coefficient; initialize b =2,

Input: sθ'$_{qrs2}$, r, $x_{03}, y_{03}, x_{01}, y_{01}$
Output: Extracted bits (*Ex_3*)

u_3: number of rows in sθ'$_{qrs2}$
Generate chaotic sequence $H_3(x_{03}, y_{03}, u_3)$ using (8)
$X_3 = int\_sort(H_3)$
for i = 1 to u_3
    no_samples= $R(X_3(i))$
    row_selected= sθ'$_{qrs2}$ ($X_3(i)$, 1: no_samples) .

    [sA_{3i} sD_{3i}]= IWT (*row_selected*, db4)
    v_{3i}: number of columns in sA_{3i}
    Generate chaotic sequence H_1 (x_{01}, y_{01}, v_{3i}) using (8)
    $X_1 = int\_sort(H_1)$
    rr_i=*maximum*(sA_{3i})
    Z_{2i}= length (*binary* (rr_i))   // find number of bits required to convert largest approximate coefficient in a row into binary
    M_{2i}: Z_i -r_2
    $D \leftarrow 1$

  for j= 1 to v_{3i}
      Selected_coff = $sA_{3i}(X_1(j))$
      Bin_ coff = *binary* (*Selected_coff, L*)
      Ex_3(D:D-(b-1)) ← *Bin_ coff* (M_{2i}: M_{2i}-(b-1) ⊕ *Bin_ coff* ($LSB_0 : LSB_{(b-1)}$)
      $D= D + b$;
  end for
end for

Step 4: Extracted bits = [*Ex_1 Ex_2 Ex_3*]

4 Results and discussion

The technique proposed in this work has successfully achieved the prime goals of steganography viz. imperceptibility, robustness and payload capacity. Although steganography causes irreparable loss to the ECG signal but the proposed technique aims to restrain the loss to its minimal. This is evidently demonstrated in Fig. 6 that the amount of error occurred in the stego ECG is trivial even after embedding secret information to their maximum capacity (4996 bits) in 3000 samples of record 100 of MIT-BIH arrhythmia database. The proposed steganography approach is blend of both spatial and transform domain techniques and shows impeccable performance with high embedding capacity and minimal deterioration in signal quality. Various statistical parameters such as PRD, PRD1024, normalised PRD (PRDN), mean square error (MSE), root mean square error (RMS), SNR, PSNR, kullback leibler divergence (KL-Divergence) [27, 40] are computed to analyse its efficacy. Clinically critical metrics such as weighted percentage root mean square difference (WWPRD) [2] and wavelet energy based diagnostic distortion (WEDD) [22] are also measured to evaluate the performance of the

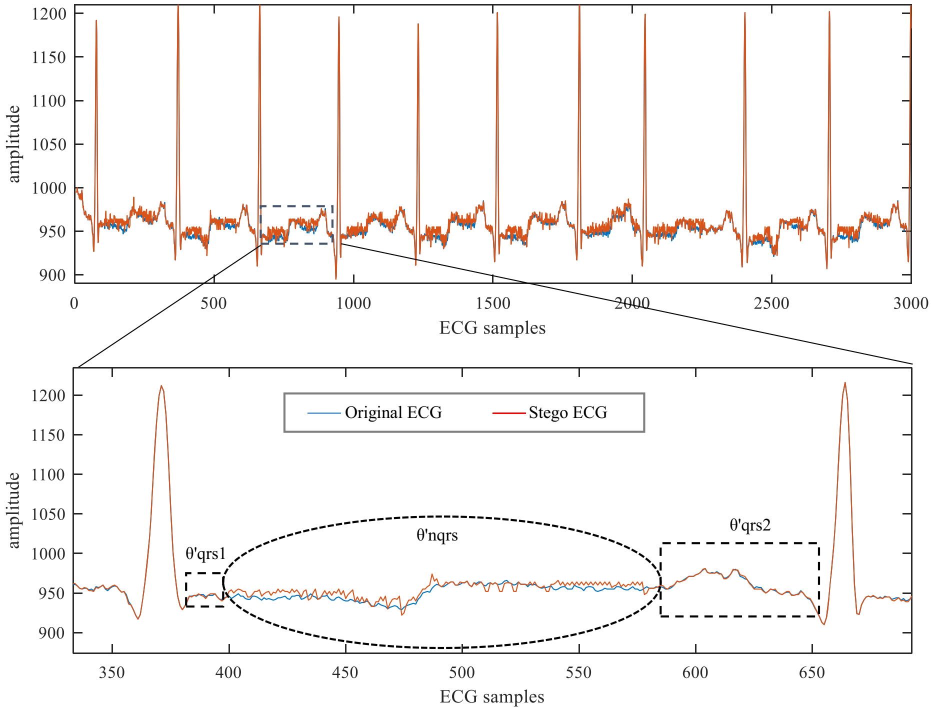


Fig. 6 Original and stego ECG signals alongwith the amount of error occurred when embedding secret information to their maximum capacity in 3000 samples of record 100 of MIT-BIH arrhythmia database

proposed technique. The results are computed with two bits embedded at the LSB positions of the approximate coefficients obtained from IWT in blocks θ'_{qrs1} and θ'_{qrs2} while PI-PVD based steganography is applied in θ'_{nqrs} region. The overall results in terms of statistical and diagnostic errors as well as measures regarding the payload capacity and BER on all 48 records of MIT-BIH arrhythmia database of 5 mins duration, 18 records of MIT-BIH NSR database of 5 mins duration, 15 records of BIDMC-CHF of 1.5 mins duration and 20 records of self-recorded data of 5 mins duration are displayed in Tables 2, 3, 4 and 5 respectively. Average PRD, PRD1024, PRDN, SNR, PSNR, KL-Divergence, WWPRD and WEDD obtained in case of MIT-BIH arrhythmia database of 5 mins duration are 4.32×10^{-3}, 4.52×10^{-2}, 0.066, 48.27, 51.51, 9.42×10^{-6}, 0.152 and 0.042 respectively at EC of 1.58 and zero BER; in MIT-BIH NSR database 1.8×10^{-2},4.8×10^{-3}, 0.0628,35.28, 44.71, 2.2×10^{-4}, 0.062 and 0.051 respectively at EC of 1.69 and zero BER; in BIDMC-CHF database 1.77×10^{-2}, 7.5×10^{-3}, 0.073, 37.53, 44.174, 3.37×10^{-4}, 0.1595, 0.044 respectively at EC of 1.38 and zero BER and in self-recorded database 8.63×10^{-3}, 0.01046, 0.02563, 41.5497, 52.10, 4.15×10^{-5}, 0.06588 and 0.01623 respectively with average EC calculated as 1.9572 at zero BER.

4.1 Effect of ECG duration on the performance metrics

The effect of ECG duration on the performance of the proposed algorithm is studied. Table 6 shows the average of performance metrics when determined on all 48 records of MIT-BIH arrhythmia database at varying durations. An average PRD, PSNR, KL-Divergence,

Table 2 Performance evaluation measures on all 48 records of MIT-BIH arrhythmia database of 5 mins duration

Record	PRD	PRD1024	PRDN	SNR	PSNR	KL-Divergence	WWPRD	WEDD	EC	Number of bits embedded	BER
100	0.0044335	0.058175	0.121108	47.06604	49.51323	8.79×10^{-6}	0.23723	0.087085	1.598	173,946	0
101	0.002401	0.026818	0.035418	52.3932	56.22994	2.98×10^{-6}	0.089761	0.024278	1.112	104,414	0
102	0.004125	0.062932	0.104592	47.69257	50.19551	7.84×10^{-6}	0.187039	0.075981	1.508	162,556	0
103	0.005331	0.066798	0.081347	45.46395	48.84231	1.37×10^{-5}	0.179014	0.053886	2.129	224,442	0
104	0.005468	0.084591	0.118162	45.24385	48.16577	1.27×10^{-5}	0.184484	0.077422	1.972	96,326	0
105	0.003903	0.050238	0.060997	48.17238	51.35736	7.56×10^{-5}	0.162626	0.038092	1.499	157,240	0
106	0.003905	0.050748	0.056482	48.16779	51.54104	7.31×10^{-6}	0.125759	0.037548	1.481	155,572	0
107	0.005452	0.031683	0.033039	45.26812	49.35676	1.44×10^{-5}	0.078227	0.016991	2.030	214,884	0
108	0.004498	0.04654	0.049154	46.91393	50.69122	8.33×10^{-6}	0.093476	0.033808	1.572	94,814	0
109	0.005076	0.050911	0.057616	45.88997	48.8329	1.25×10^{-5}	0.169139	0.030098	1.875	193,008	0
111	0.005523	0.092472	0.113469	45.1571	47.53557	1.44×10^{-5}	0.302409	0.062149	2.144	227,344	0
112	0.007065	0.034246	0.126268	43.01816	45.79692	1.98×10^{-5}	0.287734	0.070872	2.296	240,100	0
113	0.004498	0.046885	0.049335	46.93927	50.67012	8.47×10^{-6}	0.094764	0.034808	1.569	167,712	0
114	0.007888	0.036549	0.137045	42.52662	44.44722	2.07×10^{-5}	0.326392	0.074149	2.550	100,454	0
115	0.006415	0.047725	0.083841	43.85588	47.84231	1.66×10^{-5}	0.156494	0.054922	2.249	232,820	0
116	0.005451	0.020104	0.036891	45.27	50.78236	1.33×10^{-5}	0.06249	0.023768	1.692	178,624	0
117	0.007489	0.037655	0.13457	42.51166	44.43222	2.09×10^{-5}	0.316639	0.073671	2.522	269,440	0
118	0.004345	0.063238	0.115921	47.25679	50.23551	7.93×10^{-6}	0.171039	0.078144	1.521	200,460	0
119	0.005285	0.022339	0.04162	45.53868	50.39971	1.29×10^{-5}	0.106279	0.027383	1.656	175,938	0
121	0.007261	0.035758	0.109365	42.78005	46.10393	2.02×10^{-5}	0.331378	0.054679	2.403	251,692	0
122	0.006776	0.031129	0.078941	43.38019	46.64872	1.86×10^{-5}	0.195814	0.044015	2.143	227,688	0
123	0.006585	0.03291	0.092371	43.62939	48.0365	1.68×10^{-5}	0.200153	0.057297	2.218	236,568	0
124	0.006643	0.031423	0.067316	43.55299	47.98522	1.82×10^{-5}	0.177777	0.038303	2.192	230,906	0
200	0.001517	0.018931	0.019978	56.38314	59.894	1.21×10^{-6}	0.054463	0.011658	0.934	98,690	0
201	0.003789	0.072937	0.097247	48.43045	50.42183	6.83×10^{-6}	0.242583	0.061485	1.441	147,652	0
202	0.004486	0.074158	0.093358	46.96305	49.62881	9.09×10^{-6}	0.250252	0.059144	1.669	177,472	0
203	0.000895	0.008915	0.009499	60.96622	64.55792	4.26×10^{-7}	0.026337	0.00458	0.852	93,602	0
205	0.002644	0.032202	0.06806	51.55569	53.78346	3.31×10^{-6}	0.138578	0.050503	1.086	118,786	0
207	0.002198	0.028218	0.031893	52.41468	56.3384	2.82×10^{-6}	0.100315	0.019934	1.091	97,340	0
208	0.000563	0.00588	0.006174	64.98576	68.46416	1.63×10^{-7}	0.017384	0.003175	0.434	165,718	0
209	0.004055	0.06535	0.076386	47.84041	50.70106	7.43×10^{-6}	0.150689	0.055786	1.417	154,384	0
210	0.001907	0.03106	0.036157	54.39181	56.78835	1.87×10^{-6}	0.086475	0.023122	0.977	132,610	0
212	0.005311	0.075205	0.082436	45.49596	48.50445	1.2×10^{-5}	0.165125	0.053937	1.850	201,448	0

Table 2 (continued)

Record	PRD	PRD1024	PRDN	SNR	PSNR	KL-Divergence	WWPRD	WEDD	EC	Number of bits embedded	BER
213	0.005018	0.034508	0.037997	45.98921	50.38792	1.15×10^{-5}	0.087005	0.024206	1.656	181,150	0
214	0.003454	0.035741	0.037626	49.23355	52.81266	6.02×10^{-6}	0.09806	0.025433	1.307	150,104	0
215	0.003616	0.058651	0.065126	48.83535	52.4198	5.91×10^{-6}	0.128673	0.046739	1.226	134,070	0
217	0.004785	0.038441	0.039884	46.40263	49.92949	1.02×10^{-5}	0.095787	0.024045	1.636	177,724	0
219	0.004706	0.028014	0.047486	46.54699	50.36159	1.06×10^{-5}	0.103443	0.031831	1.575	171,248	0
220	0.005401	0.038254	0.079204	45.35107	48.96218	1.26×10^{-5}	0.138432	0.054327	1.737	188,672	0
221	0.003929	0.056143	0.064775	48.11492	51.18198	7.31×10^{-6}	0.168254	0.043331	1.443	157,548	0
222	0.005273	0.129138	0.181075	45.55908	47.48404	1.24×10^{-5}	0.375751	0.12312	1.935	210,814	0
223	0.004002	0.027793	0.047487	47.95542	51.72653	7.93×10^{-6}	0.112476	0.031396	1.434	156,350	0
228	0.00239	0.029618	0.032193	52.43268	56.3084	2.83×10^{-6}	0.101541	0.020293	1.070	116,512	0
230	0.005122	0.062685	0.069009	45.81185	49.25031	1.18×10^{-5}	0.153313	0.045627	1.899	206,186	0
231	0.003467	0.049358	0.059733	49.20117	52.44906	5.7×10^{-6}	0.126437	0.043602	1.344	146,478	0
232	0.004536	0.109898	0.152546	46.86579	48.36091	9.29×10^{-6}	0.321597	0.103941	1.634	177,872	0
233	0.002794	0.024305	0.025325	51.07549	54.55783	3.99×10^{-6}	0.064622	0.017096	1.095	120,018	0
234	0.005646	0.077157	0.087188	44.96563	48.30819	1.39×10^{-5}	0.199129	0.053809	2.087	227,350	0
Average	**0.004324**	**0.045266**	**0.066957**	**48.27814**	**51.51508**	$\mathbf{9.42 \times 10^{-6}}$	**0.15289**	**0.042967**	**1.5869**	**171,390.54**	**0**
SD	**0.001668**	**0.024356**	**0.036009**	**4.650006**	**4.551161**	$\mathbf{5.36 \times 10^{-6}}$	**0.079757**	**0.024071**	**0.4268**	**46,098.298**	**0**

Table 3 Performance evaluation measures on all records of MIT-BIH NSR database of 5 mins duration

Record	PRD	PRD1024	PRDN	SNR	PSNR	KL-Divergence	WWPRD	WEDD	EC	Number of bits embedded	BER
16,265	0.01409	0.00504	0.03441	37.02265	47.36757	1.2×10^{-4}	0.03924	0.02735	1.79945	69,099	0
16,272	0.02087	0.00498	0.10139	33.60749	42.34303	2.1×10^{-4}	0.1001	0.08423	1.9631	75,383	0
16,273	0.0132	0.00699	0.04226	37.58596	47.11102	9×10^{-5}	0.04348	0.0326	1.96539	75,471	0
16,420	0.01944	0.00534	0.07729	34.22398	43.61341	1.9×10^{-4}	0.07604	0.06936	2.02266	31,068	0
16,483	0.01562	0.00657	0.07665	36.12772	43.82047	1.1×10^{-4}	0.07388	0.06302	1.93406	74,268	0
16,539	0.02185	0.00483	0.07297	33.21188	43.70313	2.5×10^{-4}	0.07359	0.06286	1.79294	68,849	0
16,773	0.0136	0.00554	0.03723	37.32836	47.19777	1×10^{-4}	0.0373	0.02948	1.71685	65,927	0
16,786	0.01999	0.00437	0.04009	33.9837	46.2077	2.6×10^{-4}	0.04308	0.03112	1.68307	64,630	0
16,795	0.01541	0.00657	0.08446	36.24566	42.80819	1.1×10^{-4}	0.09173	0.06432	1.99245	30,604	0
17,052	0.01709	0.00504	0.0862	35.34468	43.95916	1.5×10^{-4}	0.08851	0.07321	1.88664	72,447	0
17,453	0.01708	0.00511	0.04989	35.34928	45.99127	1.7×10^{-4}	0.05332	0.04121	1.91945	73,707	0
18,177	0.00739	0.00191	0.0275	42.62571	50.28831	3×10^{-5}	0.03076	0.01926	0.94492	14,514	0
18,184	0.01355	0.00624	0.05475	37.36037	46.02032	9×10^{-5}	0.05438	0.04594	1.78216	68,435	0
19,088	0.02979	0.00376	0.10087	30.51834	39.9005	4.3×10^{-4}	0.09544	0.08154	1.53292	51,201	0
19,090	0.01162	0.00238	0.04185	38.69753	46.9894	7×10^{-5}	0.04263	0.0349	1.0729	35,836	0
19,093	0.01427	0.00684	0.05196	36.9105	44.75635	1×10^{-4}	0.04553	0.04126	2.05638	68,685	0
19,140	0.0284	0.00351	0.06581	30.93286	42.31207	4.6×10^{-4}	0.06169	0.05297	1.42906	47,732	0
19,830	0.03905	0.00328	0.09518	28.16859	40.74797	8.4×10^{-4}	0.08891	0.07669	1.44337	50,375	0
Average	**0.01858**	**0.00489**	**0.06281**	**35.2884**	**44.7141**	$\mathbf{2.2 \times 10^{-4}}$	**0.06252**	**0.05123**	**1.69845**	**55,859.31**	**0**
SD	**0.00716**	**0.00141**	**0.02288**	**3.15266**	**2.49522**	$\mathbf{1.9 \times 10^{-4}}$	**0.02165**	**0.0195**	**0.30302**	**17,722.20**	**0**

Table 4 Performance evaluation measures on all records of BIDMC-CHF database of 1.5 mins duration

Record	PRD	PRD1024	PRDN	SNR	PSNR	KL-Divergence	WWPRD	WEDD	EC	Number of bits embedded	BER
chf01	0.027924	0.004362	0.05925	31.08056	41.35665	5.62×10^{-4}	0.131648	0.031651	1.818978	40,927	0
chf02	0.011651	0.00648	0.051554	38.67302	43.70894	6.75×10^{-5}	0.130074	0.027965	1.731378	38,956	0
chf03	0.007777	0.003306	0.050437	42.18368	45.84597	2.8×10^{-5}	0.126408	0.032519	1.105689	24,878	0
chf04	0.006491	0.00196	0.069772	43.75401	47.47474	2.18×10^{-5}	0.145595	0.043817	0.870756	19,592	0
chf05	0.031633	0.003519	0.072866	29.99733	42.69253	6.8×10^{-4}	0.135546	0.048742	1.466533	32,997	0
chf06	0.018946	0.003176	0.075675	34.44947	42.20649	2.16×10^{-4}	0.149713	0.051081	1.229778	27,670	0
chf07	0.010508	0.0037	0.065822	39.56957	42.87684	1.8×10^{-4}	0.130328	0.045028	1.200667	27,015	0
chf08	0.019149	0.005723	0.141944	34.35707	38.34644	2.32×10^{-5}	0.256312	0.107893	1.2332	27,747	0
chf09	0.003974	0.021287	0.024029	48.01442	55.22563	7.57×10^{-7}	0.047518	0.016544	1.426578	32,098	0
chf010	0.031633	0.003519	0.072866	29.99733	42.69253	6.8×10^{-4}	0.135546	0.048742	1.466533	32,997	0
chf011	0.004394	0.016415	0.016563	47.14332	52.14213	3.9×10^{-4}	0.034065	0.009921	1.4008	31,518	0
chf012	0.024757	0.004521	0.094785	32.12618	37.71978	4.4×10^{-4}	0.247582	0.056191	0.806667	18,150	0
chf013	0.050658	0.018336	0.226901	25.907	35.09532	1.47×10^{-3}	0.516157	0.102876	1.770578	39,838	0
chf014	0.012261	0.009155	0.071074	38.22917	42.84321	6.73×10^{-5}	0.172836	0.038123	2.282	51,345	0
chf015	0.00416	0.008493	0.01178	47.6096	52.3941	1.55×10^{-5}	0.03399	0.00426	1.0035	22,580	0
Average	**0.017728**	**0.007597**	**0.073688**	**37.53945**	**44.17475**	**0.000337**	**0.159555**	**0.044357**	**1.387576**	**31,220.53**	**0**
SD	**0.01297**	**0.005925**	**0.051295**	**6.876125**	**5.445474**	**0.000382**	**0.113597**	**0.028121**	**0.381257**	**8578.206**	**0**

Table 5 Performance evaluation measures on self-recorded database of 20 subject each of 5 mins duration

Record	PRD	PRD1024	PRDN	SNR	PSNR	KL-Divergence	WWPRD	WEDD	EC	Number of bits embedded	BER
1	0.008784	0.011388	0.033573	41.12579	50.46073	3.6×10^{-5}	0.118083	0.020506	2.050653	308,418	0
2	0.010727	0.006656	0.01746	39.39079	53.09244	1.04×10^{-4}	0.060179	0.011358	2.074147	311,122	0
3	0.010243	0.009059	0.030385	39.79149	49.78893	5.55×10^{-5}	0.097453	0.017543	2.17436	326,154	0
4	0.006749	0.008628	0.012104	43.4154	56.5927	1.93×10^{-5}	0.014947	0.008434	1.96036	294,054	0
5	0.008567	0.012786	0.02099	41.34331	52.31362	3.32×10^{-5}	0.064176	0.012383	2.27716	341,574	0
6	0.008712	0.012634	0.028422	41.19791	50.77462	2.82×10^{-5}	0.095453	0.016372	2.091827	313,774	0
7	0.00857	0.013592	0.037659	41.34024	48.655	3.22×10^{-5}	0.090499	0.020785	2.101213	315,182	0
8	0.008912	0.011846	0.027001	41.00076	51.05343	1.45×10^{-5}	0.068798	0.015525	2.142133	321,320	0
9	0.008655	0.010419	0.024614	41.25439	50.50484	4.01×10^{-5}	0.070765	0.016024	2.029607	304,441	0
10	0.00488	0.011657	0.012255	46.23152	57.9593	1.05×10^{-5}	0.025193	0.007018	2.162	324,300	0
11	0.008237	0.011098	0.021119	41.68442	52.15811	3.56×10^{-5}	0.034766	0.012689	2.051387	307,708	0
12	0.007983	0.006383	0.011551	41.95719	56.14813	1.38×10^{-5}	0.037372	0.007617	1.952287	292,843	0
13	0.010965	0.009001	0.030672	39.79652	49.78472	5.51×10^{-5}	0.097574	0.017236	2.17536	326,174	0
14	0.014085	0.00674	0.030851	37.0251	49.55885	5.84×10^{-5}	0.096389	0.020827	2.184207	327,631	0
15	0.005717	0.010469	0.053612	44.85674	51.04958	1.44×10^{-5}	0.078621	0.043037	0.896213	134,432	0
16	0.008455	0.010209	0.019189	41.45755	53.16097	7.16×10^{-5}	0.034098	0.012793	2.128933	319,340	0
17	0.008711	0.007044	0.014599	41.19909	54.53414	7.46×10^{-5}	0.050314	0.009271	1.955087	293,263	0
18	0.0057	0.014362	0.015629	44.88298	56.19292	1.68×10^{-5}	0.024079	0.009498	2.019307	302,896	0
19	0.010426	0.009521	0.035041	39.6376	48.8887	6.08×10^{-5}	0.055698	0.023373	2.203413	330,512	0
20	0.007582	0.015658	0.035792	42.40461	49.36322	5.35×10^{-5}	0.103099	0.022375	2.07856	311,784	0
Average	**8.63×10^{-3}**	**0.01045**	**0.025626**	**41.54967**	**52.10175**	**4.15×10^{-5}**	**0.065878**	**0.016233**	**1.957**	**305,346.1**	**0**
SD	**1.95×10^{-3}**	**0.00250**	**0.01023**	**2.00269**	**2.68821**	**2.37×10^{-5}**	**0.09185**	**0.00770**	**0.424**	**40,252.3**	**0**

Table 6 Average of all the performance metrics when measured on different durations of MIT-BIH arrhythmia databases

Duration	PRD	PRD 1024	PRDN	SNR	PSNR	KL-Divergence	WWPRD	WEDD	EC	Number of bits embedded	BER
5 mins	4.32×10^{-3}	0.0452	0.0669	48.278	51.515	9.42×10^{-6}	0.1528	0.0429	1.5869	171,390.5	0
10 mins	4.37×10^{-3}	0.0457	0.0672	48.236	51.223	9.86×10^{-6}	0.1539	0.0427	1.5832	341,613.3	0
15mins	4.37×10^{-3}	0.0456	0.0669	47.914	50.854	9.44×10^{-6}	0.1476	0.0427	1.5419	498,988	0
20mins	4.12×10^{-3}	0.0412	0.0653	47.878	50.067	9.43×10^{-6}	0.1409	0.0438	1.5632	675,302.1	0
25 mins	4.09×10^{-3}	0.041	0.06	48.223	50.984	9.85×10^{-6}	0.1532	0.0466	1.5717	848,718	0
30mins	4.32×10^{-3}	0.0447	0.0661	48.866	51.065	9.77×10^{-6}	0.154	0.0423	1.5734	1,019,536.2	0

WWPRD, WEDD and EC when measured for ECG signal of (i) short duration (5 mins) are 4.32×10^{-3}, 51.515, 9.42×10^{-6}, 0.152, 0.0429 and 1.5869 (ii) medium duration (20 mins) are 4.12×10^{-3}, 50.06, 9.43×10^{-6}, 0.1409, 0.0438 and 1.5632 (iii) long duration (30mins) are 4.32×10^{3}, 51.065, 9.77×10^{-6}, 0.154, 0.0423 and 1.573 respectively. It has been observed that the performance is nearly same for ECG signals of all durations which shows that the increase in length of ECG signal increases the number of bits embedded in the signal while the impact is minimal on other parameters. Based on the amount of secret data to be embedded, the minimum length of the ECG signal required can be decided in advance.

4.2 Impact of embedding on ECG signal with unique approaches

The proposed approach applies ECG feature specific steganography techniques on clinically separated QRS and non-QRS region based ECG blocks, possessing different embedding capacities. Table 7 displays the number of bits embedded in individual blocks of all 48 records of MIT-BIH arrhythmia database of 5 min duration when 2-bits are embedded in each coefficient obtained in regions θ'_{qrs1} and θ'_{qrs2} using IWT-mLSB approach and embedding multiple secret bits in all the possible ECG sample pairs obtained in θ'_{nqrs} region using PI-PVD approach. The average number of bits embedded in blocks $\theta'_{qrs1,}$ θ'_{nqrs} and θ'_{qrs2} are 3448.5, 118,884.6 and 49,057.42 respectively with average total bits embedded in the complete signals are 171,390.5. The influence of applying integrated approaches on the ECG signal is demonstrated in Fig. 7. The amplitudes of original and stego-ECG of record 100 after embedding 2-LSB bits in approximate coefficients of regions θ'_{qrs1} and θ'_{qrs2} and embedding multiple bits in all possible ECG sample pairs in region θ'_{nqrs} of 2D ECG image are analysed. It has been found that IWT-LSB approach efficaciously hides the secret bits with negligible distortion, however embedding in non-QRS region through PI-PVD technique improves the EC to manifolds. To further extend this analysis, the performance evaluation metrics are computed for variable embedding techniques. For this, the number of LSB bits embedded in QRS regions (θ'_{qrs1} and θ'_{qrs2}) with IWT-mLSB approach and the percentage of possible ECG pairs selected to embed secret bits in non-QRS region (θ'_{nqrs}) are varied. The bar graphs in Fig. 8 displays the amount of variation occured in EC, number of bits embedded, PRD, PSNR, KL-Divergence, WWPRD and WEDD when LSB bits of approximate coefficients in blocks θ'_{qrs1} and θ'_{qrs2} vary as 1-bit, 2-bits, 3-bits and 4-bits and the percentage of possible ECG sample pairs selected to embed secret bits in θ'_{nqrs} block vary from 25% to 100% of possible sample pairs with an increment of 25%. It is found that increase in percentage of embedding in non-QRS region has huge impact on the embedding capacity and other parameters also.

4.3 HRV analysis of original and stego-ECG

HRV is an important parameter that provides meaningful information about the cardiovascular system [41]. The impact of embedding the secret information on the HRV is analysed in terms of time domain (standard deviation of NN-interval (SDNN), standard deviation of the averages NN interval for 5mins segment (SDANN), root mean square of successive RR-interval differences (RMSSD), NN50 and percentage of successive RR intervals that differ by more than 50 ms (pNN50) and non-linear measurements (SD1, SD2 and SD1/SD2) [18, 35]. Table 8 shows the aggregated time scale parameters when measured on all the 48 original and stego-ECG records of MIT-BIH arrhythmia database. The percentage error is calculated as the

Table 7 Amount of bits embedded in individual blocks of all 48 records of MIT-BIH arrhythmia database of 5 mins

Record	Total bits embedded	Bits embedded in block θ'_{qrs1}	Bits embedded in block θ'_{nqrs}	Bits embedded in block θ'_{qrs2}	Record	Total bits embedded	Bits embedded in block θ'_{qrs1}	Bits embedded in block θ'_{nqrs}	Bits embedded in block θ'_{qrs2}
100	173,946	3330	126,768	43,848	202	177,472	2376	122,700	52,396
101	104,414	3078	19,992	81,344	203	93,602	4428	3144	86,030
102	162,556	3294	103,248	56,014	205	118,786	4086	50,232	64,468
103	224,442	3186	198,318	22,938	207	97,340	3168	0	94,172
104	96,326	3366	0	92,960	208	165,718	4554	117,828	43,336
105	157,240	3744	98,004	55,492	209	154,384	4374	104,100	45,910
106	155,572	2970	93,192	59,410	210	132,610	3978	61,938	66,694
107	214,884	3168	183,414	28,302	212	201,448	4158	172,626	24,664
108	94,814	3996	0	90,818	213	181,150	4950	142,338	33,862
109	193,008	3888	161,250	27,870	214	150,104	3420	82,536	64,148
111	227,344	3114	203,994	20,236	215	134,070	5094	74,616	54,360
112	240,100	3852	223,536	12,712	217	177,724	3258	127,242	47,224
113	167,712	2592	108,660	56,460	219	171,248	3420	116,262	51,566
114	100,454	2394	3450	94,610	220	188,672	3186	140,748	44,738
115	232,820	2844	208,680	21,296	221	157,548	3654	99,222	54,672
116	178,624	3564	127,398	47,662	222	210,814	3294	184,170	23,350
117	269,440	2250	256,920	10,270	223	156,350	3600	93,282	59,468
118	200,460	3258	161,058	36,144	228	116,512	3168	33,594	79,750
119	175,938	2934	120,816	52,188	230	206,186	3564	174,792	27,830
121	251,692	2718	235,476	13,498	231	146,478	2628	76,128	67,722
122	227,688	3798	202,110	21,780	232	177,872	2646	131,190	44,036
123	236,568	2232	207,282	27,054	233	120,018	4662	48,762	66,594
124	230,906	2268	200,448	28,190	234	227,350	4158	209,286	13,906
200	98,690	3906	9432	85,352	**Average**	**171,390.5**	**3448.5**	**118,884.6**	**49,057.42**
201	147,652	3960	86,280	57,412	**SD**	**177,472**	**2376**	**122,700**	**52,396**

No embedding in θ'_{nqrs} regions in ECG records 104, 108 and 207 implies that the shortest beat in the signal is so small that the regions θ'_{qrs1} and θ'_{qrs2} overlaps without leaving any sample in θ'_{nqrs} region.

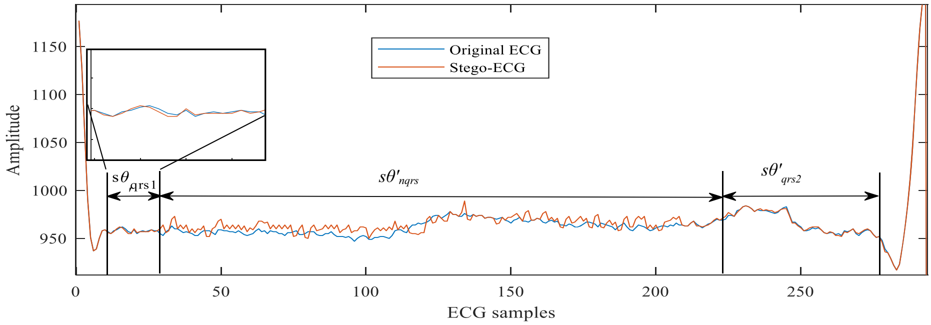


Fig. 7 Impact of embedding secret bits in blocks θ'_{qrs1} and θ'_{nqrs} of row 2 of original and stego 2D ECG using IWT-LSB and PI-PVD approaches respectively

difference between the parameters obtained from the original and stego-ECG divided by the original average and is given as:

$$Error(\%) = \frac{original-stego}{original} \text{x } 100$$

As observed in Table 8, the amount of error caused in the ECG signal due to embedding is inconsequential to affect the diagnosis [18].

4.4 Security analysis

4.4.1 Key space

The length of the key is an important parameter that makes the system invulnerable to stego attacks. Therefore in the proposed steganography approach, the key length is kept sufficiently large to curtail the risk of illicit access of sensitive information by intruders. The key consists of the three sets of initial parameters (x_{01}, y_{01}, x_{02}, y_{02}, x_{03}, y_{03}) used to generate three chaotic maps used in the steganography technique, length of confidential information L_c and values of shifting factors (r_1 and r_2) used in regions θ'_{qrs1} and θ'_{qrs2}. The format of key is shown in Fig. 9. If the initial parameters are set to precision of 14 decimals then as per IEEE 754 standard of converting decimal numbers into binary [30], the length of the key is calculated as $2^{64*6+16+3*2} = 2^{406}$ bits which is sufficiently large to avoid any malicious attack.

4.4.2 Key sensitivity

Key sensitivity is another security parameter that measures the strength of the key. It shows the amount of variation occur in the secret information when extracted with the wrong key. The key space in the proposed algorithm consists of initial and control parameters of three chaotic maps, length of the confidential information and shifting factors. The chaotic maps are so sensitive to initial conditions that even a small change at 14th decimal point alter the whole chaotic sequence. It results in wrong selection of embedded locations at the receiver and hence extraction of erroneous secret information. It is demonstrated in Fig. 10 that extraction with correct key results in correct information retrieval whereas a small change in value of y_{01} at 14th decimal place results in

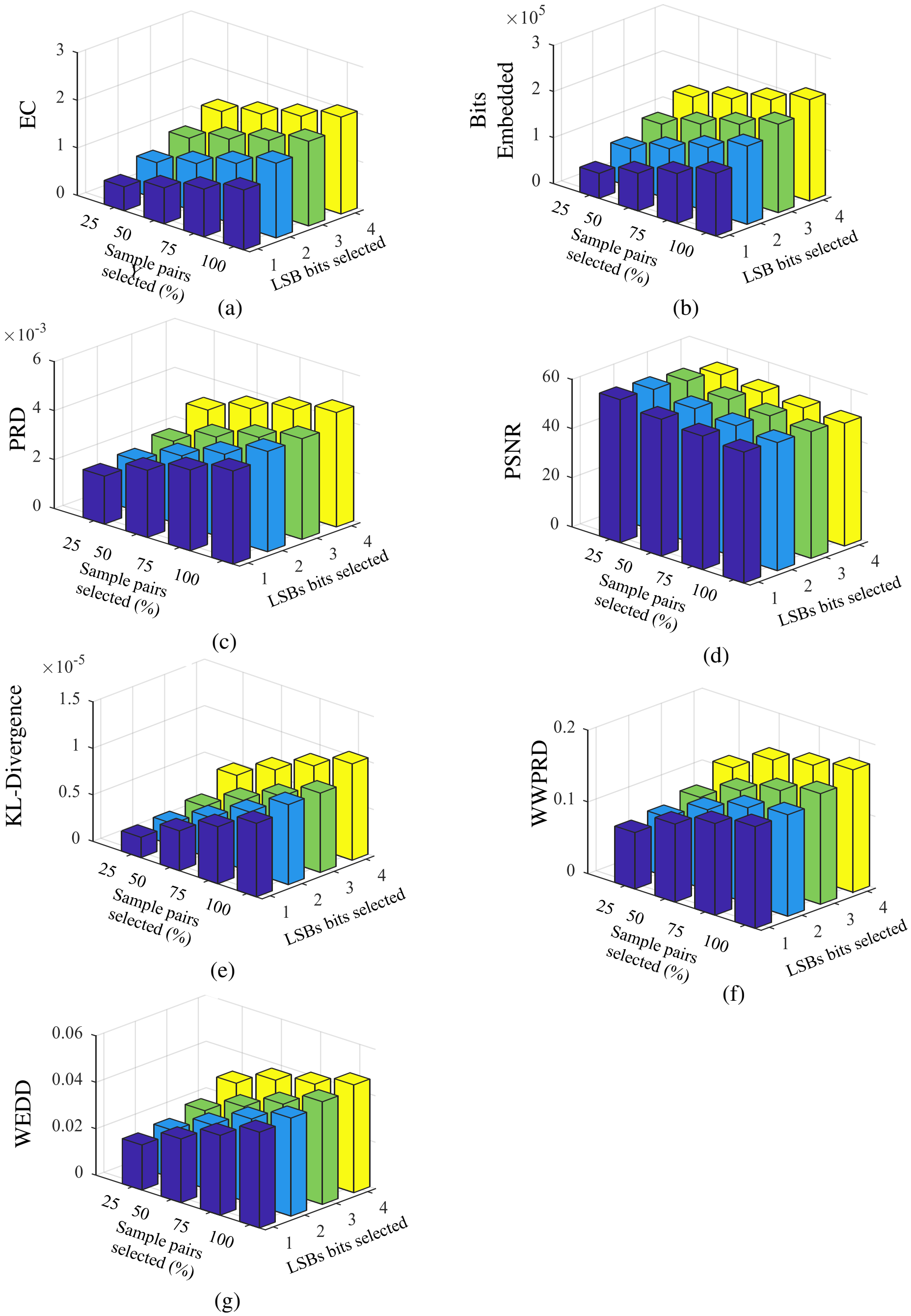


Fig. 8 Bar graph plots of (**a**) EC (**b**) Bits Embedded (**c**) PRD (**d**) PSNR (**e**) KL-Divergence (**f**) WWPRD (**g**) WEDD with varying amount of selected sample pair in θ'_{nqrs} region and number of bits selected for embedding in θ'_{qrs1} and θ'_{qrs2} regions of all the 48 records of MIT-BIH arrhythmia database of 5 mins

Table 8 Average of time scale HRV parameters and percentage error over all the 48 ECG records of MIT-BIH arrhythmia database of 5mins duration

	Parameters	Original ECG	Stego-ECG	Error (%)
Time Domain Measurement	SDNN	39.58791	39.75903	0.4323
	SDANN	1.32×10^{-12}	1.28×10^{-12}	3.03×10^{-14}
	RMSSD	55.34523	55.35972	2.618×10^{-4}
	NN50	67.44444	67.31111	1.97×10^{-3}
	pNN50	0.169317	0.168926	2.362×10^{-3}
Non-linear measurement	SD1	38.54997	38.8162	6.906×10^{-3}
	SD2	38.20965	38.21682	1.876×10^{-4}
	SD1 /SD2	0.912464	0.909939	2.76×10^{-3}

extraction of corrupted information. However the impact of varying the key is insignificant on the stego ECG.

For example as per the key space, structure the correct (Y_1) and incorrect keys (Y_2) are

Correct key Y_1:

{0.897655762990, 3.99534613560**1**, 0.933453564978, 3.886954532619, 0.994357334262, 3.973256778521, 5000, 5, 5}

Incorrect key Y_2:

{0.897655762990, 3.99534613560**8**, 0.933453564978, 3.886954532619, 0.994357334262, 3.973256778521, 5000, 5, 5}

4.5 Comparative analysis of the proposed work

The efficacy of the proposed work is evaluated by comparing its results with the state of the art techniques. In comparison to the outcomes shown by the currently published papers, the proposed technique surpasses in terms of payload capacity and PSNR at very low PRD, KL-Divergence, WWPRD and WEDD. The figures in Table 9 evidently show that the PRD and KL-Divergence of 4.2×10^{-3} and 8.95×10^{-6} respectively achieved in proposed method are too low at payload capacity of 11.2 k bits as compared to PRD and KL-Divergence of 5.9×10^{-3} and 0.15 respectively achieved in [12] at payload capacity of 2800 bits. The PRD, KL-Divergence and PSNR computed in [13] are 0.0132, 0.144 and 43.44 respectively for 4016 bits embedded as compared to 0.017, 2.28×10^{-4} and 44.85 respectively after embedding 28.6 k bits by proposed algorithm. Besides, the relative amount of error occurred in proposed method is trivial as compared to the techniques discussed in [27, 28] for considerable difference in their ECs. Therefore, from the comprehensive analysis it is apparent that the proposed algorithm is much competent as compared to the recently published state of the art techniques.

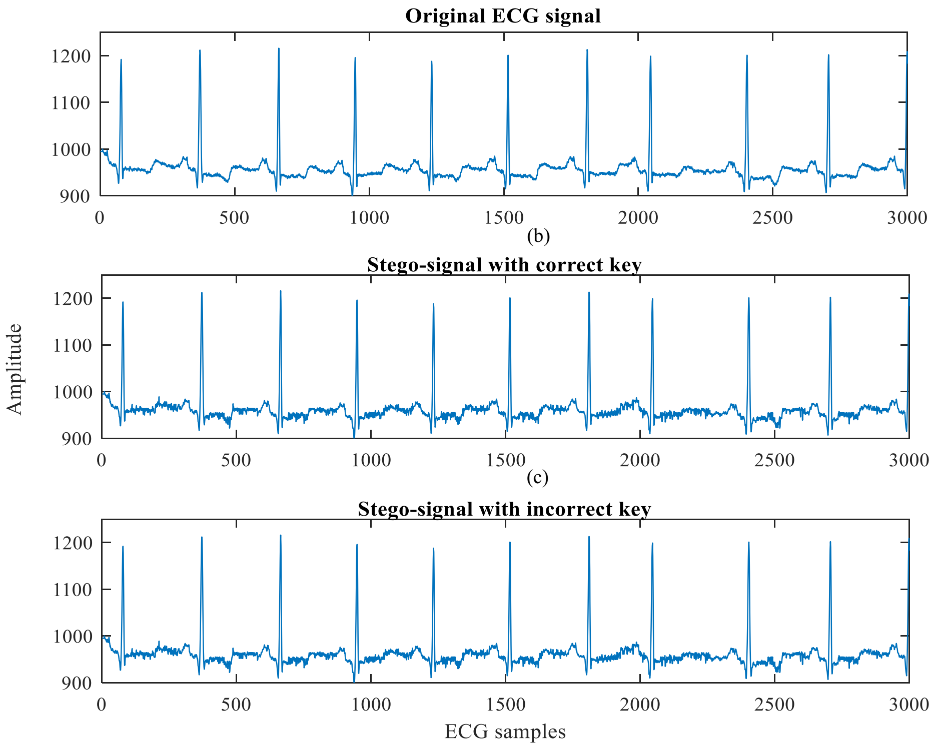
5 Conclusion

In comparison to the existing techniques in which single common approach of steganography is applied over the complete ECG signal, a feature specific hybrid approach for data hiding in

x_{01}	y_{01}	x_{02}	y_{02}	x_{03}	y_{03}	L_c	r_1	r_2
(64 bits)	(64 bits)	(64 bits)	(64 bits)	(64 bits)	(64 bits)	(16 bits)	(3 bits)	(3 bits)

Fig. 9 Structure of key space

(a)



(d)

Fig. 10 (**a**) Extraction of patient's confidential information with correct and incorrect keys (**b**) Original ECG signal (**c**) stego-signal recovered with correct key (**d**) stego-signal recovered with incorrect key

2D ECG is proposed. An integration of IWT and modified LSB technique is applied to embed information in the pivotal QRS regions whereas PI-PVD method is used to incorporate secret information in the non-QRS region. The blend of spatial and transform domain approaches used in the proposed algorithm significantly outperforms other ECG steganography techniques by achieving low PRD, PRD1024, PRDN,KL-Divergence, WWPRD and WEDD at high EC. An average PRD, PRD1024, PRDN, SNR, PSNR, KL-Divergence, WWPRD and WEDD evaluated on typically 5mins duration of ECG signal of MIT-BIH arrhythmia database are 4.32×10^{-3}, 0.0452, 0.066, 48.27, 51.51, 9.42×10^{-6}, 0.152 and 0.042 respectively. The number of bits embedded and EC achieved for the same set of data are 1.58 and 171,390.5 respectively at zero BER which is exorbitantly high as compared to the techniques reported in literature. Further, the efficiency of the proposed algorithm is measured on both normal (MIT-BIH NSR) and abnormal (BIDMC-CHF) ECG databases as well as on self-recorded data of 20 subjects. In addition to statistical and clinical parameters, the impact of steganography is measured on HRV in which both time domain and non-linear parameters are analysed. The results show negligible error in HRVs of original and stego ECG. The performance is studied for different durations with variable number of bits embedded in QRS regions at varying percentage of data embedded in the non QRS regions. The performance is evaluated with maximum QRS complex duration of 0.15 s. The limitation of the proposed technique is that if the duration of any QRS complex exceeds this value then that QRS complex has to be

Table 9 Performance comparison of the proposed technique with other state-of-the-art techniques

			Performance parameters evaluated using Existing/Proposed Techniques					
Sr. No	Existing work	Database used	Payload (bits)	PRD	KL-Divergence	PSNR	WWPRD	WEDD
1.	DWT + SVD (2014) [12]	MIT-BIH arrhythmia (76,800 samples)	2800/ **11.2 k**	5.9×10^{-3}/$\mathbf{4.2 \times 10^{-3}}$	0.15/ $\mathbf{8.95 \times 10^{-6}}$	50.4/**51.9**	–	–
2.	Curvelet Transform (2015) [13]	MIT-BIH NSR	4016/ **28.6 k**	0.0132/**0.017**	0.144/$\mathbf{2.28 \times 10^{-4}}$	43.4/ **44.8**	–	–
3.	DWT + SVD + CACO (2016) [14]	MIT-BIH NSR (at varying payload size)	0.89 k 1.3 k 1.77 k 2.2 k 2.67 k 3.07 k	1.8×10^{-3} /$\mathbf{6.1 \times 10^{-4}}$ 4×10^{-3}/ $\mathbf{1.8 \times 10^{-3}}$ 7×10^{-3}/ $\mathbf{2.2 \times 10^{-3}}$ 0.015/$\mathbf{2.5 \times 10^{-3}}$ 0.03/ $\mathbf{2.8 \times 10^{-3}}$ 0.06/ $\mathbf{2.9 \times 10^{-3}}$	0.02/$\mathbf{2.89 \times 10^{-5}}$ 0.1/$\mathbf{4.56 \times 10^{-5}}$ 0.21/ $\mathbf{6.08 \times 10^{-5}}$ 0.68/$\mathbf{7.67 \times 10^{-5}}$ 2.03/ $\mathbf{9.34 \times 10^{-5}}$ 2.04/$\mathbf{1.05 \times 10^{-4}}$	62.8/**55.7** 54.7/**53.5** 51.1/**52.3** 45.1/**51.2** 39.5/**50.3** 34.4/**49.8**	–	–
4.	CMSaVD (2017) [27]	MIT-BIH arrhythmia (20 mins)	21 k/ **675.302 k**	0.26/ $\mathbf{4.1 \times 10^{-3}}$	3.3×10^{-6} /$\mathbf{9.4 \times 10^{-6}}$	55.49/ **50.06**	0.10/ **0.14**	0.02/ **0.043**
5.	Data embedding + encryption (2019) [28]	MIT-BIH arrhythmia (30 mins)	2.4 k/ **1019.536 k**	0.05/$\mathbf{4.32 \times 10^{-3}}$	–	70.58/ **51.065**	1.94×10^{-2} /**0.15**	4.01×10^{-3} /**0.0423**

excluded from embedding to avoid error. The effect of excluding the QRS region is however minimal on the overall performance of the proposed technique. To ensure the security of the embedded information, chaotic maps are incorporated that provides sufficiently large key space and high key sensitivity. The comprehensive analysis of the proposed approach of feature based data hiding in ECG signal yields excellent results and recommended as a proficient and authentic approach for ECG steganography. The program code can be shared with the reader on request to the corresponding author.

Funding This research work does not receive any grants from any funding agency.

Compliance with ethical standards

The ethical principles for medical research of World Medical Association (WMA's) Declaration of Helsinki have been followed for data acquisition.

Conflict of interest No conflict of interest

References

1. Al-Dmour H, Al-Ani A (2016) Quality optimized medical image information hiding algorithm that employs edge detection and data coding. Comput Methods Prog Biomed 127:24–43
2. Al-Fahoum AS (2006) Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure. IEEE Trans Inf Technol Biomed 10(1):182–191
3. Algeria-Barrero E, Algeria-Ezquerra E (2008). When to perform pre-operative ECG. European Society of Cardiology 7(13)
4. Berkaya SK, Uysal AK, Gunal ES, Ergin S, Gunal S, Gulmezoglu MB (2018) A survey on ECG analysis. Biomedical Signal Processing and Control 43:216–235
5. Calderbank AR, Daubechies I, Sweldens W (1998) Wavelet transform that maps integers to integers. Appl Comput Harmon Anal 5(3):332–369
6. Chou HH, Chen YJ, Shiau YC, Kuo TS (2006) An effective and efficient compression algorithm for ECG signals with irregular periods. IEEE Trans Biomed Eng 53(6):1198–1205
7. Daubechies I, Sweldens W (1998) Factoring wavelet transforms into lifting steps. J Fourier Anal Appl 4(3): 247–269
8. English A, Summers R, Lewis J, Coleman C (2015). Confidentiality, third-party billing & the health insurance claims process: implications for title X. Accessed on 11 November 2015
9. Hua Z, Zhou Y, Pun CM, Chen CLP (2015) 2D sine logistic modulation map for image encryption. Inf Sci 297:80–94
10. Hussain M, Wahab AWA, Idris YIB, Ho ATS, Jung KH (2018) Image steganography in spatial domain: a survey. Signal Process Image Commun 65:46–66
11. 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
12. Jero SE, Ramu P, Ramakrishnan S (2014) Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission. J Med Syst 38:132
13. Jero SE, Ramu P, Ramakrishnan S (2015) ECG steganography using curvelet transform. Biomedical Signal Processing and Control 22:161–169
14. Jero SE, Ramu P, Ramakrishnan S (2016) Imperceptibility—robustness tradeoff studies for ECG steganography using continuous ant colony optimization. Expert Syst Appl 49(1):123–135
15. Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. Computer 31:26–34
16. Kanan HR, Nazeri B (2014) A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst Appl 41(14):6123–6130
17. Kieu TD, Chang CC (2011) A steganographic scheme by fully exploiting modification directions. Expert Syst Appl 38(8):10648–10657
18. Kim KK, Lim YG, Kim JS, Park KS (2007) Effect of missing RR-interval data on heart rate variability analysis in the time domain. Physiol Meas 28(12):1485–1494

19. Kozat SS, Vlachos M, Lucchese C, Herle H, Yu PS (2009) Embedding and retrieving private metadata in electrocardiograms. J Med Syst 33(4):241–259
20. Liji CA, Indiradevi KP, Anish Babu KK (2016) Integer-to-integer wavelet transform based ECG steganography for securing patient confidential information. International Conference on Emerging Trends in Engineering, Science and Technology, Procedia Technology 24:1039–1047
21. Lin YK (2012) High capacity reversible data hiding scheme based upon discrete cosine transformation. Systems and Software 85(10):2395–2404
22. Manikandan MS, Dandapat S (2007) Wavelet energy based diagnostic distortion measure for ECG. Biomedical Signal Processing and Control 2(2):80–96
23. Martínez-González RF, Díaz-Méndez JA, Palacios-Luengas L, López-Hernández J, Vázquez-Medina R (2016) A steganographic method using bernoulli's chaotic maps. Comput Electr Eng 54:435–449
24. Nambakhsh MS, Ahmadian A, Zaidi H (2011) A contextual based double watermarking of PET images by patient ID and ECG signal. Comput Methods Prog Biomed 104:418–425
25. www.physionet.org/cgi-bin/atm/ATM accessed in November 2018.
26. Pan J, Tompkins WJ (1985) A real-time QRS detection algorithm. IEEE Trans Biomed Eng BME-32(3): 230–236
27. Pandey A, Saini BS, Singh B, Sood N (2017) An integrated approach using chaotic map & sample value difference method for electrocardiogram steganography and OFDM based secured patient information transmission. J Med Syst 41:187
28. Pandey A, Singh B, Saini BS, Sood N (2019) A novel fused coupled chaotic map based confidential data embedding- then–encryption of electrocardiogram signal. Biocybernetics and Biomedical Engineering 39(2):282–300
29. Parah SA, Ahad F, Sheikh JA, Bhat GM (2017) Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J Biomed Inform 66:214–230
30. Rajaram V (2016) IEEE standards for floating point numbers. Resonance 21(1):11–30
31. Reichel J, Menegaz G, Nadenau MJ, Kunt M (2001) Integer wavelet transform for embedded lossy to lossless image compression. IEEE Trans Image Process 10(3):383–392
32. Rubio ÓJ, Alesanco Á, García J (2013) Secure information embedding into 1D biomedical signals based on SPIHT. J Biomed Inform 46(4):653–664
33. Saini I, Singh D, Khosla A (2013) QRS detection using K-nearest neighbor algorithm (KNN) and evaluation on standard ECG databases. J Adv Res 4(4):331–344
34. Leo Schamroth. An introduction to electro cardiography, Wiley, 7th edition.
35. Shaffer F, Ginsberg JP (2017) An overview of heart rate variability metrics and norms. Front Public Health 5:258
36. Shen SY, Huang LH (2015) A data hiding scheme using pixel value differencing and improving exploiting modification directions. Computers & Security 48:131–141
37. Shiu HJ, Lin BS, Huang CH, Chiang PY, Lei CL (2017) Preserving privacy of online digital physiological signals using blind and reversible steganography. Comput Methods Prog Biomed 151:159–170
38. Singh B, Singh D, Jaryal AK, Deepak KK (2012) Ectopic beats in approximate entropy and sample entropy-based HRV assessment. Int J Syst Sci 43(5):884–893
39. Slimane ZEH, Naït-Ali A (2010) QRS complex detection using empirical mode decomposition. Digital Signal Processing 20(4):1221–1228
40. Soni N, Saini I, Singh B (2019) Morphologically robust chaotic map based approach to embed patient's confidential data securely in non-QRS regions of ECG signal. Australas Phys Eng Sci Med 42(1):111–135
41. Task force of the European society of cardiology and the North American society of pacing and electrophysiology (1996) Heart rate variability: standards of measurement, physiological interpretation and clinical use. Eur Heart J 17(3):354–381
42. The Personal Information Protection and Electronic Documents Act (PIPEDA), Office of the privacy Commissioner of Canada.
43. Trinder J, Kleiman J, Carrington M, Smith S, Breen S, Tan N, Kim Y (2001) Autonomic activity during human sleep as a function of time and sleep stage. J Sleep Res 10(4):253–264
44. Wang CM, Wu NI, Tsai CS, Hwang MS (2008) A high quality steganographic method with pixel-value differencing and modulus function. J Syst Softw 81(1):150–158
45. Yang C, Wang W (2016) Effective electrocardiogram steganography based on coefficient alignment. J Med Syst 40(3):1–15
46. Zhou Y, Bao L, Chen CLP (2014) A new 1D chaotic system for image encryption. Signal Process 97:172–182

Neetika Soni received her M.Tech Degree from Punjab Technical University, Punjab India in year 2008 and currently pursuing her PhD in Biomedical Signal Processing. She is working as an Assistant Professor in Department of Electronics and Communication Engineering, GNDU, Regional Campus, Jalandhar, Punjab, India. since 2004. Her areas of interest includes Biomedical Signal Processing and Embedded System Design.

Indu Saini received her B. Tech degree in Electronics and Communication Engineering from Guru Nanak Dev University, India, in 1994 and then obtained her M. Tech (by Research) and PhD degree in Electronics & Communication Engineering from Dr. B. R. Ambedkar National Institute of Technology Jalandhar, where she is also serving as Assistant Professor in Electronics & Communication Engineering Department since 2002. Her professional research interests are Very Large Scale Integration (VLSI) design, Biomedical Signal/Image Processing, and Machine Learning Algorithms.

Butta Singh received his Bachelor's degree in Electronics and Communication Engineering from Guru Nanak Dev Engineering College, Ludhiana, Punjab, India in 2002, Master's degree in Instrumentation and Control Engineering from Sant Longowal Institute of Engineering and Technology, Longowal, Sangrur, Punjab, India in 2005 and Ph.D. in Engineering from National Institute of Technology, Jalandhar, Punjab, India. He is serving as Assistant Professor in the Department of Electronics and Communication Engineering, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab, India. His professional research interests are in signal processing, in particular, applied to biomedical applications. He has published over 50 research articles in internationally reputed journals and conference proceedings.