Australasian Physical & Engineering Sciences in Medicine (2019) 42:111–135
https://doi.org/10.1007/s13246-018-00718-1

SCIENTIFIC PAPER

A morphologically robust chaotic map based approach to embed patient's confidential data securely in non-QRS regions of ECG signal

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

Received: 27 June 2018 / Accepted: 17 December 2018 / Published online: 7 January 2019

Abstract

In e-healthcare paradigm, the physiological signals along with patient's personal information need to be transmitted to remote healthcare centres. Before sharing this sensitive information over the unsecured channel, it is prerequisite to protect it from unauthorised access. The proposed method explores ECG signal as the cover signal to hide patient's personal information without disturbing its diagnostic features. Chaotic maps are used to randomly select the embedding locations in the non-QRS region while excluding the sensitive QRS region of ECG train. Optimum Location Selection algorithm has been designed to select the embedding locations in non-QRS embedding region. The proposed algorithm is thoroughly examined and the distortion is measured in terms of statistical parameters and clinical measures such as PRD, PRDN, PRD1024, PSNR, SNR, MSE, MAE, KL-Divergence, WWPRD and WEDD. The robustness of the algorithm is verified using the parameters such as key space and key sensitivity. The implementation has been extensively tested on all the 48 records of the standard MIT-BIH Arrhythmia database, abnormal databases [CU-VT, BIDMC-CHF and PTB (leads I, II and III)] and self-recorded data of 20 subjects. The algorithm yields average PRD, MSE, KL-Divergence, PSNR, WWPRD and WEDD of 4.7×10^{-3}, 1.13×10^{-5}, 1.29×10^{-5}, 50.28, 0.15 and 0.04 at an average maximum EC of 0.45(96876 bits) on MIT-BIH Arrhythmia database and 0.016, 3.38×10^{-5}, 1.8×10^{-4}, 46.03, 0.13 and 0.03 respectively at an average maximum EC of 0.47 (102571 bits) on self-recorded data which clearly reveals the competency of the proposed algorithm in comparison with the other state of the art ECG steganography approaches.

Keywords ECG steganography · Chaotic maps · Embedding capacity (EC) · Key sensitivity · Wavelet based weighted percentage root mean square difference (WWPRD) · Wavelet energy based diagnostic distortion (WEDD)

Introduction

The advancement in technology has helped the medical industry to reduce the barriers of remote healthcare monitoring and provides assistance to home bound patients [1, 2]. These e-healthcare solutions are more reliable in emergency services as patients' medical information which includes biological signals such as electrocardiogram (ECG) or electroencephalogram (EEG) can be immediately sent to the doctors and appropriate actions can be taken without any delay. Along with the signal it is requisite to transmit additional information namely the patient's personal details, his/her clinical reports and medical history for the purpose of identification and early diagnosis. But transmitting this vital information over the insecure channel is risky. As per the U.S. Health Insurance Portability and Accountability Act (HIPAA) privacy rule and the Affordable Care Act (ACA) also, it is mandatory to protect individuals' confidential medical information [3]. Therefore the prime concern in e-healthcare systems is to protect patient's sensitive information from unauthorized access. There are different ways for hiding this information viz. cryptography, steganography, watermarking [4, 5], but steganography is preferred in which the secret information is interleaved in the cover signal without making any distinguishable change in it so that any doctor can diagnose the stego-signal but only an authorized administrative personnel can extract the hidden secret

✉ Neetika Soni
neetikabhalla@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

information [6]. In this paper, ECG signal has been used as a cover media and secret information includes patient's personal details (e.g., his age, DOB, sex, identity number, phone number, thumb impression), pathological reports (e.g., blood pressure, glucose level, body temperature) and his medical history (medication, allergies etc). Though steganography causes irreversible degradation in the cover signal but the main aim in ECG steganography is to retain the diagnostic features intact despite of deterioration.

Related work

Although, tremendous research has been done in field of steganography, but very few researchers addressed steganography in ECG signals. In [7, 8] medical images such as angiogram, positron emission tomography (PET) and X-ray images were used to interleave the patient's details. Ibaida et al. [9] suggested data hiding in ECG signal using spatial domain where secret bits were embedded in ECG samples according to some special range of numbers. The results show that for embedding 32 secret bits, the number of possible locations were 2.1475×10^9 with percentage residual difference (PRD) of 0.0247% and EC of 2500 bits in 2500 ECG samples. Later in 2013, same author proposed ECG steganography in transform domain [10] using Haar wavelet and the encrypted secret bits were embedded in the subbands of wavelet coefficients. The average PRD for Normal, Ventricular Tachycardia and Ventricular Fibrillation ECG segments of 10 s comes out to be 0.47129, 0.27599 and 0.56718 respectively with data size of 2.4 kb. The method required specific transmitter/receiver pairs to decrypt the secret information which resulted in additional hardware complexity. In [11], Chen et al. opted three transform domains i.e., discrete Fourier transform (DFT), discrete cosine transform (DCT) and discrete wavelet transform (DWT) to implement the quantized ECG based watermarking technique. Further, a group of researchers developed 2D based ECG steganography techniques using different transforms [12–14]. Jero et al. applied DWT and singular value deposition (SVD) approach to decompose and to embed the secret information in a selected subband respectively. The method was applied on 76,800 ECG samples from Massachusetts Institute of Technology-Beth Israel Hospital (MIT-BIH) Arrhythmia database with payload of 350 bytes achieved PRD, peak signal to noise ratio (PSNR) and Kullback Leibler Divergence (KL-Divergence) of 0.0059, 50.44 and 0.15 respectively at zero bit error rate (BER) [12]. The method has very low embedding capacity (EC). Later in 2015 [13], the same research group presented discrete curvelet transform based ECG steganography using coefficient identification. The method achieved PSNR 43.44dB, PRD 0.0132, KL-Divergence 0.1448 and mean square error (MSE) 2.94 with zero BER at payload of 502 bytes when experimented on 128 trains from normal sinus rhythm (NSR) database. In another work [14], they proposed continuous ant colony optimization (CACO) based ECG steganography technique to identify multiple scaling factors that improves the trade-off between PSNR and robustness. Yang and Wang [15] proposed two methods of data hiding in ECG signal based on coefficient alignment. The Lossy method has average signal to noise ratio (SNR) of 56.34 dB and payload of 7.5 kb with bundle size equal to 4 whereas the reversible data hiding method has average SNR and mean absolute error (MAE) of 42.27 dB and 1.84 with payload of 14.7 kb for lead I and SNR and MAE of 46.31 dB and 1.49 respectively with payload of 14.5 kb for lead II. The SNR and MAE calculated is without taking into account the side information. Pandey et al. [16] presented integrated approach using chaotic maps and sample value differencing where difference between the sample values was used to hide the secret bits and chaotic maps were used to determine the embedding locations. The method achieved PSNR of 55.49 at PRD and wavelet based weighted percentage root mean square difference (WWPRD) of 0.26 and 0.10 respectively for ECG signal of 20 min.

The key trait of steganography is trade-off amongst signal degradation, EC and security. The above discussed techniques are marked with progress either in EC or in lowering the signal degradation that also lacks in the security features. The proposed method is designed to conciliate among all the attributes of steganography. P, QRS, T and U waves are key features of an ECG signal [17, 18]. The above mentioned approaches exploits the whole ECG (QRS as well as non-QRS region) to embed the secret information to increase the EC but exploiting the QRS region for secret data embedding degrade the clinical features and increases distortion. Therefore, in this work, the pivotal QRS region is completely excluded from embedding the secret information and clinically insignificant non-QRS region is explored to embed the secret information. The excellence of the algorithm is that albeit embedding secret information in the non-QRS region its impact is minimum on P and T waves, thus reduces the risk of diagnostic error. Further, to strengthen the attributes of imperceptibility and security, mathematical tools such as chaotic maps are involved. The chaotic maps are the non-linear functions that produce random signals having features of ergodicity, unpredictability and sensitivity to initial conditions and control parameters [19–23] which makes them suitable in the design of steganographic algorithms. In this paper, a new method of ECG steganography is proposed that assures secure embedding of patient's confidential data along with the patient's physiological signal. The proposed technique works in the spatial domain where random embedding locations are identified in non-QRS region by thresholding the R-peaks. The threshold values are also inserted in the ECG signal as side information along with the secret bits to extract the correct embedding locations at the receiver. Despite adding side information in embedded ECG, the technique affirms negligible diagnostic distortion. The chaotic maps are used to randomly select the locations and amplitudes for embedding the secret bits which intensifies the security of the confidential information.

The rest of the paper is organized as follows: "Preliminaries" section discusses the preliminaries that includes the chaotic properties of logistic, sine and coupled chaotic maps and the ECG database used for analysis of proposed technique. "Proposed methodology" section describes the proposed methodology of ECG steganography. Experimental results and embedding performances are analysed and evaluated in "Results" section and finally discussion and conclusion is mentioned in "Discussion and conclusion" section.

Preliminaries

Chaotic maps

Chaotic maps can be classified into two categories: one-dimensional and multi-dimensional. Multi-dimensional chaotic maps have complex structures, more hardware/software requirements and more computational complexity [19]. Hence in this paper, one-dimensional chaotic maps are used that have simple structures and are easy to implement. In the subsequent section, 1D logistic, sine and combined logistic-sine (CLS) maps are briefly discussed and their behaviours are analysed with the help of bifurcation diagrams (to verify their chaotic range) and statistical tests (to check the amount of randomness).

Logistic map

The mathematical equation of logistic map is:

$$f_{\text{logistic}}(x_1, r_o, l): \quad x_{n+1} = r_o x_n \left(1 - x_n\right); \quad n = 1, 2, 3, \ldots l \tag{1}$$

where r_o is the control parameter, x_1 is its initial value [19–21] and l is the length of the sequence. The bifurcation diagram of logistic map given in Fig. 1a can be expressed as

$0 \le r_o < 1;$ insignificant,

$1 \le r_o < 3;$ non-trivial fixed point,

$3 \le r_o < 3.57;$ periodic doubling,

$3.57 \le r_o \ge 4;$ pure chaotic behaviour.

Sine map

The mathematical equation for sine map of length l is [20]

$$f_{\sin e}(x_1, r_o, l): \quad x_{n+1} = r_o \sin\left(\frac{\pi x_n}{4}\right) \tag{2}$$

The sine map shows similar behaviour as logistic map with chaotic range varies between [3.5, 4] as shown in Fig. 1b. Both these seed maps have a drawback of limited chaotic range. To overcome this limitation, these maps are combined together to generate coupled chaotic sequence [19, 23] that exhibits excellent chaotic behaviour over the entire range of r_o within (0, 4].

Combined logistic-sine (CLS) map

The mathematical expression for *CLS* map is:

$$CLS(x_1, r_o, l): \quad x_{n+1} = \left(r_o x_n \left(1 - x_n\right) + \left(4 - r_o\right) \sin\left(\frac{\pi x_n}{4}\right)\right) \bmod 1 \tag{3}$$

The bifurcation diagram in Fig. 1c illustrates uniform chaotic distribution over the entire range of r_o.

$0 \le r_o < 4;$ pure chaotic behaviour

Beside bifurcation diagrams, the maps are also examined using the National Institute of Standards and Testing (NIST)

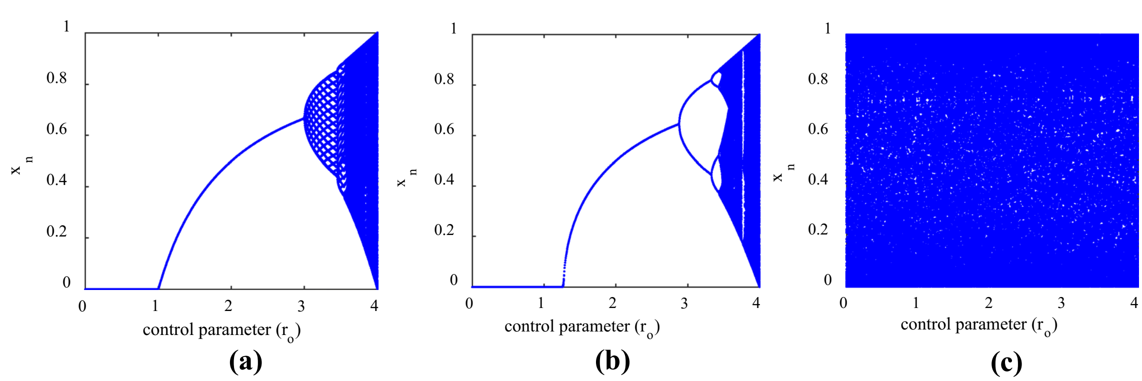


Fig. 1 Bifurcation diagram of **a** logistic map, **b** sine map, **c** CLS map

Statistical Test Suite to quantify the amount of randomness. These tests help to determine whether the sequences exhibit all those attributes that a random sequence must possess. NIST is a well-known statistical package which provides quantitative measure of the randomness [24]. It consists of 15 tests that are sufficient to test the randomness of the binary sequence. These tests are performed on the sequences generated with logistic, sine and the CLS map with identical initial conditions and control parameters. The results compiled in Table 1 reveals that logistic and sine maps failed in certain tests and hence behaves non-randomly at some regions whereas randomness in sequences generated with CLS maps is effusively confirmed. The magnificent results displayed by CLS map encouraged us to apply this map in our work.

ECG database

Though the ultimate goal is to apply the steganographic algorithm on real time ECG signals acquired under clinical environment but for the purpose of performance comparison it is required to use standard databases. Various standard databases as well as self-recorded database used in this work to evaluate the performance of the proposed algorithm includes [25]:

Massachusetts Institute of Technology-Beth Israel Hospital (MIT-BIH) Arrhythmia database

It contains 48 ECG records, approximately 30 min two-channel ambulatory ECG recordings, obtained from 47 subjects studied by BIH Arrhythmia Laboratory. ECG signal is recorded with 11-bit resolution over 10 mV range with sampling frequency of 360 Hz per channel. The performance is evaluated on the first channel of all the 48 records of this database.

Creighton University Ventricular Tachyarrhythmia (CU-VT) database

CU-VT database includes 35 8-min ECG recordings of human subjects who experienced episodes of sustained ventricular tachycardia, ventricular flutter and ventricular fibrillation. Record cu01 was obtained from a long-term ECG (Holter) recording while the other recordings were digitized in real time high level (1 V/mV nominal) analog signals from patient monitors. The analog ECG signals are sampled at 250 samples per second with 12-bit resolution over a range of 10 mV. Each record contains 127,232 samples (slightly less than 8.5 min).

Beth Israel Deaconess Medical Centre (BIDMC) Congestive Heart Failure (BIDMC-CHF) database

BIDMC-CHF database comprises of long term ECG recordings of 15 subjects (11 men aged (22–71), and 4 women aged 54–63) with severe congestive heart failure. Each recording is about 20 h in duration and contains two ECG signals, digitised at 250 samples per second with 12-bit resolution over a range of ± 10 mV.

Physikalisch-Technische Bundesanstalt (PTB) database

PTB database contains 549 records from 290 subjects (209 men with mean age 55.5, 81 women with mean age 61.6 and the age of 1 woman and 14 male men was not recorded). Each record includes 15 simultaneously measured signals (I, II, III, avr, avl, avf, v1, v2, v3, v4, v5, v6) with each signal is digitized at 1000 samples per second with 16 bit resolution over the range of ± 16.384 mV. The ECGs in this collection were obtained using a non-commercial PTB prototype recorder.

Self-recorded database

The ECG signals were recorded using lead II from the local population in the Biomedical Signal Processing laboratory at Department of Electronics and Communication Engineering, Dr B.R. Ambedkar National Institute of Technology, Jalandhar using BIOPAC® MP150 under standard conditions in a quiet room, at comfortable light and temperature levels. The recorded signals were A/D converted at 500 Hz sampling frequency, 12-bit resolution and then stored. The informed written consent of 100 different subjects was taken prior to the recording.

Proposed methodology

The architecture of proposed ECG steganography is shown in Fig. 2. It includes pre-processing of ECG signal, ciphering of patient's personal information, hiding secret bits in ECG signal and finally transmitting the stego-ECG signal. The major steps involved in performing the ECG steganography include.

R-peak detection

The raw ECG signal acquired is processed to detect R-peaks from the cover ECG signal (ECG_c). There are enormous methods in the literature to perform this operation [26–28], however in this work Pan Tompkins algorithm for QRS detection has been employed to find location (*loc_RR*) and amplitude (*amp_RR*) of R-peaks [26]. The proposed method

Table 1 Results of NIST tests performed on the chaotic sequences generated using logistic, sine and CLS maps

S no.	Name of the test	Logistic map x_n: 0.997655762999 r_o: 3.989999995601		Sine map x_n: 0.997655762999 r_o: 3.989999995601		CLS_1 map x_{n1}: 0.8976557629901 r_{o1}: 3.9953461356011		CLS_2 map x_{n2}: 0.933453564978 r_{02}: 3.886954532619		CLS_3 map x_{n3}: 0.994357334262 r_{03}: 3.973256778521	
		P-value	Result	P-value	Result	P-value	Result	P-value	Result	P-value	Result
1	The frequency test	0.0389	S	0.4201	S	0.7422	S	0.1531	S	0.4990	S
2	Frequency test within the block	0.5267	S	1	S	0.5560	S	0.9497	S	0.9543	S
3	The runs test	0.0945	S	-	F	0.8245	S	0.4500	S	0.4790	S
4	Test for the longest run for ones in a block	0.7494	S	0	F	0.8199	S	0.1021	S	0.1427	S
5	Binary matrix rank test	0.3021	S	0.3455	S	0.0476	S	0.6745	S	0.9444	S
6	The discrete Fourier transform test	0.3114	S	4.8×10^{-293}	F	0.2120	S	0.8967	S	0.8152	S
7	The overlapping template matching test	0.321×10^{-23}	F	2.6×10^{-107}	F	0.1069	S	0.7212	S	0.4015	S
8	Maurer's "universal statistical" test	0.6937	S	4.8×10^{-272}	F	0.7109	S	0.5903	S	0.7955	S
9	The linear complexity test	0.4790	S	0.2762	S	0.5813	S	0.2006	S	0.0803	S
10	The serial test	p1 = 0.3651 p2 = 0.2268	S	0	F	p1 = 0.4367 p2 = 0.5853	S	p1 = 0.2767 p2 = 0.8679	S	p1 = 0.9621 p2 = 0.7457	S
11	The approximate entropy test	0.4352	S	0	F	0.4157	S	0.1101	S	0.1909	S
12	The cumulative sums test	0.0487	S	0.5155	S	0.6737	S	0.2834	S	0.4993	S
13	The random excursions test										
	x = − 4	0.0175	S	0.0136	S	0.6758	S	0.2309	S	0.8101	S
	x = − 3	0.2629	S	0.0056	F	0.5522	S	0.1305	S	0.8053	S
	x = − 2	0.5335	S	0.1315	S	0.4226	S	0.2503	S	0.7353	S
	x = − 1	0.5331	S	0.0046	F	0.3693	S	0.2955	S	0.3505	S
	x = 1	0.2834	S	0.0034	F	0.6789	S	0.7043	S	0.3221	S
	x = 2	0.0424	S	0.0078	F	0.2823	S	0.6765	S	0.3168	S
	x = 3	0.4615	S	0.0001	F	0.7733	S	0.2440	S	0.6834	S
	x = 4	0.3934	S	0.0033	F	0.5673	S	0.4812	S	0.4758	S
14	The random excursions variant test										
	x = − 9	0.4755	S	0.0144	S	0.2311	S	0.9412	S	0.6295	S
	x = − 8	0.1544	S	0.0305	F	0.1486	S	0.8046	S	0.4007	S

Table 1 (continued)

S no.	Name of the test	Logistic map x_n: 0.997655762999 r_o: 3.989999995601		Sine map x_n: 0.997655762999 r_o: 3.989999995601		CLS_1 map x_{n1}: 0.8976557629901 r_{o1}: 3.9953461356011		CLS_2 map x_{n2}: 0.933453564978 r_{02}: 3.886954532619		CLS_3 map x_{n3}: 0.994357334262 r_{03}: 3.973256778521	
		P-value	Result	P-value	Result	P-value	Result	P-value	Result	P-value	Result
	x = −7	0.1955	S	0.0058	F	0.1286	S	0.9431	S	0.4633	S
	x = −6	0.2008	S	0.0005	F	0.1153	S	0.8052	S	0.4096	S
	x = −5	0.0951	S	0.0015	F	0.1591	S	0.7792	S	0.3274	S
	x = −4	0.0852	S	0.0196	S	0.2574	S	0.8321	S	0.4522	S
	x = −3	0.1641	S	0.3994	S	0.4140	S	0.5307	S	0.5714	S
	x = −2	0.2206	S	0.8802	S	0.3561	S	0.2628	S	0.4260	S
	x = −1	0.2238	S	0.4169	S	0.2781	S	0.1987	S	0.4807	S
	x = 1	0.2699	S	0.0872	S	0.4079	S	0.1410	S	0.5268	S
	x = 2	0.2739	S	0.1408	S	0.1663	S	0.0917	S	0.7051	S
	x = 3	0.3055	S	0.3850	S	0.1529	S	0.0644	S	0.9275	S
	x = 4	0.4104	S	0.5039	S	0.1283	S	0.0520	S	0.4471	S
	x = 5	0.5337	S	0.5620	S	0.0979	S	0.0910	S	0.5025	S
	x = 6	0.3482	S	0.5522	S	0.4804	S	0.3171	S	0.5174	S
	x = 7	0.1747	S	0.3593	S	0.9180	S	0.5685	S	0.3601	S
	x = 8	0.1697	S	0.2224	S	0.8886	S	0.5544	S	0.3240	S
	x = 9	0.1787	S	0.1839	S	0.8626	S	0.5037	S	0.4299	S

S success, *F* failure

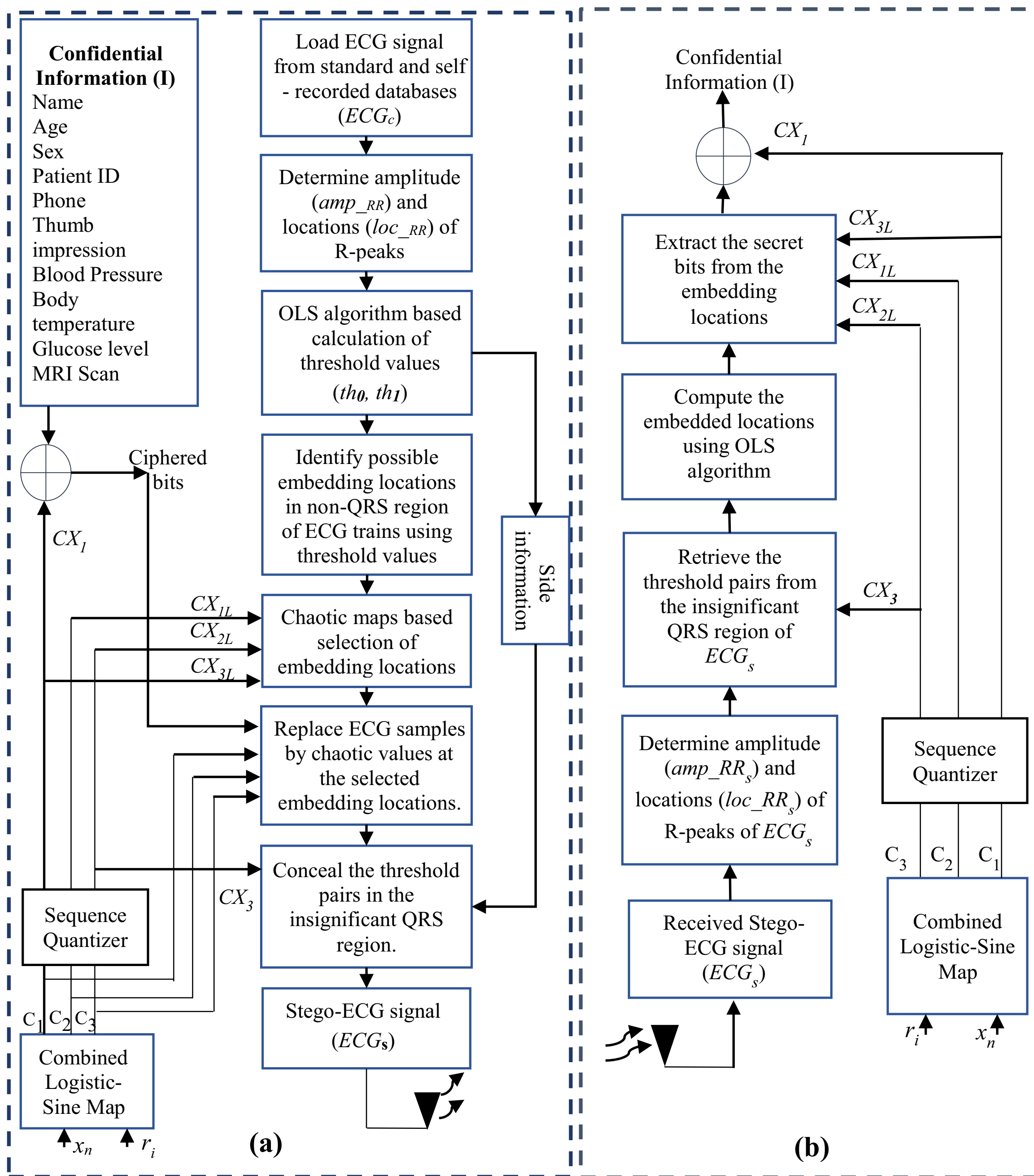


Fig. 2 Proposed procedure of secret data **a** embedding and **b** extraction in ECG signals

is dependent on the amplitude and locations of R-peaks, hence it is important to detect correct R-peaks from the signal. False R-peak detection results the data embedding in QRS segments hence increases the PRD and signal distortion. Selectivity (Se) and positive predictivity (+P) are the measures that evaluates the accuracy of R-peak detection and are given as [29]

$$\mathrm{Se}\ (\%) = \mathrm{TP}/(\mathrm{TP} + \mathrm{FN}) \tag{4}$$

$$+\mathrm{P}\ (\%) = \mathrm{TP}/(\mathrm{TP} + \mathrm{FP}) \tag{5}$$

where true positive (*TP*) is the number of correctly detected R-peaks; false negative (*FN*) is the number of undetected R-peaks and false positive (*FP*) is the number of falsely detected R-peaks. Se (%) is the percentage of correctly detected heartbeats and +P (%) is the percentage of real true heartbeats.

Sorting based quantization of chaotic maps

The random sequence generated using CLS map lies in the range of (0, 1). In order to obtain integer values, the chaotic sequence is quantized using sorting based approach. The samples of the chaotic sequence are sorted in ascending order and their original positions (i.e. locations before sorting) are retained which are used as the random sequence. The chaotic sequence C generates the sorted quantized sequence CX as:

$$Quantize\_ch : \begin{cases} Q = sorted\ values\ of\ C \\ CX = orignal\ positions\ of\ sorted\ sequence \end{cases}$$

The procedure to generate quantized chaotic sequence is mentioned in Algorithm 1.

Ciphering the confidential information

Though protection of the hidden data is always the prime focus of steganography but in this work, additional measures have been taken to safeguard patient's crucial information by performing XOR operation between confidential information and the chaotically generated values before interleaving it into the cover signal. The information acquired from different sources is accumulated in an array I (ASCII) prior to ciphering. Algorithm 2 explains the steps to perform the ciphering operation.

Algorithm 1: Sorting based quantization of chaotic sequence

L_n: length of chaotic sequence
Input: initial parameters for chaotic map (x_n, r_o, L_n)
Output: Quantized sequence (CX)

Generate chaotic sequence $C = CLS(x_n, r_o, L_n)$
Sort sequence C of length l_n to get the quantized integer values where $l_n < L_n$
$CX = Quantize\_ch(C, l_n)$

For *example,*
$C = (0.11, 0.02, 0.13, 0.1, 0.3, 0.15, \ldots\ldots)$
$l_n = 5$
Apply $Quantize\_ch(C, 5)$ (sort first five elements of C)
$Q = 0.02, 0.1, 0.11, 0.13, 0.3$
$CX = 2, 4, 1, 3, 5$

Algorithm 2: Ciphering of patient's confidential information

Input: I: Confidential Data (ASCII), initial parameters; $x_{n1} = 0.8976557629901$, $r_{o1} = 3.9953461356011$, $L_n = 500000$
Output: ciphered bits (s_bits)

Convert I (ASCII) to 8 bit unsigned integer
D = uint8 (I)
len: length of D,
Generate chaotic sequence $C_1 = CLS(x_{n1}, r_{o1}, L_n)$
$CX_1 = Quantize\_ch(C_1, len^{**})$
for $cp = 1 : len$
  $s\_bits = D(cp) \oplus CX_1(cp)$
end for
For example: $len = 1000$;
$D = [D_1\, D_2\, D_3\, D_4 \ldots\ldots\ldots D_{1000}]$, $CX_1 = [X_1\, X_2\, X_3\, X_4 \ldots\ldots\ldots\ldots X_{1000}]$
Perform XOR operation between binary bits of D and X symbol wise
$S\_bits = [(D_1 \oplus X_1)(D_2 \oplus X_2)(D_3 \oplus X_3) \ldots\ldots (D_{1000} \oplus X_{1000})]$

** *len* depends upon the size of confidential information.
In above example, since *len*=1000; therefore 10 binary bits are required to represent D and X.

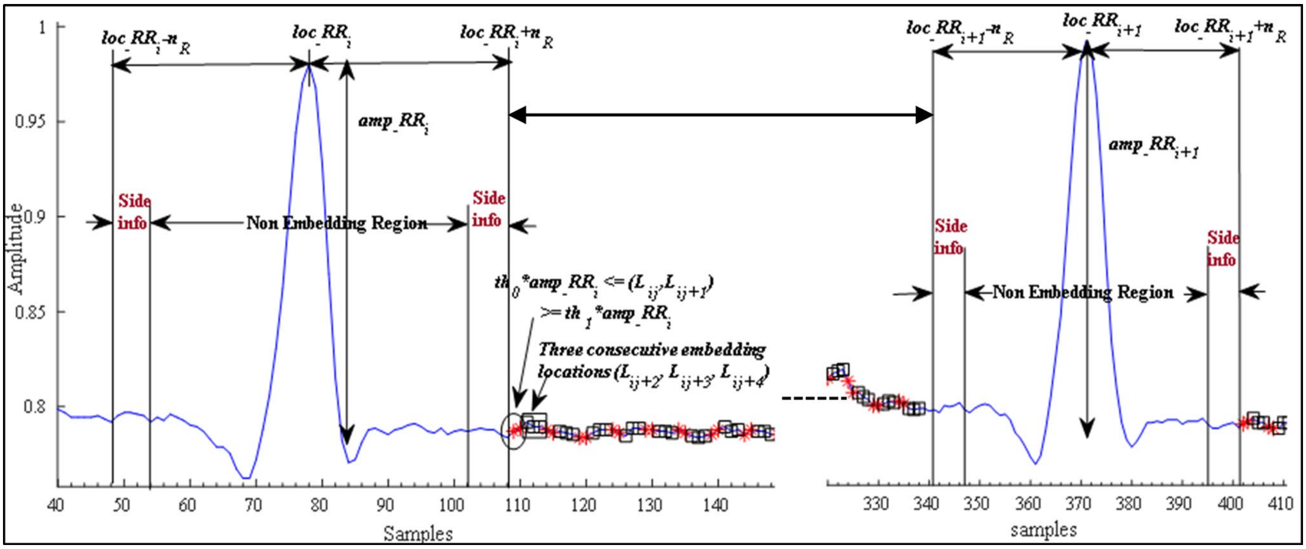


Fig. 3 The detailed view of the embedding and non-embedding regions in an ECG train of record 100

Embedding location identification in non-QRS region

The choice of optimal locations to hide the secret bits is an important factor that affects the performance of steganography and minimizes the chance of brute force attack. In the present work a novel method of ECG steganography has been proposed to select maximum possible locations that can act as effective hosts for hiding the secret bits. The Optimum Location Selection (OLS) algorithm has been designed to identify ECG sample pairs in non-QRS region having magnitude lies between thresholded amp_RR (th_0* amp_RR_i and th_1* amp_RR_i) and embedding is done in next three ECG locations. The sensitive QRS region is excluded from confidential information embedding. Figure 3 illustrates the detailed view of the embedding and non-embedding regions in first and second ECG trains of record 100 of MIT-BIH Arrhythmia database along with the locations identified by OLS algorithm for interleaving the ciphered bits. As per the proposed algorithm if locations $L_{i,j}$ (*j*th sample of *i*th ECG train) and $L_{i,j+1}$ satisfies the OLS condition, then the sites $L_{i,j+2,}$ $L_{i,j+3}$ and $L_{i,j+4}$ are suitable for embedding secret bits. The process of threshold selection and recognizing the embedding sites is explained in Algorithm 3. Figure 4 illuminates the implementation of Algorithm 3 and demonstrates the process of selection of embedding and non-embedding locations at calculated threshold values along with the regions for embedding the side information for 10 min long ECG record 100 of MIT-BIH Arrhythmia database. The amplitude of ECG signal is initially normalised by dividing it to its maximum value. As shown in Figs. 3 and 4 the first and second R-peaks are detected at locations 78 and 371 respectively, therefore the regions 78 ± 30 and 371 ± 30 i.e. locations 48–108 and 341–401 are not included for embedding secret bits. Hence OLS algorithm selects possible locations to embed confidential information amongst the first and second R-peaks lying within locations 109–340 and the side information is inserted in the non-significant locations from 48 to 54 and 102–108 around first R-peak and 341–347 and 395–401 around the second R-peak of the QRS-region. Confidential data is embedded in chaotically selected locations amongst these possible locations as given in Algorithm 4.

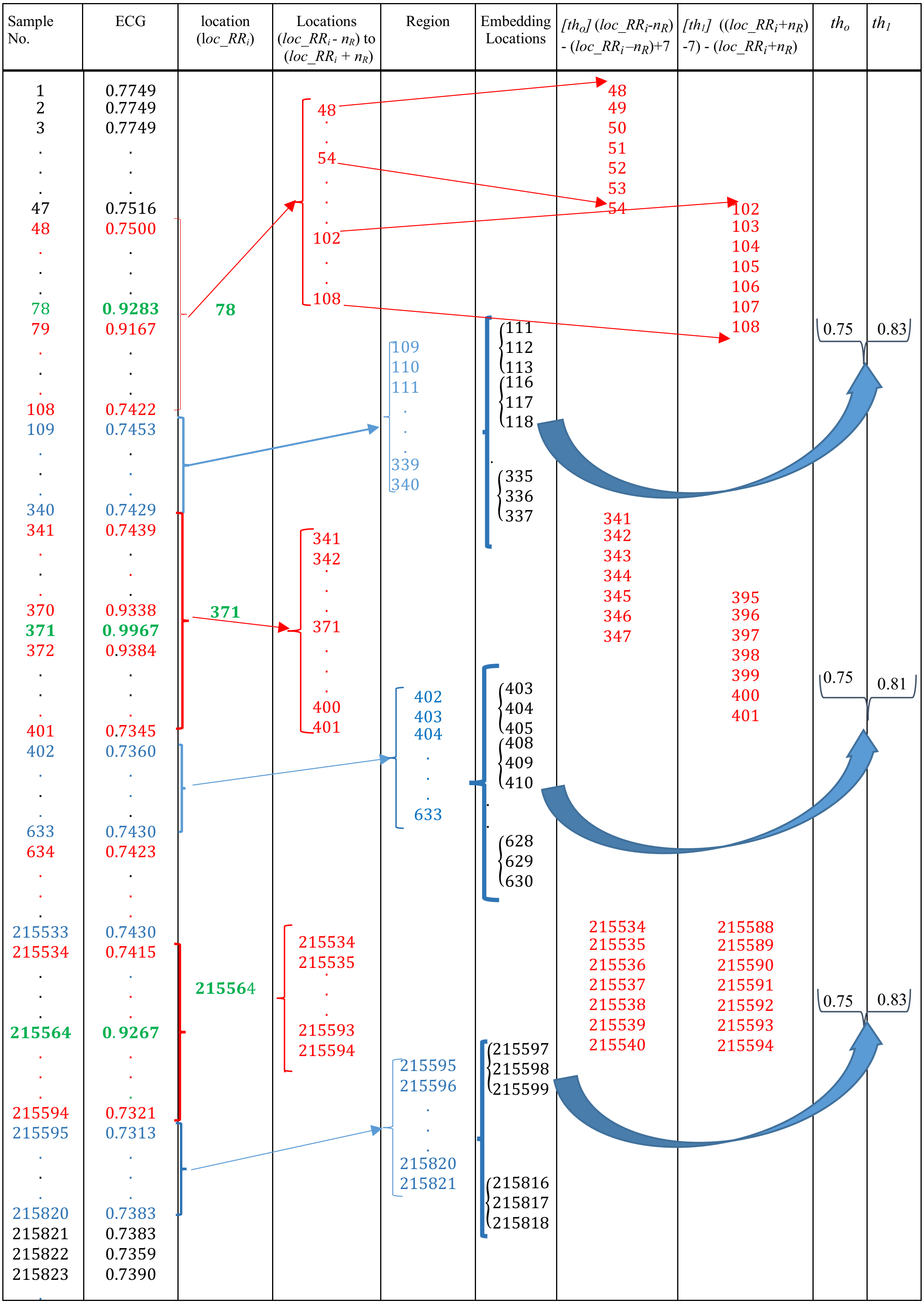


Fig. 4 Description of embedding and non-embedding regions for record 100 of MIT-BIH Arrhythmia database

Algorithm 3: OLS algorithm to find the embedding locations for N ECG_c trains

```
th0 : lower threshold
δ: step size
N: number of R-peaks in ECGc
amp_RRi : amplitude of RR peak of ith ECG train
loc_RRi : location of RR peak of ith ECG train
Input: ECGc, th0 (typically chosen to vary between 10% to 75% of amp_RRi), δ=0.1 (varies from 0.1 to
        0.15), amp_RR , loc_RR
Output: tho (i), th1(i), loc_emb, Embedding Locations (Embed_loc)
 for i=1 to N
      j= (loc_RRi + (nR+1))#
      r←1
   while δ < 0.15
      for th0 =0.1 to 0.75
          th1= th0 + δ
          α0= th0* amp_RRi and α1= th1* amp_RRi
          k←1
          while (j < loc_RR i+1 – (nR+1))#
              if α0 ≤ [amp(ECGc(i,j)) && amp(ECGc(i,j+1)) ] ≥ α1   //OLS Condition
                 T_loc(k)←j+1
                 j←j+5;
                 k←k+1;
                 else j←j+1;
              end if
          end while
                 t_tho (r) ←th0;
                 t_th1 (r) ←th1;
                 t_emb_loc (r)←T_lock;
                 no_loc T_lock(r)←k;
                 r←r+1
      end for
      δ= δ+1;
   end while
   rmax_count ← max(no_loc T_lock)
   th0(i)← t_tho( rmax_count)        // threshold values for ith train that contains maximum
                                      number of embedding sites //
   th1(i)← t_th1( rmax_count)
  loc_emb← t_emb_loc( rmax_count)
  end for
 for h= 1: length of loc_emb
   Embed_loc= loc_emb(h)+1, loc_emb(h)+2 and loc_emb(h)+3
 end for
```

Average duration of QRS complex is 0.08 to 0.10 sec [30] and number of samples (n_q) required to represent QRS region on each side of R-peak is $\lceil (fs * 0.10)/2 \rceil$. However, $n_R = n_q + 12$ samples are excluded on each side of R-peak to avoid any error in case of prolonged QRS duration (up to 0.165 sec). In the analysis, MIT-BIH Arrhythmia database is used with f_s =360 Hz, accordingly n_R is set to 30.

Embedding process of secret information

In steganography, this stage requires special measures to ensure high data security. In the proposed algorithm the chaotic maps are engaged, firstly to identify the embedding positions and secondly, to generate chaotic values as a substitute of ECG samples at selected embedding locations (*Embed_loc*) according to 0's and 1's of the secret bits. Since the values of both ECG samples and chaotic maps lies between 0 and 1 hence the amplitudes inserted at the embedding sites also lies between 0 and 1 only, hence the problem of underflow or overflow does not arises in the proposed algorithm. Moreover, with respect to each embedding site, three bits are stored in three consecutive ECG samples, the security is boosted by using different chaotic maps for each bit. The embedding process is thoroughly discussed in Algorithm 4.

along with stego-ECG signal. In the proposed technique, this side information is entrenched into the chaotically selected ECG beats using least significant bit (LSB) method of data hiding [31] as explained in Algorithm 5. The imbedding is done cautiously in the insignificant QRS region in order to avoid any overlapping with samples carrying secret bits.

Algorithm 4: Embedding of secret bits in ECG signal

L: number of sets of embedding location pairs (*loc_emb*)
l: length of ciphered bits (*s_bits*)
L_n: length of chaotic sequences (randomly choosen)
z_1 and z_2: scaling factor
Input: ECG_c, L, z_1=0.998, z_2=0.999, L_n= 500000 C_1, C_2 and C_3, *s_bits*, initial parameters for chaotic maps
  x_{n1} = 0.897655762990, r_{01} = 3.9953461356011
  x_{n2} = 0.933453564978, r_{02} = 3.886954532619
  x_{n3} = 0.994357334262, r_{03} = 3.973256778521
Output: ECG with embedded secret bits (ECG_w)

```
Generate chaotic sequences C1 = CLS (xn1, ro1, Ln), C2 = CLS (xn2, r02, Ln) and C3 = CLS (xn3, r03, Ln) and hence
      CX1L= Quantize_ch(C2, L)
      CX2L= Quantize_ch(C3, L)
      CX3L= Quantize_ch(C1, L)
   w ←1
 for a = 1:3
     for  u = 1 to L
          Loci,j ← loc_emb (CXaL (u))
          Avg←average (ECGc (Loci,j), ECGc (Loci,j-1)
           R1←z1*Avg
           R2←z2*Avg
           new_amp ← minimum (Ca ≥ R1 && Ca ≤ R2)
      if  s_bits(w) == 0
        Loci,j+a ← new_amp
        else
        Loci,j+ a ← Avg
     end if
     if w < l
     w ←w+1
     end if
   end for
 end for
```

Embedding of the side information

Since the threshold values computed by OLS algorithm are essential at the receiver to identify the confidential data embedding locations, it is indispensable to send these values

Algorithm 5: LSB based side information embedding

th_{0i}, th_{1i}: lower and upper threshold values for all ECG trains // (from algorithm 3)
N: number of ECG trains in ECG_w
Input: ECG_w, th_{0i}, th_{1i}, N, C_3 ,
Output: Stego-ECG (ECG_s)

CX_3=$Quantize\_ch(C_3, N)$
for $i= 1$ to N
  Select an R-peak and find positions around it for hiding threshold bits
    $\Phi= CX_3(i)$
    $Th_0\_left(i) \leftarrow loc\_RR_\Phi - n_R{}^{\#*}$
    $Th_1\_right(i) \leftarrow loc\_RR_\Phi + n_R$
  LSB embedding of $th_0(i)$ and $th_1(i)$ in 7 consecutive ECG samples
  ($Th_0\_left(i)$ to $Th_0\_left(i)$+ 7) and ($Th_1\_right(i)$ to $Th_1\_right(i)$-7) respectively
end for

Out of n_R excluded samples, last 7 samples from both sides of R-peaks are used for threshold concealing.
* threshold values varies within 10 to 90 which can be easily represented by 7-bit binary code.

Extraction process

At the receiver, the embedded bits are extracted following the reverse procedure of the transmitter side. To extract the correct bits, the receiver should have the same key which includes initial parameters of chaotic maps and scaling factor z_1 and z_2. The extraction stage follows the following steps:

1. Determine the locations (loc_RR_s) and amplitude (amp_RR_s) of R-peaks of stego-ECG signal using Pan–Tompkin algorithm.
2. Regenerate chaotic sequences

$$C_1 = CLS\ (x_{n1}, r_{o1}, L_n)$$
$$C_2 = CLS\ (x_{n2}, r_{02}, L_n)$$
$$C_3 = CLS\ (x_{n3}, r_{03}, L_n)$$
$$CX_{1L} = Quantize\_ch(C_2, L)$$
$$CX_{2L} = Quantize\_ch(C_3, L)$$
$$CX_{3L} = Quantize\_ch(C_1, L)$$
$$CX_3 = Quantize\_ch(C_3, N)$$

3. Follow algorithm 5 to retrieve the threshold values from the LSBs of the locations lying in the non-significant QRS-region of chaotically selected R-peaks using chaotic map CX_3.

$$\Phi = CX_3(i)$$
$$Th_0\_left(i) \leftarrow loc\_RR_F - n_R$$
$$Th_1\_right(i) \leftarrow loc\_RR_F + n_R$$

4. Apply OLS algorithm to recover the embedding locations (Emb_loc). //follow Algorithm 3.
5. Extract the hidden bits from ECG samples. The decision rule to retrieve 0 or 1 is

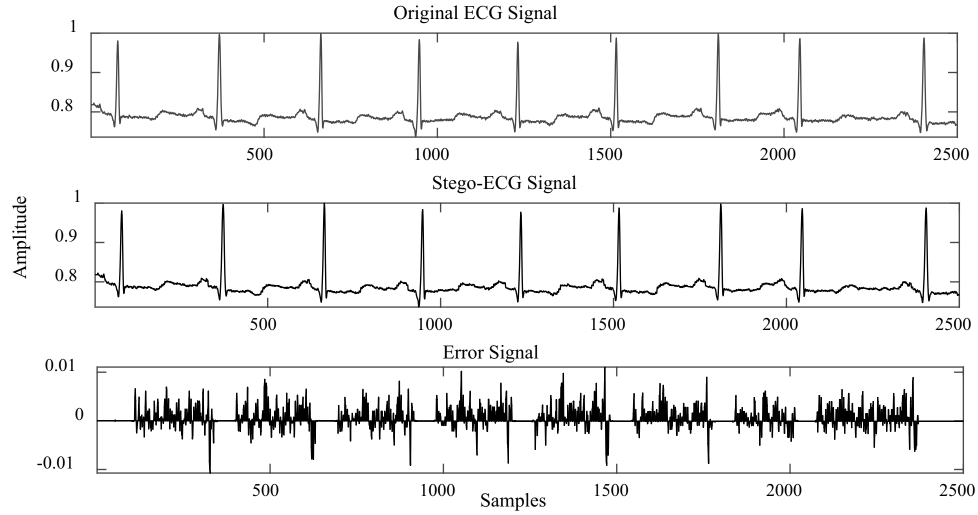
$$\textbf{\textit{if}}\ ECG_s(Embed\_loc_s) == Avg \quad //\ \text{follow Algorithm 4}$$
$$bit\ embedded = 1$$
$$\textbf{\textit{else}}$$
$$bit\ embedded = 0$$

6. Perform **XOR** operation between the recovered bits and the binary equivalent of the values of chaotic map (CX_1) to recover the original secret bits.

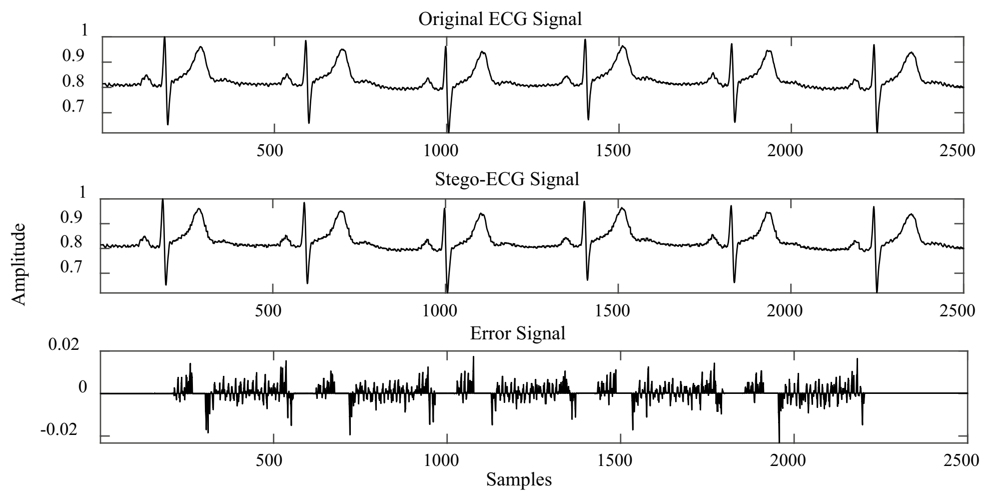
Results

Imperceptibility and undetectability are the key issues that need to be addressed in steganography. The proposed technique of ECG steganography has been applied on normal and abnormal ECG databases to evaluate its performance. Statistical error evaluation parameters such as PRD, Normalised PRD (PRDN), PRD1024, MSE, SNR, PSNR, MAE and KL-Divergence ("Appendix") distributes the error equally over whole ECG signal [32, 33] that misleads the diagnostic interpretation. Hence clinically robust measures; WWPRD and wavelet energy based diagnostic distortion (WEDD) (Appendix) are also employed to assess the stego-ECG by monitoring the local distortion and estimating the weighted significant features [32–35]. Moreover, the amount of bits that can be imbedded into the signal and rate at which these bits got corrupted while extracting are also the important measures of steganography and are evaluated in terms of EC and BER.

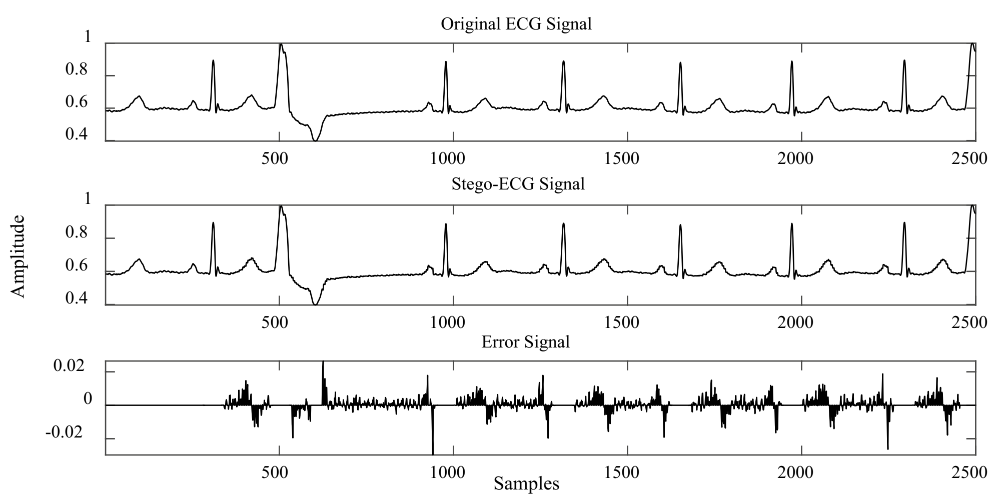
Figure 5 shows the amount of error incurred after inserting 1 kb of secret data in first 2500 samples of normal (100)


Original ECG Signal
Stego-ECG Signal
Error Signal
Amplitude
Samples

(a)


Original ECG Signal
Stego-ECG Signal
Error Signal
Amplitude
Samples

(b)


Original ECG Signal
Stego-ECG Signal
Error Signal
Amplitude
Samples

(c)

◂**Fig. 5** First 2500 samples of original, stego and error signals of ECG records: **a** 100, **b** 117 and **c** 119 of MIT-BIH Arrhythmia database after inserting 1 kb of secret bits

and abnormal (117 and 119) records of MIT-BIH Arrhythmia database. Visual inspection of original and stego-ECG signals confirm the imperceptibility of two signals. The error signal clearly indicates that there is no distortion in the QRS region while the error is negligible in the non-QRS region. This error is too subtle to alter the diagnostic features of an ECG signal.

Tables 2 and 3 shows the complete results of statistical, clinical and embedding performance measures in all 48 records of MIT-BIH Arrhythmia database and in the self-recorded dataset respectively of 10 min duration after embedding secret information to the maximum EC of the signal. Average PRD, PRD1024, PRDN, MSE, SNR, PSNR, MAE, KL-Divergence, WWPRD and WEDD observed are 0.004, 0.0517, 0.0672, 1.13×10^{-5}, 46.88, 50.28, 2.06, 1.29×10^{-5}, 0.15 and 0.04 respectively for MIT-BIH Arrhythmia database and 0.016, 0.029, 0.055, 3.38×10^{-5}, 36.51, 46.03, 6.43, 1.8×10^{-4}, 0.13 and 0.037 respectively for the self-recorded dataset. These results are achieved at average EC and amount of bits embedded of 0.45 and 96,876 & 0.47 and 102,571 respectively for the two datasets which reveals that the proposed method based on optimal location selection is capable to host plethora of secret information at nominal error. The large value of standard deviation in bits embedded (Tables 2, 3) shows that the EC is effected by the morphological features of ECG signals. Although the MIT-BIH Arrhythmia database includes both normal and abnormal ECG records but to guarantee balanced results, the performance has been evaluated on abnormal; CU-VT, BIDMC-CHF and leads I, II and III of PTB database. Table 4 displays the average PRD, PRD1024, PRDN, MSE, SNR, PSNR, MAE, KL-Divergence, WWPRD and WEDD obtained from 30,000 ECG samples of all records in these databases. Average PRD, PSNR and bits embedded in first 30,000 ECG samples of lead 1 of BIDMC-CHF, CU-VT and leads I, II and III of PTB databases is measured as 0.015, 44.72 and 9049; 0.019, 45.29 and 6580; 0.026, 41.65 and 9465; 0.018, 42.43 and 9930; 0.014, 43.06 and 8882 respectively. These results signifies that the proposed method is equally competent on aberrant ECG signals also. The performance of the proposed method depends upon the duration and morphological features of the ECG signal. To assess the effect of these factors we have evaluated the proposed method in terms of (i) effect of embedding on stego-ECG and (ii) effect of ECG duration on EC.

Effect of ECG duration on EC

The degradation in the quality of ECG signal due to embedding confidential information and side information is probed. For this, the secret information upto the maximum EC of an ECG signal is evaluated for 8 different durations varying from 1 min to 30 min on all 48 ECG records of MIT-BIH Arrhythmia database as illustrated graphically using boxplots in Fig. 6.

Although the average number of bits embedded in ECG signal proportionally increases with ECG duration but the average EC is found to be nearly same. Moreover, other evaluation parameters are also least effected with variation in signal duration. The versatility of the proposed technique lies in the fact that duration of ECG signal can be selected in accordance with the amount of secret information without affecting its performance. The outliers in the box plot shows the dependence of EC and other parameters on the morphology of ECG signal hence justifies the large values of the standard deviation. Table 5 demonstrates the variation in the distortion parameters by varying the cover ECG signal duration from 1 to 30 min when averaged over all 48 records from MIT-BIH Arrhythmia database.

Effect of EC on stego-ECG

The amount of distortion in the stego-ECG is measured by varying the secret data size embedded in all 48 records of MIT-BIH Arrhythmia database of 10 min duration. The average PRD, PSNR, KL-Divergence, WWPRD and WEDD in case of (i) low EC (1 kb) is 0.00015, 72.96, 8.66×10^{-9}, 0.00049 and 0.00012 (ii) medium EC (20 kb) is 0.0010, 56.61, 1.15×10^{-7}, 0.0091 and 0.0021 (iii) high EC (50 kb) is 0.0019, 52.80, 5.93×10^{-6}, 0.017 and 0.0084 respectively.

Effect of LSB based side information embedding

Embedding side information in the ECG signal can reduce the quality of the stego-signal, but in the proposed method, the threshold values are inserted in the insignificant regions such that its impact is unnoticeable in the stego-ECG. It is demonstrated in Fig. 7 that interleaving threshold values in the stego-ECG signal is trivial and causes nominal degradation in overall signal quality.

Effect of scaling factor (z_1 and z_2)

Scaling factors z_1 and z_2 are significant in regulating the variation in amplitudes of the two signals. The method to embed secret bits (Algorithm 4) includes two variables R_1 and R_2 that defines the range of chaotic values required to choose a magnitude for substituting secret bit and the variables R_1 and R_2 are dependent on z_1 and z_2. The values of

Table 2 Performance evaluation metrics of the proposed method for 48 records from MIT-BIH Arrhythmia database of 10 min duration

Record	PRD	PRD 1024	PRDN	MSE	SNR	PSNR	MAE	KL-Divergence	WWPRD	WEDD	BER	Bits embed	EC
100	0.0028	0.0366	0.0690	4.29×10^{-6}	51.1634	53.6768	1.4151	3.63×10^{-6}	0.1448	0.053	0	101,055	0.4678
101	0.0044	0.0515	0.0690	7.95×10^{-6}	47.1554	50.9962	1.9687	9.46×10^{-6}	0.1599	0.0438	0	104,646	0.4845
102	0.0037	0.0561	0.0898	7.59×10^{-6}	48.6974	51.2003	1.6694	6.71×10^{-6}	0.1522	0.0552	0	101,361	0.4693
103	0.0037	0.0461	0.0567	6.31×10^{-6}	48.6061	51.9998	1.9100	6.67×10^{-6}	0.1282	0.0401	0	103,032	0.477
104	0.0106	0.1419	0.1486	5.32×10^{-6}	39.5259	42.7402	3.3853	5.6×10^{-5}	0.2474	0.0628	0	95,724	0.4432
105	0.0044	0.0564	0.0671	9.32×10^{-6}	47.1001	50.3040	2.0698	9.58×10^{-6}	0.1795	0.0428	0	98,322	0.4552
106	0.0054	0.0685	0.0701	1.24×10^{-5}	45.4247	49.0623	2.6793	1.39×10^{-5}	0.1547	0.052	0	103,464	0.479
107	0.0075	0.0430	0.0398	2.19×10^{-5}	42.5165	46.5869	2.7985	2.82×10^{-5}	0.1002	0.0304	0	75,932	0.3515
108	0.0035	0.0546	0.0713	6.84×10^{-6}	49.1898	51.6524	1.3253	5.97×10^{-6}	0.1766	0.0427	0	82,284	0.3809
109	0.0043	0.0434	0.0457	9.5×10^{-6}	47.2387	50.2229	2.1275	9.19×10^{-6}	0.1383	0.0333	0	97,008	0.4491
111	0.0037	0.0609	0.0663	7.85×10^{-6}	48.7020	51.0521	1.8277	6.59×10^{-6}	0.1881	0.0426	0	90,522	0.4191
112	0.0039	0.0191	0.0724	7.87×10^{-6}	48.2907	51.0407	1.6403	7.19×10^{-6}	0.1647	0.0444	0	99,191	0.4592
113	0.0059	0.0629	0.0513	1.47×10^{-5}	44.5612	48.3138	2.6852	1.66×10^{-5}	0.122	0.0456	0	102,501	0.4745
114	0.0058	0.1318	0.1957	2.13×10^{-5}	44.6826	46.7131	1.2863	1.78×10^{-5}	0.2936	0.0905	0	84,729	0.3923
115	0.003	0.0230	0.0398	3.64×10^{-6}	50.4231	54.3858	1.5186	4.47×10^{-6}	0.0767	0.0267	0	105,627	0.4890
116	0.007	0.0259	0.0462	1.38×10^{-5}	43.0844	48.6016	2.9295	2.5×10^{-5}	0.0897	0.0326	0	109,174	0.5054
117	0.0037	0.0182	0.0677	8.79×10^{-6}	48.5942	50.5593	1.6387	6.82×10^{-6}	0.1677	0.0381	0	96,117	0.4450
118	0.0073	0.0325	0.0679	1.74×10^{-5}	42.7222	47.6070	3.0515	2.65×10^{-5}	0.1582	0.039	0	100,413	0.465
119	0.006	0.0255	0.0464	1.17×10^{-5}	44.4666	49.3257	2.4563	1.83×10^{-5}	0.1203	0.0315	0	109,464	0.5068
121	0.003	0.0153	0.0479	4.33×10^{-6}	50.3279	53.6351	1.4424	4.56×10^{-6}	0.1581	0.0182	0	106,323	0.4922
122	0.0047	0.0218	0.0517	1×10^{-5}	46.5599	49.9992	2.1105	1.11×10^{-5}	0.1438	0.0328	0	98,265	0.4549
123	0.0046	0.0233	0.0679	7.68×10^{-6}	46.7512	51.1485	2.1385	1.04×10^{-5}	0.1496	0.0453	0	110,460	0.5114
124	0.0036	0.0161	0.0306	4.19×10^{-6}	48.7813	53.7732	1.6041	6.83×10^{-6}	0.084	0.0151	0	105,285	0.4874
200	0.0067	0.0755	0.1015	1.99×10^{-5}	43.5097	47.0025	2.3073	2.28×10^{-5}	0.2005	0.0457	0	88,191	0.4083
201	0.0025	0.0492	0.0623	3.94×10^{-6}	52.0533	54.0460	1.2669	2.96×10^{-6}	0.1606	0.0425	0	97,575	0.4517
202	0.0036	0.0406	0.0694	6.83×10^{-6}	48.7870	51.6556	1.9778	6.44×10^{-6}	0.2004	0.047	0	107,226	0.4964
203	0.0068	0.0593	0.0549	1.48×10^{-5}	43.3974	48.3112	2.4860	2.36×10^{-5}	0.1059	0.0304	0	79,782	0.3694
205	0.0027	0.0346	0.0690	4.44×10^{-6}	51.3406	53.5288	1.2766	3.6×10^{-6}	0.1305	0.0436	0	93,846	0.4345
207	0.0042	0.0463	0.0415	8.1×10^{-6}	47.4551	50.9155	0.7409	1.01×10^{-5}	0.143	0.021	0	52,750	0.2442
208	0.005	0.0511	0.0492	1.14×10^{-5}	45.9378	49.4372	2.4192	1.3×10^{-5}	0.1356	0.0352	0	91,563	0.4239
209	0.0048	0.0779	0.0869	1.2×10^{-5}	46.3391	49.2097	2.2235	1.15×10^{-5}	0.1705	0.0668	0	104,462	0.4822
210	0.0044	0.0734	0.0768	1.13×10^{-5}	47.0637	49.4676	1.7163	9.86×10^{-6}	0.1913	0.0466	0	91,230	0.4224
212	0.0081	0.1105	0.1130	3.13×10^{-5}	41.8337	45.0468	3.8671	3.27×10^{-5}	0.23	0.0577	0	94,287	0.4365
213	0.0082	0.0569	0.0588	2.41×10^{-5}	41.7147	46.1767	3.7849	3.40×10^{-5}	0.1304	0.0418	0	98,079	0.4541
214	0.005	0.0516	0.0489	1.03×10^{-5}	46.0396	49.8921	2.2863	1.28×10^{-5}	0.1416	0.0323	0	98,295	0.4551
215	0.0064	0.1012	0.1087	1.79×10^{-5}	43.8707	47.4739	2.8737	2.05×10^{-5}	0.211	0.0505	0	89,010	0.4121
217	0.0058	0.0464	0.0401	1.49×10^{-5}	44.7242	48.2804	2.4830	1.66×10^{-5}	0.1002	0.0329	0	88,058	0.4077
219	0.0046	0.0268	0.0426	8.1×10^{-6}	46.7839	50.9169	1.9831	1.09×10^{-5}	0.0605	0.0301	0	100,449	0.4650
220	0.0035	0.0247	0.0510	5.07×10^{-6}	49.2102	52.9516	1.6942	5.72×10^{-6}	0.083	0.0363	0	107,530	0.4978
221	0.0036	0.0517	0.0513	6.49×10^{-6}	48.8304	51.8745	1.8482	6.53×10^{-6}	0.1479	0.0365	0	98,193	0.4546
222	0.003	0.0689	0.0928	5.86×10^{-6}	50.3696	52.3225	1.4350	4.46×10^{-6}	0.1762	0.0686	0	91,620	0.4242
223	0.0034	0.0249	0.0425	4.9×10^{-6}	49.3629	53.0952	1.5624	5.76×10^{-6}	0.1032	0.0265	0	95,985	0.4444
228	0.0049	0.0607	0.0615	9.27×10^{-6}	46.2698	50.1215	2.0920	1.21×10^{-5}	0.2018	0.0297	0	102,436	0.4742
230	0.0037	0.0473	0.0533	6.03×10^{-6}	48.7308	52.1933	1.8346	6.7×10^{-6}	0.1167	0.0359	0	102,033	0.4724
231	0.0035	0.0531	0.0641	5.74×10^{-6}	49.1898	52.4102	1.8928	5.72×10^{-6}	0.1317	0.0442	0	110,289	0.5106
232	0.0034	0.0793	0.1047	7.74×10^{-6}	49.3413	51.1120	1.4943	5.67×10^{-6}	0.2202	0.0452	0	92,231	0.4270
233	0.0063	0.0552	0.0541	1.69×10^{-6}	43.9897	47.7287	2.4735	2.02×10^{-5}	0.141	0.0371	0	94,651	0.4382
234	0.0032	0.0420	0.0466	4×10^{-6}	49.8732	53.9775	1.6213	4.92×10^{-6}	0.1102	0.0283	0	99,360	0.46

Table 2 (continued)

Record	PRD	PRD 1024	PRDN	MSE	SNR	PSNR	MAE	KL-Divergence	WWPRD	WEDD	BER	Bits embed	EC
Average	0.0048	0.052	0.0672	1.13×10^{-5}	46.8872	50.2864	2.0692	1.29×10^{-5}	0.1509	0.0411	0	96,876	0.4485
SD	0.0017	0.0271	0.0290	8.44×10^{-6}	2.82	2.52	0.6426	9.98×10^{-6}	0.0459	0.0134	0	10,031	0.05

SD standard deviation

Table 3 Performance evaluation metrics of the proposed method for 20 records of self-recorded data of 10 min duration

Record	PRD	PRD 1024	PRDN	MSE	SNR	PSNR	MAE	KL-Divergence	WWPRD	WEDD	BER	Bits embed	EC
1	0.0146	0.0189	0.0566	2.48×10^{-5}	36.7	46.05	8.84	1.2×10^{-4}	0.1612	0.0414	0	91,854	0.42
2	0.0186	0.0115	0.0302	1.48×10^{-5}	34.61	48.31	4.34	3.15×10^{-4}	0.0418	0.0215	0	105,108	0.49
3	0.0208	0.0182	0.0616	4.3×10^{-5}	33.63	43.66	4.79	2.53×10^{-4}	0.1588	0.0470	0	105,840	0.49
4	0.0271	0.0347	0.0489	3.54×10^{-5}	31.32	44.51	8.1	5.54×10^{-4}	0.0540	0.0367	0	93,414	0.43
5	0.0097	0.0171	0.0256	8.29×10^{-6}	40.26	50.81	3.78	5.69×10^{-5}	0.0630	0.0180	0	106,779	0.49
6	0.0114	0.0165	0.0373	1.44×10^{-5}	38.84	48.42	3.58	7.29×10^{-5}	0.0976	0.0271	0	106,155	0.49
7	0.0204	0.0325	0.0898	7.67×10^{-5}	33.77	41.15	7.89	2.25×10^{-4}	0.1978	0.0474	0	105,984	0.49
8	0.0194	0.0268	0.0600	3.8×10^{-5}	34.23	44.2	6.45	2.09×10^{-4}	0.1360	0.0385	0	102,945	0.48
9	0.0238	0.1019	0.139	1.49×10^{-4}	32.47	38.26	16.81	3.04×10^{-4}	0.3351	0.0663	0	95,394	0.44
10	0.0116	0.0278	0.0296	9.33×10^{-6}	38.67	50.3	6.85	7.54×10^{-5}	0.0623	0.0205	0	110,799	0.51
11	0.0115	0.0277	0.0296	9.15×10^{-6}	38.02	50.4	6.65	7.51×10^{-5}	0.0623	0.0203	0	110,543	0.51
12	0.0146	0.0421	0.0469	2.47×10^{-5}	36.71	46.07	7.75	1.14×10^{-4}	0.1095	0.0344	0	101,751	0.47
13	0.0085	0.0402	0.0620	2.03×10^{-5}	41.34	46.93	4.9	3.87×10^{-5}	0.1607	0.0472	0	105,897	0.49
14	0.0073	0.0369	0.0562	1.42×10^{-5}	42.65	48.47	4.22	2.66×10^{-5}	0.1284	0.0413	0	111,582	0.52
15	0.0057	0.0105	0.0544	7.81×10^{-6}	44.85	51.07	5.96	1.67×10^{-5}	0.1390	0.0367	0	102,864	0.48
16	0.0163	0.0175	0.0514	2.41×10^{-5}	35.72	46.19	4.06	1.45×10^{-4}	0.1176	0.0381	0	101,352	0.47
17	0.0208	0.0182	0.0616	4.3×10^{-5}	33.63	43.66	4.79	2.53×10^{-4}	0.1588	0.0470	0	105,840	0.49
18	0.0236	0.0318	0.0608	5×10^{-5}	32.52	43.01	7.75	3.31×10^{-4}	0.1616	0.0443	0	100,851	0.47
19	0.0162	0.0345	0.0535	3.1×10^{-5}	35.79	45.09	6.38	1.4×10^{-4}	0.1469	0.0372	0	102,852	0.48
20	0.0202	0.0227	0.0472	3.83×10^{-5}	33.89	44.17	4.47	3.02×10^{-4}	0.1167	0.0331	0	83,361	0.39
Average	0.0161	0.0295	0.0552	3.38×10^{-5}	36.51	46.03	6.43	1.8×10^{-4}	0.1305	0.0372	0	102,571	0.47
SD	0.0057	0.0185	0.0236	3.06×10^{-5}	3.51	3.21	2.79	1.29×10^{-4}	0.063	0.0124	0	6627	0.031

Table 4 Average of performance evaluation metrics of all records of first 30,000 ECG samples of CU-VT, BIDMC-CHF and leads I, II and III of PTB database

Database	PRD	PRD 1024	PRDN	MSE	SNR	PSNR	MAE	KL-Divergence	WWPRD	WEDD	BER	Bits	EC
BIDMC-CHF	0.015	0.017	0.090	7.1×10^{-5}	38.44	44.72	2.615	1.8×10^{-4}	0.194	0.059	0	9049	0.30
CU-VT	0.019	0.058	0.083	1.07×10^{-4}	37.58	45.29	6.21	8.7×10^{-5}	0.152	0.054	0	6580	0.23
PTB-I	0.026	0.045	0.077	8.7×10^{-5}	33.04	41.65	9.10	3.4×10^{-4}	0.230	0.038	0	9465	0.31
PTB-II	0.018	0.042	0.061	7.2×10^{-5}	35.64	42.43	8.69	9.3×10^{-5}	0.182	0.028	0	9930	0.37
PTB-III	0.014	0.028	0.055	5.6×10^{-5}	38.01	43.06	6.31	4.2×10^{-4}	0.169	0.025	0	8882	0.29

scaling factors are kept near to but less than 1 with z_2 greater than z_1. The right choice of z_1 and z_2 results in less deviation in amplitude at the embedding location in the stego signal. This is demonstrated in Fig. 8 for three sets of scaling factors which proves that the larger the difference between z_1 and z_2, the more is the deviation between original and stego-ECG signal at embedding locations.

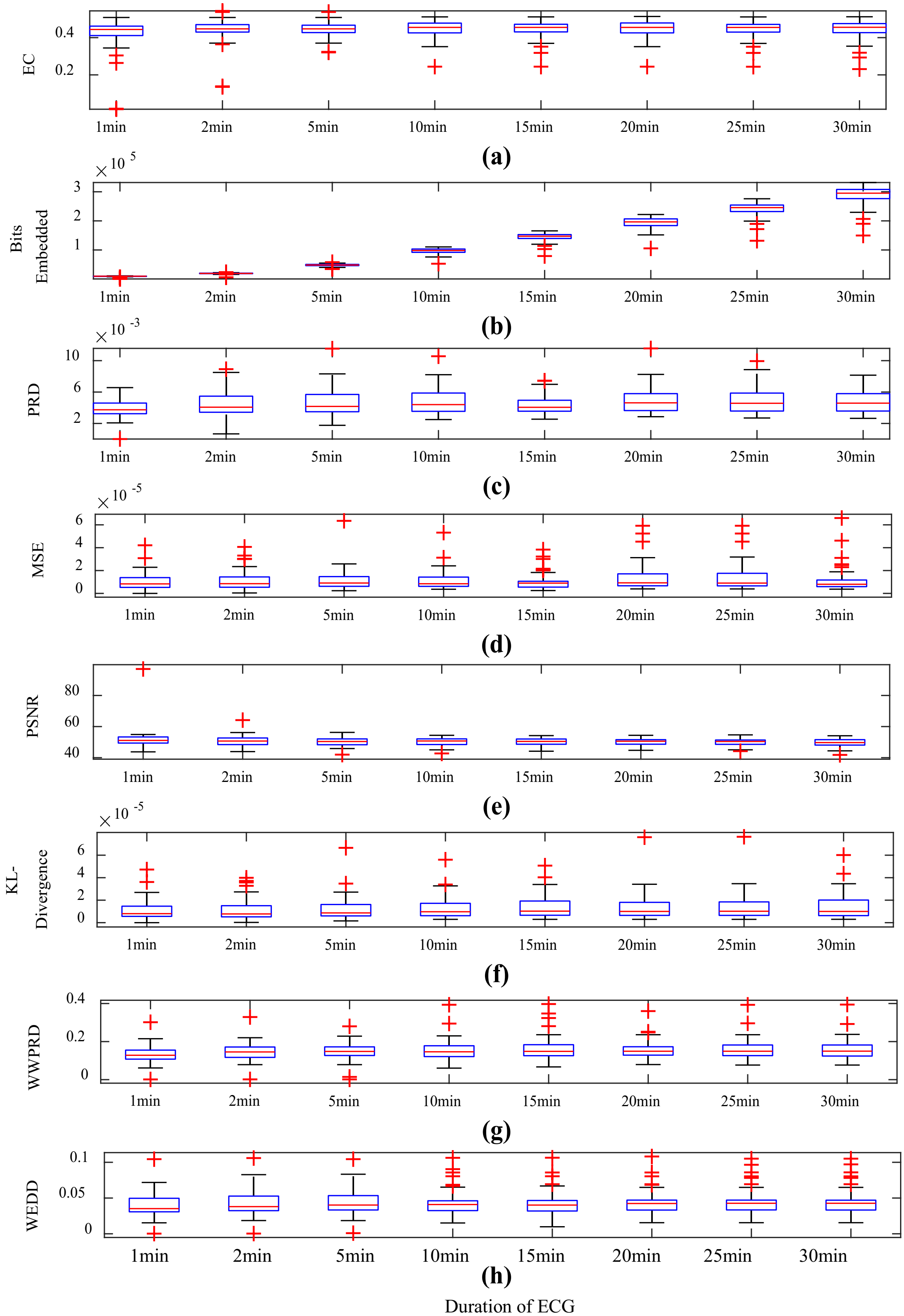


Fig. 6 Box-plot representation of average: **a** EC, **b** bits embedded, **c** PRD, **d** MSE, **e** PSNR, **f** KL-Divergence, **g** WWPRD, **h** WEDD versus duration of ECG signal for all 48 ECG records of MIT-BIH Arrhythmia database for different durations

Table 5 Average variation in distortion and EC measuring metrics by varying ECG signal durations for all 48 ECG records of MIT-BIH Arrhythmia database

Metrics	Duration (min)							
	1	2	5	10	15	20	25	30
EC	0.4166	0.4368	0.4441	0.4485	0.4455	0.4487	0.4450	0.4404
Bits embedded	9066	18,871	47,971	96,876	144,302	193,842	240,351	285,420
PRD	0.0039	0.0045	0.0046	0. 0047	0. 0044	0.00489	0.00482	0.00473
PSNR	52.035	50.62	50.39	50.28	50.30	50.2	50.189	49.80
MSE	1.06×10^{-5}	1.12×10^{-5}	1.12×10^{-5}	1.13×10^{-5}	1.03×10^{-5}	1.34×10^{-5}	1.39×10^{-5}	1.18×10^{-5}
KL-Divergence	1.10×10^{-5}	1.15×10^{-5}	1.22×10^{-5}	1.29×10^{-5}	1.39×10^{-5}	1.4×10^{-5}	1.42×10^{-5}	1.46×10^{-5}
WWPRD	0.13084	0.1450	0.1454	0.1508	0.1576	0.1563	0.1579	0.15633
WEDD	0.0392	0.0424	0.0428	0.04102	0.0419	0.04396	0.04403	0.0448

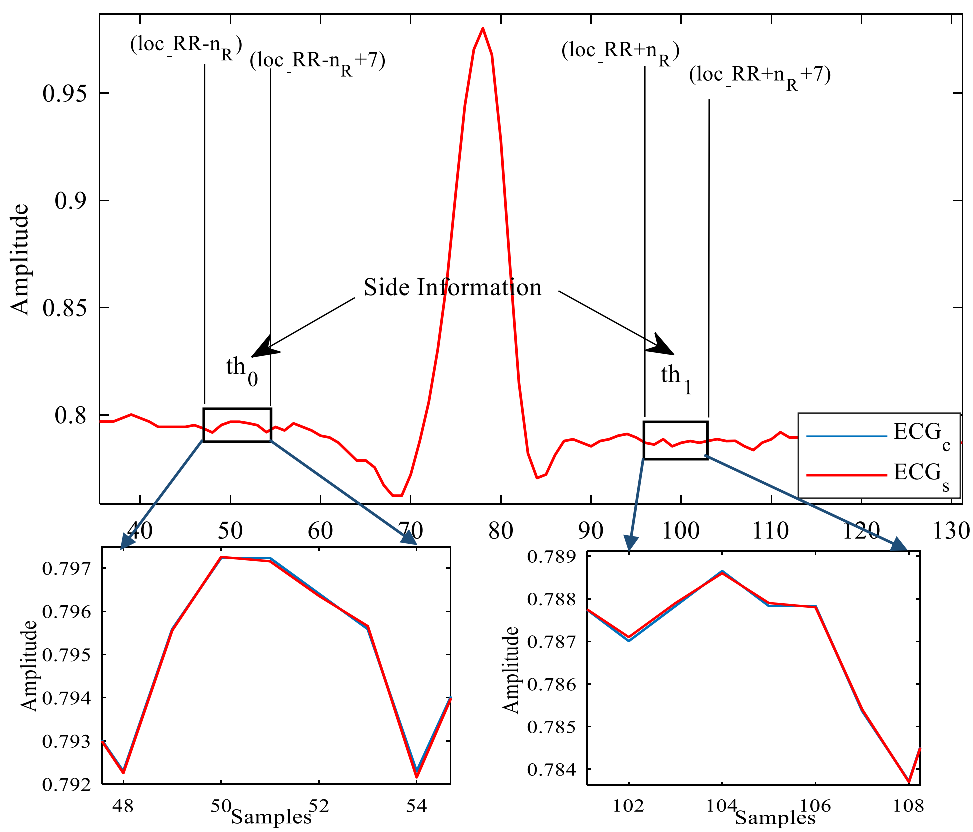


Fig. 7 Variation in amplitude of ECG signal after inserting side information in QRS region

Security analysis

The security of the patient's personal information is the key feature of steganography and the security performance of the proposed method is analysed on the basis of key space and key sensitivity.

Key space analysis

Key space is defined as the length of the key used for steganography and for a good stego-system it should be wider atleast more than 2^{128} [23]. In the proposed algorithm, CLS map is used to generate three chaotic sequences with different initial conditions and control parameters. Thus the key generated composed of (i) initial parameters of these chaotic maps (ii) scaling factor (z_1 and z_2). If the initial parameters of chaotic maps are set to the precision of 14 decimals and z_1 and z_2 are set to 3 decimals then according to IEEE 754 standard [36], the keyspace of the proposed algorithm is $2^{64\times6+64+32\times2} \approx 2^{484}$ bits which is sufficiently large to resist the brute attack force. The structure of the key is given in Fig. 9.

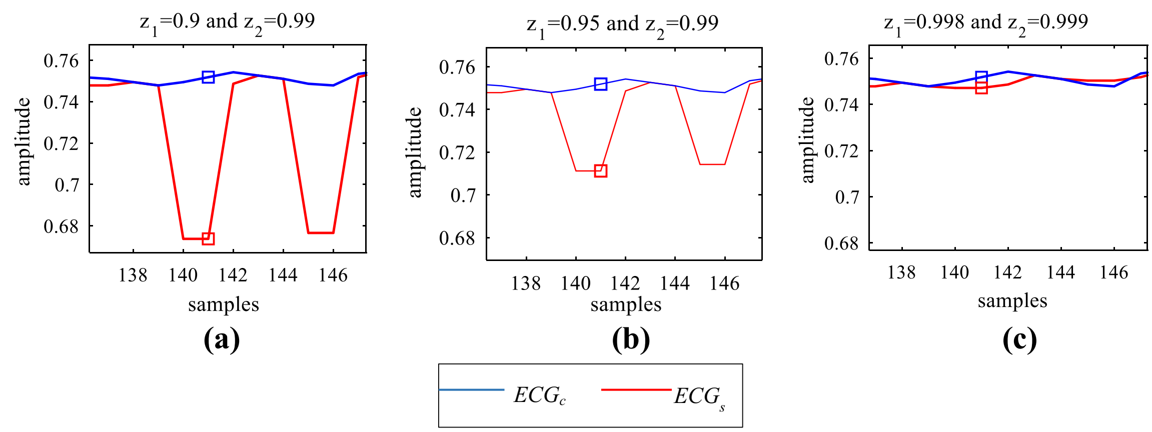


Fig. 8 Variation in amplitude of stego-ECG with respect to cover-ECG at embedding location for different values of z_1 and z_2: **a** 0.9 and 0.99, **b** 0.95 and 0.99, **c** 0.998 and 0.999

Fig. 9 Structure of the key space

x_{n1} (64 bits)	r_{o1} (64 bits)	x_{n2} (64 bits)	r_{02} (64 bits)	x_{n3} (64 bits)	r_{03} (64 bits)	L_n (64 bits)	z_1 (32 bits)	z_2 (32 bits)

Key sensitivity analysis

Key sensitivity defines the amount of change that occur in the extracted secret information with a small change in the key. It is an important security measure to estimate the sensitivity of the key which in turn measures the strength of the developed algorithm. Since chaotic maps are very sensitive to initial conditions and control parameters, a minute change at 14th precision level can modify the chaotic sequence completely resulting in retrieval of incorrect information. The findings are well illustrated with the help of an example in Fig. 10 where 1 kb of secret information is embedded in 2500 samples of record 100 of MIT-BIH Arrhythmia database. The correct key extracts the secret information with zero BER whereas the incorrect key surges the erroneous information with BER of 0.4998. It is exhibited from the findings that the impact of using incorrect key is significant on the secret information, however it does not influence the quality of stego-signal.

The key structure consists of {x_{01}, r_{01}, x_{02}, r_{02}, x_{03}, r_{03}, L_n, z_1, z_2}

Key **K** = {0.897655762990, 3.99534613560 11, 0.933453564978, 3.886954532619, 0.994357334262, 3.973256778521, 500000, 0.998, 0.999}

The confidential information consists of name, patient ID, age, sex, phone no, blood pressure, body temperature, glucose level is stored as

Confidential Information : 'Neetika Soni, 123456789, 37, F, 9876543210, 130/80, 99.1F, 100 mg/dL'

Comparison of the proposed method with existing steganography techniques

Table 6 shows the comparison of the proposed method of ECG steganography with the recently published approaches over various metrics to measure the quality of the stego-ECG. The proposed method outperforms the existing techniques in terms of EC at low values of PRD, KL-Divergence, MSE, RMSE and rRMSE. As compared to 2800 bits embedded at 0.59% PRD using DWT and SVD approach suggested by Jero et al. [12], the proposed technique embeds 32,032 bits at 0.4% PRD on 76,800 ECG samples of 48 records of MIT-BIH Arrhythmia database. Average EC achieved in [11] on first 4096 samples of 10 ECG records of same database was only 0.078 at average RMSE and rRMSE = 18.83 and 0.151 respectively. Whereas the average EC achieved by the proposed method is 3.67 at average RMSE and rRMSE of 4.22 and 4.3×10^{-3} respectively. The number of bits embedded, KL-Divergence and MSE obtained with the proposed approach are 5790, 1.02×10^{-4} and 4.86×10^{-5} respectively as compared to 4016, 0.1448 and 2.94 respectively obtained by Jero et al. [13] on MIT-BIH NSR database. Furthermore, inspite of embedding the side information, the SNR = 47.62 achieved by the proposed algorithm is higher than SNR = 42.27 achieved by coefficient alignment approach [15] on 30, 000 ECG samples of MIT-BIH Arrhythmia database. The proposed method achieve EC = 0.45 at low PRD = 4.8×10^{-3} as compared to EC = 0.4 at PRD = 0.26 as achieved by Pandey et al. [16]. Hence it is evident from the performance obtained that the proposed method transcends over the other state of the art

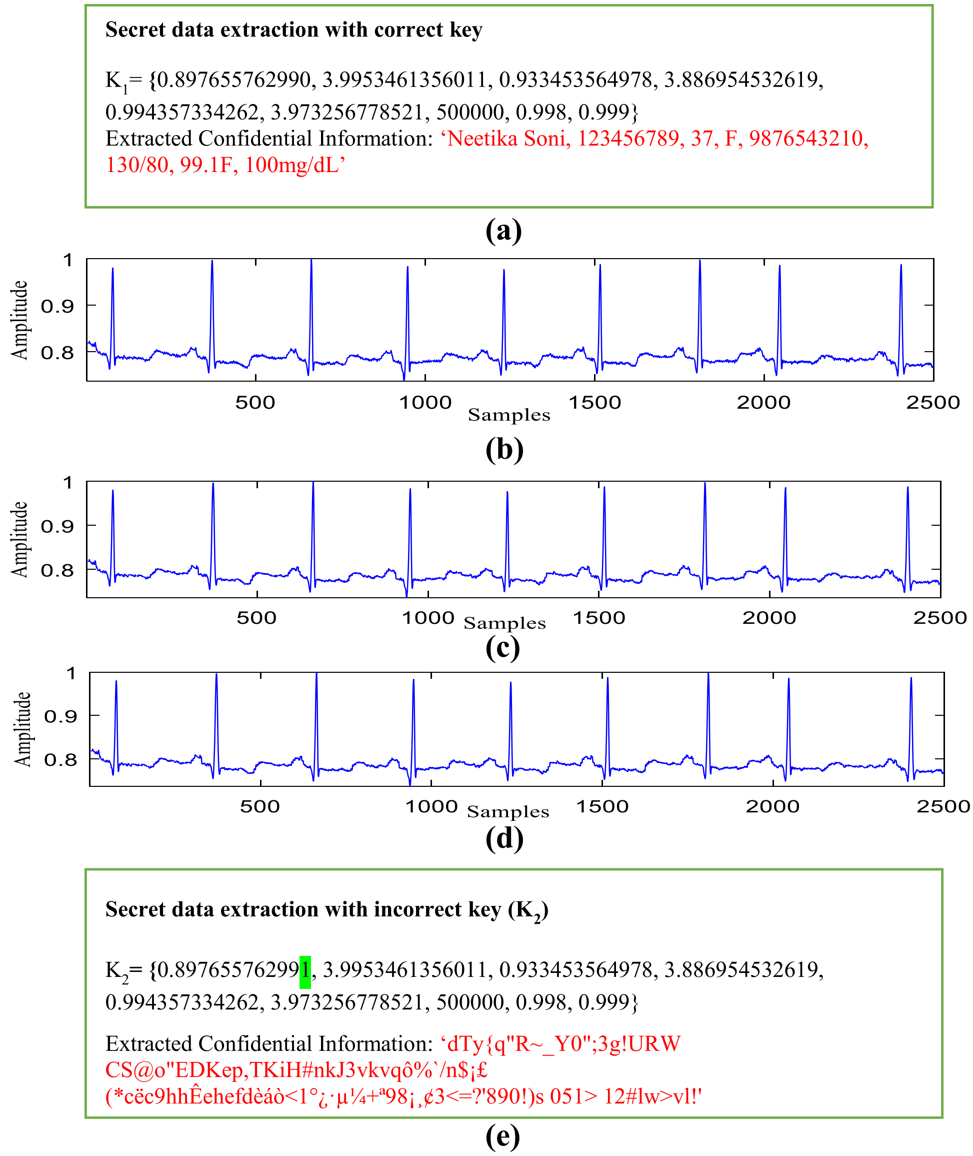


Fig. 10 **a** Secret information extracted with correct key (K_1), **b** original ECG, **c** ECG recovered with correct key, **d** ECG recovered with incorrect key (K_2), **e** secret information extracted with incorrect key

steganography techniques in terms of higher EC and low PRD, MSE, rRMS, KL-Divergence etc. thus confirming the efficacy of the proposed method.

Discussion and conclusion

A chaotic map based technique of ECG steganography to embed patient's confidential information in spatial domain is proposed by exploring the non-QRS region of ECG signal. OLS algorithm has been formulated to select the random embedding location pairs using chaotic maps by R-peak magnitude based adaptive thresholding of ECG trains. This formulated approach outperformed other ECG steganographic techniques by achieving high EC, PSNR and lower PRD, MSE and KL-Divergence. Moreover clinically robust measures; WWPRD and WEDD have also been evaluated to examine the performance of proposed method. Typically for 10 min duration of ECG signal of MIT-BIH Arrhythmia database, average PRD, MSE, PSNR, KL-Divergence, WWPRD and WEDD are 4.7×10^{-3}, 1.13×10^{-5}, 50.28, 1.29×10^{-5}, 0.15 and 0.04 respectively have been achieved with average maximum payload of 96,876 bits and for 30 min ECG durations the results are 4.73×10^{-3}, 1.18×10^{-5}, 49.80, 1.46×10^{-5}, 0.156 and 0.0448 at average maximum payload of 285,420 bits. Performance of the proposed method has also been evaluated at varying ECG signal durations. Besides standard database, self-recorded data of 20 subjects has also been employed to verify the versatility of the proposed approach. An average PRD, MSE, PSNR, MAE, KL-Divergence, WWPRD and WEDD for ECG duration of 10 min observed are 0.016, 3.38×10^{-5}, 46.03, 6.42,

Table 6 Comparison of the proposed method with the existing techniques

Technique used	Database used	Parameters studied	Existing/proposed method
DWT and SVD Jero et al. [12]	MIT-BIH Arrhythmia 76,800 ECG samples (on 48 records)	Payload (bytes)	350/4004
		PSNR	50.44/50.42
		PRD%	0.59/0.4
		KL-Divergence	$0.15/1.22\times10^{-5}$

		Record no.	Bits embedded (bits) existing/proposed method	RMSE existing/proposed method	rRMSE existing/ proposed method	Amplitude similarity existing/proposed method
Transform domain quantization Chen et al. [11]	MIT-BIH Arrhythmia 4096 ECG samples of 10 records (100–109)	100	32/1782	14.907/2.3672	$0.054/2.4\times10^{-3}$	100/99.94
		101	32/1878	18.197/3.3835	$0.132/3.5\times10^{-3}$	100/99.93
		102	32/1809	14.583/3.404	$0.080/3.5\times10^{-3}$	99.92/99.9394
		103	32/1767	22.847/3.5063	$0.53/3.5\times10^{-3}$	99.96/99.948
		104	32/1521	21.987/6.2986	$0.45/6.2\times10^{-3}$	99.8/99.93
		105	32/1665	21.130/3.6854	$0.076/3.7\times10^{-3}$	99.93/99.936
		106	32/1749	15.671/6.4604	$0.024/6.4\times10^{-3}$	99.96/99.942
		107	32/1125	17.488/7.1109	$0.087/7.2\times10^{-3}$	99.96/99.94
		108	32/35	16.678/1.2015	$0.01/1.3\times10^{-3}$	99.94/100
		109	32/1689	24.879/4.9024	$0.067/5.2\times10^{-3}$	99.94/99.96

		Parameters studied	Existing/proposed method
Curvelet transform Jero et al. [13]	MIT-BIH NSR	PSNR	43.44/45.75
		PRD	0.0132/0.013
		Payload (bits)	4016/5790
		KL-Divergence	$0.1448/1.02\times10^{-4}$
		MSE	$2.94/4.86\times10^{-5}$
DWT with SVD and CACO Jero et al. [14]	MIT-BIH NSR (on all 18 records)	PSNR	34.46/43.4
		PRD	0.06/0.02
		Payload (kb)	3.07/4.4
		KL-Divergence	$2.04/5.93\times10^{-4}$

		Parameters studied	Existing (without side information)	Proposed method (with side information)
Coefficient alignment Yang and Wang [15]	MIT-BIH Arrhythmia 30,000 ECG samples (on 48 records)	EC	0.48/0.44	
		SNR	42.27/47.6207	
		MAE	1.84/1.89	

		Parameters studied	Pandey et al./Proposed method
CMSaVD Pandey et al. [16]	MIT-BIH Arrhythmia 20 min ECG samples (on all the 48 records)	PRD	$0.26/4.8\times10^{-3}$
		KL-Divergence	$3.34\times10^{-6}/1.4\times10^{-5}$
		EC	0.4/0.45
		PSNR	55.49/50.2
		WWPRD	0.10/0. 15
		WEDD	0.02/0.04

1.8×10^{-4}, 0.13 and 0.037 respectively have been achieved with average payload of 102,571 bits. To ensure its implementation in case of irregular ECGs, the algorithm is also tested on database with abnormal ECG records such as CU-VT, BIDMC-CHF and PTB (leads I, II and III). Three coupled chaotic maps used in the proposed approach induce sufficiently large key space. Furthermore, key sensitivity analysis has also been performed to evaluate the hiding capability and sensitiveness to the key parameters. The novelty of the proposed approach lies in its capability to protect the morphological features of ECG signal despite high EC. Hence the proposed method is recommended as a highly effective and reliable approach for ECG steganography.

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

Compliance with ethical standards

Conflict of interest No conflict of interest.

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

Appendix

Performance evaluation metrics

Statistical parameters

- PRD is the measure of acceptable fidelity and degree of distortion and it is given as [10, 37]:

$$PRD = \sqrt{\frac{\sum_{n=1}^{N} \left(x_c(n) - x_s(n)\right)^2}{\sum_{n=1}^{N} \left(x_c(n)\right)^2}}$$

  where $x_c(n)$ is the nth sample of original ECG signal; $x_s(n)$ the nth sample of stego-ECG.
- PRD1024 is similar to PRD, but in this base value of 1024 is removed which was added in MIT-BIH Arrhythmia database [37].

$$PRD\,1024 = \sqrt{\frac{\sum_{n=1}^{N} \left(x_c(n) - x_s(n)\right)^2}{\sum_{n=1}^{N} \left(x_c(n) - 1024\right)^2}}$$

- The normalised PRD (PRDN) does not depend upon the mean of signal value [37].

$$PRDN = \sqrt{\frac{\sum_{n=1}^{N} \left(x_c(n) - x_s(n)\right)^2}{\sum_{n=1}^{N} \left(x_c(n) - mean\right)^2}}$$

- PSNR represents the measure of peak error and expressed in terms of logarithmic decibels (dB) [12]

$$PSNR = 20\log_{10}\left(\frac{\max\left(\left(x_c(n)\right)\right)}{\sqrt{1/N \sum_{n=1}^{N} \left(x_c(n) - x_s(n)\right)^2}}\right)$$

- SNR is a measure of degree of noise energy introduced in decibel (dB) scale [15].

$$SNR = 10\log_{10}\left(\frac{\sum_{n=1}^{N} \left(x_c(n)\right)^2}{\sum_{n=1}^{N} \left(x_c(n) - x_s(n)\right)^2}\right)$$

- MSE measures the difference between the original and stego-ECG signal as [35]

$$MSE = \frac{1}{N}\sum_{n=1}^{N} \left(x_c(n) - x_s(n)\right)^2$$

- MAE is defined as [15]

$$MAE = \frac{1}{N}\sum_{n=1}^{N} \left|x_c(n) - x_s(n)\right|$$

- KL-Divergence measures the distance between the histograms of the cover and stego signals. It can be expressed as [13]

$$D\left(p_c, p_s\right) = \int p_c(x)\ \log\frac{p_s(x)}{p_c(x)}dx$$

  where D is the KL-Divergence, p_c is the probability of the cover signal and p_s is the probability of the stego-ECG signal.

Clinical measures

- WWPRD is method of finding error based on the weighting criteria where the subbands of the transformed ECG signal are multiplied with the computed weights [10, 35]. It is given as

$$WWPRD = \sum_{j=0}^{j=L} w_j PRD_j$$

$$\text{where } w_j = \frac{\sum_{i=1}^{n_j} \left|a_j(i)\right|}{\sum_{j=1}^{L+1}\sum_{i=1}^{n_j} \left|a_j(i)\right|};\quad j = 1,\ 2, \ldots ..L + 1$$

  w_j are the weights computed from ECG signal, $j = 0$ represents the approximate subband, j = 1 to L represents the detail subband, n_j is the number of wavelet coefficient in the jth subband, a_j is an original coefficient within jth subband.

- WEDD [35, 37] calculates the energy of the wavelet coefficients is utilized to compute the dynamic weight of each subband. It is given as

$$WEDD = \sum_{j=0}^{j=L} w_j^* PRD_j$$

$$w_j^* = \frac{\sum_{i=1}^{n_j} a_j^2(i)}{\sum_{j=1}^{L+1} \sum_{i=1}^{n_j} a_j^2(i)} \quad \text{where } j = 1,\ 2, \ldots ..L + 1$$

w_j^* is the weight computed from jth subband.

- EC is defined as the hiding capacity of the signal and expressed as the ratio between the total number of hidden secret bits and the total number of samples in the ECG signal.
- BER gives the measure of percentage of data loss [12] and can be written as.

$$\mathrm{BER} = \frac{\text{Bits retrieved correctly}}{\text{Total bits embedded}} \times 100$$

References

1. Goceri E, Songul C (2018) Biomedical information technology: Image based computer aided diagnosis systems. In International conference on advanced technologies, Antalya, pp 132
2. Goceri E, Songul C (2018) Mobile health technologies for patients with mental illness. In International conference on advanced technologies, Antalya, pp. 146
3. English A, Summers R, Lewis J, Coleman C (2015) Confidentiality, third-party billing & the health insurance claims process: implications for title X. Accessed 11 Nov 2015
4. Subhedar MS, Mankar VH (2014) Current status and key issues in image steganography: a survey. Comput Sci Rev 13–14:95–113
5. Pandey A, Singh B, Saini BS, Sood N (2016) A joint application of optimal threshold based discrete cosine transform and ASCII encoding for ECG data compression with its inherent encryption. Australas Phys Eng Sci Med 39:833–855
6. Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. Computers 31(2):26–34
7. Nambakhsh MS, Ahmadian A, Zaidi H (2011) A contextual based double watermarking of PET images by patient ID and ECG signal. Comput Methods Programs Biomed 104(3):418–425
8. 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
9. Ibaida A, Khalil I, Al-Shammary D (2010) Embedding patients confidential data in ECG signal for healthcare information systems. In: 32nd international conference of IEEE Buenos Aires, Argentina, pp. 3891–3894
10. 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
11. Chen ST, Guo YJ, Huang HN, Kung WM, Tseng KK, Tu SY (2014) Hiding patients confidential data in the ECG signal viaa transform-domain quantization scheme. J Med Syst 38(6):1–8
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. Biomed Signal Process Control 22:161–169
14. Jero SE, Ramu P, Ramakrishnan S (2016) Imperceptibility—robustness trade-off studies for ECG steganography using continuous ant colony optimization. Expert Syst Appl 49:123–135
15. Yang CY, Wang WF (2016) Effective electrocardiogram steganography based on coefficient alignment. J Med Syst 40:66
16. 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
17. Malmivuo J, Plonsey R (1995) Bioelectromagnetism: principles and applications of bioelectric and biomagnetic fields. Oxford University Press, New York
18. Poole JE, Singh JP, Birgersdotter-Green U (2016) QRS duration or QRS morphology: what really matters in cardiac resynchronization therapy. J Am Coll Cardiol 67(9):1104–1117
19. Zhou Y, Bao L, Chang CLP (2014) A new 1D chaotic system for image encryption. Sig Process 97:172–182
20. Hua Z, Zhou Y, Pun CM, Chang CLP (2015) 2D sine logistic modulation map for image encryption. Inf Sci 297:80–94
21. Kanso A, Smaoui N (2009) Logistic chaotic maps for binary numbers generations. Chaos Solitons Fractals 40(5):2557–2568
22. 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
23. Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R (2016) Chaos based crossover and mutation for securing DICOM image. Comput Biol Med 72: 170–184
24. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E et al (2010) A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Testing, Washington, DC
25. http://www.physionet.org/cgi-bin/atm/ATM
26. Pan J, Tompkins WJ (1985) A real-time QRS detection algorithm. IEEE Trans Biomed Eng BME 32(3):230–236
27. Slimane ZEH, Naït-Ali A (2010) QRS complex detection using empirical mode decomposition. Digit Signal Proc 20(4):1221–1228
28. Saini I, Singh D, Khosla A (2013) QRS detection using K-Nearest Neighbor algorithm (KNN) and evaluation on standard ECG databases. J Adv Res 4:331–344
29. Rodríguez R, Mexicano A, Bila J, Cervantes S, Ponce R (2015) Feature extraction of electrocardiogram signals by applying adaptive threshold and principal component analysis. J Appl Res Technol 13:261–269
30. Carr JJ, Brown JM (2004) Introduction to biomedical equipment technology, 4th edn. Pearson Education, New Delhi
31. Yang H, Sun X, Sun G (2009) A high-capacity image data hiding scheme using adaptive LSB substitution. Radio Eng 18(4):509–516
32. Chen J, Itoh S (1998) A wavelet transform-based ECG compression method guaranteeing desired signal quality. IEEE Trans Biomed Eng 45(12):1414–1419

33. Al-Fahoum AS, Ishijima M (1993) Fundamentals of the decision of optimum factors in the ECG data compression. IEICE Trans Inf Syst E76-D(12):1398–1403
34. 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
35. Manikandan MS, Dandapat S (2007) Wavelet energy based diagnostic distortion measure for ECG. Biomed Signal Process Control 2(2):80–96
36. Rajaraman V (2016) IEEE standard for floating point numbers. Resonance 21(1):11–30
37. Pandey A, Singh B, Saini BS, Sood N (2016) A 2D electrocardiogram data compression method using a sample entropy-based complexity sorting approach. Comput Electr Eng 56:36–45