Computing (2021) 103:1883–1917
https://doi.org/10.1007/s00607-020-00881-y

SPECIAL ISSUE ARTICLE

Bio-signal data sharing security through watermarking: a technical survey

N. Sharma[1] · A. Anand[1] · A. K. Singh[1]

Received: 14 August 2020 / Accepted: 23 November 2020 / Published online: 6 January 2021

Abstract
Due to smart healthcare systems highly connected information and communications technologies, sensitive medical information and records are easily transmitted over the networks. However, stealing of healthcare data is increasing crime every day to greatly impact on financial loss. In order to this, researchers are developing various cost-effective bio-signal based data hiding techniques for smart healthcare applications. In this paper, we first introduce various aspects of data hiding along with major properties, generic embedding and extraction process, and recent applications. This survey provides a comprehensive survey on data hiding techniques, and their new trends for solving new challenges in real-world applications. Then, we survey the various notable bio-signal based data hiding techniques. The summary of some notable techniques in terms of their objective, type of data hiding, methodology and database used, performance metrics, important features, and limitations are also presented in tabular form. At the end, we discuss the major issues and research directions to explore the promising areas for future research.

Keywords Data hiding · Watermarking · Steganography · Bio signals · Security

Mathematics Subject Classification 68U10

1 Introduction

With the widespread advancement of Information and Communications Technologies (ICT), it has become possible to share diagnosis data of the patient along with the physiological signals to achieve better tele-medicine, tele-diagnosis, tele-consultation and healthcare services [1]. Now a days sharing of biomedical data and medical images over wireless media becomes common to get the facility of remote healthcare system [2]. These signals are widely used in medical services for both

✉ A. K. Singh
amit_245singh@yahoo.com

[1] Department of CSE, NIT Patna, Patna, Bihar, India

diagnoses and interpretation of health status of any individual. Now a days different "Point-of-Care" (POC) services like POC documentation, POC testing are used to provide a cost-effective, fast and 24×7 medical service to the patients [3]. Further, these POC services are used to collect patient's data including temperature, biomedical signals, blood pressure and glucose level using sensors in short intervals [4]. This data is then sent to healthcare experts using various techniques [4]. It helps in saving patient's life and reduces burden on hospitals. Additionally, medical records including patients' details and other significant medical data is stored on the cloud which is handled by various hospitals and healthcare center [5]. This information adds up in taking more appropriate decisions by the healthcare professionals. On other hand, transfer of the medical records might bring many issues [2,5]. Generally, medical records are transmitted using digital imaging and communications in medicine (DICOM) standard [6]. Here, a header is appended with the DICOM images which carry the important patient data. However, DICOM is not much effective for reliable healthcare communication [6]. In case of sharing the bio-signals through the open network it should be noted that the distortion of the signal at the time of receiving should be minimum. To solve this problem machine learning algorithms is used at the receiver side for real time feature extraction and binary classification of the received signal [7,8]. Presently, Coronavirus pandemic has been declared as a global health emergency by the World Health Organization (WHO) [9]. During these times, a lot of significant patient data is stored in the local server of the medical centre and distributed from once centre to other hospitals via unsecure network. However, this may lead to high risk of data security and privacy in the current advanced healthcare systems [10]. In order to solve these issues, data hiding techniques are used to provide confidentiality, integrity and authenticity requirements of medical data [11]. Some notable applications of data hiding approaches are illustrated in Fig. 1 [12]. As pointed out by various researchers, watermarking is more popular and robust among similar technologies (see Fig. 2) that facilitate embedding information into digital content for authentication or protection purpose of healthcare data [2,5,13]. Table 1 indicated the clear difference between popular data hiding techniques. Watermarking technique can be used for hiding data efficiently within cover bio signal. Special domain techniques like LSB embedding and correlation modifications are widely used as those are fast and simple but are more prone to attacks. Frequency domain techniques like discrete wavelet transform (DWT) and discrete cosine transform (DCT) are more advanced techniques

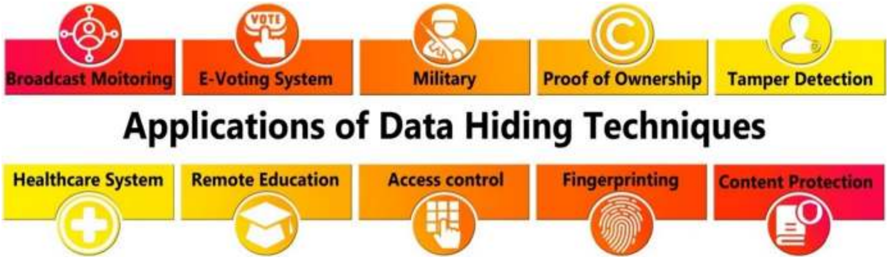


Fig. 1 Notable applications of data hiding technique

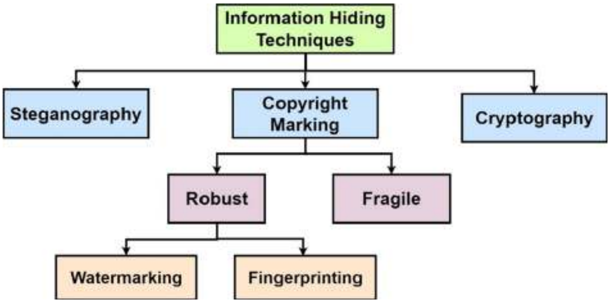


Fig. 2 Different types of data hiding [17]

which provides better security and robustness at the time of insertion and extraction from the signal [6]. Bio-signals are very important for diagnosis purposes and are classified in two types; action potential and event related potential. Action potential includes electrocardiography (ECG), electroencephalography (EEG), and electromyogram (EMG). However, electrogastrogram (EGG), phonocardiogram (PCG), carotid pulse (CP) are of event related potentials [14]. Different types of electrical and physiological activities are captured with physiological instruments and these measurements are used in biomedical signal processing to give the health status of a patient [15]. It is very important to maintain the authenticity and integrity of these bio signal data while transmission over the unsecure network. Watermarking can be a suitable approach to add some secret data within the bio signals to resolve any ownership conflict, tracking of data and content authenticiation [16].

The main contributions of this paper are given as follows.

- We introduce the preliminary concepts of data hiding techniques and its importance in advanced healthcare domain, noticeable applications, important properties and embedding and extraction process.
- We present a brief introduction about different types of bio-signals. The bio-signal includes ECG, EEG, EMG, EGG, PCG, and CP.
- We survey the various notable bio-signal based data hiding techniques with their objective, type of data hiding, methodology and database used, performance metrics, important features, and limitations
- Finally, we investigate the potential issues that existing approaches of bio-signals based data hiding face.

2 Basic properties of watermarking techniques

Watermarking techniques facilitate embedding sensitive information into digital content for authentication or copyright protection purpose. Robustness, invisibility, and capacity are the notable properties for any watermarking system. However, it has been proven that maintaining a trade-off between these parameters is very important [12]. The relationship between these parameters is clearly illustrated in Fig. 3. The basic properties of watermarking techniques are given as follows [12,13].

Table 1 Difference between different types data hiding techniques

Property	Watermarking	Steganography	Cryptography
Definition	The secret data, also called watermark, is embedded within the cover media [18]	By manipulating and scrambling the pixels the secret data is embedded within host data [19]	Meaningful content is transformed into encoded form to provide security [19]
Purpose of use	Proof the ownership i.e. authentication purpose and to provide robustness [13,20]	To provide confidentiality and is highly secure [13,20]	Maintain the integrity of the data. Provides data secrecy, information uprightness, verification and non-repudiation [20]
Cover image selection [21]	Here the cover image should be related with the embedded message	The cover image may be or may not be related with the embedded message	There is no need of relating cover image with embedded message
Communication type	One-to-many [13,22]	One-to-one [13]	One-to-many [13]

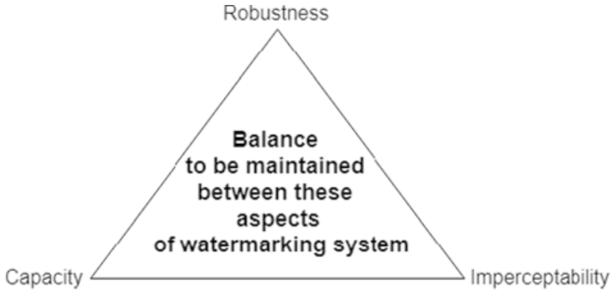


Fig. 3 Relationship between major parameters of watermarking

- **Imperceptibility** refers the similarity of cover and marked data will not be noticeable for any viewer. Data should be highly imperceptible for a reliable transmission.
- **Robustness** demands the hidden (secrete) data should be resistant to any kind of attacks.
- **Embedding capacity** refers to the amount of secret information imperceptibly hidden into cover.
- **Security** refers that the system should be designed in such a way that no unauthorized user can access, remove or alter the watermark easily.
- Detectability refers that the marked data should be extracted by authorized users only.
- **Computational complexity** is the cost associated with the process of data insertion and extraction from the cover**.**
- **False positive rate** refers to the probability of recognizing non-watermark portion of the cover as watermarks.

3 Generic embedding and extraction process

The basic process of data hiding method is shown in Fig. 4. In the embedding process, the secret data is marked within the cover bio-medical signal by using some secret key and data hiding algorithms. In this stage, other techniques like encryption, encoding, scrambling and hashing functions can also be applied to ensure the security of the secret signal while transmitting through the open unsecure network [12]. In the receiver side, the same key is used to recover the hidden data from the marked signal.

Generally, watermarking system is classified in to blind, semi-blind and non-blind [12,23,24]. In blind system, cover information is not required for the recovery of hidden mark. However, cover information is used for the recovery of hidden mark in the non-blind system. In semi-blind system, cover information is not required and only know about the watermark for the recovery of hidden mark. These systems are frequently used in various potential applications [23,24].

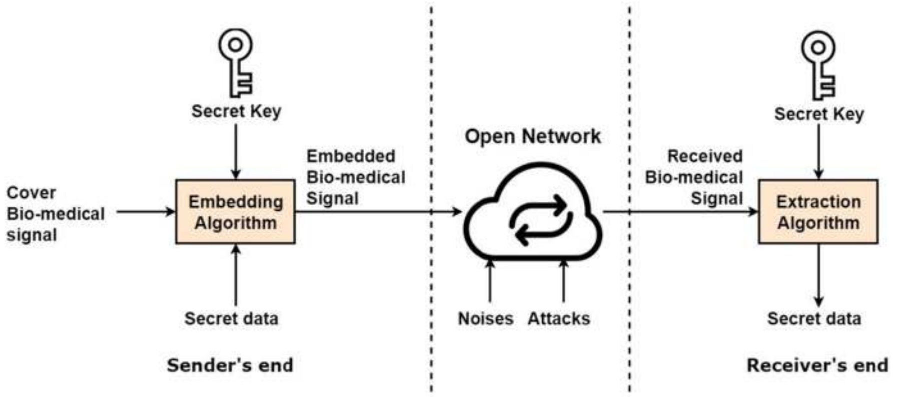


Fig. 4 Embedding and extraction process in data hiding for bio-medical signals [12]

4 Performance metrics

Different metric is used to measure performance of the bio-signals based data hiding algorithms. Some of the notable metrics are discussed below.

4.1 Bit error rate (BER)

BER is defined as the percentage of erroneous bits (say B_{err} may occur in the received data) in comparison with total number of bits transmitted (B_{Total}) over the channel [12]. BER should be ideal for any reliable watermarking system

$$BER = \frac{B_{err}}{B_{Total}} \times 100\% \tag{1}$$

4.2 Peak signal to noise ratio (PSNR)

The PSNR refer the similarity between the cover and the marked signal. It is the ratio between maximum amplitude i.e., peak of cover ECG signal and the mean square error between the cover and watermarked ECG signal. High value of PSNR defines that the method is highly imperceptible [25]. It is defined as,

$$PSNR = 20\log_{10}\left(\frac{\max |x_{c|}}{\sqrt{\frac{1}{N}\sum_{n=1}^{N} |x_c - x_w|^2}}\right) \tag{2}$$

Here N represents the total number of samples, x_c and x_w are the amplitude of the cover and watermarked ECG signals.

4.3 Percentage residual difference (PRD)

PRD is used to measure the imperceptibility of the secret data by comparing the distortion between the cover bio-signal (x_c) and the marked bio-signal $\left(x_w\right)$. It measures the distortion level of two bio-signals as follows [26,27]:

$$PRD\% = \sqrt{\left(\frac{\sum_{i=1}^{N}\left(x_c - x_w\right)^2}{\sum_{i=1}^{N}\left(x_c\right)^2}\right)} \times 100 \tag{3}$$

where, N represents the total number of samples in the bio-signal.

4.4 Kullback–Leibler (KL) divergence

KL divergence is used to measure the distance between the histograms of the cover and marked signal. The distance can be calculated by using the following equation [25]:

$$D\left(p_c, p_w\right) = \int p_c(x) \log \frac{p_w(x)}{p_c(x)} dx \tag{4}$$

where D represents the KL divergence, p_c and p_w represent the probability of cover and watermarked ECG signals.

5 Related work

In this section, we provide basic concepts of important bio-signals and then moved to surveys focused on ECG, EEG, EMG, EGG, PCG, and CP based state-of-the-art data hiding are discussed in detail.

5.1 ECG based data hiding techniques

ECG signal is a graphical representation generated by the electrical activity of the heart and is very important to detect any cardio vascular disease. One ECG signal consists of various cardiac cycles and each cycle is composed of P wave followed by QRS complex and a T wave [6]. The maximum energy is concerted in the QRS complex portion of the ECG signal. As the size of the ECG signal is good enough, so some confidential data of the patient can be hidden here for a secure transmission [26]. The Normal ECG samples are presented in Fig. 5. Watermarking and steganography is used to embed data into 1-D and 2-D ECG signals to provide secure transmission over public network [25,28]. It is established that the secret data can be

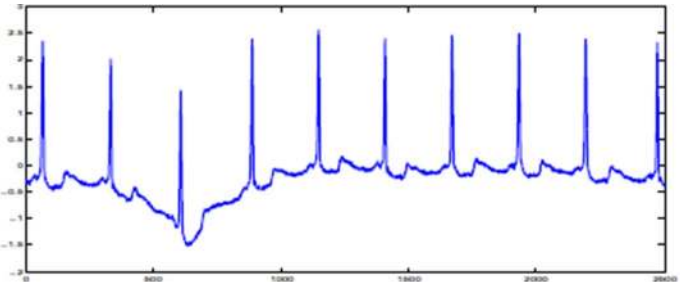


Fig. 5 Normal ECG sample [31]

marked within the QRS region or non-QRS region of the signal as for the requirements. To avoid any distortion of the original signal, non-QRS region is used to embed the watermark [29]. To enhance the privacy of the secret data, it can be hidden in any position of the ECG signal without making any kind of distortion or quality degradation [30].

Some of the recent ECG based data hiding are discussed below.

In [6], Dey et al. proposed self-recovering blind watermarking method for hiding binary data into ECG signal using stationary wavelet, spread-spectrum and quantization. It is useful for the authentication of source of information. The author reduces the complexity by implementing self-authentication and removing the concept of sharing session key between sender and receiver. The suggested method is robust and can also be used for copyright protection. Ibaida et al. proposed an imperceptible steganography technique to securely transmit confidential details of the patient [26]. It uses Shift Special Range Transform for concealing the confidential details of patients into most significant positions of the ECG signal. The performance of this method is measured by PRD value and it experimentally depicts that security of the hidden data is high. In [29], Zheng and Qian proposed a reversible data hiding method to imperceptibly embed the watermark data into the non-QRS region of the ECG signal. The cover signal is decomposed using Haar based lifting wavelet transform. Prior to embedding the secret data is scrambled using Arnold transform to provide more security. Authors of [31] proposed watermarking technique where bio medical information is marked into ECG signal using LSB embedding technique. Also, the ECG signal is pre-processed using simple linear transformation technique. It provides patient authentication with low complexity.

Sanivarapu et al. proposed a DWT based robust watermarking method for hiding patient data into the ECG signal [32]. Patient information is embedded as a QR image to improve imperceptibility and embedding capacity. Further, Pan–Tompkins algorithm is used to convert the 1D-ECG signal to 2D-ECG image. The proposed work outperforms in terms of imperceptibility when compared with existing state-of-the-art [33,34]. Nambakhsh et al. proposed lossless dual watermarking technique to securely transmit ECG signal and patient ID and avoid diagnosis mismatching [35]. In this method, ECG signal and patient ID are considered as watermarks which are embedded into PET image using multi-resolution wavelet transform. Further, texture feature extraction method is used to identify the locations for imperceptibly and robustly concealing the marks. This proposed method provides better result in terms of imperceptibility as compared with existing methods [36]. In [19], Mathivanan et al. proposed a secure steganography technique to transmit ECG signal and diagnosis data in color image. The ECG signal and diagnosis data are converted into corresponding QR codes improving the error handling capacity. These QR codes are then embedded within the components of color image by using pixel permutation. Further, embedded points are encrypted using 1D chaotic encryption technique increasing the security. The suggested scheme offered superior performance when compared with similar techniques [37,38,39]. In [40], the DWT based scheme embeds the motion data including homemade exercise data and in-field screening into ECG signal. The method uses Holter equipment to capture the data. It helps in keeping track real-time physical activities of patients in natural environment without additional storage or media channel. The experimental result shows that the proposed method is imperceptible and robust.

To get secure communication of patient details, wavelet-based steganography technique is proposed by the authors to hide mark inside ECG signal [41]. XOR ciphering technique is used for encryption to prevent unauthorized access of data. The quality of the proposed method is measured in terms of PSNR and MSE and found that the method is secure and highly imperceptible. In [42], Nagaraju and ParthaSarath proposed a secure watermarking approach where patient details and ECG signal are marked within medical images. Before embedding, ASCII format of these marks are encrypted and then embedded into host image using LSB algorithm. The suggested scheme is robust and fault tolerant.. In [43], Anandini et al. proposed a watermarking technique for secure transmission of ECG data over insecure network. The ECG signal of the patient is embedded into high frequency plane of a color image using Haar wavelet. Jero and Ramu proposed another curvelet transformation based steganographic technique to hide patient data into ECG signal [33]. Quantization technique is used to embed the data into the coefficient's values. Further, Simple sequence approach is used to get the locations of embedding the marks. It is found that in terms of imperceptibility simple sequence approach is better than random location approach.

A Secure and imperceptible steganography method is proposed in [44] where the diagnosis data is concealed within the ECG signal. Special range numbers of the ECG signals are used to mark the diagnosis data. It maintains the privacy of the user by providing access control mechanism along with providing privacy to sensitive medical data whilst reducing the storage and bandwidth capacity. In this model, the data is arranged in a hierarchical tree like structure and only authorized users can access the nodes with the corresponding keys. In [45], the authors proposed a robust and imperceptible steganography method using combination of DWT and SVD and continuous ant colony optimization (CACO) technique to conceal the medical data within ECG signal. After the decomposition of the signal using DWT, SVD along with additive quantization method is used to embed the confidential data in the high frequency sub bands of ECG signal. Here, CACO algorithm is used to identify the multiple scaling factors which are useful in maintaining the quality of the signal. Tseng et al. suggested a robust and feasible watermarking technique for secure transmission of patient data and ECG and also reduce the transmission overhead [46]. Quantization based encryption technique is used to maintain the integrity and security of the ECG signal prior the DWT based decomposition. The mark is embedded into the lowest frequency coefficient to ensure better security. The proposed method is tested against various types of attacks and found that it is robust and reliable [30]. In [27], Wang et al. proposed two reversible data hiding techniques to maintain the integrity and security of the patient data and the ECG signal. In the first technique, Histogram shifting and prediction-error expansion (PPE) based reversible data hiding technique is proposed to maintain the shape of the ECG signal at the receiver side. This method ensures high imperceptibility of the watermarked ECG signal. The other technique uses unified embedding-scrambling method for concealing the medical information. This method ensures higher embedding capacity and better security since the marked ECG signal is in decoded form. Swierkosz and Augustyniak have proposed an irreversible watermarking technique for ECG signal [47]. Forward wavelet transform is used to decompose the cover ECG signal and create the data container, followed by replacing intrinsic noises of the signal with the diagnosis data. Further, to increase the security, LSB embedding is applied on the watermarked signal. The marked signal is also checked against various types of attacks and found that the method is imperceptible and reliable. The proposed method works superior in terms of imperceptibility when compared with some existing methods [31,33,48,49]. A DWT based data hiding technique is proposed by Mathivanan et al. in [50] where QR code containing the patient data is treated as watermark and concealed within the ECG signal. After the decomposition of the signal using DWT, the code is marked into the lowest coefficient values using swapping technique. It is experimentally proved that the proposed method is highly secured and imperceptible. In [51], Duy et al. proposed an LSB based adaptive data hiding technique to secure patient data inside the non-essential components of the ECG signal. The security is enhanced by applying SHA3 and AES algorithm for encryption of patient information before the embedding. A DWT based secure and imperceptible watermarking method is proposed by Engin et al. in [52] to authenticate of the ECG signal by embedding authentication information within the signal. To increase the robustness, pseudo random sequence is used for embedding. Another secure and imperceptible steganography technique is proposed by Mathivanan et al. in [34] where the encoded patient data is transmitted through ECG signal. The 1D ECG signal is converted into 2D image using DWT technique. To further improve the security, the secret data is converted into QR code which has error handling capacity. This code is embedded within the decomposed signal using additive quantization method to provide double security. In terms of imperceptibility, the proposed method is superior to the existing methods [25,33, 35,53–56]. In [57], Pandey et al. proposed an imperceptible and robust data hiding technique for secure transmission of patient data into ECG signal based on SVD. Coupled chaotic map is used to generate the pseudo-random locations for embedding and the secret data is marked into those locations using sample value difference approach and SVD. Further, OFDM method is used to transmit the watermarked signal in the network and to get real time access of data. In terms of imperceptibility, the proposed work outperforms the existing state-of-art [18,25,28,45,58]. Curvelet transform based data hiding technique is proposed by Patil et al. in [59] to conceal encrypted form of patient data into ECG signal. Security of the secret data is improved by applying chaotic encryption method. Curvelet transform is applied on the cover signal to get the coefficient values, on which adaptive LSB embedding technique is performed. Experimental results show that the method is imperceptible and the data can be extracted completely at receiver side. In [60], Sahu et al. proposed another reliable data hiding technique for secure transmission of ECG signal and diagnosis data using DWT. To make the system more energy efficient, the secret data is embedded within the decomposed signal using Unequal steganography embedding method. Further, the robustness is enhanced by using Unequal error protection technique during embedding.

Table 2 shows the summary of some notable ECG signal-based data hiding techniques in terms of their objective, type of data hiding, methodology and database used, performance metrics, important features, and limitations for healthcare applications.

5.2 EEG based data hiding techniques

Electroencephalography (EEG) is a medical technique for recording electrical signal generated from the brain. EEG signals (see in Fig. 6) are mainly used for clinical diagnosis of epileptic seizures, sleep disorders, encephalopathy and brain death [61]. These signals can be used as cover signal in telemedicine due their large size and important in many non-clinical researches [62]. The frequency ranges of the EEG signals are defined from 0.01 Hz to 100 Hz. The range can be further divided into five frequency bands which are used to determine the current state of the brain [63]. Based on the feature selection, the EEG control signals is further divided into Time domain, Frequency domain and time–frequency domain [64]. To do the embedding in frequency domain, the EEG signal is first converted into 2D matrix and then decomposed into sub bands like HH, HL, LH and LL. The embedding of secret data is mainly performed into the HH sub bands [65].

Some of the notable ECG based data hiding are discussed below.

In [61], Duy et al. proposed an imperceptible and blind watermarking technique based on pattern recognition to securely transmit secret data marked within EEG signals using DWT. Patient information and signature are used as watermarks and to increase the security, Arnold transform is used to scramble the mark. Further, the watermarked data is embedded within the decomposed signal using mean value relationship of the coefficients. At receiver side, support vector data description (SVDD) is used to efficiently extract the mark. The suggested scheme can handle different types of common attacks. In [64], authors proposed a reversible and blind watermarking technique where electronic patient record is embedded as watermark into the EEG signal to achieve data authenticity and maintain signal integrity along with restriction in copy process. After applying rectification and round off techniques on the signal, Alattar's method is used to mark the EPR into the processed signal to ensure reversibility of the technique. The experimental results show that the proposed method is imperceptible and highly secure. Pham et al. proposed

Table 2 Summary of ECG signal-based data hiding techniques

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[6]	2012	Binary watermarking approach to achieve better robustness	Robust and blind	SWT, Spread-spectrum, quantization	PSNR = 24.7 dB, CC = 0.81	No need of session key as self-authentication technique is used	NA	Suraha Nursing Home, Kolkata	Lossy and security can be further improved by using encoding technique
[26]	2010	An imperceptible and robust steganography method	Highly secure	Shift special range transform	PRD = 0.4493	MSB can be used for embedding for getting better security	312.5 bytes	Creighton University Ventricular Tachyarrhythmia Database	To enhance the security frequency domain approaches can be proposed using DCT
[29]	2008	Reversible data hiding technique	Imperceptible and robust	Lifting wavelet transform, Arnold transform	NRMSE = 0.1196	To make the system more robust, the secret data is scrambled before embedding	74.6 kb	MIT-BIH database	This method can also be applied on seismic signals, electroencephalogram signals etc
[31]	2011	Secure watermarking technique with high embedding capacity	High integrity	LSB and simple linear transformation	PRD < 1%. (up to 5 bits)	The method will reduce power consumption and is suitable for wearable devices	1250 bytes	Creighton University Ventricular Tachyarrhythmia Database	In future data encryption can be added with the present method

Table 2 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[32]	2020	Robust and imperceptible watermarking	Robust	DWT, QR decomposition	PSNR > 40%, NCC = 1.0 and PRD	The QR coded secret data is embedded within the cover signal to increase the security factor	64 × 64	MIT- BIH normal sinus rhythm database	Other identifiers can be used in place of QR code to decrease time and space
[35]	2010	Contextual double digital watermarking technique to provide robustness against attacks	Secure	Haar mother wavelet transformation, LSB, IDWT	CC (ECG) = 93.36%, (PatID) = 91.05, PSNR(ECG) = 70.12 dB, (PatID) = 61.34 dB, SSIM(ECG) = 0.901, (PatID) = 0.935	Texture feature extraction is used to find the secure embedding locations	32 × 32	PET images: Geneva university hospital.ECG signal: MIT database	Image quality will degrade after rotation
[19]	2018	Secure and robust QR code-based steganography method	Secure	Pixel permutation, chaos encryption (1D logistic map)	NPCR = 99.63, UACI = 35.29 and Entropy = 7.993, CC = 0.0007	The secret data is embedded into the color components of the cover image and then encrypted for increasing further security	NA	MIT- BIH database	The proposed method shows average execution time

Table 2 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[40]	2019	A secure watermarking technique to efficiently store the homemade exercise data	Secure and blind	DWT and IDWT, motion data encoder	Mean and Standard deviation	The coding bit depth is determined by calculating the noise present in the signal	542 bits per sec	CSE records recommended by IEC60601-2-51 standard	Should be tested in real time Implementation of data watermarking technique
[41]	2015	Secure watermarking technique in PoC system to maintain confidentiality	High Imperceptibility And secure	DWT, IDWT, XOR ciphering	PSNR > 70%, MSE < 0.0060and PSD < 0.0316	To enhance security, a user defined key based encryption technique is used here	NA	N.A	Other encryption algorithms can also be used
[42]	2014	Secure data hiding technique to achieve efficient storage and robust transmission in spatial domain	Robust	LSB	NRMSE = 0.1205 and PSNR = 72.135 dB	The secret data and the ECG signal, both are encrypted before embedding into cover image	100 character	Physionet online database	Adding noise in interleaving images will degrade the imperceptibility of marked image
[43]	2016	Watermarking technique for secure and reliable transmission	Secure and imperceptible	DWT,	PSNR = 35.0129 dB, MSE = 20.66, NPCR = 0.2705 and UACI = 0.0057	G-component based colour image is used for embedding the ECG data	NA	N.A	Compression techniques can be used for reducing size of embedded data

Table 2 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[33]	2016	A steganography technique for ensuring imperceptibility and security	Imperceptible	Quantization, curvelet transformation	PSNR = 38.06 dB, PRD = 2.45, KL = 0.119, MSE = 10.14 and BER = 46.35	According to size of the secret data, coefficient points are selected and its value should be near to zero	502 bytes	MIT-BIH database	The bit error rate is significantly affected with increasing the watermarked size
[44]	2013	A steganography method to control the access and maintain the confidentiality of data	Highly secure	Secret key, SSL, special range numbers	N.A	The secret data are placed in hierarchical structure to stop unauthorized access	504 bytes	Online available database in the internet	Other cryptographic technique as well as key management and distribution can be added with the existing scheme
[45]	2016	Steganography technique for secure and imperceptible data transmission	Imperceptible and robust	CACO, DWT, SVD and additive quantization	PSNR = 62.87 dB, PRD = 0.0018, KL = 0.02 and BER = 0	The performance is improved by using Multiple scaling factors instead of Single scaling factor	(0.89–3.07) Kb	MIT-BIH database	Can be applied in real time applications to check the performance. Here the size of the watermark signal is a limitation

Table 2 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[46]	2014	Secure watermarking method with compression technique to ensure the confidentiality and reliability	Robust and feasible	DWT and wavelet method for compression	SNR = 32 dB, BER = 0, CR = 1.28 and CNR = 16.25	For getting better robustness and security, lowest frequency wavelet coefficients are taken for embedding purpose	32 bits per signal	MIT-BIH Arrhythmia Database	Can be used for verification purpose
[27]	2015	A reversible watermarking technique with high privacy, security and payload	Reversible and secure	UES, LLP, PEE, HS, RDH	BPS = 0.10 and PRD = 0.504	The confidentiality of the data is enhanced using scrambling method	7.8962 bits per sample	MIT-BIH Arrhythmia database	Can work in real time processing of data
[47]	2018	An irreversible robust watermarking technique	Imperceptible and secure	LSB, forward and inverse watermarking technique	PRD = (0.06–0.51)	Intrinsic noises of the signal are replaced with secret data to get a secure embedding	140.5 bits per sec	CSE Multilead Database	To check the efficiency of the proposed model, it should be tested against various additive noises

Table 2 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[50]	2019	An imperceptible steganography technique to reduce the errors	Secure and imperceptible	DWT and swapping method	PSNR = 41.02 dB and PRD = 0.06	Patient data is embedded as QR code to increase security. Swapping process is performed during embedding to achieve robustness	2632 bytes	MIT-BIH database	Embedding capacity can be increased without affecting the imperceptibility of the watermark
[51]	2017	An Adaptive data hiding technique to maintain integrity of the signal after embedding	Imperceptible and maintain data integrity	LSB, SHA3 and AES	SNR = 78.96 dB, PRD = 0.013 and MSE = 0	Secret data is encrypted using AES and key is made using SHA3 to increase the security during transmission	450 bytes	PhysioNet's PTB diagnostic database	An automated disease diagnosis system will be implemented based on the ECG signal features
[52]	2005	A secure and imperceptible watermarking technique to maintain integrity and authenticity	Imperceptible	DWT and pseudo random sequence	SNR = 34.05 dB	Security is increased by using some pseudo random function at the time of embedding	NA	MIT-BIH Arrhythmia database	This method can also be applied to EEG signals

Table 2 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[34]	2018	A reliable and imperceptible steganography technique to provide better security	Imperceptible and robust	DWT, additive quantization and QR code	PSNR = 57.43 dB, PRD = 0.246 and KL = 0	Imperceptibility of the proposed method is inversely proportional to the scaling factor	(16–229) bytes	MIT-BIH database	The overall performance can be measured with different types of external attacks and scaling parameters
[57]	2017	Secure data steganography technique to maximize the payload and resists attacks	Highly imperceptible and secure	SVD, chaotic map and OFDM	PSNR = 55.49 dB, PRD = 0.26, KL = 0.000003 and BER	To make the embedding process more robust, chaotic map is used to provide random locations	21 Kb	MIT-BIH arrhythmia database	The proposed method cannot achieve reversibility because of the presence of reconstruction error in the cover signal
[59]	2018	A secure ECG steganography method	Imperceptible	LSB, curvelet transform, chaos encryption and FDCT	PSNR = 60.28 dB, PRD = 0.0011 MSE = 8.29 and BER = 0	To increase the confidentiality of the secret data, chaotic encryption is applied	3 bits per sample	MIT-BIH database	With the proposed method dependable steganography technique can be implemented

Table 2 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[60]	2017	A secure steganography technique for confidential and energy efficient transmission	Robust and reliable	USE, UEP and DWT	WWPRD < 0.45%	Unequal error protection technique is applied on the watermarked data to increase the robustness	NA	MIT-BIH Database	For the same amount of noise in the channel, USE gives better result than ESE in terms of correlation value

PRD Percentage residual difference, *BPS* bits per sample point, *LLP* local linear prediction, *PEE* prediction error expansion, *HS* histogram shift, *RDH* reversible data hiding, SSRT: shift special range transform, *SSL* secure socket layer, *DWT* discrete wavelet transform, *LSB* least significant bit, *CNR* contrast to noise ratio, *OFDM* orthogonal frequency division multiplexing, *UEP* unequal error protection, *UES* unequal steganography embedding. NRMSE normalized rms error

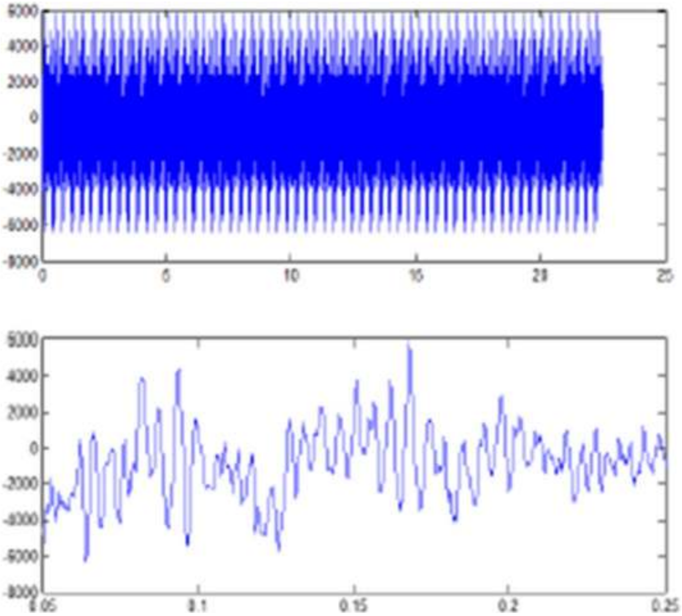


Fig. 6 Original EEG signal [64]

a blind watermarking method in [65] to ensure the security of EEG signal using fusion of DWT and SVD. EEG signal is transformed into 2-D form and then decomposed using DWT. Further, SVD is used on this decomposed signal to embed the watermark and ensure blind detection. A fragile watermarking technique is proposed by hiding EPR and hospital logo within EEG signal to ensure the authenticity and integrity of the transmitted data [66]. The method is proposed for colour image. The watermark image is embedded within the cover signal using MSB bits. To make the system robust, File Checksum Integrity Verifier is used for data tracking. Experimental results show that the proposed method is robust and can reduce payload.

In [67], the authors proposed two steganography methods where patient data is marked within magnetic resonance image using similarity and fuzzy logic based LSB algorithm. Here, the hidden data is composed of EEG signal, patient details and comments by the doctors. To enhance the security and reduce the size, this secret data is compressed using LZW and Huffman compression techniques. Further, to provide better protection to the compressed data, Rijndael symmetric encryption is used. This encrypted data is concealed within the cover image based on Fuzzy logic based LSB and Similarity based LSB using gray level difference of pixels. Both steganography methods are suitable for reducing transmission and storage overhead. The proposed method is better than existing methods in terms of embedding capacity and imperceptibility [36] [68–72].

In [73], author proposed a secure and lossless data hiding technique to embed patient EEG signal within encoded video sequences with high embedding capacity. H.264/AVC encoder is used to mark the samples of the signal within the motion vectors. Duy et al. proposed another blind scheme where secret data is embedded within EEG signal using approximation coefficient values and SVDD based extraction is practiced for watermark retrieval [74]. Owner signature and logo is taken as watermark and Arnold transformation is applied to it prior embedding. DWT is applied to the signal for decomposition. Further the scrambled data is embedded using the mean value modulation and approximate coefficient values. At the receiver side the watermarked signal is extracted without any loss using trained SVDD model. The proposed method is highly robust and imperceptible. Parashar et al. proposed a robust data hiding technique to securely embed confidential data of patient within EEG signal using lifting based integer wavelet [75]. The secret data is encrypted prior embedding and pseudo random number is used to conceal the data in a distributed fashion. In [76], Pundkar and Joshi proposed a blind and secure steganography technique to conceal the patient data within EEG signal based on Lifting wavelet transform. ECG image and information of the patient are treated as watermark and encrypted using Arnold transform prior embedding. The encrypted data is embedded within the transformed signal using mean modulation relationship of approximation coefficients and at the receiver side the marked data is extracted using SVDD. The proposed method is imperceptible and can handle different processing attacks.

Table 3 provides the brief summary of some notable ECG signal-based data hiding techniques.

5.3 Other biomedical signal-based data hiding techniques

Some of the other bio signal (EOG, PPG, EMG) are equally important as ECG and EEG signal. Electrooculography (EOG) is a medical test to detect any abnormality in human eyes by monitoring movement of eye ball in rapid eye movement and with no rapid movement during sleep period. EOG signal is the graphical representation of electrical response of the sensitive rods and cons cells and motor nerves present inside the eye [77]. Figure 7 gives the representation of EOG signal.

Photoplethysmography (PPG) is a very sensitive and uncomplicated medical diagnostic tool to detect various types of cardio-vascular diseases (see Fig. 8). PPG is a non-invasive method where a light source and photo detector is used at the surface level of the skin to measure the variation relative blood volume in the blood vessels [79]. Analysis of PPG signal is very important as various cardio diseases like atherosclerosis and arterial stiffness can be detected from the second derivative of the signal [11].

EMG signal analysis is performed to measure and record the biceps muscle activity during exercise [80]. These EMG signals (See fig. 9) are also used as diagnostic tools to detect various diseases of muscles by recording electrical signal of muscles. Using this EMG signal, the reason of muscle weakness can be detected that whether it is caused by the breakdown of a nerve attached with the muscle or neurological disorder [78].

Some of the notable other bio-signal (EOG, PPG, EMG) based-data hiding techniques are discussed below.

Table 3 Summary of EEG signal-based data hiding techniques

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[61]	2016	Blind watermarking method to achieve transmission security	Blind, imperceptible and robust	DWT, Arnold transform, pattern recognition, SVDD	PSNR = 66.55 dB, Normalized Correlation (NC) = 1 and BER = 0	Learning based trained model can be used at receiver side for lossless extraction of data	1024 bits	DEAP dataset	Simple machine learning algorithm can be used to reduce computational complexities. ECC can be applied to increase robustness
[64]	2012	Reversible watermarking technique to achieve copy right protection	Blind and reversible	Alattar's method	SNR = 3.3960 and CC = 1	Alattar's method is used to increase data hiding capacity and reduce data loss	NA	Suraha Nursing Home, Kolkata	High computational complexity
[65]	2015	Blind watermarking technique to get high quality of transmitted signal	Imperceptible, blind	DWT and SVD	PSNR = 57.53 dB	SVD method is used for embedding to achieve blind detection at receiver side	NA	DEAP dataset	In future embedding can be applied on EEG signal for a secure and reliable transmission

Table 3 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[66]	2015	A secure binary watermarking technique to provide tamper detection and authentication	Fragile	MSB, file checksum integrity verifier	N.A	Data tracking and copy right protection can be achieved	9 bits		The proposed method can also be applied for ECG, EMG, EEG etc. signals and can use colour watermark
[67]	2015	Steganography method to increase security and reduce transmission overhead	Imperceptible and secure	Huffman compression, LZW, fuzzy logic and similarity based LSB and Rijndael symmetric encryption	PSNR = (53.87–62.99)dB and MSE = (0.04–0.36)	A combination of compression then encryption techniques is used to ensure the security	(6794- 64,586) bytes	Epilepsy dataset from Department of Neurology at Gazi University	In future embedding capacity can be increased by reducing noise and redundant data
[73]	2015	A lossless data hiding technique to provide good embedding capacity and low complexity	Secure and lossless	H.264/AVC encoder	PSNR(difference) = 0.011 dB, BRI (bit rate change) = 0.4459%	Encoder is used to increase the security factor	45,598 bits	CHB-MIT Scalp EEG Database	Concepts of encryption and compression can be added

Table 3 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Watermark size	Database used	Noticed Limitation/ Future work
[74]	2017	Blind and imperceptible watermarking technique to handle different type of attacks	Blind, Secure and robust	DWT, Arnold transform, SVDD, mean value modulation	PSNR = 66.55 dB, BER = 0 and NC = 1	ML based learning algorithms are used to make the system more robust and imperceptible	32 × 32	DEAP dataset	High computational complexity
[75]	2011	A blind and imperceptible data hiding technique to ensure the integrity	Blind and secure	IWT, pseudo random number	PSNR = 43 dB and MSE = 0.2029	To increase the robustness, low frequency sub band is used for embedding	(108–300) bits		The proposed method cannot handle attacks in spatial domain
[76]	2019	Secure steganography method for reliable transmission	Blind and robust	Lifting wavelet transform, Arnold transform SVDD	MSE = 0	Data secrecy is enhanced by applying encryption prior the embedding	NA	Online websites	Patient data can be concealed within cover signal to provide source authentication

LZW Lempel–ziv-welch compression, *CC* correlation coefficient, *MSE* mean square error, *PSNR* data description, *NC* normalized correlation

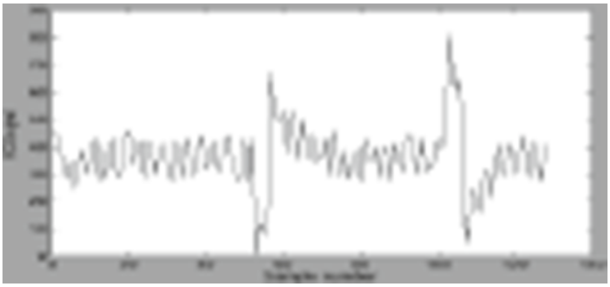
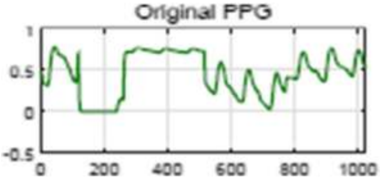


Fig. 7 Original EOG signal [78]

Fig. 8 Original PPG signal [4]



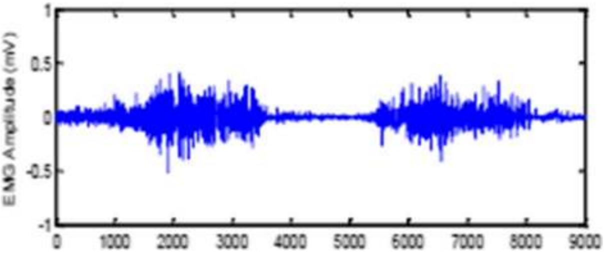


Fig. 9 Original EMG signal [78]

In [4], Abuadbba and Khalil proposed a 3D steganography method to securely embed secret data within bio signal preserving the integrity and authenticity of the signal. Fast Walsh Hadamard transform technique is used to decompose signal. Less important coefficient values are replaced at the time of embedding. The secret data is first encrypted using AES method. Using the rotation factor on the key, a 3D template is generated and further the secret data are randomly embedded using this template. The proposed method is highly secure when compared with similar techniques [31]. Bio-signal based blind watermarking techniques are proposed by Dey et al. in [78] where EMG signal is used as cover signal. It proposed session key and self-recovery watermarking methods using spread spectrum and stationary wavelet transformation (SWT). Self-authentication verifies the integrity and source of the confidential information. Based on experimental results, it is concluded that self-recovery model works superior in comparison to key based model since there is no burden of exchanging session key between sender and receiver. In [79], Dey et al. proposed a blind watermarking technique where patient data is embedded within PPG signal to provide source authentication. Prediction error algorithm is used to securely imperceptibly embed the EPR into the transformed PPG signal.

Dey et al. in [81] further suggested a blind scheme to verify the integrity of the EOG signal and to reduce the computation time and complexity. The mean value of the blink frequency and blink interval of the EOG signal is used as watermark. The watermark is concealed using difference expansion algorithm. A reversible steganography method is proposed by Rahman et al. where secret data of the patient is embedded as errors within the bio signals to achieve source authentication [82]. To achieve reversibility, the bio signal samples are encoded using extended binary golay code before embedding. Further the secrecy of the hidden data is increased by random selection of the embedding point using pseudo random sequence. Results proved that the scheme is reliable offered the high embedding capacity. In [77], another blind watermarking technique is proposed by Dey et al. to provide data authenticity along with access control in EOG signal. Authors used frequency domain techniques to imperceptibly embed the gray scale mark image. The proposed method is imperceptible and can provide security against unauthorized access and copying. A blind and reversible steganography technique is proposed by Shiu et al. in [56] where secret data is securely embedded within physiological signals. It achieves privacy and authenticates data in time of transmission through the insecure network. The signal is transformed into bit of stream using error correcting codes. Further, confidential data of the patient is embedded within the transformed signal using hamming code. The proposed system has high embedding capacity and can reduce the payload. Also, when compared with similar techniques [28,29,58,83], this technique offers better results.

A blind recognition of surface EMG based on watermarking is proposed by Yina and Dawei in [84]. To provide more security, Arnold transformation is used to scramble the secret image. DWT is used to decompose the EMG signal. Synchronization codes are used to get the embedding locations and then embedding is done using adaptive coefficients. Experimental results show that the proposed method is robust against various types of processing attacks. A reversible and blind watermarking technique is proposed by Dey et al. to ensure the authenticity of PPG signal when transmitted over open channel [85]. It uses binary image as watermark. The PPG signal is cropped according to the mark size and then decomposed using lifting wavelet transform method. The watermark image is embedded within the decomposed signal using pseudo random sequence. This session key based secure watermarking technique is secure and imperceptible.

Table 4 provides the brief summary of some notable EOG, PPG, and EMG signal-based data hiding techniques.

Table 4 summary of other bio signal-based data hiding techniques

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Water mark size	Database used	Noticed Limitation/ Future work
[4]	2016	A 3D steganography method to preserve the integrity and authenticity	Secure and robust	Walsh Hadamard Transform and AES	PRD = 0.1056	Less significant coefficient values are used for embedding to ensure minimum distortion	328 Kb	ECG and PPG signal: "PhysioNet" repository. EEG signal: Neurodynamics Laboratory	The proposed multi-dimensional method is both expensive and complex
[78]	2014	A secure watermarking technique to provide authentication	Blind and secure	SWT, spread spectrum	PSNR = 13.0631 dB and CC = 0.8525	Self-authentication method is used as it reduces transmission overhead	NA	Suraha Nursing Home, Kolkata	To get high security value, small amount of imperceptibility had to tolerate
[79]	2012	Reversible watermarking technique to achieve source authentication	Blind	Prediction error algorithm	PSNR = 105.70 dB and CC = 1	Prediction error algorithm is used for embedding to get reversibility at receiver side	NA	Suraha Nursing Home, Kolkata	Concepts of encryption and compression can be added
[81]	2012	Secure reversible watermarking technique to maintain the integrity	Imperceptible and robust	Difference expansion algorithm	SNR = 33.038 dB and BER = 0	Watermark is generated using mean value of blink frequency and blink interval frequency of original signal	64 bits	Suraha Nursing Home, Kolkata	The proposed method can be compared with the state-of-art

Table 4 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Water mark size	Database used	Noticed Limitation/ Future work
[82]	2020	A secure and reversible steganography technique with source authentication	Highly imperceptible and secured	Extended binary golay error correction code	BER = 0 and PRD = 0.0069	The embedding capacity is triple of the number of samples in the signal	3 bits per sample	Physionet repository	It can be applied to aggregated bio signals to solve source authenticity problem
[77]	2012	A blind and secure watermarking technique to achieve source authenticity and access control	Secure and imperceptible	DWT, DCT and SVD	PSNR = 31.5572 dB and CC = 0.9965	A combination of decomposition method is applied on secret data and cover signal to achieve imperceptible concealing	NA	PDS lab	Concepts of encryption and compression can be added
[56]	2017	Secure and reversible steganography technique	Blind, robust	Error correcting codes, hamming code	NRMSE = 0.1036 and SNR = 19.69 dB	The method achieves low complexity and high embedding capacity after applying hamming code	66.67 Kbits	MIT-BIH arrhythmia database	Concepts of encryption and compression can be added

Table 4 (continued)

Ref no	Year	Objective	Data hiding type	Methodology	Performance metrics	Other important features	Water mark size	Database used	Noticed Limitation/ Future work
[84]	2012	A blind and semi-fragile watermarking technique to provide robustness against various processing attacks	Blind and secure	Synchronization code, Arnold transform, adaptive coefficient, DWT	RMS of EMG signals in mV	A robust and secure watermark can be obtained by applying scrambling encryption	NA	Surface EMG signals are recorded by placing electrodes on the forearm muscles	Recurrent neural network can be used to enhance the performance of the model in detecting gestures properly
[85]	2012	Reversible and blind watermarking techniques to ensure authenticity	Blind and robust	Lifting wavelet transform, pseudo random number	PSNR = 12.46 dB and CC = 0.8974	Session key-based embedding and extraction of watermark to achieve high security and reliability	NA	Suraha Nursing Home, Kolkata	High computational complexity

SWT stationary wavelet transform, *SVD* singular value decomposition, *BER* bit error rate, *NRMSE* normalized rms error, *PSNR* peak signal to noise ratio, *PRD* Percentage residual difference, *RMS* root mean square, SNR: signal to noise ratio, *CC* correlation coefficient

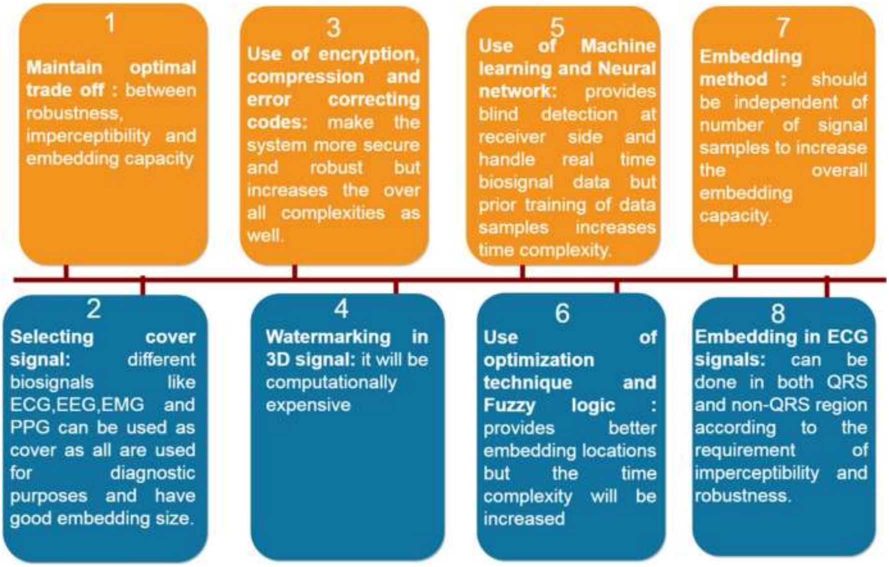

1
Maintain optimal trade off : between robustness, imperceptibility and embedding capacity
3
Use of encryption, compression and error correcting codes: make the system more secure and robust but increases the over all complexities as well.
5
Use of Machine learning and Neural network: provides blind detection at receiver side and handle real time biosignal data but prior training of data samples increases time complexity.
7
Embedding method : should be independent of number of signal samples to increase the overall embedding capacity.
2
Selecting cover signal: different biosignals like ECG,EEG,EMG and PPG can be used as cover as all are used for diagnostic purposes and have good embedding size.
4
Watermarking in 3D signal: it will be computationally expensive
6
Use of optimization technique and Fuzzy logic : provides better embedding locations but the time complexity will be increased
8
Embedding in ECG signals: can be done in both QRS and non-QRS region according to the requirement of imperceptibility and robustness.

Fig. 10 Identified issues for bio signal based watermarking

6 Identified issues

Various notable watermarking approaches have been developed. However, a lot of other significant issues still need to be addressed in near future. Through our comprehensive survey, we have identified numerous open issues and valuable research directions are discussed and also shown in Fig. 10.

- We need to maintain an optimal balance between imperceptibility, robustness and embedding capacity while embedding secret data into biomedical signals.
- Security of the significant information and computational cost is equally important for any practical application.
- Different optimization techniques and Fuzzy logic concepts can be added with watermarking technique for getting better embedding locations. However it will increase the time complexity as well.
- While developing the watermarking scheme, different types of attacks should be considered.
- The embedding methods need to be chosen in such a way that it should be independent of the number of samples present in the cover signal to maximize the overall capacity.
- Similar to ECG signal, other bio signals also have importance in diagnosis respective and can also be used as cover to achieve a secure transmission.
- The embedding location in the ECG signal should be chosen according to the requirement of the application that whether to maintain high imperceptibility or try to minimize the distortion.

- To control the access and confidentiality of the data cryptographic techniques as well as key management and distribution model can be added with data hiding methods. However, it should enhance the cost as well.
- To enhance the security of data in spatial domain, different error correcting codes can be applied at receiver side to increase robustness and to achieve reversibility.
- Machine learning algorithm can be used with watermarking techniques to increase the robustness and blind detection of time series bio medical data. However, it increases the computational complexities as well.
- Scrambling operations can be added with the existing methods to increase the imperceptibility and confidentiality of the cover signal. However, the integrity of the data should not be altered.
- Along with the data hiding method, different encryption and compression scheme can also be merged to increase the overall security and imperceptibility of the system. However, the overall complexity of the system will increase.
- In order to handle real time data from any application, neural network based watermarking techniques can be used.
- Data hiding scheme for 3D signal are computationally expensive.

7 Conclusion

Data hiding techniques plays a significant role to provide copyright protection and content authentication in digital world. No universal bio-signal data hiding techniques has been proposed to effectively provide the complete robustness and security of the medical data. This paper outlines and surveys the bio-signal based data hiding scheme in several aspects. We introduced basic concepts of data hiding along with major properties, generic embedding and extraction process, and recent applications. Then, traditional and recently developed bio-signal based data hiding techniques are reviewed and compared by highlighting their objective, type of data hiding, methodology and database used, performance metrics, and important features. At the end, some open issues and research directions are discussed. Author is confident that this survey would motivates more research into bio-signal based data hiding in secure healthcare application, and we believe that in the future, the concept will become a standard for dealing with sensitive bio-signal data.

Acknowledgements This research is supported by research project entitled "Copyright protection tool for digital data" order no. DLRL/21CR0003/SW-CC&ENT/GN/LP dt. 29 August, 2020, Defence Electronics Research Laboratory (DLRL), Ministry of Defence, DRDO, Hyderabad.

References

1. Wang W, Peng D, Wang H, Sharif H and Chen HH (2007) Optimal image component transmissions in multirate wireless sensor networks.https://doi.org/10.1109/GLOCOM.2007.188
2. Anand A, Singh AK (2020) Joint watermarking-encryption-ECC for patient record security in wavelet domain. IEEE Multimed. https://doi.org/10.1109/MMUL.2020.2985973

3. Konwar AN, Borse V (2020) Current status of point-of-care diagnostic devices in the Indian healthcare system with an update on COVID-19 pandemic. Sensors Int 1(101):100015. https://doi.org/10.1016/j.sintl.2020.100015
4. Abuadbba A, Khalil I (2016) Walsh-hadamard based 3D steganography for protecting sensitive information in point-of-care. IEEE Trans Biomed Eng 9294(2):1–10. https://doi.org/10.1109/TBME.2016.2631885
5. Anand A, Singh AK (2020) Compression-then-encryption-based secure watermarking technique for smart healthcare system. IEEE Multimed 27:133–143
6. Dey N, Roy AB, Das A (2012) Stationary wavelet transformation based self-recovery of blind-watermark from electrocardiogram signal in wireless telecardiology. Springer, Berlin, pp 347–357
7. Mitra K, Bit A, Bhattacharyya S, Dey A (2018) Medical signal processing in biomedical and clinical applications. J Healthc Eng. https://doi.org/10.1155/2018/3932471
8. Khan A, Tahir SF, Majid A, Choi TS (2008) Machine learning based adaptive watermark decoding in view of anticipated attack. Patt Recognit. https://doi.org/10.1016/j.patcog.2008.01.007
9. Raptis CA, Hammer MM, Short RG, Shah A, Hope MD, Henry TS (2020) Chest CT and coronavirus disease (COVID-19): a critical review of the literature to date. AJR Am J Roentgenol 215:839–842
10. Mundo R, Cruz CO (2020) Personal data usage and privacy considerations in the COVID-19 global pandemic. Ciência Saúde Coletiva. https://doi.org/10.1590/1413-81232020256.1.11792020
11. Castaneda D, Esparza A, Nazeran H (2018) A review on wearable photoplethysmography sensors and their potential future applications in healthcare. Int J Biosens bio Electron 4:195–202
12. Anand A, Singh AK (2020) Watermarking techniques for medical data authentication: a survey. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-08801-0
13. Mohanty SP, Sengupta A, Guturu P, Kougianos E (2017) Everything you want to know about watermarking: from paper marks to hardware protection: from paper marks to hardware protection. IEEE Consum Electron Mag 6:83–91
14. Rajeswari J, Jagannath M (2017) Advances in biomedical signal and image processing—a systematic review. Inform Med Unlocked 8:13–19
15. Biomedical Signal Processing.https://www.embs.org/about-biomedical-engineering/our-areas-of-research/biomedical-signalprocessing. Accessed 02 Aug 2020
16. Goudar V and Potkonjak M (2014) Addressing Biosignal Data Sharing Security Issues with Robust Watermarking. In: 2014 Elev Annu IEEE Int Conf Sensing Commun Netw, pp. 618–626
17. Pratap S and Chauhan S (2013) A survey :digital audio watermarking techniques and applications. In: 2013 4th Int Conf Comput Commun Technol, pp. 185–192
18. Chen S, Guo Y, Huang H (2014) Hiding patients confidential datainthe ECG Signal viaa transform-domain quantization scheme. J Med Syst. https://doi.org/10.1007/s10916-014-0054-9
19. Mathivanan P, Ganesh AB (2018) QR code based color image cryptography for the secured transmission of ECG signal. Multimed Tools Appl 78:6763–6786
20. Gupta A, Verma P, Sambyal RS (2018) A comparison of different data hiding techniques. Int J Sci Res Comput Sci Eng Inf Technol 4:183–188
21. Singh L, Singh AK, Singh PK (2018) Secure data hiding techniques : a survey. Multimed Tools Appl 79:15901–15921
22. Priya S, Santhi B, Swaminathan P, Jayabal R (2017) Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. Opt Int J Light Electron Opt. 145:655–671
23. Agarwal N, Singh AK, Singh PK (2019) Survey of robust and imperceptible watermarking. Multimed Tools Appl 78:8603–8633
24. Ni R, Ruan Q, Cheng HD (2005) Secure semi-blind watermarking based on iteration mapping and image features. Pattern Recognit 38:357–368. https://doi.org/10.1016/j.patcog.2004.08.006
25. Jero SE, Ramu P, Ramakrishnan S (2015) ECG steganography using curvelet transform. Biomed Signal Process Control 22:161–169. https://doi.org/10.1016/j.bspc.2015.07.004
26. Ibaida A, Khalil I and Al-shammary D 2010 Embedding Patients Confidential Data in ECG Signal For HealthCare Information Systems. In: 32nd Annu Int Conf IEEE EMBS, pp. 3891–3894
27. Wang H, Zhang W, Yu N (2016) Protecting patient confidential information based on ECG reversible data hiding. Multimed Tools Appl. 75:13733–13747

28. 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. Article number: 132 (2014):1–11
29. Zheng K, Qian X, Beijing T, Engineering I, and District H 2008 Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms. In: 2008 Int Conf Comput Intell Secur Revers, pp. 295–299. https://doi.org/10.1109/CIS.2008.71
30. Dey N, Mukhopadhyay S, Das A, Chaudhuri SS (2012) Analysis of P-QRS-T components modified by blind watermarking technique within the electrocardiogram signal for authentication in wireless telecardiology using DWT. Int J Image Graph Signal Process. https://doi.org/10.5815/ijigsp.2012.07.04
31. Ibaida A, Khalil I, Van Schyndel R (2011) A low complexity high capacity ECG signal watermark for wearable sensor-net Health monitoring system. Comput Cardiol 2010:393–396
32. Sanivarapu PV, Rajesh KNVPS, Rajasekhar Reddy NV, Reddy NCS (2020) Patient data hiding into ECG signal using watermarking in transform domain. Eng Sci Med Phys. https://doi.org/10.1007/s13246-019-00838-2
33. Jero SE, Ramu P (2016) Curvelets-based ECG steganography for data security. Electron Lett 52(4):4–5. https://doi.org/10.1137/05064182x
34. Mathivanan P, Edward S, Palaniappan J, Athi R, Ganesh B (2018) QR code based patient data protection in ECG steganography. Australas Phys Eng Sci Med. https://doi.org/10.1007/s13246-018-0695-y
35. Nambakhsh M, Ahmadian A, Zaidi H (2010) A contextual based double watermarking of PET images by patient ID and ECG signal. Comput Methods Programs Biomed 104(3):418–425. https://doi.org/10.1016/j.cmpb.2010.08.016
36. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. Med Bio Eng Comput. https://doi.org/10.1007/s11517-006-0081-x
37. Kalpana J, Murali P (2015) An improved Color Image Encryption Based on Multiple DNA sequence operations with DNA synthetic image and Chaos. Opt Int J Light Electron Opt. https://doi.org/10.1016/j.ijleo.2015.09.091
38. Wang X, Zhang H (2015) A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt Commun 342:51–60. https://doi.org/10.1016/j.optcom.2014.12.043
39. Wei X, Guo L, Zhang Q, Zhang J, Lian S (2012) A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw 85(2):290–299. https://doi.org/10.1016/j.jss.2011.08.017
40. Augustyniak P (2019) Application of Watermarking Technique to Embedding Homemade Exercise Test Data into a Standard ECG Signal. In: 2018 Int Conf Appl Math Comput Sci, pp. 71–715, https://doi.org/10.1109/ICAMCS46079.2018.00013
41. Singh NA (2015) Steganography of ECG signals for hiding of patient confidential data. Int J Comput Organ Trends 5:5–8
42. Nagaraju C and ParthaSarathi S (2014) Embedding ECG and Patient Information In Medical Image. In: IEEE Int Conf Recent Adv Innov Eng
43. Anandini VSM, Gopalakrishna YH, Raajan NR (2016) Secure electrocardiograph communication through discrete wavelet transform. Soft Comput. https://doi.org/10.1007/978-81-322-2671-0
44. Mai V, Khalil I, and Ibaida A (2013) Steganography-based Access Control to Medical Data Hidden in Electrocardiogram. In: 35th Annu Int Conf IEEE EMBS
45. Ramu EJSP, Swaminathan R (2016) Imperceptibility—Robustness tradeoff studies for ECG steganography using continuous ant colony optimization. Expert Syst With Appl 49:123–135. https://doi.org/10.1016/j.eswa.2015.12.010
46. Tseng K, He X, Kung W, Chen S, Liao M, Huang H (2014) Wavelet-based watermarking and compression for ECG signals with verification evaluation. Sensors. https://doi.org/10.3390/s140203721
47. Swierkosz A, Augustyniak P (2018) Optimizing wavelet ECGWatermarking to Maintain measurement performance according to industrial standard. Sensors. https://doi.org/10.3390/s18103401
48. Jero SE, Ramu P and Ramakrishnan S (2015) Steganography in Arrhythmic Electrocardiogram Signal. In: IEEE, pp. 1409–1412
49. Awasarmol SP (2017) Securely Data H iding and T ransmission in an ECG Signal using DWT. In: 2017 Int Conf Energy Commun Data Anal Soft Comput, pp. 2850–2854
50. Mathivanan P, Jero SE, and Ganesh AB (2019) QR Code-Based Highly Secure ECG Steganography. Int Conf Intell Comput Springer

51. Duy LD, Nguyen T, Minh T, Thanh TH (2017) Adaptive steganography technique to secure patient confidential information using ECG signal. In: 2017 4th NAFOSTED Conf Inf Comput Sci, pp. 336–340
52. Engin M, Engin EZ (2005) Wavelet Transformation based watermarking technique for human electrocardiogram (ECG). J Med Syst 29:589–594
53. He X, Tseng K, Huang V, Chen S, Tu S and Zeng F (2012) Wavelet-based Quantization Watermarking for ECG Signals. In: 2012 Int Conf Comput Meas Control Sens Netw. https://doi.org/10.1109/CMCSN.2012.119
54. Rubio ÓJ, Alesanco Á, García J (2013) Secure information embedding into 1D biomedical signals based on SPIHT. J Biomed Inform 46(4):653–664. https://doi.org/10.1016/j.jbi.2013.05.002
55. Soltani Panah A and van Schyndel R (2014) A lightweight high capacity ECG watermark with protection against data loss. In: Proc. 8th Int Conf Pervasive Comput Technol Heal, pp. 93–100
56. 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 Programs Biomed. https://doi.org/10.1016/j.cmpb.2017.08.015
57. 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
58. Yang C, Wang W (2016) Effective electrocardiogram steganography based on coefficient alignment. J Med Syst springer. https://doi.org/10.1007/s10916-015-0426-9
59. Patil V and Patil M 2018 Curvelet Based ECG Steganography for Protection of Data. In: Springer Int Publ
60. Sahu N, Peng D, and Sharif H 2017 Unequal Steganography with Unequal Error Protection for Wireless Physiological Signal Transmission. IN: IEEE ICC 2017 SAC Symp. E-Health Track
61. Duy TP, Tran D, and Ma W (2016) A Proposed Pattern Recognition Framework for EEG-Based Smart Blind Watermarking System. In: 2016 23rd Int Conf Pattern Recognit, pp. 955–960
62. Birvinskas D, Jusas V, Martisius I, Damasevicius R (2015) Fast DCT Algorithms for EEG data compression in embedded systems. Comput Sci Inf Syst 12(1):49–62. https://doi.org/10.2298/CSIS140101083B
63. Jiang X, Bian GB, Tian Z (2019) Removal of artifacts from EEG signals : a review". Sensors. https://doi.org/10.3390/s19050987
64. Dey N , Das P, Das A, and Chaudhuri SS (2012) Feature Analysis for the Blind—Watermarked Electroencephalogram Signal in Wireless Telemonitoring using Alattar 's Method Categories and Subject Descriptors. In: ACM, pp. 87–94
65. Pham TD, Tran D and Ma W (2015) A Proposed Blind DWT-SVD Watermarking Scheme for EEG Data. In: Springer Int, pp. 69–76, 2015. https://doi.org/10.1007/978-3-319-26561-2
66. Mukherjee A, Dey G, Dey M (2015) Web-based intelligent EEG signal authentication and tamper detection system for secure Telemonitoring. Brain-Comp Interfaces Springer. https://doi.org/10.1007/978-3-319-10978-7
67. Karakış R, Güler İ, Çapraz İ, Bilir E (2015) A novel fuzzy logic-based image steganography method to ensure medical data security. Comput Biol Med. https://doi.org/10.1016/j.compbiomed.2015.10.011
68. S Miaou and C Hsu (2000) A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability for Electronic Patient Records. In: 22nd Annu EMBS Int Conf, pp. 280–283
69. MS Nambakhsh, A Ahmadian, M Ghavami, and RS Dilmaghani 2006 A Novel Blind Watermarking of ECG Signals on Medical Images Using EZW Algorithm. In: Proc. 28th IEEE EMBS Annu. Int. Conf., vol. 2, no. 1, pp. 3274–3277
70. D Anand and UC Niranjan 1998 WATERMARKING MEDICAL IMAGES WITH PATIENT INFORMATION. In: Proc 20th Annu Int Conf IEEE Eng Med Biol Soc 20(2): 703–706
71. Acharya UR, Subbanna Bhat P, Kumar S, Min LC (2003) Transmission and storage of medical images with patient information. Comput. Biol. Med. 33:303–310. https://doi.org/10.1016/S0010-4825(02)00083-5
72. Acharya UR, Niranjan UC, Iyengar SS, Kannathal N, Min LC (2004) Simultaneous storage of patient information with medical images in the frequency domain. Comput Methods Programs Biomed. https://doi.org/10.1016/j.cmpb.2004.02.009
73. Peña R, Ávila A, Muñoz D, Lavariega J (2015) A data hiding technique to synchronously embed physiological signals in H. 264 / AVC encoded video for medicine healthcare. BioMed Res Int 2015:1–11

74. Duy TP, Tran D, and Ma W (2017) An intelligent learning-based watermarking scheme for outsourced biomedical time series data. IEEE, pp. 4408–4415
75. Parashar S, Parveen S and Izharuddin (2011) An Electronic Health Record for Medical Signal using Spread Data Hiding. In: 2011 Int Conf Multimedia, Signal Process Commun Technol, pp. 64–67
76. Pundkar H, Joshi A (2019) Steganographic scheme for outsourced biomedical time series data using an intelligent learning-a research. Int Res J Eng Technol 6:197–203
77. Dey N, Biswas D, Roy AB, and Chaudhuri SS (2012) DWT-DCT-SVD based blind watermarking technique of gray image in Electrooculogram signal. IEEE, pp. 680–685
78. Dey N, Dey G, Chakraborty S, Chaudhuri SS (2014) Feature analysis of blind watermarked electromyogram signal in wireless telemonitoring. Springer Int Publ. https://doi.org/10.1007/978-3-319-06844-2
79. Dey N, Biswas S, and Roy AB (2012) Analysis of Photoplethysmographic Signals Modified by Reversible Watermarking Technique using Prediction-Error in Wireless Telecardiology. In: Int Conf Intell infrastructure, 47th Annu Natl Conv CSI
80. Burhan N, Kasno MA , Ghazali R , Jali MH, Said R (2017) Discrete wavelet transform approach on the electromyography signal processing during rehabilitation exercise. Int J Basic Appl Sci 17:1–6
81. Dey N , Maji P, Das P, Biswas S, Das A 2012 embedding of blink frequency in electrooculography signal using difference expansion based reversible watermarking technique. Trans Electron Commun Vol. 57, no. 71
82. Rahman MS, Khalil I, Yi X (2020) Reversible Biosignal Steganography Approach for Authenticating Biosignals using Extended Binary Golay code. Heal Inform Biomed. https://doi.org/10.1109/JBHI.2020.2988449
83. Wu W, Liu B, Zhang W and Chen C (2015) Reversible data hiding in ECG signals based on histogram shifting and thresholding. In: 2nd Int Symp Futur Inf Commun Technol Ubiquitous Heal. China, May 28–30, pp. 1–5
84. Yina G, Dawei Z (2012) Single channel surface electromyography blind recognition model based on watermarking. J Vib Control. https://doi.org/10.1177/1077546310395966
85. Dey N, Biswas S, Das P A Das and Chaudhuri SS (2012) Lifting wavelet transformation based blind watermarking technique of photoplethysmographic signals in wireless telecardiology. IEEE, pp. 230–235

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.