Natgunanathan *et al.*
EURASIP Journal on Advances in Signal Processing (2024) 2024:85
https://doi.org/10.1186/s13634-024-01180-w

EURASIP Journal on Advances in Signal Processing

RESEARCH Open Access

Double-layer data-hiding mechanism for ECG signals

Iynkaran Natgunanathan[1], Chandan Karmakar[1*], Sutharshan Rajasegarar[1] and Tianrui Zong[1]

*Correspondence: karmakar@deakin.edu.au

[1] School of Information Technology, Deakin University, Burwood Campus, Geelong, VIC 3220, Australia

Abstract

Due to the advancement in biomedical technologies, to diagnose problems in people, a number of psychological signals are extracted from patients. We should be able to ensure that psychological signals are not altered by adversaries and it should be possible to relate a patient to his/her corresponding psychological signal. As far as our awareness extends, none of the existing methods possess the capability to both identify and verify the authenticity of the ECG signals. Consequently, this paper introduces an innovative dual-layer data-embedding approach for electrocardiogram (ECG) signals, aiming to achieve both signal identification and authenticity verification. Since file name-based signal identification is vulnerable to modifications, we propose a robust watermarking method which will embed patient-related details such as patient identification number, into the medically less-significant portion of the ECG signals. The proposed robust watermarking algorithm adds data into ECG signals such that the patient information hidden in an ECG signal can resist the filtering attack (such as high-pass filtering) and noise addition. This is achieved via the use of error buffers in the embedding algorithm. Further, modification-sensitive fragile watermarks are added to ECG signals. By extracting and checking the fragile watermark bits, we can determine whether an ECG signal is modified or not. To ensure the security of the proposed mechanism, two secret keys are used. Our evaluation demonstrates the usefulness of the proposed system.

Keywords: ECG signal, Authenticity, Information hiding, Watermarking, Biomedical signal processing, Discrete cosine transform

1 Introduction

In the recent years, large amount of psychological signals are used for examining patients' health. Due to the advancement of communication and the Internet technologies, these psychological signals are transmitted and shared among healthcare professionals to provide better health care services. Therefore, it is important to correctly link a patient's details such as an identification number with the person's corresponding psychological signal. Traditionally, a patient's details are included in the meta-data of the psychological signal, which can easily be corrupted. In addition to this problem, it is also important to ensure the authenticity of the psychological signal. These two problems are applicable to all the physiological signals, such as electrocardiogram (ECG), electroencephalogram (EEG), mechanomyogram (MMG), and electrooculography (EOG); however, in this paper, we limit our attention to ECG signals.

Examining ECG signals is a promising way to diagnose problems related to heart. In a modern day healthcare environment, a massive number of ECG signals are generated every day. To provide better and real-time healthcare services, ECG signal is remotely monitored [1, 2]. Since ECG signals may be examined in various healthcare facilities, it is vital to ensure that the patient details associated with those ECG signals are preserved. It is also possible that the ECG signals may be modified unintentionally. Hence, it is necessary to make sure that the healthcare professional is accessing the un-altered version of the ECG signal. We believe that data-hiding is a promising technique to address the aforementioned requirements.

The electrical activity that takes place within the heart is represented by an ECG signal. A medically significant portion of a typical ECG signal is shown in Fig. 1. In an ECG signal, points P, Q, R, S, and T are considered to be important, together with the related time intervals that are popularly known as PR-segment, QRS-complex, ST-segment, QT-interval, and PR-interval.

One of the conventional ways to relate patient details with their corresponding ECG signal is to include them in the file name of an ECG signal. However, filenames can be easily modified. To solve this problem, patient details can be included in the ECG signal itself using data-hiding techniques which are commonly referred as watermarking techniques [3, 4]. Watermarking techniques are primarily developed for multimedia contents such as an audio, image [5, 6], and video [8] to hide information (generally the copyright-related information) into the multimedia signal without noticeably reducing the perceptual quality of the original multimedia signal. The majority of them are developed for image watermarking which handles two-dimensional data. Therefore, they will not satisfy the requirement for ECG data hiding. For the aforementioned reason, it will also be difficult to use other health-image-related data hiding mechanisms such as sonar images [7] for ECG data hiding.

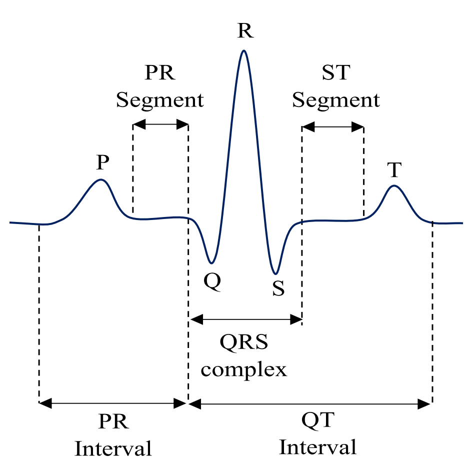

Fig. 1 A typical ECG signal that shows important points P, Q, R, S, T, and time durations QT interval, PR segment, and QRS segment

Although ECG signals are also one-dimensional signals similar to audio signals, we cannot apply audio watermarking methods for ECG data-hiding due to the difference in requirements and other constrains.

In addition to relate patient details with his/her corresponding ECG signals, it is also important to ensure the authenticity of an ECG signal. ECG signals can be intentionally or unintentionally modified for various purposes such as getting a life insurance policy. Therefore, a healthcare professional needs to know whether an ECG signal is authentic or not before he/she process or examines the signal. To the best of our knowledge, there are very limited number of approaches proposed in the literature to check the authenticity of an ECG signal.

In this paper, we propose a new double-layer data-hiding mechanism. The proposed approach contains two major parts: A robust watermarking mechanism and a fragile watermarking mechanism. The purpose of the robust watermarking mechanism is to embed patient details into the ECG signal that can withstand unintentional filtering and addition of noise. Conversely, the fragile watermarking involves incorporating watermarks that exhibit high sensitivity to all types of processing, facilitating the location identification of any unauthorized alterations within the ECG signal. Both layers of watermarks are added without lowering the medical significance of the ECG signal.

The main contribution of the proposed mechanism can be summarized as follows:

- The paper introduces a new algorithm designed to identify specific locations within an ECG signal for watermark embedding, regardless of its content or whether it has been subjected to attacks. This means it can pinpoint regions of interest within the ECG signal, even if the signal has been altered or tampered with.
- The paper presents a one-of-a-kind double-layer watermarking algorithm. What's remarkable about this approach is that it allows for the addition of a second layer of watermarking without causing interference with the watermarks added in the first layer. This innovation is crucial for ensuring the security and robustness of the watermarked ECG signals.
- The proposed watermarking mechanism in this paper has demonstrated its robustness against common types of attacks, such as filtering and noise addition. This means that the watermarked ECG signals remain intact and can be reliably retrieved even in the presence of such attacks, making it a valuable tool for ensuring data integrity and authenticity.
- In this work, fragile watermarks are employed to identify any modifications made to the original ECG signals. Fragile watermarks are sensitive to any alterations, and their presence or absence can be used to detect whether the ECG signal has been tampered with or modified. This contributes to the security and trustworthiness of ECG signal data.

The remainder of the paper is organized as follows. Section 2 discusses the related data-hiding mechanisms and their drawbacks. Section 3 presents the proposed double-layer data-hiding mechanism. The simulation results are shown in Sects. 4, and 5 concludes the paper.

2 Related work

In this section, we briefly examine contemporary techniques of data hiding that have been formulated specifically for ECG signals.

One of the pioneering works on data-hiding techniques for ECG signals was done by Engin et al. [9]. In this work, using discrete wavelet transform (DWT), an ECG signal is divided into eight bands. These bands are ordered according to the total average power. The DWT coefficients are modified based on a pseudo-random sequence, which represents the patient-related information. The embedded watermark bits are extracted by comparing the watermarked ECG signal with the original un-watermarked signal in DWT domain. Therefore, this method necessitates the availability of the un-watermarked ECG signal, thereby falling short of the initial watermarking intention as there remains a need to associate patients' information with their respective un-watermarked ECG signals. Additionally, the procedure outlined in [9] can only extract less than 85% of embedded watermark bits without error.

A DWT-based reversible data-hiding technique is presented in [10] for ECG signals. Firstly, using B-spline wavelet transform, QRS complex is identified. In the next step, watermark bits are inserted by shifting a non-QRS high-frequency wavelet coefficient bit, in the Haar lifting wavelet transform domain. The primary limitation of the approach detailed in [10] is its potential to disrupt vital medically important features in an ECG signal.

In [11], Jero et al. proposed a Curvelet-based ECG signal watermarking mechanism that considers the quality reduction due to watermark addition at the embedding end. An ECG signal is split into sub-bands using Curvelet transform. Watermarks are embedded into higher frequency bands using quantization index modulation. The approach described in [11] involves the possibility of implanting watermarks within the region of medical significance.

Using the optimized DWT, Swierkosz and Augustyniak proposed a mechanism in [12] to embed watermark bits into an ECG signal. To utilize the localized nature of the frequency content, in [12], watermarks are added in the time–frequency domain. Firstly, watermark signals are converted into a spreading sequence, and then, the sequence is added in the suitable regions in the time–frequency domain. While this method safeguards the medically crucial details within the ECG signal, the watermarks introduced through this technique lack resilience against filtering attacks.

In [13], another DWT-based approach for ECG data-hiding is presented. Firstly, a two-dimensional matrix is generated from an ECG signal. In the next step, QR codes representing patient details are obtained. QR decomposition is applied to the QR code. By altering the detailed coefficients, watermarks are embedded into the ECG signal. The primary issue with this approach lies in its dependency on the un-watermarked ECG signal for the extraction of the watermark.

In [14], authors proposed a tampered region detection mechanism for ECG signal using reversible watermarking. In this approach, artificial neural networks are employed to predict certain sample values form other samples. The difference between the estimated value and the actual value is modified to embed watermark bits. The watermarks introduced through this technique exhibit sensitivity to filtering.

As a result, the approach presented in [14] is unsuitable for concealing patient information within an ECG signal for the purpose of identification.

In [15], coefficient-alignment-based ECG watermarking mechanism is presented. In this approach, watermark bits are added in the time domain. Firstly, two group of samples are generated. The watermark bits are embedded by changing the averages of those groups. While the suggested method in [15] improves computational efficiency, the watermarks it incorporates are not robust against filtering.

In [16], authors proposed a watermarking mechanism using lead-to-lead difference of values in the baseline of an ECG. In this approach, the watermark data containing the patient information is added as noise. In [16], special attention is paid to make the added data mimic the actual noise characteristics. The approach presented in [16] lacks any form of protection against filtering attacks.

Another reversible ECG watermarking method is proposed in [17]. In [17], random forest regression, support vector regression and artificial neural network are anticipate the ECG samples and prediction error expansion technique is used to embed watermark bits into ECG signals. A significant limitation of this approach is that its reversible watermarking technique can be leveraged by adversaries to erase the incorporated patient information.

In the study presented in [18], the ECG signals undergo a watermarking process for patient identity protection. This is achieved by employing the Adaptive Normalization Factor and Least Significant Bit watermarking technique to prevent any potential mix-up between the ECG signals and the patient's personal information. Notably, this study does not focus on the medically more critical segment of the ECG signal, and alterations are also introduced within these medically significant regions.

In [19], ECG signals are embedded with patient-specific biomedical data to ensure the integrity of the patient-ECG connection. Various scenarios have been experimented with, involving different levels of signal modification resulting from the watermarking process. However, a notable limitation of this approach is its susceptibility to attacks like filtering, which can compromise the embedded watermarks.

3 Proposed double-layered watermarking mechanism

In this section, the proposed patient double-layer information hiding mechanism is presented. In the proposed mechanism, firstly, we embed patient's information in a robust manner without compromising the medical significance of an ECG signal. The purpose of this mechanism is to hide patient's information in such a manner that it will not be removed by any un-intentional attacks such as filtering and noise addition. Secondly, after robust watermarks are embedded, fragile watchmakers are added to the ECG signal without disturbing the already added robust watermarks and psychological information in the ECG signal. Only the ECG signals which are watermarked in two layers are either stored, shared or transmitted for medical diagnostic purposes.

Before processing an ECG signal, the fragile watermark bits are extracted to check whether the ECG signal underwent any modifications. If the ECG signal is unmodified, then the robust watermark bits are extracted to identify the patient associated with that ECG signal. Figure 2 shows overall structure of the proposed mechanism.

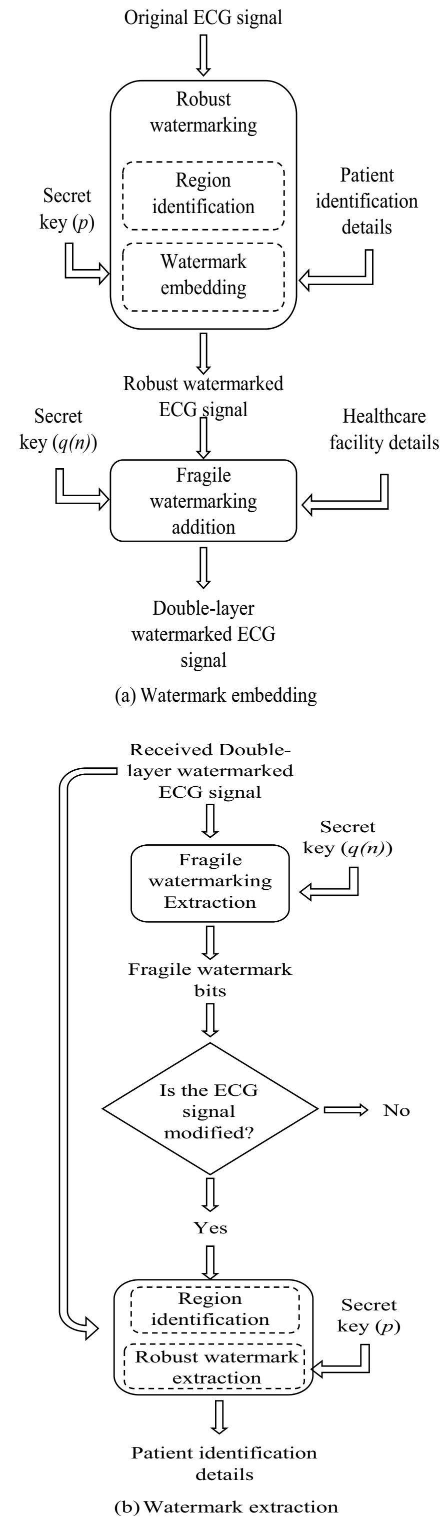

Fig. 2 The overall architecture of the proposed double -layer watermarking mechanism **a** The double layer watermark embedding mechanism **b** The watermark extraction mechanism

3.1 Robust watermarking

In this subsection, the proposed robust watermarking technique is explained in detail. The proposed technique embeds watermark bits in the less significant region of an ECG signal to preserve the medical usefulness of the signal. During the ECG signal processing, ECG signals are filtered using bandpass filter with the band pass cut-off frequencies of 0.4 and 40 Hz as a preprocessing step. Therefore, the proposed robust mechanism is developed to withstand the aforementioned unintentional bandpass filtering attack. Further, the proposed watermarking technique is designed to withstand noise addition. To add information to the ECG signal regardless of the signal content, we have proposed a novel location-finding algorithm. The experiments showed us that the location-finding algorithm can find the embedded location even when the embedded ECG signal is exposed to attacks such as filtering and noise addition.

3.1.1 Embedding area selection

In this paper, we proposed a computationally efficient technique to find the less significant region of an ECG signal for robust watermark embedding. Let us denote an ECG signal by $x(n)$. To remove the high frequency variations, a low pass filter with the cut-off frequency of f_{l1} is applied to $x(n)$ as follows:

$$x_l(n) = \mathrm{filt}_L(x(n), f_{l1}), \tag{1}$$

where "$\mathrm{filt}_L(x(n), f_l 1)$" performs low-pass filtering operation on $x(n)$ with the cut-off frequency of f_{l1}.

To identify the peak of the R-wave signal, in the next step, indices of $x_l(n)$ which are higher than a predefined value T are calculated as follows:

$$l_h(n) = \mathrm{find}(x_l(n) > T_1), \tag{2}$$

where function $find(x_l(n) > T_1)$ returns the indices of elements in $x_l(n)$ that are greater than T_1. The threshold T_1 is chosen empirically. In the next step, we find the locations of local maximums in $x_l(n)$ using

$$l_{\max}(n) = \mathrm{localMax}(x_l(n)), \tag{3}$$

where $\mathrm{localMax}(x_l(n))$ returns the local maximums by considering the gradients of $x_l(n)$. A local maximum is identified when the gradient changes from positive to a negative value. Then, we identify the indices of $x_l(n)$ corresponding to higher values (i.e., $> T$) and local maximums as follows:

$$l_1(n) = l_h(n) \wedge l_{\max}(n), \tag{4}$$

where $\wedge$ denotes the logical AND operation. In order to utilize the unique properties of an ECG signal, we also identify the troughs neighboring the peak values (corresponding to Q and S signals). To accomplish that, first we define

$$l_t(n) = \mathrm{find}(x_l(n) < T_2), \tag{5}$$

where T_2 is an empirically chosen parameter. Similar to Eq. (3), we define

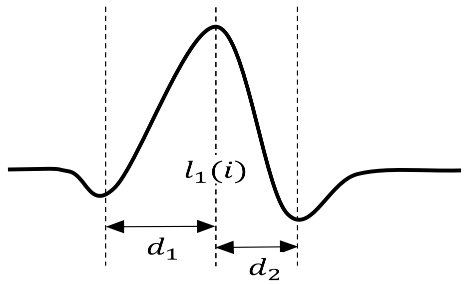

Fig. 3 An example d_1 and d_2 calculated via Eq. (9). In this example, $l_1(i)$ represents the identified peak location

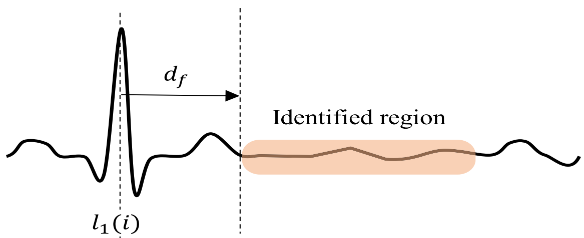

Fig. 4 An example of an ECG signal with identified robust watermark embedding region

$$l_{\min}(n) = \text{localMin}(x_l(n)), \tag{6}$$

where localMin$(x_l(n))$ returns the indices of local minimums of $x_l(n)$. A local minimum is identified when the gradient changes from negative to a positive value. Then, from Eqs. (5) and (6), a parameter $l_2(n)$ is derived as,

$$l_2(n) = l_t(n) \wedge l_{\min}(n). \tag{7}$$

From (7), we can see that $l_2(n)$ contains the locations of toughs in the signal which have values lower than T_2. To calculate the closeness of Q and S signal troughs to the identified peak locations $l_1(n)$, for the ith element on $l_1(n)$, in we define

$$[d_1, d_2] = \text{dist}(l_1(i), l_2(n)), \tag{8}$$

where dist$(l_1(i), l_2(n))$, identifies and returns the distances d_1 and d_2 (in terms of samples) between $l_1(i)$ and the closest trough locations in $l_2(n)$ on both sides of $l_1(i)$ as shown in Fig. 3.

A spike location $l_1(i)$ is considered to be valid only if it satisfies

$$d_m \geq \max(d_1, d_2), \tag{9}$$

where d_m is a predefined parameter chosen via experiments and function *max*() returns the maximum value. A region is considered to be suitable for watermarking d_f samples after a valid spike location $l_1(i)$. This is depicted in Fig. 4.

The main advantages of this region selection process can be summarized as follows:

- It can clearly identify less-significant section of an ECG signal.
- The proposed technique can accurately re-identify the region after watermark bits are added.
- This technique is specifically designed to identify the location even after unintentional filtering attack during the watermark extraction process.
- The proposed technique can work well with ECG signals that have considerable amount of fluctuations in the less significant region of the watermark signal.

3.1.2 Robust patient information embedding algorithm

Firstly, patient-related data such as patient identification number is converted into a binary sequence $w_p(n)$.

In the next step, we consider L number of consecutive samples from the selected region where L denotes the segment length. We denote a segment by $x'(n)$. Then, DCT coefficients of L samples are computed. Let us denote these coefficients as $D(k)$, which are defined as follows [20]:

$$D(k) = r(k) \sum_{n=0}^{L-1} x'(n) \cos\left\{\frac{\pi(2n+1)k}{2L}\right\} \tag{10}$$

where $k = 0, 1, ..., L-1$, and

$$r(k) = \begin{cases} \frac{1}{\sqrt{L}}, & if\ k = 0 \\ \sqrt{\frac{2}{L}}, & if\ 1 \leq k < L \end{cases}$$

To make the embedded watermarks robust against unintentional filtering, from $D(k)$, we select $D'(k)$ coefficients corresponding to a frequency range $[f_l, f_h]$. The purpose of this selection is to avoid embedding into very low and high frequency components of the signal.

To embed multiple watermark bits into one segment, N_f number of fragment pairs are generated from $D'(k)$ based on a secret key p. The secret key p is made out of randomly generated indices corresponding to $D'(k)$ that will assist in generating $2N_f$ groups of DCT coefficients. From these fragments, we form N_f fragment pairs. The fragment pair generation process is illustrated in Fig. 5. It should be noted that only one watermark bit is embedded into one fragment pair. To withstand filtering attach without compromising the quality of the ECG signal, multiple samples are used to hide a watermark.

We denote ith fragment pair by $D_i^1(k)$ and $D_i^2(k)$. Fragment pairs absolute valued averages are calculated as follows:

$$m_1 = E(|D_i^1(k)|), \tag{11}$$

$$m_2 = E(|D_i^2(k)|), \tag{12}$$

$$m = E(|[D_i^1(k), D_i^2(k)]|) \tag{13}$$

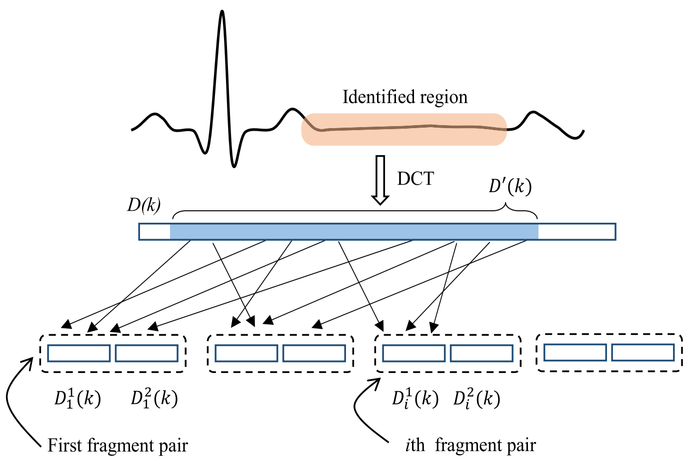

Fig. 5 Fragment pair generation from a typical ECG signal. Fragment pairs are formed using the selected DCT coefficients. A secret key p determines the DCT coefficients belong to a particular fragment pair

where $E(\cdot)$ and $|\cdot|$ denote averaging and absolute value operation, respectively. The parameter m represents the absolute valued average of the fragment pair.

Let us denote the watermarked counterparts of $D_i^1(k)$ and $D_i^2(k)$ by $Y_i^1(k)$ and $Y_i^2(k)$, respectively. We empirically chose a constant $\alpha(> 0.1)$. In the proposed approach, watermark bits are embedded according to the following rule.

- Embedding of watermark bit "0″:

  If $(m_1 - m_2) \geq \alpha.m$, then

  $Y_i^1(k) = D_i^1(k)$

  $Y_i^2(k) = D_i^2(k)$

  Otherwise (i.e., If $(m_1 - m_2) < \alpha.m$),

  $Y_i^1(k) = D_i^1(k) \times \left(\frac{\alpha m + m_2}{m_1}\right)$,

  $Y_i^2(k) = D_i^2(k)$.
- Embedding of watermark bit "1″:
  If $(m_2 - m_1) \geq \alpha.m$, then
  $Y_i^1(k) = D_i^1(k)$
  $Y_i^2(k) = D_i^2(k)$ *Otherwise* (i.e., If $(m_2 - m_1) < \alpha.m$),
  $Y_i^1(k) = D_i^1(k)$,
  $Y_i^2(k) = D_i^2(k) \times \left(\frac{\alpha m + m_1}{m_2}\right)$.

After all the watermark bits are embedded, from robust watermark embedded fragments pairs (i.e., $Y_i^1(k)$ and $Y_i^2(k)$), the watermarked ECG signal $y(n)$ is constructed by applying Inverse Discrete Cosine Transform (IDCT).

In the next step, fragile watermarks are added to $y(n)$. We denote the fragile watermark added version of $y(n)$ as $y_f(n)$. Fragile watermark adding mechanism is specifically designed to cause negligible amount of distortion to the signal. Details of the proposed fragile watermarking technique are described in Sub-section 3.2. For the illustrative convenience, we assume that the $y(n) \approx y_f(n)$, during the robust watermark extraction phase.

It is worthwhile to mention here that only a small number of bits are necessary to embed the patient identification data. In other words, we only require n_p number of bits to denote 2^{n_p} patients. For example, 26 bits can be used to represent more than 50 million patients. Since we require small number of bits to identify the patients, we embed patient information multiple times in a given ECG signal. As a result, it is always possible to link patients' information with their corresponding ECG signal even if the signal is exposed to an unintentional filtering or noise addition.

3.1.3 Robust patient information extraction mechanism

At the patient information extraction end, only the received patient information embedded signal $y'(n)$ and the secret key p are available. Clearly, at the absence of attacks, $y'(n) = y(n)$.

To extract the patient information, first the information embedded region is identified from the $y'(n)$. To perform that the embedding area selection technique described previously is utilized. It should be noted that since the proposed embedding area selection technique uses certain frequency region and the medically significant QRS complex region, it is able to successfully detect the embedded area with and without un-intentional attacks.

From the identified regions, using the secret key p generate the fragment pair $Y_i'^1(k)$ and $Y_i'^2(k)$. The fragment pair $Y_i'^1(k)$ and $Y_i'^2(k)$ is the received counterpart of the fragment pair $Y_i^1(k)$ and $Y_i^2(k)$, respectively.

Let us define the absolute average values of $Y_i'^1(k)$ and $Y_i'^2(k)$ as

$$m_1' = E(|Y_i'^1(k)|), \tag{14}$$

$$m_2' = E(|Y_i'^2(k)|). \tag{15}$$

The embedded watermark bits $w_p'(n)$ are extracted by comparing m_1' and m_2' as follows:

$$w_p'(n) = \begin{cases} 0, & \text{if } m_1' > m_2' \\ 1, & \text{if } \textit{Otherwise}. \end{cases} \tag{16}$$

After all the embedded watermark bits are extracted patients' information can be gathered using majority rule.

Let us first consider the without attack scenario. From (14) we can write

$$\begin{aligned} m_1' &= E(|Y_i'^1(k)|), \\ &= E(|Y_i^1(k)|), \end{aligned} \tag{17}$$

$$\begin{aligned} m_2' &= E(|Y_i'^2(k)|), \\ &= E(|Y_i^2(k)|). \end{aligned} \tag{18}$$

From Eqs. (17) and (18), and the embedding rule we can easily derive

$$\begin{aligned} m_1' - m_2' =& E(|Y_i^1(k)|) - E(|Y_i^2(k)|), \\ & \geq \alpha m, \end{aligned} \tag{19}$$

$$\begin{aligned} &> 0, \\ m_1' &> m_2' \end{aligned} \tag{20}$$

Therefore, we can successfully extract the embedded watermark bit from a watermark embedded DCT fragment pair.

The proposed watermarking algorithm does not use frequency coefficients which are removed by conventional band-pass filtering. This is taken into account when selecting the values for f_l and f_h. Therefore, the patient information hidden by the proposed watermarking algorithm can resist the unintentional filtering.

Let us assume that the watermark signals experience noise addition attack. We realistically assume white noise. Therefore, we can write

$$|Y_i'^1(k)| = |Y_i^1(k)| + |n_1(k)|, \tag{21}$$

$$|Y_i'^2(k)| = |Y_i^2(k)| + |n_2(k)|, \tag{22}$$

where $|n_1(k)|$ and $|n_2(k)|$ are components added to $|Y_i^1(k)|$ and $|Y_i^2(k)|$, respectively, due to the addition of noise. Now, let us consider

$$\begin{aligned} m_1' - m_2' =& E(|Y_i^1(k)| + |n_1(k)|) \\ & - E(|Y_i^2(k)| + |n_2(k)|), \\ =& E(|Y_i^1(k)|) + E(|n_1(k)|) \\ & - E(|Y_i^2(k)|) - E(|n_2(k)|), \\ \geq& \alpha m + \epsilon, \end{aligned} \tag{23}$$

where $\epsilon = E(|n_1(k)|) - E(|n_2(k)|)$. In order to successfully extract a watermark bit, we require $(\alpha m + \epsilon) \geq 0$. Due to the nature of noise, we can assume that $\alpha m > \epsilon$. Hence, we can extract the embedded watermark bits without errors even the watermark embedded ECG signal is exposed to noise addition attack.

From the embedding algorithm and the discussion above, one can see that the constant α is introduced to create an error buffer.

3.2 Fragile watermarking

The primary purpose of fragile watermarking is to identify whether the ECG signal is modified by an unauthorized person or not. Similar to robust watermarks, the fragile watermarks should not degrade medical significance of the ECG signal. However, unlike robust watermarks, fragile watermarks should be embedded into all the sections of an ECG signal as it is important to ensure the authenticity of the medically significant sections (such as QRS complex) of an ECG signal.

Firstly, we convert a generic healthcare data such as hospital identification number and convert it to a binary sequence $w_f(n) \in \{0, 1\}$. Then, using a secret key $q(n) \in \{0, 1\}$

that is made out of a random binary sequence, we generate the encrypted version of $w_f(n)$ using

$$w'_f(n) = w_f(n) \oplus q(n), \tag{24}$$

where $\oplus$ denotes the logical XOR operation.

In the next step, every sample in the ECG signal $y(n)$ is transformed into a binary sequence. Let us denote the Least Significant Bit (LSB) of all the samples by $y^{LSB}(n) \in \{0,1\}$ and its watermarked counterpart by $y_f^{LSB}(n)$. The fragile watermark bits are added using the following rule:

$$y_f^{LSB}(n) = \begin{cases} 0, & \text{if } w_f(n) = 0 \\ 1, & \text{if } w_f(n) = 1 \end{cases} \tag{25}$$

After all the LSBs are modified, from $y_f^{LSB}(n)$s, fragile watermarked ECG signal $y_f(n)$ is constructed.

At the extraction end, from $y'_f(n)$, the LSBs $y'^{LSB}_f(n)$s are generated. The signal $y'_f(n)$ and sequence $y'^{LSB}_f(n)$ are the received counterparts of $y_f^{LSB}(n)$ and $y_f(n)$, respectively. An ECG signal is considered to be unaltered when $y'^{LSB}_f(n) = y_f^{LSB}(n)$ and only the authentic ECG signals are used for diagnosis as well as further processing.

Since fragile watermarks are embedded into every sample in the ECG signal, these watermark bits are embedded into every section of the ECG signal. As a result, it is possible to identify the altered sections of an ECG signal.

From the embedding rule, we can clearly see that to embed fragile watermark bits, for half of the $y_f^{LSB}(n)$s, we do not have to do any modifications. Further, when we need to modify, only the LSB is modified. Therefore, the quality degradation of an ECG signal due to fragile watermarking is negligible.

4 Simulation results

In this section, we evaluate the performance of the proposed mechanism via simulations. For the simulations, 200 randomly selected single-channel ECG signals belonging to 20 different people are used. Each ECG signal has an approximate duration of 20 min, and all the ECG signals are sampled at a rate of 128 Hz. The simulations are performed using MATLAB in an HP workstation with Intel Core i7-4700 MQ processor, 16 GB random access memory, and Windows 10 operating system.

The embedding rate is 130 bits/s. This includes fragile watermarking of 128 bits/s and robust watermarking of 2 bits/s. It is noteworthy to mention here that we do not require higher embedding capacity as we just need to include the patient information into the ECG signal.

4.1 Evaluation of the proposed robust watermarking mechanism

To evaluate the performance of the proposed robust watermarking mechanism, in the simulations, we used $f_{l1} = 20Hz$, $f_l = 8Hz$, $f_h = 35Hz$, $T_1 = 4000$, $T_2 = -100$, $d_m = 5$, $d_f = 5$ and $\alpha = 0.8$, unless mentioned otherwise.

Figure 6 shows an example robust watermarked ECG signal together with the original ECG signal. From Fig. 6, we can see that the patient information addition does not modify the perceptually significant sections of the ECG signal.

In the first section of our simulations, we evaluate the robustness of the proposed robust watermarking mechanism in terms of robustness. To objectively measure the robustness, we define Bit-Error-Rate (BER) as follows:

$$\text{BER} = \left(\frac{\text{No. of incorrectly extracted watermarks}}{\text{No. of watermarks embedded}} \right) \times 100\%.$$

In Table 1, we compare the BERs of the proposed robust watermarking mechanism for all the 20 subjects under different scenarios. Across all the subjects, proposed mechanism can extract all the embedded watermark bits without any errors. Typically, ECG signals are pre-processed by applying low-pass filter with a cut-off frequency of 40 Hz, and high-pass filter with a cut-off frequency of 0.3 Hz. From Table 1, we can see that proposed mechanism can extract watermark bits with BERs less than 0.04%. Since patients' information is embedded multiple time, we can successfully extract the embedded patients' information via majority rule.

4.2 Sensitivity analysis

It is important to examine how sensitive the method is to parameters [21] and [22]. In the propose approach when we changed the frequency range, we observed that the medically significant information in an ECG signal could be affected. Therefore, we fix the frequency range.

The main parameter that affects the quality of the information embedded ECG signal is α. This is because the value of α is directly proportional to the error buffer size for a give fragment pair. Therefore, to find out of the effect of α in the quality of the watermarked ECG signal, in the simulations, we used the Peak-Signal-to-Noise-Ratio (PSNR) which is defined as:

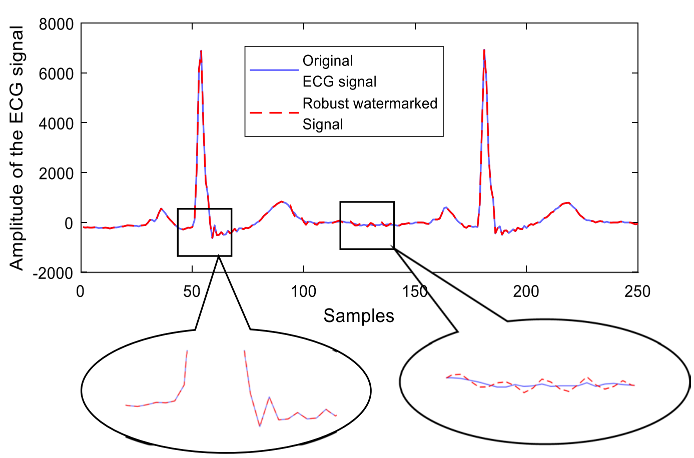

Fig. 6 An example ECG signal is plotted against amplitude and samples. The solid lines and dashed lines represent ECG signals before and after robust watermarks are added

Table 1 BERs when band-pass filter with cut-off frequencies [0.3 Hz, 40 Hz], [0.3 Hz, 38 Hz], [0.3 Hz, 36 Hz], and [0.3 Hz, 34 Hz] are applied

Signal No.	BER (%)				
	No filtering	[0.3–40] Hz	[0.3–38] Hz	[0.3–36] Hz	[0.3–34] Hz
1	0	0.02	0.03	0.06	0.45
2	0	0.01	0.02	0.18	1.02
3	0	0.01	0.04	0.16	1.25
4	0	0	0.01	0	2.48
5	0	0.01	0.03	0.34	2.61
6	0	0.02	0.03	0.15	2.01
7	0	0.01	0.05	0.48	3.81
8	0	0	0.03	0.64	2.17
9	0	0.01	0.04	0.57	2.61
10	0	0.02	0.03	0.7	3.15
11	0	0.02	0.03	0.48	3.48
12	0	0.01	0.04	0.31	3.19
13	0	0.03	0.04	0.48	3.13
14	0	0	0.03	0.42	2.94
15	0	0.01	0.04	0.53	2.17
16	0	0.01	0.03	0.21	3.78
17	0	0.01	0.08	0.47	2.8
18	0	0.02	0.03	0.29	3.14
19	0	0	0.04	0.48	2.7
20	0	0.02	0.03	0.18	2.44

Table 2 Average PSNR1 and PSNR2 values of the proposed method against varying α values

α	PSNR1 (dB)	PSNR2 (dB)
0.20	53.30	53.20
0.40	52.22	52.13
0.60	50.20	50.14
0.80	50.27	50.22
1.00	49.41	49.37
1.20	48.62	48.59
1.40	47.87	47.85
1.60	47.17	47.16
1.80	46.51	46.50
2.00	45.91	45.90

$$PNR = 10 \times \log_{10}\left(\frac{x_p^2}{MSE}\right), \tag{26}$$

where x_p^2 is the peak signal value and MSE denotes the means square error between the original signal and the signal with watermark/noise. We evaluated PSNR of the proposed mechanism for different values of α in Table 2. In Table 2, PSNR1 and PSNR2 denote the PSNR values before and after fragile watermarks are added.

Table 2 shows how the parameter α influences the quality of the ECG signal measure in terms of PSNR values when signal and double layer watermarks are added to the

ECG signal. Using Table IV, one can choose the α value based on the specific application needs. From Table 2, one can see that PSNR values decrease with increasing values of α, as expected. Moreover, closeness of the PSNR1 and PSNR2 values shows that the addition of fragile watermarks does not have any significant impact on the quality of the watermarked ECG signals. It should be highlighted that even though PSNR increases with α, regardless of the value of α, no robust watermarks are embedded into the medically significant portion of the ECG signal.

4.3 Robustness analysis

To assess the proposed robust watermarking technique under severe filtering, we applied band-pass filter with cut-off frequencies of [0.3 Hz, 38 Hz], [0.3 Hz, 36 Hz], and [0.3 Hz, 34 Hz]. As expected, BER increases with the severity of the attack. However, the proposed mechanism can achieve BERs of less than 4% under all the considered filtering attacks.

We also compare the robustness of the proposed mechanism against two recently published approaches presented in [13] and [15]. Table 3 provides BERs of all three methods under band-pass filtering with cut-off frequencies 0.3 Hz, 40 Hz], [0.3 Hz, 38 Hz], [0.3 Hz, 36 Hz], and [0.3 Hz, 34 Hz]. From Table 3, we can clearly see that all three methods can extract the watermark bits where there is no filtering applied. However, the methods in [13] and [15] completely fail under all the considered filtering attacks as in most cases their BERs are closer to the chance level of 50%. Across all the considered attacks the proposed method's BER values are less than 3%.

To make sure we performed a fair comparison, we also compared the PSNR of the proposed mechanism with methods in [13, 15, 18] and [19]. We also made the embedding capacities of other methods similar to the proposed method. Results of the comparisons are presented in Table 4. From Table 4, we can observe that the proposed method obtains a higher PSNR value compared to the methods in [13, 15, 18] and [19].

In addition to the filtering, we also evaluate the robustness of the proposed method against noise addition. We calculate the BERs of the proposed method when white Gaussian noise is added to the watermarked signal. Table 5 shows the BERs when the SNR values are 20 dB, 15 dB, 10 dB, 5 dB, 0 dB, and -5 dB. We can see from Table 5 that the proposed robust mechanism is extremely robust to the noise addition. For ECG signals belong to all the 20 subjects, the proposed method achieves 0% BERs when SNR

Table 3 Average BERs of the proposed method with the methods in [13, 15, 18] and [19], when band-pass filter with different cut-off frequencies are applied

Band-pass frequencies (Hz)	BER (%)				
	Method in [13]	Method in [15]	Method in [18]	Method in [19]	Proposed method
No filtering	0.00	0.00	0.00	0.00	0.00
0.3-40	44.27	36.74	32.63	35.72	0.012
0.3-38	48.61	34.43	35.14	37.64	0.035
0.3-36	45.34	37.49	41.64	41.94	0.357
0.3-34	49.71	45.62	43.17	42.18	2.57

Table 4 Average PSNR values of the methods in [13, 15, 18, 19] and the proposed method when all the methods have similar embedding capacity

Methods	PSNR (dB)
[13]	48.7412
[15]	24.3187
[18]	47.9427
[19]	46.1746
Proposed	50.22

Table 5 Average BERs of the proposed method, when different amounts of noise are applied to the watermarked ECG signal

Signal No.	BER (%)					
	SNR=20 dB	SNR=15 dB	SNR=10 dB	SNR=5 dB	SNR=0dB	SNR=-5 dB
1	0	0	0	0	0	0
2	0	0	0	0	0.03	0.03
3	0	0	0	0	0	0
4	0	0	0	0	0.1	0.11
5	0	0	0	0	0.022	0.41
6	0	0	0	0	0	0
7	0	0	0	0	0	0.01
8	0	0	0	0	0.01	0.03
9	0	0	0	0	0.01	0.02
10	0	0	0	0	0.01	0.01
11	0	0	0	0	0	0.01
12	0	0	0	0	0	0
13	0	0	0	0	0.09	0.18
14	0	0	0	0	0	0
15	0	0	0	0	0	0.02
16	0	0	0	0	0.03	0.14
17	0	0	0	0	0.15	0.18
18	0	0	0	0	0.07	0.16
19	0	0	0	0	0	0
20	0	0	0	0	0.02	0.024

values are equal to 5dB or above. As anticipated, the BERs increase with the amount of noise addition. However, the proposed mechanism achieves BERs less than 0.2% across all amounts of noise additions.

4.4 Evaluation of the proposed fragile watermarking mechanism

As mentioned previously, the purpose of the proposed fragile watermarking is to assist the detection of any unauthorized modification of the ECG signal. As a result, we embedded watermark bits throughout the entire ECG signal. Hence, it is important to ensure that the medical usefulness of the ECG signal is preserved after the addition of the Fragile watermarks.

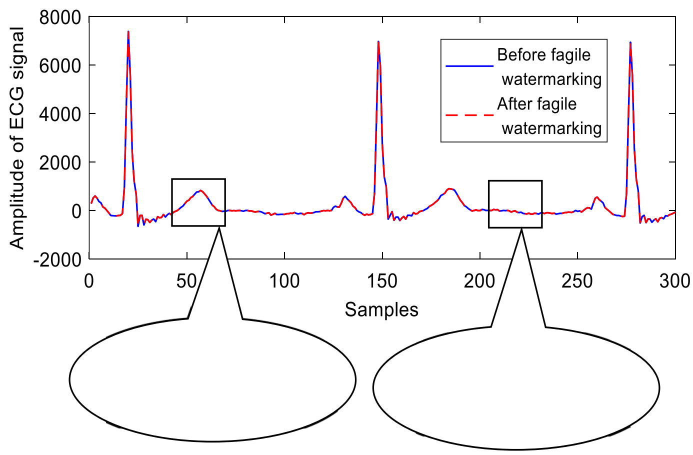

Fig. 7 A randomly selected real-world ECG signals is plotted against amplitude and samples. The solid lines and dashed lines represent ECG signals before and after fragile watermarks are added

Table 6 PSNR values of the proposed method after only robust watermark bits are added (denoted by PSNR1) and after both robust and fragile watermark bits are added (denoted by PSNR2)

Signal No.	PSNR1 (dB)	PSNR2 (dB)
1	51.426	51.413
2	49.843	49.784
3	50.147	50.122
4	48.814	48.807
5	51.343	51.329
6	48.671	48.663
7	50.144	50.127
8	49.768	49.745
9	50.414	50.398
10	48.976	48.718
11	51.261	51.242
12	50.312	50.304
13	49.67	49.653
14	50.786	50.764
15	51.122	51.114
16	50.537	50.521
17	49.687	49.658
18	50.25	50.241
19	51.043	51.024
20	50.241	50.228

Figure 7 shows a randomly selected ECG signals before and after fragile watermarking. From Fig. 7, we can clearly see that the ECG signals before and after fragile watermarks are added look near identical. Therefore, we can conclude that the fragile watermarking does not affect the previously embed robust watermarks and do not degrade the medical significance of the ECG signal.

To quantitatively asses the quality of the ECG signals before and after fragile watermark embedding across different ECG signal, we evaluate the PSNR values which are presented in Table 6. From Table 6, it can be seen that PSNR values before (PSNR1) and after (PSNR2) adding fragile watermarks are extremely closer to each other. This implies that addition of fragile watermark bits has a negligible impact on the quality of the ECG signals.

The primary requirements of fragile watermarks are error-free detection when there is no modification and vulnerability to any form of modification. To experimentally verify this, we calculated the BERs with and without filtering attacks. Table 7 shows the BERs when there is no filtering, and band-pass filtering with cut-off frequencies [0.3 Hz, 40 Hz], [0.3 Hz, 45 Hz], [0.3 Hz, 50 Hz], [0.3 Hz, 55 Hz], and [0.3 Hz, 60 Hz]. From Table 7, it is evident that we can extract all the embedded fragile watermark bits in the absence of filtering (i.e., without any processing) and fragile watermarks are completely disturbed when there is a filtering attacks. We can come to this conclusion because when fragile watermark bits are exposed to the filtering attacks the BERs are very closer to the chance level of 50%. Therefore, using the proposed fragile watermarking technique we can identify the modified regions of an ECG signal.

4.5 Summary of comparison with other methods

In this section, we summarize the performance of the proposed method with related resent methods in [13, 15–18] and [19] with the proposed approach. The review presented in this paper shows that the proposed method has all essential features and the

Table 7 Fragile watermark BERs of the proposed method, when band-pass filter with cut-off frequencies [0.3 Hz, 40 Hz], [0.3 Hz, 45 Hz], [0.3 Hz, 50 Hz], [0.3 Hz, 55 Hz], and [0.3 Hz, 60 Hz] are applied

Signal No.	BER (%)					
	No filtering	[0.3–40] Hz	[0.3–45] Hz	[0.3–50] Hz	[0.3–55] Hz	[0.3–60] Hz
1	0	49.83	50.17	50.05	50.16	50.19
2	0	49.99	49.9	49.71	50.12	50.11
3	0	50.21	50.12	49.97	50.11	49.82
4	0	49.75	49.88	50.01	49.89	50.07
5	0	50.11	49.79	49.86	49.91	49.95
6	0	50.24	50.12	50.16	50.86	49.87
7	0	49.94	49.87	49.91	49.9	49.93
8	0	49.97	50.11	49.9	50.27	50.07
9	0	50.08	49.78	50.18	50.16	50.09
10	0	49.96	49.96	49.97	50.08	49.79
11	0	50.13	50.07	50.2	49.86	50.16
12	0	49.77	49.85	49.95	50.15	49.94
13	0	49.86	50.16	50.09	49.7	50.03
14	0	50.13	49.94	50.17	50.17	49.86
15	0	50.04	50.07	49.95	49.85	50.04
16	0	49.82	49.75	50.14	50.04	49.91
17	0	49.96	49.85	49.91	49.97	49.82
18	0	50.17	50.2	50.07	49.83	50.18
19	0	50.09	49.87	49.88	50.14	49.92
20	0	50.18	50.17	49.86	50.16	49.9

other methods cannot detect small changes to an ECG signal and they are not robust to filtering attacks.

In addition, as previously shown in Tables 3 and 4, the proposed methods outperform other methods in terms of robustness while maintaining better signal quality.

To the best of our knowledge, there is no ECG watermarking or other mechanism that can simultaneously detect any changes to any part of the ECG signal and add patient information in a robust manner without affecting the medical usefulness of the ECG signal.

5 Conclusion

In this paper, a novel double-layer data-hiding mechanism is presented. The proposed mechanism not only hides patient information into an ECG signal but also helps ECG signal modification detection.

By considering the unique characteristics of QRS complex region of an ECG signal, an algorithm is proposed to identify the medically less significant regions of an ECG signal. The embedding region identification mechanism is specifically designed to ensure re-identification of the region after watermarks are added. Further, the region identification mechanism can withstand unintentional filtering and noise addition. A new algorithm is proposed for robust watermarking in DCT domain. The proposed robust watermarking algorithm embeds watermarks by changing the relationship between certain DCT coefficients. The DCT coefficients are selected using a secret key to ensure the security. We have theoretically shown and experimentally verified that the robust watermarks can resist unintentional filtering and noise addition. This is mainly achieved through the introduction of an error buffer during the embedding process and careful selection of the DCT coefficients. Experimental results show the superior performance of the proposed robust watermarking method in terms of robustness and quality compared to the recent ECG watermarking methods presented in [13] and [15].

In the proposed data-hiding mechanism, fragile watermark bits are added after robust watermarks are embedded. At the receiver end, firstly, fragile watermark bits are extracted to determine whether the ECG signal underwent any modification or not. To accomplish this, modification-sensitive fragile watermark bits are added throughout the entire ECG signal. We have shown in the paper that the addition of fragile watermarks has negligible effect on the quality of the ECG signal.

Currently, all the ECG signals are treated by the same algorithm. The experimental results show that the proposed approach works well across all the ECG signals considered in terms of both quality (reflected by PSNR) and robustness (assessed in terms of BER). While this is a strength of the proposed algorithm, the embedding rate may need to be improved when there is a need for large amount of data to be embedded. To further enhance the embedding rate, accuracy and quality of the ECG signals, more specific algorithms can be developed after classifying the ECG signals using mechanism such as the one presented in [23]. This will be our future work.

Acknowledgements
We acknowledge other researches who provided valuable advice to improve the quality of the paper.

Author contributions
IN developed the concept, proposed the solution, performed the experiments, and wrote the first draft of the paper. CK assisted in the development of the core idea, revised the paper, and supervised the project. SR contributed to the interpretation of the results and revision of the paper. TZ helped with the formation of the proposed solution and the experimentation.

Funding
The authors have no funding to declare.

Availability of data materials
The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Authors have the consent for the publication.

Competing interest
The authors have no conflict of interest to declare.

Received: 2 May 2023 Accepted: 16 October 2023
Published online: 16 September 2024

References
1. Y. Lin, I. Jan, P. Ko, Y. Chen, J. Wong, G. Jan, A wireless PDA-based physiological monitoring system for patient transport. IEEE Trans. Inf Technol. Biomed. **8**(4), 439–447 (2004)
2. F. Hu, M. Jiang, M. Wagner, D. Dong, Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/ software codesign. IEEE Trans. Inf Technol. Biomed. **11**(6), 619–627 (2007)
3. S.G. Rizzo, F. Bertini, D. Montesi, Fine-grain watermarking for intellectual property protection. EURASIP J. Inform. Secur. **10**(1), 1–20 (2019)
4. S. Thakur, A.K. Singh, S.P. Ghrera et al., Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed Tools Appl. **78**, 3457–3470 (2019)
5. R. Biswas, S.K. Bandyapadhay, Random selection based GA optimization in 2D-DCT domain color image steganography. Multimedia Tools Appl. **79**, 7101–7120 (2019)
6. M. Azhdari, A. Mahmoodzadeh, M. Khishe, M. Rezaii, Digital image watermarking using the combination of genetic algorithm and spread spectrum method in the field of discrete cosine transform. Iran. J. Marine Sci. Technol. **25**(97), 14–32 (2021)
7. M. Mousavi, Y.H. Khani, E. Shafiee, M. Khishe, Watermark retrofitting in side scan sonar images using advanced encryption standard algorithm. Iran. J. Mar. Sci. Technol. **22**(85), 1–11 (2018)
8. M.Z. Konyar, O. Akbulut, S. Öztürk, Matrix encoding-based high-capacity and high-fidelity reversible data hiding in HEVC. SIViP **14**(5), 897–905 (2020)
9. M. Engin, O. Cidam, E.Z. Engin, Wavelet transformation based watermarking technique for human electrocardiogram (ECG). J. Medical Syst. **29**(6), 589–594 (2005)
10. K. Zheng, X. Qian, Reversible data hiding for electrocardiogram signal based on wavelet transforms. Proc. Int. Conf. Comput. Intell. Secur. **1**, 295–299 (2008)
11. S.E. Jero, P. Ramu, Curvelets-based ECG steganography for data security. Electron. Lett. **52**(4), 283–285 (2016)
12. A. Swierkosz, P. Augustyniak, Optimizing wavelet ECG watermarking to maintain measurement performance according to industrial standard. Sensors **18**(10), 3401 (2018)
13. P.V. Sanivarapu, K.N.V.P.S. Rajesh, N.V.R. Reddy, N.C.S. Reddy, Patient data hiding into ECG signal using watermarking in transform domain. Phys. Eng. Sci. Med. **43**, 213–226 (2020)
14. S. Bhalerao, I.A. Ansari, A. Kumar, D.K. Jain, A reversible and multipurpose ECG data hiding technique for telemedicine applications. Pattern Recogn. Lett. **125**, 463–473 (2019)
15. C.-Y. Yang, W.-F. Wang, Effective electrocardiogram steganography based on coefficient alignment. J. Med. Syst. **40**(66), 1–15 (2016)
16. P. Augustyniak, Differential watermarking of multilead ECG baseline, in *Proceedings 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2019, pp. 5681-5684
17. S. Bhalerao, I. A. Ansari and A. Kumar, Reversible ECG Data Hiding: Analysis and Comparison of ANN, Regression SVM and Random Forest Regression, in *Procedings 2020 International Conference Communication and Signal Processing (ICCSP)*, 2020, pp. 0667-0671
18. B. Halder and S. Mitra, Modified watermarked ECG signals by using adaptive normalization factor, in *Proceedings IEEE 2nd International Conference on Recent Trends in Information Systems (ReTIS)*, Kolkata, India, 2015, pp. 434-439
19. A. Ibaida, I. Khalil, and R. van Schyndel, A low complexity high capacity ECG signal watermark for wearable sensor-net health monitoring system, *Comput. Cardiol.*, Hangzhou, China, 2011, pp. 393-396
20. J.L. Wu, J. Shin, Discrete cosine transform in error control coding. IEEE Trans. Commun. **43**(5), 1857–1861 (1995)

21. T. Hu, M. Khishe, M. Mohammadi, G.-R. Parvizi, S.H.T. Karim, T.A. Rashid, Real-time COVID-19 diagnosis from X-Ray images using deep CNN and extreme learning machines stabilized by chimp optimization algorithm. Biomed. Signal Process. Control **68**, 102764 (2021)
22. C. Wu, M. Khishe, M. Mohammadi, K.S.H. Taher, T.A. Rashid, Evolving deep convolutional neutral network by hybrid sine-cosine and extreme learning machine for real-time COVID19 diagnosis from X-ray images. Soft Comput. **27**(6), 3307–3326 (2021)
23. S. Afrakhteh, M. Mosavi, M. Khishe, A. Ayatollahi, Accurate classification of EEG signals using neural networks trained by hybrid population-physic-based algorithm. Int. J. Autom. Comput. **17**(1), 108–122 (2020)

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