IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 14, 2020, accepted August 27, 2020, date of publication September 21, 2020, date of current version October 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3025533

Robust Patient Information Embedding and Retrieval Mechanism for ECG Signals

IYNKARAN NATGUNANATHAN, (Member, IEEE), CHANDAN KARMAKAR, (Member, IEEE), SUTHARSHAN RAJASEGARAR, (Member, IEEE), TIANRUI ZONG, AND AHSAN HABIB, (Graduate Student Member, IEEE)
School of Information Technology, Deakin University, Geelong, VIC 3220, Australia

Corresponding author: Chandan Karmakar (karmakar@deakin.edu.au)

ABSTRACT At present, a patient's demography, such as name, age, and gender are stored separately from the acquired electrocardiogram (ECG) signal. This multiple storage mechanisms can create a severe threat to the reliability of diagnostics if the link between the demography data and the ECG signal breaks, either intentionally or unintentionally. This issue has become more prominent in recent years due to the use of a large number of wearable devices for physiological signal collection, especially in remote or non-clinical settings. In order to address this problem, in this paper, we propose a novel mechanism to embed patient's information within an ECG signal without degrading the accuracy of the physiological information contained in the ECG signal. In this work, a methodology is presented to find the less-significant region of the ECG signal. Then, the patient information is hidden in this region by modifying the selected discrete cosine transform (DCT) coefficients of the signal using our proposed embedding and decoding algorithms. Moreover, the patient information hidden in the ECG signal is able to resist filtering attack, such as high-pass filtering, which generally occur with the ECG signal processing. This is achieved via the use of error buffers in the embedding algorithm. The proposed mechanism can extract the embedded patient information, either in the presence or without the filtering attack. Moreover, a specifically designed synchronization sequence is added to identify the patient data embedded regions of the ECG signal at the decoding end. Further, as a security measure, the embedded patient details are scrambled using a secret key to protect the privacy of the patient. Our evaluation demonstrates the usefulness of the proposed methodology in successfully embedding the patient information without distorting the important medical information in an ECG signal.

INDEX TERMS ECG signal, information hiding, watermarking, physiological signal processing, discrete cosine transform.

I. INTRODUCTION

Due to the advancement in biomedical related technologies and the increasing elderly population, a huge amount of physiological signals are generated, transmitted, processed, and stored every day. In general, patient's details, such as patient ID, age, and date of birth form part of the medical record, and traditionally they are stored separately from the other diagnostic information. For example, a patient's medical signal, such as an electrocardiogram (ECG), is usually linked to the patient's details via the filename of the medical record. Although some identification process is being used for tracking the patient from whom these data were collected, they are vulnerable to cyber attacks, given the volume of the data, and face the consequences from minimal adoption of advanced technologies in the medical settings. Since this can cause serious harm to patients and other organizations, such as health insurance companies, it is important to use a robust mechanism to relate the patient's details with his/her corresponding biological signal. While it is vital to tag patient's physiological signals, such as Electrocardiogram (ECG), Electroencephalogram (EEG), Mechanomyogram (MMG), and Electrooculography (EOG), in this paper, we limit our focus to ECG signals.

The number of cardiac or cardiovascular patients has increased in recent years, partly due to unhealthy eating habits and a sedentary lifestyle. One of the popular mechanisms to detect cardiac (heart) abnormalities is via an ECG examination. A large number of people undergo relatively easier and pain-free ECG examinations, and therefore, a massive amount of ECG signals are generated every day. Furthermore, the advancement in the medical field enabled remote ECG patient monitoring as a part of point-of-care applications in hospitals [1], [2]. Typically, in remote ECG

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed Farouk.

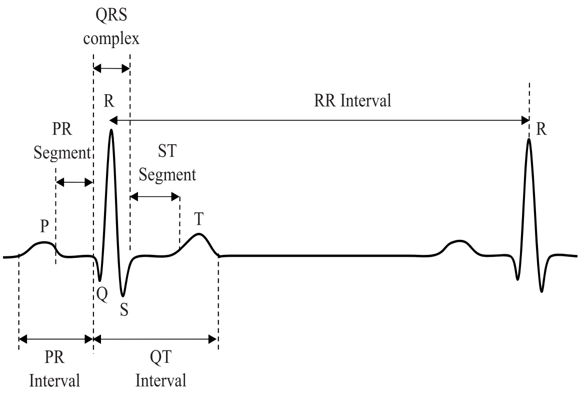


FIGURE 1. A typical ECG signal that shows significant points P, Q, R, S, and T, and significant regions PR interval, QT interval, PR segment, QRS segment (series of three deflections that reflect the current associated with right and left ventricular depolarization), QRS complex, ST segment, and RR interval.

patient monitoring, patient's ECG signals are generated using body sensors and transmitted to health care facilities primarily via the Internet. Because the ECG signals are generated in various places, such as hospitals and patients' houses, transmitted via insecure communication channels, and then processed in different places, there is a need to ensure that the patients' identity details are not lost, and can be accurately obtained from corresponding ECG signals.

Similar to most of the physiological signals, it is important to preserve the biological content of an ECG signal. In other words, modifications made to the ECG signal should not compromise the utility of the signal, since alteration in the underlying physiological phenomena of a signal has the potential to create misdiagnosis and life-threatening problems in patients.

An ECG signal measures the electrical activity that takes place within the heart. Primary activities of the heart generate portions of the ECG signal, known as P-wave (atrial depolarization), QRS-complex (includes Q-wave, R-wave, and S-wave, which are a series of three deflections that reflect the current associated with right and left ventricular depolarization), and T-wave (ventricular repolarization) [3]. Therefore, in an ECG signal, points P, Q, R, S, and T are considered to be important, together with the related time intervals which are commonly known as PR-interval, PR-segment, QRS-complex, ST-segment, QT-interval, and RR-interval. Fig. 1 shows a typical ECG signal with important points and the time intervals. From Fig. 1, one can clearly see that, since the region covered by PR-interval and QT-interval contains crucial data, this section of the ECG signal should not undergo any alteration. Therefore, in the proposed mechanism we embed the patients' information within the non-significant region of the ECG signal, as shown in Fig. 2.

The traditional procedures, where a patient's details are linked using the file name of the medical record, can sufferer from issues such as accidental alteration of the filename. To overcome this problem, patients' details can be embedded in the ECG signal. In order to embed this information, watermarking techniques can be used [4], [5], where the patient's details are the watermarks. Watermarking is a technique in which information is hidden inside a host signal (such as an audio, image [6], video [7], and ECG signal) without significantly degrading the quality of the host signal. A good patient detail embedding algorithm should exhibit the following properties:

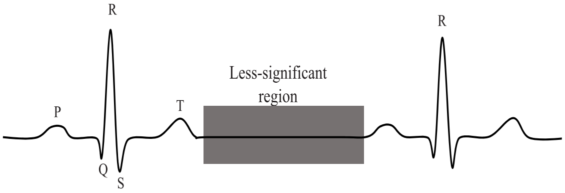


FIGURE 2. A typical ECG signal that shows the region of less-significance together with the points P,Q, R, S, and T.

- All the bio-medically significant information in an ECG signal should be preserved.
- It should be possible to extract all the embedded information from the ECG signal whenever necessary.
- The embedding and the extraction algorithms should ensure that the patient's details can be extracted even after any filtering operation performed, as it is usually applied as a pre-processing step in the ECG signal processing.
- The algorithm designed to embed the metadata and extract the required information in the ECG signal should have low computational complexity. This enables real-time embedding.
- The algorithm should be robust to security attacks, i.e., an adversary should not be able to steal the embedded patient's information from the ECG signal, even if the adversary has the knowledge of the embedding and the extraction algorithms.

Incorporating the above requirements, in this paper, we propose a quantization index modulation (QIM) based patient information embedding and identification mechanism for ECG signals. In particular, an ECG signal is partitioned into segments, and the suitability of each segment for watermark embedding is determined using a proposed region identification algorithm. This ensures that the biomedical information in the ECG signal is not disturbed. Specially designed synchronization bits are added to the eligible segments to facilitate the identification of watermarked segments at the decoding end, during the retrieval process. Then, the scrambled patient's information, in the form of one dimensional binary vector, is embedded into the segment by modifying the selected discrete cosine transform (DCT) coefficients of the signal. The modification is performed based on the proposed QIM based watermarking algorithm. Our proposed extraction mechanism can extract all the embedded information without requiring any ECG related prior information. Further, an error buffer is introduced in the watermark embedding process to ensure successful watermark extraction at the decoding end, when the watermarked ECG signal is exposed to filtering attack.

One of the primary objectives of this work is to ensure that the patient-related information is not removed unintentionally during the normal usage of the ECG signal. The filtering operation, also known as filtering attack, is considered in this work because, in usual ECG signal processing stages, very low and high frequency components are often removed to enhance the ECG signal, without compromising the medical significance of the ECG signal. The robustness of our proposed algorithm for filtering attack is demonstrated in the evaluation section.

The remainder of the paper is organized as follows. Section II discusses the existing mechanisms and their drawbacks. Section III presents the proposed patient information embedding and identification mechanisms. The simulation results are shown in Section IV, and Section V concludes the paper.

II. RELATED WORK

In this section, existing works related to data hiding in ECG signals are briefly discussed together with the popular mechanisms that are designed to hide data into audio signals. The related works in audio signals are considered here as they are one dimensional signals, similar to ECG signals.

A. DATA HIDING METHODS DEVELOPED FOR ECG SIGNALS

A few approaches have been developed in the literature related to data hiding in ECG signals, and here we briefly survey them. One of the early works of data hiding related to ECG signal was done by Engin *et al.* [8]. In this approach, an ECG signal is split into eight bands using a dyadic wavelet transform. The eight bands are sorted according to an overall average power. The patient's information, represented by a pseudo-random sequence, is added to the DWT coefficients. The embedded watermarks are extracted by comparing the watermarked ECG and the original (un-watermarked) ECG signal. In other words, this method requires the original ECG signal for extraction. This limits the usage of this method in practical applications. In addition, the approach in [8] has a bit-error-rate (BER) of more than 15%.

In [9], the authors proposed another DWT based reversible data hiding technique for ECG signals. In their method, firstly, QRS complex is detected by applying a B-spline wavelet transform on the un-watermarked ECG signal. Then, in the Haar lifting wavelet transform domain, the watermark bits are embedded by shifting a non-QRS high-frequency wavelet coefficient bit to the left. Due to the nature of the algorithm, for certain ECG signals, the algorithm presented in [9] can degrade the biomedical information in the ECG signal. The problems associated with this method include the modification of biologically significant regions.

By considering the ECG signal distortion due to the addition of watermark bit (i.e., patient's detail), a Curvelets-based method is proposed by Jero *et al.* in [10]. In [10], a Curvelet transform is used to decompose the ECG signal into frequency sub-bands. Then, in the high frequency subbands, watermark bits are embedded using QIM. The positions of the modified coefficients are passed to the decoder. Using the position information and the threshold selection algorithm, watermark bits are extracted. The method in [10] can disturb certain important parts of an ECG signal. The method in [10], alters the signal even in the medically significant region and therefore limiting the usability in practice.

In [11], Swierkosz and Augustyniak presented a mechanism, which uses optimized DWT to embed watermark bits into ECG signals. This method embeds watermark bits into the time-frequency ECG representation. The watermark sequence is first transformed into noise like samples. Then, the noise in the data container area of the time-frequency ECG representation is replaced by the noise like sample. This technique is used to make the watermark bits undetectable and protect the medical information in the ECG signal. A major problem with this method is that it is vulnerable to filtering attacks.

Another DWT based ECG data hiding mechanism is proposed in [12]. Here, first, the authors generated two dimensional (2D) data matrix from one dimensional ECG data, and using a third-party application, a QR code is obtained corresponding to the patients' information. Then the 2D ECG data is decomposed using the wavelet transform. QR decomposition is applied to the QR code and the detailed coefficients of the wavelet. The watermark coefficients are embedded into the ECG signal by modifying the coefficients obtained as a result of QR decomposition. A major drawback of the method is that it requires the original (i.e., un-watermarked) ECG signal components at the watermark extraction end.

A reversible ECG watermarking mechanism is presented in [13]. The primary goal of this paper is to address false ownership claims and detect the tampered region of the ECG data. In the proposed work, authors use artificial neural networks to estimate a particular sample value from neighbouring sample values. The prediction error (i.e., the difference between the predicted value and the actual value) is modified to embed watermark bits. The mechanism in [13] embeds watermark bits by modifying the least significant bits (LBSs). Since this method uses LBS technique, the method in [13] is vulnerable to typical ECG processing, which includes unintentional filtering.

Two coefficient-alignment based ECG data hiding mechanism is proposed in [14]. Unlike most of the ECG data hiding mechanisms, in here, the authors have embedded the watermarks directly into the ECG samples in the time domain. Firstly, two average values corresponding to two adjacent groups of ECG samples are computed. Then the watermark bits are embedded by effectively changing the difference between those two average values. Although the process is less complex for watermark embedding, it is vulnerable to filtering attacks. Further, the approach modifies the data in all parts of an ECG signal, including the medically significant region.

B. DATA HIDING METHODS DEVELOPED FOR AUDIO SIGNALS

In this subsection, we briefly introduce the popular techniques used for audio watermarking and discuss the advantages and limitations when applying them to the ECG signals for data hiding.

Since ECG signals are one dimensional signals, one dimensional multimedia watermarking techniques, such as audio watermarking techniques, can be considered for direct application with the ECG signals. For example, in audio watermarking there are several mechanisms developed using techniques, such as patchwork [15]–[18], spread spectrum [21]–[27], echo-hiding [28]–[35], and support vector regression [38]–[40]. These techniques satisfy the requirements of audio watermarking, such as imperceptibility and robustness. In audio watermarking, a small amount of signal distortion is permitted as the human auditory system (HAS) is incapable of detecting small changes. However, we cannot allow signal distortions in medically significant regions of an ECG signal. Moreover, in audio watermarking, plenty of samples are available, therefore it is relatively easier to hide a large amount of information into an audio signal. For example, the typical sampling rate of an audio signal is 44.1 kHz, while the typical sampling rate of an ECG signal is 128 Hz. In other words, 44100 samples are available from one second of an audio clip compared to 128 samples from one second of an ECG signal.

In the patchwork based audio watermarking techniques [15]–[20], two or more groups are formed from features extracted from the audio signals (such as Fourier transform or DCT coefficients). Then, the relationship between the statistical properties (such as the average of absolute values) of those groups is modified based on the watermark bit. At the decoding end, watermarks are extracted by comparing the statistical properties of the feature groups. In order to make this method robust, a large amount of elements in each group is required. Therefore this method cannot be easily used to embed data into ECG signals.

There is a large amount of spread spectrum based watermarking methods available in the literature [21]–[27]. In a typical spread spectrum based audio watermarking method, pseudo-noise (PN) sequence is added to the audio signal in a specific domain, such as the time domain or the frequency domain. The watermark bits are embedded by changing the polarity of the entire PN sequence. At the detection end, watermarks are extracted by correlating the watermarked audio signal with the PN-sequence. Theoretically, the spread spectrum based method can successfully extract all the embedded bits when they are infinitely long. For finite-length sequences, host signal interference causes errors in detection. To minimize this error, sufficiently longer sequences should be used. Since we do not have a large number of samples in a typical ECG signal, this technique cannot be directly applied for data hiding in ECG signals.

In audio watermarking, echo-hiding [28]–[37] based techniques are used, as they use the inability of HAS to detect low amplitude echo with short delays. In a classical echo based watermarking method, artificially created echo delays are adjusted based on the watermark bit. At the decoding end, the echo delays are detected in Cepstrum domain. Echo-hiding based methods also require a large amount of samples for successful watermark extraction. In addition, echo-hiding based methods have very low embedding capacities. These drawbacks limit their application to ECG signals.

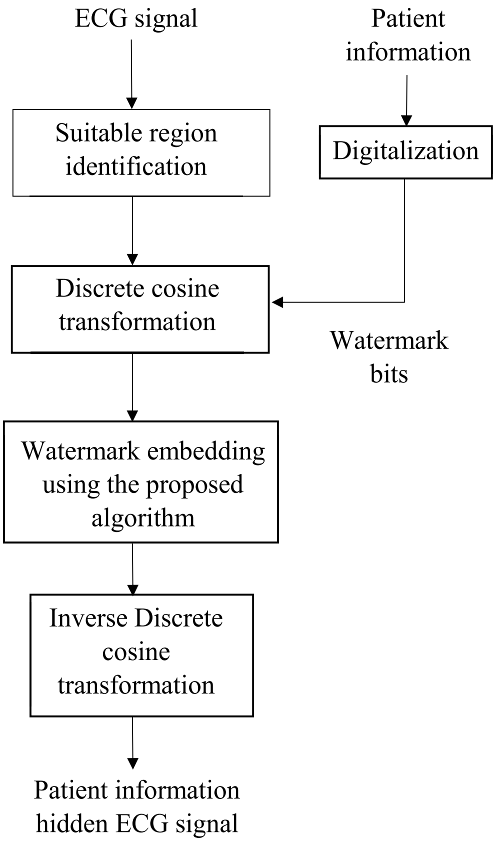

ECG signal
Patient information
Suitable region identification
Digitalization
Discrete cosine transformation
Watermark bits
Watermark embedding using the proposed algorithm
Inverse Discrete cosine transformation
Patient information hidden ECG signal

FIGURE 3. The proposed patient information embedding mechanism.

Support vector regression (SVR) [38]–[40] based watermarking methods primarily use a universal classification algorithm to identify the embedded watermark bits. The SVR based methods are initially trained using training sequences. Then the trained model is used to extract the embedded watermark bits. For robust watermark embedding, the watermark embedding mechanisms used in [38]–[40] require a considerably large amount of samples, and therefore, SVR based methods are not ideally suitable for data hiding in ECG signals.

III. PROPOSED PATIENT IDENTIFICATION MECHANISM

In this section, a patient information hiding mechanism is proposed. In the first subsection, the technique used in the proposed mechanisms to identify suitable regions in an ECG signal is explained. Fig. 3 shows the proposed patient information hiding mechanism. The following two subsections elaborate the patient information hiding and extraction mechanism, respectively.

A. REGION IDENTIFICATION

Similar to most of the physiological signals, it is very important to preserve the biological content of an ECG signal. In other words, modifications made to the ECG signal should

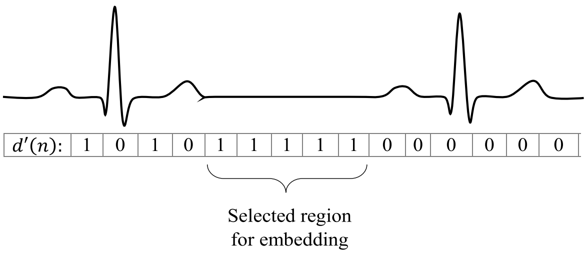


FIGURE 4. An example ECG signal with corresponding $d'(n)$ calculated via Eq. (3). In this example, the region with more than 4 (i.e. $L_s = 4$) consecutive "1" for $d'(n)$ values are selected for watermark embedding.

not compromise the utility of the signal, as an alteration in underlying physiological information of a signal has the potential to create life-threatening problems in patients.

The fundamental idea behind the development of the proposed region identification technique is to automatically identify the regions without considerable fluctuations. Let us denote the ECG signal by $e(n)$ and length of the ECG signal by N samples. We denote the moving average at n^{th} sample $M(n)$ as,

$$M(n) = \left\{ \frac{e(n-L_w) + \cdots e(n) + \cdots + e(n+L_w)}{2L_w + 1} \right\} = \frac{1}{(2L_w+1)} \left(\sum_{i=(n-L_w)}^{(n+L_w)} e(i) \right) \quad (1)$$

where, empirically chosen parameter L_w denotes half of the averaging window size. The average value $M(n)$ can be calculated using Eq. (1).

After calculating $M(n)$ for all n values, deviation of each sample $d(n)$ from the corresponding $M(n)$ is computed by

$$d(n) = |e(n) - M(n)|, \quad (2)$$

where $|\cdot|$ denotes the absolute value operator and $n = 1, 2, \ldots, N$. Define $d'(n)$ as

$$d'(n) = \begin{cases} 1, & \text{if } d(n) \leq T_1 \\ 0, & \text{Otherwise,} \end{cases} \quad (3)$$

where parameter T_1 is an empirically chosen threshold value.

Let us assume that the length of a data hiding segment is L_s. The information is hidden in the regions which can give at least L_s continuous values, denoted as $d'(n)$ equal to "1". Fig. 4 shows an example of the region suitable for information hiding.

B. PATIENT INFORMATION HIDING

1) PREPROCESSING OF PATIENT INFORMATION

In order to hide the information, such as patient ID and date-of-birth, first, the information is converted into one dimensional stream $w(n)$ of ones and zeros.

To protect the private details of the patient, a binary sequence secret key $s(n)$ can be used. The key is used to scramble $w(n)$ and generate another binary sequence $w'(n)$ which can be written as

$$w'(n) = w(n) \odot s(n), \quad (4)$$

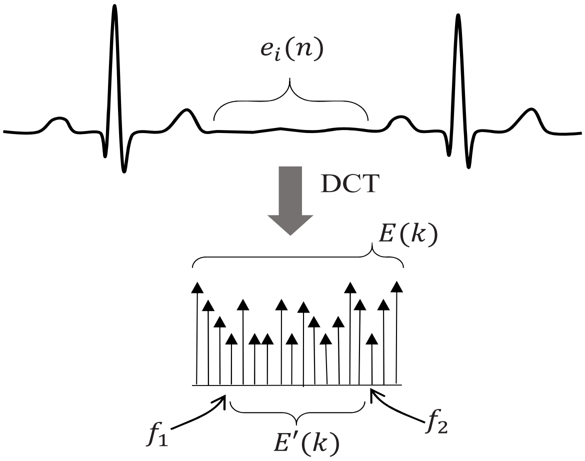


FIGURE 5. A typical ECG signal with region selected for watermark embedding $e_i(n)$ is shown together with the corresponding DCT coefficients $E(k)$. From $E(k)$, suitable DCT coefficients $E'(k)$ are chosen by considering the minimum and maximum frequencies, f_1 and f_2, respectively.

where $\odot$ represents any scrambling operation, such as an XOR operation. The scrambling ensures that no one can access the patient's details without knowing the secret key $s(n)$, even if they have the knowledge about the patient information hiding algorithm.

2) PATIENT INFORMATION HIDING ALGORITHM

In the proposed mechanism, we developed a unique watermarking algorithm considering patient identification and requirements related to the ECG signal. In this context $w'(n)$ acts as the watermark.

As an initial step, we segment the samples in time domain with a fixed sample length of L_s. We denote the ith segment as $e_i(n)$. In the next step, the suitability of a segment $e_i(n)$ for watermark embedding is checked by the aforementioned region identification algorithm. For the suitable segments, DCT (discrete cosine transform) coefficients are computed. Let us denote these coefficients as $E(k)$, which are defined as follows [41]:

$$E(k) = t(k) \sum_{n=0}^{L_s-1} e_i(n) \cos \left\{ \frac{\pi(2n+1)k}{2L_s} \right\} \quad (5)$$

where $k = 0, 1, \ldots, L_s - 1$, and

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

After all the DCT coefficients corresponding to $e_i(n)$ are calculated, DCT coefficients $E'(k)$ corresponding to a certain frequency range $[f_1, f_2]$ are selected. This process ensures that the embedded information can withstand the unintentional commonly occurring filtering operations during ECG processing. Fig. 5 illustrates the $E'(k)$ generation process. The patient identification information in the binary form (i.e., $w'(n)$) is embedded via modifying $E'(k)$. We extract the magnitudes and signs of the elements in $E'(k)$ as follows.

$$E_a(k) = |E'(k)|, \tag{6}$$

$$S(k) = \text{sign}(E'(k)), \tag{7}$$

where $E_a(k)$ and $S(k)$ represent the magnitudes and the signs of the $E'(k)$, and the modified sign$(\cdot)$ is given by

$$\text{sign}(E'(k)) = \begin{cases} +1, & \text{if } E'(k) \geq 0 \\ -1, & \text{if } E'(k) < 0. \end{cases}$$

Even though we should be able to use the region identification algorithm at the decoding end to identify the watermark embedded segments in an ideal scenario, we may not be able to identify all of them correctly when the watermark embedded signal is exposed to the filtering attack. Therefore, another technique is necessary to identify the watermarked segments at the extraction end. To facilitate this, we embed special bits, called synchronization bits, at the start of each segment.

Considering the importance of the synchronization bits at the detection end, we developed a new method to embed synchronization bits. We first generate a synchronization bit sequence of length L_y using alternating ones and zeros (i.e., $1, 0, 1, 0 \ldots$). In the synchronization bit embedding process, the samples in $E_a(k)$ are set closer to a predefined value. To minimize the disturbance caused to the signal, we choose two predefined values E_1 and E_2 satisfying the conditions,

$$E_1 \ll E_2, \tag{8}$$

and

$$E_{min} < \{E_1, E_2\} < E_{max}, \tag{9}$$

where E_{min} and E_{max} denote the minimum and the maximum values $E_a(k)$ can take, respectively. Then the mean value of $E_a(k)$ is calculated. Let us denote the mean value of the corresponding L_y number of DCT coefficients in $E_a(k)$ by m_E. The predefined value of a given segment E_t is determined by

$$E_t = \begin{cases} E_1, & \text{if } |m_E - E_1| \leq |m_E - E_2| \\ E_2, & \text{if } |m_E - E_1| > |m_E - E_2|. \end{cases} \tag{10}$$

Let us denote the modified counterpart of $E_a(i)$ as $E_w(i)$, The synchronization bits are embedded into $E_a(k)$ via

$$E_w(i) = \begin{cases} (1-\alpha)E_t, & \text{if syn bit is “0”} \\ (1+\alpha)E_t, & \text{if syn bit is “1”}. \end{cases} \tag{11}$$

where α is a constant satisfying $0 < \alpha < 1$ and index i denotes the ith element in $E_w(k)$.

After all the synchronization bits are embedded, watermark bits are embedded using a quantization index modulation based algorithm. Let us denote the step size and the error buffer size as S_s and B_s, respectively. We define parameters P_1 and P_2 as follows.

$$P_1 = \text{floor}\left(\frac{E_a(i)}{S_s}\right), \tag{12}$$

$$P_2 = \text{mod}\,(P_1, 2)\,, \tag{13}$$

where floor$(\cdot)$ is a function which rounds the elements to the nearest integer towards minus infinity, and mod$(P_1, 2)$ returns the reminder of the division $P_1/2$. In the proposed mechanism, a watermark bit w_b is embedded according to Algorithm 1. In Algorithm 1, shaded areas denote the sections of the algorithm corresponding to watermark bits “0” and “1”, respectively

Algorithm 1 Algorithm to Embed Watermark Bits

```
Input: $w_b, P_1, P_2, E_a(i), S_s, B_s$
Output: $E_w(i)$
Set $E_w(i) = E_a(i)$
if $w_b = 0$ then
    if $P_2 = 0$ then
        if $E_a(i) < (P_1 \cdot S_s + B_s)$ then
            $E_w(i) = P_1 \cdot S_s + B_s$
        else if $E_a(i) > ((P_1 + 1) \cdot S_s - B_s)$ then
            $E_w(i) = (P_1 + 1) \cdot S_s - B_s$
        else
            Do Nothing
        end if
    else
        if $E_a(i) < (P_1 \cdot S_s + S_s/2)$ then
            $E_w(i) = P_1 \cdot S_s - B_s$
        else
            $E_w(i) = (P_1 + 1) \cdot S_s + B_s$
        end if
    end if
else
    if $P_2 = 1$ then
        if $E_a(i) < (P_1 \cdot S_s + B_s)$ then
            $E_w(i) = P_1 \cdot S_s + B_s$
        else if $E_a(i) > ((P_1 + 1) \cdot S_s - B_s)$ then
            $E_w(i) = (P_1 + 1) \cdot S_s - B_s$
        else
            Do Nothing
        end if
    else
        if $(E_a(i) < (P_1 \cdot S_s + S_s/2))$
        and $(P_1 \cdot S_s - B_s) > 0$ then
            $E_w(i) = P_1 \cdot S_s - B_s$
        else
            $E_w(i) = (P_1 + 1) \cdot S_s + B_s$
        end if
    end if
end if
return $E_w(i)$
```

After all the watermark bits are embedded, by using the signs of DCT coefficients $S(k)$ together with modified DCT coefficient magnitudes, information embedded DCT coefficients (i.e. coefficients with signs) are generated. Then the patient information containing ECG signal is constructed by applying inverse discrete cosine transform. Let us denote the time domain information containing ECG signal using $e_w(n)$.

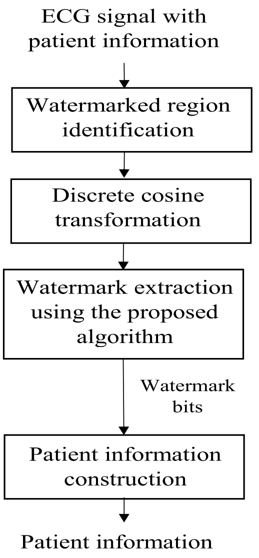

ECG signal with patient information
Watermarked region identification
Discrete cosine transformation
Watermark extraction using the proposed algorithm
Watermark bits
Patient information construction
Patient information

FIGURE 6. The proposed patient information extraction mechanism.

C. PATIENT INFORMATION EXTRACTION

Fig. 6 shows the proposed patient information extraction process. In order to extract the hidden patient information, parameters related to the proposed algorithm (L_s, f_1, f_2, S_s), need to be available at the extraction end. To perform the patient information extraction, we ideally want to have $e_w(n)$. However, in ECG single processing, ECG signal may undergo filtering. Therefore in this context, filtering can be considered as an unintentional attack on the signal $e_w(n)$. Hence, we denote the ECG signal available at the extraction end by $e'_w(n)$. Clearly, $e'_w(n) = e(n)$, when there is no attack.

Firstly, the received signal $e'_w(n)$ is segmented with a segment length of L_s. At this point, we need to determine whether the segment is a watermarked segment or not. However, we cannot use the region identification algorithm used during the patient information hiding phase. This is because the possible filtering attack may have altered the signal, and this can cause misidentification of the watermarked segments. To overcome this problem, we introduced a synchronization bit sequence detection mechanism to identify the watermarked segments.

Following the similar approach used during the embedding phase, we apply DCT transform to the segment and then select the coefficients corresponding to the frequency range $[f_1, f_2]$. Let us denote the absolute values of the selected DCT coefficients by $E'_w(k)$.

To determine whether watermark bits are embedded in $E'_w(k)$ or not, synchronization bits are used. Firstly, we calculate the mean value of the first L_y DCT coefficients m'_E as follows:

$$m'_E = \frac{1}{L_y}\left(\sum_{i=1}^{L_y} E'_w(i)\right). \tag{14}$$

From the watermark embedding algorithm, one can easily understand that the value of m'_E is closer to either E_1 or E_2. Therefore, the parameter E'_t can be calculated as follows.

$$E'_t = \begin{cases} E_1, & \text{if } |m'_E - E_1| \leq |m'_E - E_2| \\ E_2, & \text{if } |m'_E - E_1| > |m'_E - E_2|. \end{cases} \tag{15}$$

In the next step, we generate odd and even sequences S_1 and S_2, respectively, by grouping the first Ly coefficients of $E'_w(k) = \{E'_w(1), E'_w(2), \ldots, E'_w(L_y)\}$ as follows.

$$S_1 = \{E'_w(1), E'_w(3), E'_w(5), \ldots\}, \tag{16}$$

$$S_2 = \{E'_w(2), E'_w(4), E'_w(6), \ldots\}. \tag{17}$$

The segment is considered to be a watermarked segment if all of the following conditions are satisfied:

$$\begin{aligned} E'_t(1+\alpha) - \Delta &< \min(S_1), \text{ and} \\ E'_t(1+\alpha) + \Delta &> \max(S_1), \text{ and} \\ E'_t(1-\alpha) - \Delta &< \min(S_2), \text{ and} \\ E'_t(1-\alpha) + \Delta &> \max(S_2), \end{aligned}$$

where Δ is an empirically chosen parameter, introduced to tolerate changes due to potential attacks, and functions $\min(\cdot)$ and $\max(\cdot)$ return minimum and maximum values of the input elements, respectively. In our mechanism, Δ acts as an error buffer.

For the segments, which contain watermarks, parameters P'_1 and P'_2 are calculated for all the remaining coefficients in $E'_w(k)$ (i.e., for $E'_w(Ly+1), E'_w(Ly+2), \ldots$) as follows.

$$P'_1 = \text{floor}\left(\frac{E'_a(i)}{S_s}\right), \tag{18}$$

$$P'_2 = \text{mod}\left(P'_1, 2\right). \tag{19}$$

Using Eq. (19), scrambled watermark bits can be calculated using

$$\text{Extracted bit} = \begin{cases} 0, & \text{if } P'_2 = 0 \\ 1, & \text{if } \mathit{Otherwise}. \end{cases} \tag{20}$$

Once all the embedded bits are extracted, by un-scrambling using the secret key $s(n)$, the original binary stream can be generated.

Note that our goal here is to relate a patient's medical signal to his/her details. Therefore, we just need to embed an identification number into the ECG signal. Hence, In the proposed mechanism 2^{n_b} number of patients can be identified using just n_b watermark bits. For example, using 20 bits of watermarks more than 1 million patients can be identified. In other words, only a small number of bits are required to embed the patients' information into an ECG signal. This provides the luxury of embedding a patient's information multiple times into one ECG signal. As a result, even when errors occur, embedded watermark bits can be successfully extracted using the majority rule. Furthermore, embedding multiple times also assists in identifying the patient even when only a part of the ECG signal is available.

Remark 1: *The proposed algorithm not only embeds the patient's information within the less-significant region of the ECG signal, but also does not alter RR-interval. In other*

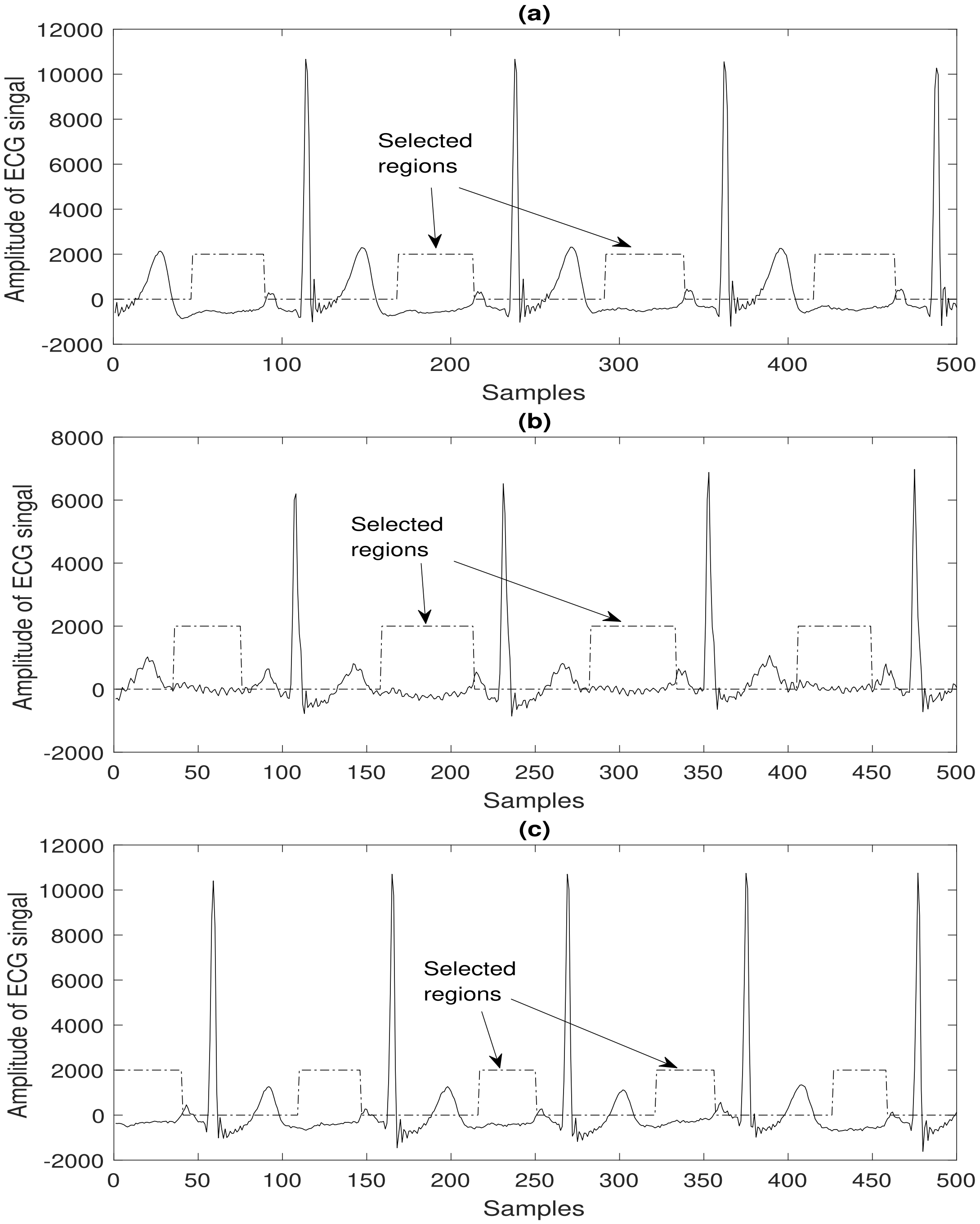


FIGURE 7. **Three randomly selected real-world ECG signals are plotted against amplitude and samples in (a), (b), and (c). The dashed lines in these figures take non-zero values when the region is suitable for watermark embedding.**

words, we can say that the proposed mechanism does not degrade the physiologically relevant information of an ECG signal.

IV. SIMULATION RESULTS

In this section, the performance of the proposed patient identification mechanism is illustrated by simulation results. In the simulations, 250 randomly selected single-channel ECG signals collected from 25 different people are used. Each ECG signal has an approximate duration of 20 minutes, and all of them are sampled at a rate of 128 Hz.

The DCT coefficients are calculated using all the ECG samples in a given segment, and we set $f_1 = 5$ Hz and $f_2 = 35$ Hz. By considering the robustness and the information content of the ECG signal, after watermark embedding, we empirically set $L_w = 15$ samples, $L_y = 6$ samples, $L_s = 30$ samples, $S_s = 100$, $B_s = 48$, $E_1 = 200$, $E_2 = 2000$, $\alpha = 0.4$, and $\Delta = 45$.

From our simulations, we observed that in a typical 20 min ECG signal, we were able to embed 5365 watermark bits. In other words, for a hospital with 1 million patient records (i.e., which requires 20 bits as $2^{20} \approx 1$ million) we can

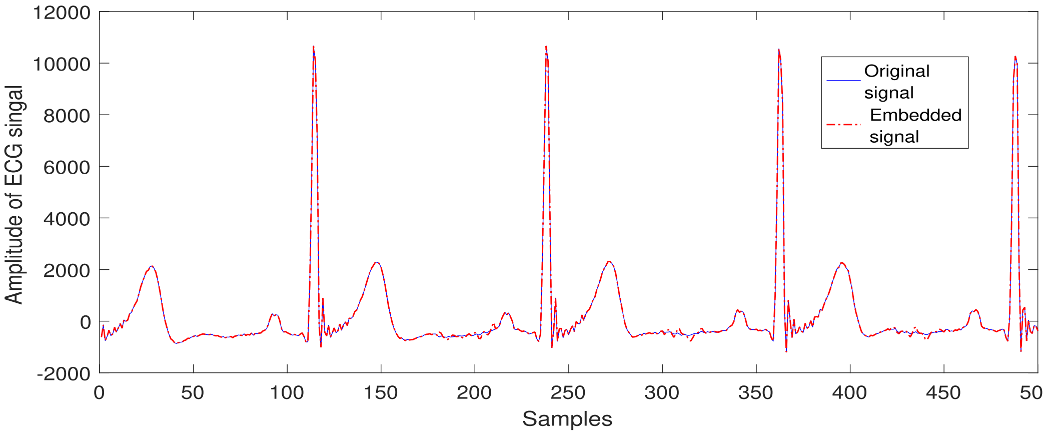


FIGURE 8. A real-world ECG signal together with its watermarked counterpart are shown against amplitude and samples. Continuous line shows the original ECG signal and the dashed line shows its watermarked version.

TABLE 1. BERs when band-pass filter with cut-off frequencies [0.3 Hz, 40 Hz], [1 Hz, 35 Hz], [1 Hz, 35 Hz], [1.5 Hz, 30 Hz], [2 Hz, 25 Hz], and [2.5 Hz, 20 Hz] are applied.

Signal No.	BER (%)					
	No filtering	[0.3-40] Hz	[1-35] Hz	[1.5-30] Hz	[2-25] Hz	[2.5-20] Hz
1	0.00	0.00	0.68	1.42	2.12	2.53
2	0.00	0.01	0.66	2.81	3.52	5.42
3	0.00	0.01	1.07	3.25	4.14	5.12
4	0.00	0.01	0.50	1.70	1.70	2.30
5	0.00	0.00	1.80	2.40	4.26	5.61
6	0.00	0.00	0.50	1.20	1.60	2.10
7	0.00	0.04	1.36	2.51	4.70	5.30
8	0.00	0.00	0.12	1.26	1.05	2.46
9	0.00	0.05	1.46	3.11	5.14	6.24
10	0.00	0.00	1.04	1.42	3.46	4.10
11	0.00	0.00	0.13	1.07	1.74	3.70
12	0.00	0.00	0.05	1.24	1.67	2.41
13	0.00	0.00	0.03	1.04	1.55	2.16
14	0.00	0.02	1.89	2.43	3.32	5.41
15	0.00	0.01	1.57	2.81	4.89	6.47
16	0.00	0.00	0.43	2.17	3.49	5.94
17	0.00	0.01	1.86	2.48	4.90	5.18
18	0.00	0.00	0.28	2.77	5.04	6.24
19	0.00	0.01	0.24	1.48	3.06	4.18
20	0.00	0.01	0.06	1.47	2.46	3.48
21	0.00	0.00	1.13	2.71	3.14	5.19
22	0.00	0.05	1.23	3.37	3.51	4.48
23	0.00	0.13	1.78	2.43	4.18	5.74
24	0.00	0.00	0.15	1.84	2.54	4.71
25	0.00	0.02	1.43	3.47	4.51	5.60

embed $5365/20 = 268$ times. Since patients' identifiers are embedded multiple times, majority rule can be used to extract the correct patients' identifiers.

TABLE 2. Average PSNR values of the ECG based data hiding methods in [12] and [14], and the proposed method.

Methods	PSNR (dB)
[12]	48.4174
[14]	22.5814
Proposed	49.8175

Firstly, we evaluate the effectiveness of the region selection algorithm. Figs. 7 (a), (b), and (c) show the embedding regions selected by the proposed region selection algorithm. From these figures, one can see that the proposed algorithm only selects the regions that are not biologically significant.

In the next part, we embed watermarks (i.e., patient's information in digital form) into the ECG signals. Fig. 8 depicts a typical ECG signal together with its watermarked counterpart. Fig. 8 clearly shows that the watermark embedding process only affects the less-significant region of the ECG signal. As proof of concept, we extract the watermark bits and compare them with embedded watermark bits. To objectively measure the performance of the watermarking algorithm, we use Bit-Error-Rate (BER), as defined below:

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

We were able to extract all the embedded watermark bits from all 250 ECG signals with 0% BER (i.e., without any error).

TABLE 3. Average BERs of the proposed method with the ECG based hiding methods in [12] and [14], when band-pass filter with different cut-off frequencies are applied.

Band-pass frequencies (Hz)	BER (%)		
	Method in [12]	Method in [14]	Proposed method
No filtering	0.00	0.00	0.00
0.3-40	48.04	36.93	0.02
1-35	49.24	39.32	0.86
1.5-30	49.46	44.27	2.15
2-25	49.63	46.61	3.27
2.5-20	50.24	49.27	4.48

TABLE 4. Average BERs of the proposed method with the methods in [24], [26], and [21], when band-pass filter with different cut-off frequencies are applied.

Band-pass frequencies (Hz)	BER (%)			
	Method in [26]	Method in [24]	Method in [21]	Proposed method
No filtering	18.10	0.00	22.35	0.00
0.3-40	21.12	1.88	27.36	0.02
1-35	21.19	5.99	27.62	0.86
1.5-30	21.37	10.97	28.12	2.15
2-25	21.53	18.29	34.41	3.27
2.5-20	22.14	22.85	38.05	4.48

A common practice in ECG signal processing is to subject the ECG signals to undergo low-pass filtering with a cut-off frequency of 40 Hz, and high-pass filtering with a cut-off frequency of 0.3 Hz. Therefore, to check the robustness of the proposed watermarking algorithm, we performed a band-pass filtering operation on the ECG signal with the cut-off frequencies of [0.3 Hz, 40 Hz], [1 Hz, 35 Hz], [1 Hz, 35 Hz], [1.5 Hz, 30 Hz], [2 Hz, 25 Hz], and [2.5 Hz, 20 Hz]. Table 1 shows the average BERs for all the 25 patients. From Table 1, it can be clearly seen that the proposed mechanism achieves BERs of less than 0.2 % across all the ECG signals when a band-pass filter with cut-off frequencies of [0.3 Hz, 40 Hz] is used. Further, BER increases with the severity of the band-pass filtering, as expected.

We compared the robustness of the proposed mechanism against two recent ECG related mechanisms presented in [12] and [14]. The Table 2 shows the PSNR values obtained for all the three methods. One can clearly see from Table 2 that the PSNR values of the proposed mechanism are greater than that of the mechanisms in [12] and [14]. Further, it should be noted that our proposed approach does not embed a watermark bit in the medically significant region of the ECG signal. In the Table 3, we compare the BERs of all the three methods against the various filtering attacks. We clearly see from Table 3 that all the three methods can successfully extract all the embedded watermark bits when there is no attack. However, the proposed method achieved less than 5% BER under all the attack scenarios, while the mechanisms in [12] and [14] achieved BERs closer to 50%. This implies that the mechanisms in [12] and [14] completely fail under all the considered filtering attack scenarios. From Tables 2 and 3, we can conclude that the proposed mechanism outperforms the methods in [12] and [14] in terms BER, while maintaining higher PSNR values.

To further evaluate the robustness of the proposed mechanism, we have compared the proposed algorithm with similar watermarking algorithms presented in [24], [26], and [21]. The results are presented in Table 4. As anticipated, BERs of all the algorithms increases with wider bandpas filtering. From Table 4, it is clear that the proposed method outperforms the methods in [24], [26], and [21], for all bandpass filtering scenarios. This is primarily due to the fact that the algorithms presented in [24], [26], and [21] require larger segment/block lengths to perform well.

TABLE 5. Average PSNR and correlation values of the proposed method against varying step size (S_S). The error buffer is set to ($S_S/2 - 2$).

S_s	PSNR (dB)	Correlation coefficient
25	51.7427	0.9997
50	51.3387	0.9997
75	50.6729	0.9996
100	49.8175	0.9995
125	48.9145	0.9994
150	47.9766	0.9993

Table 4 also shows that the proposed mechanism achieves higher BERs when the cut-off frequencies are [2 Hz, 25 Hz] and [2.5 Hz, 20 Hz]. However, it is important to consider the effect these filtering causes on the ECG signal. Fig. 9 shows a band-pass filtered ECG signal with cut-off frequencies of [2 Hz, 25 Hz] and [2.5 Hz, 20 Hz] together with the original ECG signal. From Fig. 9 it is clear that band-pass filtering the signal with the cut-off frequencies of [2 Hz, 25 Hz] and [2.5 Hz, 20 Hz] significantly alters the signal, and hence removes the usefulness of the ECG signal.

Finally, we evaluate the influence of the step size (S_s) and error buffer size (B_s) on the embedding. In this evaluation, to compare the similarities between the watermarked ECG signal and the original (i.e., un-watermarked) ECG signal, we used the peak-signal-noise ratio (PSNR) and the cross-correlation coefficients. Clearly, higher values of PSNR and cross-correlation coefficients reveal strong similarities between the watermarked ECG signal and the original ECG signal. From Tables 5 and 6, one can easily see that the closeness between the watermarked ECG signal and the original ECG signal decreases with increasing S_s and B_s.

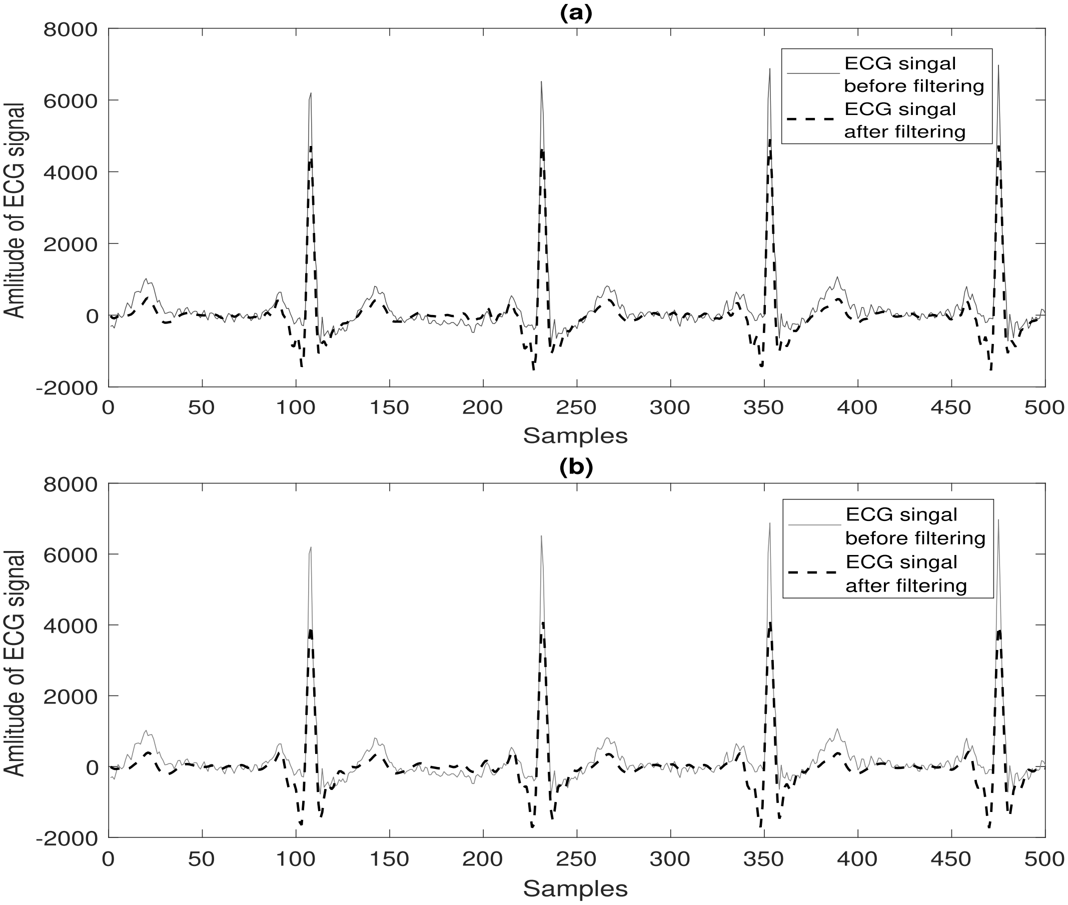


FIGURE 9. Two randomly selected real-world ECG signals are shown with their filtered counterparts. (a) The filtered ECG signal (represented by dashed line) underwent band-pass filtering, where the pass band frequency range is 2-25 Hz. (b) The filtered ECG signal (represented by dashed line) underwent band-pass filtering, where the pass band frequency range is 2.5-20 Hz.

TABLE 6. Average PSNR and correlation values of the proposed method against varying error buffer(B_s) size, where $S_s = 100$.

B_s	PSNR (dB)	Correlation coefficient
5	50.7964	0.9996
15	50.5910	0.9996
25	50.3709	0.9996
35	50.1375	0.9996
45	49.8928	0.9995

V. CONCLUSION

In this paper, we proposed a new information embedding and identification mechanism for ECG signals. By considering the fluctuations and the medically significant regions in the ECG signal, a region identification algorithm is proposed to identify the medically less-significant region of an ECG signal for embedding. An algorithm is proposed to embed the patient's information in the less-significant region of the ECG signal by modifying certain discrete cosine transform (DCT) coefficients. DCT coefficients are selected in such a way to ensure that the embedded DCT coefficients can withstand the unintentional filtering process, which commonly occurs during the ECG signal processing. The proposed watermark embedding and decoding algorithms are able to successfully embed and extract the patient's information from an ECG signal, for both with and without filtering attack scenarios. Error buffers are introduced in our embedding algorithm to enhance the robustness of our method against the filtering attack. In addition, to detect the embedded watermark segments after the attack, and to guarantee the watermark extraction from portions of the ECG signal, a specifically designed synchronization bit embedding, and detection technique is applied. Furthermore, the proposed mechanism ensures that the embedded watermarks do not alter important features, such as RR-interval, of an ECG signal. As a security feature, a secret key is used, in the proposed work, to scramble the patient's identification information before they are added to the ECG signal. This secret key is required at the decoding stage to retrieve the patient's information by de-scrambling the extracted bits. This technique prohibits an unauthorized person from accessing a patient's information. The evaluation demonstrated the robustness and the reliability of the proposed mechanisms. Further, the proposed algorithm is general and can be easily adapted to use with other signals for information embedding and retrievals, such as with electroencephalogram signals and seismic signals.

REFERENCES

[1] Y.-H. Lin, I.-C. Jan, P. C.-I. Ko, Y.-Y. Chen, J.-M. Wong, and G.-J. Jan, "A wireless PDA-based physiological monitoring system for patient transport," *IEEE Trans. Inf. Technol. Biomed.*, vol. 8, no. 4, pp. 439–447, Dec. 2004.

[2] F. Hu, M. Jiang, M. Wagner, and D.-C. Dong, ''Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign,'' *IEEE Trans. Inf. Technol. Biomed.*, vol. 11, no. 6, pp. 619–627, Nov. 2007.

[3] L. Biel, O. Pettersson, L. Philipson, and P. Wide, ''ECG analysis: A new approach in human identification,'' *IEEE Trans. Instrum. Meas.*, vol. 50, no. 3, pp. 808–812, Jun. 2001.

[4] S. G. Rizzo, F. Bertini, and D. Montesi, ''Fine-grain watermarking for intellectual property protection,'' *EURASIP J. Inf. Secur.*, vol. 2019, no. 1, p. 10, Dec. 2019.

[5] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, ''Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications,'' *Multimedia Tools Appl.*, vol. 78, p. 3457–3470, Jun. 2019.

[6] R. Biswas and S. K. Bandyapadhay, ''Random selection based GA optimization in 2D-DCT domain color image steganography,'' *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7101–7120, Dec. 2019.

[7] M. Z. Konyar, O. Akbulut, and S. Öztürk, ''Matrix encoding-based high-capacity and high-fidelity reversible data hiding in HEVC,'' *Signal, Image Video Process.*, vol. 14, no. 5, pp. 897–905, Jan. 2020.

[8] M. Engin, O. Cidam, and E. Z. Engin, ''Wavelet transformation based watermarking technique for human electrocardiogram (ECG),'' *J. Med. Syst.*, vol. 29, no. 6, pp. 589–594, Dec. 2005.

[9] K.-M. Zheng and X. Qian, ''Reversible data hiding for electrocardiogram signal based on wavelet transforms,'' in *Proc. Int. Conf. Comput. Intell. Secur.*, vol. 1, Dec. 2008, pp. 295–299.

[10] S. E. Jero and P. Ramu, ''Curvelets-based ECG steganography for data security,'' *Electron. Lett.*, vol. 52, no. 4, pp. 283–285, Feb. 2016.

[11] A. wierkosz and P. Augustyniak, ''Optimizing wavelet ECG watermarking to maintain measurement performance according to industrial standard,'' *Sensors*, vol. 18, no. 10, pp. 3401:1–3401:18, Oct. 2018.

[12] P. V. Sanivarapu, K. N. V. P. S. Rajesh, N. V. R. Reddy, and N. C. S. Reddy, ''Patient data hiding into ECG signal using watermarking in transform domain,'' *Phys. Eng. Sci. Med.*, vol. 43, pp. 213–226, Jan. 2020.

[13] S. Bhalerao, I. A. Ansari, A. Kumar, and D. K. Jain, ''A reversible and multipurpose ECG data hiding technique for telemedicine applications,'' *Pattern Recognit. Lett.*, vol. 125, pp. 463–473, Jul. 2019.

[14] C.-Y. Yang and W.-F. Wang, ''Effective electrocardiogram steganography based on coefficient alignment,'' *J. Med. Syst.*, vol. 40, no. 3, p. 66, Mar. 2016.

[15] N. K. Kalantari, M. A. Akhaee, S. M. Ahadi, and H. Amindavar, ''Robust multiplicative patchwork method for audio watermarking,'' *IEEE Trans. Audio, Speech, Language Process.*, vol. 17, no. 6, pp. 1133–1141, Aug. 2009.

[16] H. Kang, K. Yamaguchi, B. Kurkoski, K. Yamaguchi, and K. Kobayashi, ''Full-index-embedding patchwork algorithm for audio watermarking,'' *IEICE Trans. Inf. Syst.*, vol. E91-D, no. 11, pp. 2731–2734, Nov. 2008.

[17] Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, and S. Nahavandi, ''Patchwork-based audio watermarking method robust to de-synchronization attacks,'' *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 22, no. 9, pp. 1413–1423, Sep. 2014.

[18] I. Natgunanathan, Y. Xiang, Y. Rong, W. Zhou, and S. Guo, ''Robust patchwork-based embedding and decoding scheme for digital audio watermarking,'' *IEEE Trans. Audio, Speech, Language Process.*, vol. 20, no. 8, pp. 2232–2239, Oct. 2012.

[19] I. Natgunanathan, Y. Xiang, G. Hua, G. Beliakov, and J. Yearwood, ''Patchwork-based multilayer audio watermarking,'' *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 25, no. 11, pp. 2176–2187, Nov. 2017.

[20] Y. Chincholkar and S. Ganorkar, ''Audio watermarking algorithm implementation using patchwork technique,'' in *Proc. IEEE 5th Int. Conf. Converg. Technol. (ICT)*, Bombay, India, Mar. 2019, pp. 1–5.

[21] Y. Xiang, I. Natgunanathan, Y. Rong, and S. Guo, ''Spread spectrum-based high embedding capacity watermarking method for audio signals,'' *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 23, no. 12, pp. 2228–2237, Dec. 2015.

[22] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, ''Secure spread spectrum watermarking for multimedia,'' *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[23] H. S. Malvar and D. A. F. Florencio, ''Improved spread spectrum: A new modulation technique for robust watermarking,'' *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 898–905, Apr. 2003.

[24] A. Valizadeh and Z. J. Wang, ''Correlation-and-bit-aware spread spectrum embedding for data hiding,'' *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 267–282, Jun. 2011.

[25] P. Zhang, S. Xu, and H. Yang, ''Robust audio watermarking based on extended improved spread spectrum with perceptual masking,'' *Int. J. Fuzzy Syst.*, vol. 14, no. 2, pp. 289–295, Jun. 2012.

[26] X. Zhang and Z. J. Wang, ''Correlation-and-bit-aware multiplicative spread spectrum embedding for data hiding,'' in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Nov. 2013, pp. 186–190.

[27] H.-T. Hu and T.-T. Lee, ''High-performance self-synchronous blind audio watermarking in a unified FFT framework,'' *IEEE Access*, vol. 7, pp. 19063–19076, 2019.

[28] G. Hua, J. Goh, and V. L. L. Thing, ''Time-spread echo-based audio watermarking with optimized imperceptibility and robustness,'' *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 23, no. 2, pp. 227–239, Feb. 2015.

[29] G. Hua, J. Goh, and V. L. L. Thing, ''Cepstral analysis for the application of echo-based audio watermark detection,'' *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1850–1861, Sep. 2015.

[30] H. Wang, R. Nishimura, Y. Suzuki, and L. Mao, ''Fuzzy self-adaptive digital audio watermarking based on time-spread echo hiding,'' *Appl. Acoust.*, vol. 69, no. 10, pp. 868–874, Oct. 2008.

[31] O. T.-C. Chen and W.-C. Wu, ''Highly robust, secure, and perceptual-quality echo hiding scheme,'' *IEEE Trans. Audio, Speech, Language Process.*, vol. 16, no. 3, pp. 629–638, Mar. 2008.

[32] B.-S. Ko, R. Nishimura, and Y. Suzuki, ''Time-spread echo method for digital audio watermarking,'' *IEEE Trans. Multimedia*, vol. 7, no. 2, pp. 212–221, Apr. 2005.

[33] Y. Xiang, D. Peng, I. Natgunanathan, and W. Zhou, ''Effective pseudonoise sequence and decoding function for imperceptibility and robustness enhancement in time-spread echo-based audio watermarking,'' *IEEE Trans. Multimedia*, vol. 13, no. 1, pp. 2–13, Feb. 2011.

[34] Y. Xiang, I. Natgunanathan, D. Peng, W. Zhou, and S. Yu, ''A dual-channel time-spread echo method for audio watermarking,'' *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 383–392, Apr. 2012.

[35] H. J. Kim and Y. H. Choi, ''A novel echo-hiding scheme with backward and forward kernels,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 885–889, Aug. 2003.

[36] I. Natgunanathan, Y. Xiang, L. Pan, P. Chen, and D. Peng, ''Robustness and embedding capacity enhancement in time-spread echo-based audio watermarking,'' in *Proc. IEEE 11th Conf. Ind. Electron. Appl. (ICIEA)*, Hefei, China, Jun. 2016, pp. 1536–1541.

[37] S. Wang, W. Yuan, J. Wang, and M. Unoki, ''Inaudible speech watermarking based on self-compensated echo-hiding and sparse subspace clustering,'' in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Brighton, U.K., May 2019, pp. 2632–2636.

[38] S. Kirbiz and B. Gunsel, ''Robust audio watermark decoding by supervised learning,'' in *Proc. IEEE Int. Conf. Acoust. Speed Signal Process.*, May 2006, pp. 761–764.

[39] X. Wang, W. Qi, and P. Niu, ''A new adaptive digital audio watermarking based on support vector regression,'' *IEEE Trans. Audio, Speech Language Process.*, vol. 15, no. 8, pp. 2270–2277, Nov. 2007.

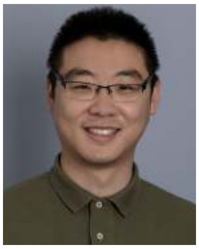
[40] D. Lakshmi, R. Ganesh, S. R. Marni, R. Prakash, and P. Arulmozhivarman, ''SVM based effective watermarking scheme for embedding binary logo and audio signals in images,'' in *Proc. IEEE Region Conf. (TENCON)*, Nov. 2008, pp. 1–5.

[41] J.-L. Wu and J. Shin, ''Discrete cosine transform in error control coding,'' *IEEE Trans. Commun.*, vol. 43, no. 5, pp. 1857–1861, May 1995.

IYNKARAN NATGUNANATHAN (Member, IEEE) received the B.Sc.Eng. degree (Hons.) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2007, and the Ph.D. degree from Deakin University, Australia, in 2012. From 2006 to 2008, he was a Software Engineer with Millennium Information Technology (Pvt.) Ltd., Malabe, Sri Lanka. He is a Research Fellow of the School of Information Technology, Deakin University. His research interests include the IoT privacy, digital watermarking, audio, image processing, and telecommunication.

CHANDAN KARMAKAR (Member, IEEE) received the B.Sc.Eng. degree in computer science and engineering from the Shahjalal University of Science and Technology, Sylhet, Bangladesh, and the Ph.D. degree from The University of Melbourne, Australia. He joined the School of Information Technology, Deakin University, in 2018, as a Lecturer. He has published one book and more than 130 research articles, including 42 journal articles. His research interests include biomedical devices and signal processing, cardiovascular and neural systems related to sleep-disordered breathing, human gait dysfunctions, cardiovascular diseases, and diabetic autonomic neuropathy.

SUTHARSHAN RAJASEGARAR (Member, IEEE) received the Ph.D. degree from The University of Melbourne, Australia, in 2009. He is currently a Senior Lecturer with the School of Information Technology, Deakin University, Melbourne, Australia. He has previously worked as a Research Fellow of the Department of Electrical and Electronics Engineering, The University of Melbourne, and as a Researcher in machine learning with the National ICT Australia (NICTA). His current research interests include anomaly/outlier detection, distributed machine learning, pattern recognition, signal processing, health analytics, wireless communications, and the Internet of Things.



TIANRUI ZONG received the B.E. degree in automation science and electrical engineering from Beihang University, China, in 2009, the M.Sc. degree in signal processing and communications from The University of Edinburgh, U.K., in 2010, and the Ph.D. degree in image processing from Deakin University, Australia. He is currently a Research Fellow of the School of Information Technology, Deakin University. His research interests include digital watermarking, privacy preservation, machine learning, data mining, and signal processing.

AHSAN HABIB (Graduate Student Member, IEEE) received the B.Sc.Eng. degree in computer science and engineering from the Shahjalal University of Science and Technology, Sylhet, Bangladesh, and the M.Eng. degree in information and communications technologies from the Asian Institute of Technology, Thailand. He is currently pursuing the Ph.D. degree with the School of Information Technology, Deakin University, Australia. His research interests include biomedical signal processing and modeling, time series analysis, machine learning, and deep learning.