Received: 5 February 2020 | Revised: 20 July 2020 | Accepted: 28 July 2020
DOI: 10.1002/ima.22477

RESEARCH ARTICLE

WILEY

ECG steganography based on tunable Q-factor wavelet transform and singular value decomposition

P. Mathivanan[1] | A. Balaji Ganesh[2]

[1]Department of Electronics and Communication Engineering, Velammal Engineering College, Chennai, India
[2]Electronic System Design Laboratory, Velammal Engineering College, Chennai, India

Correspondence
P. Mathivanan, Department of Electronics and Communication Engineering, Velammal Engineering College, Chennai 600066, India.
Email: mathiece05@gmail.com

Abstract
The article presents a novel ECG steganography scheme based on the tunable Q-factor wavelet transformation (TQWT) and also singular value decomposition (SVD) techniques that ensure better safety and confidentiality of patient information. Initial parameters such as *Q*, *r*, and *J* are used to decompose the cover signal into individual frequency sub-bands with the tunable Q-factor wavelet transform (TQWT). The singular value decomposition (SVD) technique is used to further decompose high-frequency sub-band coefficients into singular values. The watermark information is then embedded with high-frequency sub-band coefficients by involving the quantization process. The performance of this proposed system is successfully evaluated by considering various metrics, such as peak signal to noise ratio (PSNR), structural similarity index (SSIM), percentage residual difference (PRD), and bit error rate (BER). The simulation results of the proposed scheme are observed to be better than other traditional algorithms.

KEYWORDS
ECG steganography, scaling factor and performance metrics, singular value decomposition (SVD), tunable Q-factor wavelet transform (TQWT)

1 | INTRODUCTION

Cardiac disease is one of the most common chronic illnesses affecting many people's health and lives.[1,2] The remote health monitoring system offers continuous monitoring of physiological parameters, such as temperature, cardiac movement, blood pressure, etc. In order to facilitate diagnostics from a remote location,[3,4] the physiological parameters acquired via a wearable device are communicated over the internet. Patient monitoring can reduce labor costs and also reduce traffic in a medical center via a remote diagnostic procedure.[1-5] In addition, transmitting patient health information at an accurate time can save many lives, particularly in an emergency situation. Patient data tagged with diagnostic information are usually visible and altered during transmission across communication channels on a remote health monitoring application. The safety and privacy of steganography are therefore considered to be very important when transmitting information between the health center and doctors.

The US government has instructed patient privacy and patient information to be secured via the internet by a Health Insurance Portability Accountability Act (HIPAA).[6] Therefore, a suitable technique of data hiding should be employed in remote healthcare application.[1-7] Steganography is one such method used to protect private multimedia data from unauthorized users. Maximum robustness and minimum signal degradation are achieved by means of appropriate scaling factor values in the data-hiding scheme. From the literature, steganography is mainly classified into two major domains: spatial and frequency. The spatial domain technique changes data pixel values directly. The cover data is decomposed into frequency sub-bands using different transformations, namely discrete cosine transformation (DCT), Discrete Wavelet Transformation (DWT), Discrete Fourier Transformation (DFT), and so on, and the watermark data is embedded into a selective sub-band that changes the cover data. From the literature, it is found that many researchers have demonstrated data hiding by employing multimedia information, such as image, text, video, and audio. Further, significant numbers of research reports have carried the mechanism of hiding the data within electrocardiogram (ECG) signals. Nambakhsh et al[8] have proposed a watermarking system for embedding the ECG signal into medical images using EZW Wavelet Coder. Zheng and Qian, Zheng et al[9,10] have demonstrated an undistorted ECG signal watermarking technique. The watermark information is embedded into the non-QRS complex region resulting in a minimum signal deterioration. Kuar et al[11] have suggested a digital watermarking algorithm to ensure the secure transmission of ECG signals into Wireless Sensor Network architecture. A low-frequency chirp signal is used to embed the patient information.

Ibaida et al[12] have showed an ECG signal steganography scheme by shifting special range numbers and its PRD values are found to be within the ideal value for normal and abnormal ECG signals. The steganography system has a maximum payload size of 2500 bits. Ibaida et al[13] have presented an ECG steganography algorithm of high capacity for remote health monitoring application. The amount of payload that can be embedded into the test sample is approximately 10 000 bits. Ibaida and Khalil[14] have suggested a steganography process based on a discrete wavelet transformation (DWT), combining encryption and scrambling techniques to embed 2531 bytes of secret information.

Loukhaoukha et al[15] have proposed a watermarking scheme based on the Lifted Wavelet Transformation and the Singular Value Decomposition (SVD). The multiple scaling factors and robustness of the watermark algorithm are identified using Multi Objective Ant Colony Optimization techniques (MOACO). Run et al[16] have showed a SVD-based watermarking technology for embedding watermark in the principle components of a cover image. Furthermore, the DWT and DCT performance have been analyzed and the combination of DWT-SVD watermarking algorithm shows a better coefficient of correlation than the DCT-SVD combined scheme. Ali and Ahn[17] have developed an optimized self-adaptive watermarking technique based on DWT-SVD to improve the robustness and imperceptibility of data hiding.

In this study, a new watermarking algorithm is proposed to improve robustness and also imperceptibility by combining TQWT along with SVD. The work considers the frequency domain technique for hiding patient diagnosis information in a cover ECG signal. The patient watermark information is embedded in singular values of the cover signal coefficients. The ECG signal is first decomposed into a sub-band of frequencies using TQWT[18] with initial parameters, Q, r, and J. The sub-band coefficient is subsequently transformed into a cell array of M cells containing 8×8 sub-band arrays, which are further decomposed using SVD. The watermark information is then embedded into singular values by means of a quantization embedding process. The watermarked ECG signal is generated by the inverse TWQT using modified coefficient. In addition, different metrics such as the Peak signal to noise ratio (PSNR), Structural Similarity Index (SSIM) and Percentage Residual Difference (PRD) are used to measure the performance of the proposed scheme. Finally, the Bit Error Rate (BER) is used to calculate the amount in patient information that has been successfully retrieved.

The rest of the article has been made available in the following order. The brief background of TQWT and SVD is given in Section 2. The proposed watermarking scheme is described in Section 3. The result of simulation of the proposed scheme is discussed in Section 4. Finally, conclusion is presented in Section 5.

2 | THEORETICAL BACKGROUND

2.1 | Tunable-Q wavelets transform (TQWT)

In general, high-Q-factor wavelet transform is suitable for oscillatory signals, such as ECG, speech, and etc. The non-oscillating signal has a low Q factor.[18] In addition, continuous wavelet transform demonstrates the ability of tuning Q factor. Therefore, it is found that dyadic wavelet transform with low Q-factor are more suitable for decomposing non-oscillatory signals. The TQWT is also known as a powerful, discrete wavelet transform for the oscillator signal, with easily adjustable parameters.[18] The three major input parameters of TQWT are: Q factor (Q) is used to denote the extent to which oscillations of wavelet can sustain. The Q factor for an oscillatory signal is a ratio between center frequency (f_o) and bandwidth (BW).

$$Q = \frac{f_o}{BW} \tag{1}$$

Next, parameter r means redundancy, where the total over-sampling rate of the wavelet transform is calculated. The total decomposition level is indicated as J.

Transformation contains two stage filter bank, in which each filter bank's low-pass output is provided as an input to the next filter bank. Sub-bands are the output from each high-pass filter. The parameter J indicates the number of filter banks leading to $J+1$ sub-band. For example, if J is 5, it has 5 high-pass filter sub-bands along with a low-pass filter sub-band. The value of r and Q can be expressed in terms of filter bank scaling parameters α and β as given in Equation (2).

$$Q=\frac{2-\beta}{\beta}.$$

$$r=\frac{\beta}{1-\alpha} \tag{2}$$

The input signal $s[n]$ is decomposed into low pass sub-band $c^0[n]$ and high pass sub-band $d^1[n]$ with sampling frequencies $\alpha\, f_s$ and $\beta\, f_s$. Low pass filter $H_o(\omega)$ generates low frequency sub-band coefficient using scaling factor α and high pass filter $H_1(\omega)$ generates high frequency sub-band coefficient by using scaling factor β. In order to achieve perfect reconstruction of original signal and to prevent over all redundancy in TQWT, scaling parameters α and β should be within limit of 0 to 1.[18-21] Moreover, it is possible to reconstruct the original signal through a filter bank, input parameters (Q and r) as well as the scaling parameters (α and β).

$$H_0^j(\omega)=\begin{cases}\prod_{m=0}^{j-1} H_0(\omega/\alpha^m), & |\omega|\le\alpha^j\pi\\ 0, & \alpha^j\pi<|\omega|\le\pi\end{cases}$$

$$H_1^j(\omega)=\begin{cases}H_1(\omega/\alpha^{j-1})\prod_{m=0}^{j-2} H_0(\omega/\alpha^m), & (\beta-1)\alpha^{j-1}\pi<|\omega|\le\alpha^{j-1}\pi\\ 0, & \omega\in[-\pi,\pi]\end{cases} \tag{3}$$

2.2 | Singular value decomposition (SVD)

The singular value decomposition is a linear algebra-supported mathematical technique used for different applications, including signal processing and pattern analysis.[22-25] In summary, the rectangular matrix of $M\times N$ is decomposed into three matrices: U orthogonal matrix, S diagonal matrix, and V transpose of orthogonal matrix.

$$H=\left[USV^T\right]$$

$$H=\begin{bmatrix}U_{1,1} & U_{1,2} & \cdots & U_{1,m}\\ U_{2,1} & U_{2,2} & \cdots & U_{2,m}\\ \vdots & \vdots & \ddots & \vdots\\ U_{m,1} & U_{m,2} & \cdots & U_{m,m}\end{bmatrix}\begin{bmatrix}S_{1,1} & 0 & \cdots & 0\\ 0 & S_{2,2} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & S_{m,m}\end{bmatrix}\begin{bmatrix}V_{1,1} & V_{1,2} & \cdots & V_{1,m}\\ V_{2,1} & V_{2,2} & \cdots & V_{2,m}\\ \vdots & \vdots & \ddots & \vdots\\ V_{m,1} & V_{m,2} & \cdots & V_{m,m}\end{bmatrix}^T \tag{4}$$

The orthogonal matrices, U and V are in size of $M\times M$ and $N\times N$, respectively. The diagonal matrix S is $M\times N$ in size with singular values $S_{1,1}>S_{2,2}>S_{3,3}>\cdots>S_{m,m}$. In addition, column of U is known as left singular vector and column V is denoted as the right singular vector of H. SVD transform matrices are not fixed in their sizes. The changes in singular values, like transpose, translation, flips, and rotation, therefore no impact on the quality of the resulting array. The singular values are invariant with the common signal operation and should satisfy the algebraic properties.[22-25]

3 | PROPOSED METHOD

ECG signal, H from MIT-BIH is decomposed with TQWT initial parameters Q, r, and J. The cover ECG signal is decomposed into high-frequency sub-bands (W_1, W_2, W_3, W_4, and W_5) and a low-frequency sub-band (W_6). For an instance, for $J=5$, as shown in Figure 1, the ECG signal is decomposed into five high-frequency sub-bands and a

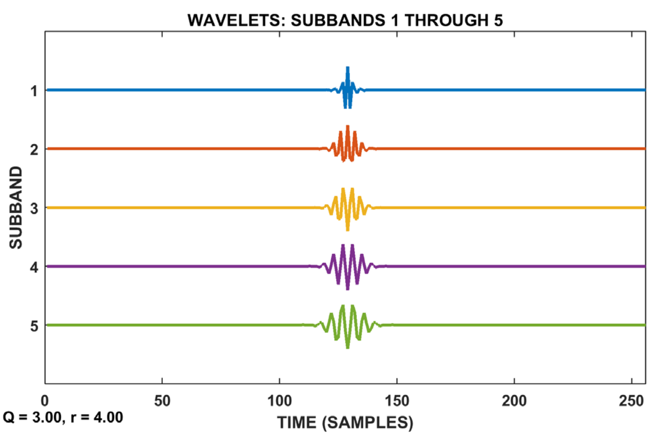


FIGURE 1 High-frequency sub-band 1 to 5 [Color figure can be viewed at wileyonlinelibrary.com]

low-frequency sub-band. In addition, the proposed scheme embeds watermarked data into high-frequency sub-band W_1. The binary bit of watermarked data is integrated into the frequency sub-band coefficient and reverse TQWT is used to obtain the subsequent watermarked ECG signal. The decomposed sub-band of $1 \times N$ array is transformed into an array of $M \times 64$ in size and each row is changed into a cell of M array with 8×8 coefficients of sub-band. Like this, watermarked data in size of $p \times q$ is altered to an array of $1 \times N$, ($N = p \times q$), which is converted to the M cell with 8×8 binary information. Sub-band coefficients of the M array are subsequently decomposed by SVD and its singular values are used to embed binary information by quantization embedding technique. Figure 2 shows the proposed ECG steganography scheme.

3.1 | Watermark embedding process

Step 1: Using TQWT, the cover ECG signal (H) is decomposed into sub-bands with high frequency and low frequency.

$$\left\{W_1, W_2, W_3, \ldots W_j, W_{j+1}\right\} = \mathrm{TQWT}[H(1,x)] \tag{5}$$

where $W_{j+1}$is a low frequency sub-band and W_1 to W_j are high-frequency sub-bands. The number of samples in each sub-band depends on scaling parameters that arranged in a cell array.

Step 2: The high-frequency sub-band coefficients $\{W_1\}$ of $1 \times N$ in size is transformed into a cell array of $M \times 64$.

Step 3: The sub-band cell array of $M \times 64$ is transformed into an array of cells of $1 \times M$ in size, in which each row of cell array $\{W_1\}$ is transformed into a cell of 8×8 in size.

$$\{W_1\} = \left\{B_{\boldsymbol{k}\,(1\times M)}\right\} = \left\{\left\{B_{1(8\times8)}\right\}, \left\{B_{2(8\times8)}\right\}, \ldots \left\{B_{\boldsymbol{M}\,(8\times8)}\right\}\right\} \tag{6}$$

where $\{B_1\}$ *to* $\{B_M\}$ are block cells with 8×8 in size.

Step 4: The secret information (Q) of $M \times 64$ is transformed into $1 \times M$ cell array blocks of size where each cell array block row is converted to a (8×8) cell.

$$\left\{Q_{\boldsymbol{k}\,(1\times M)}\right\} = \left\{\left\{Q_{1(8\times8)}\right\}, \left\{Q_{2(8\times8)}\right\}, \ldots \left\{Q_{\boldsymbol{M}\,(8\times8)}\right\}\right\} \tag{7}$$

where $\{Q_1\}$ to $\{Q_M\}$ are block cells with 8×8 in size.

Step 5: Apply SVD to each cell array block and get singular values to each cell array block $\{B_{k\ (1\times M)}\}$

$$\{B_k\} = \left[\{U_{ck}\}\{S_{ck}\}\left\{V_{ck}^T\right\}\right] \tag{8}$$

where $k = 1, 2, 3, \ldots, M$ and $\{S_{ck}\}$ are the singular values of high-frequency sub-band.

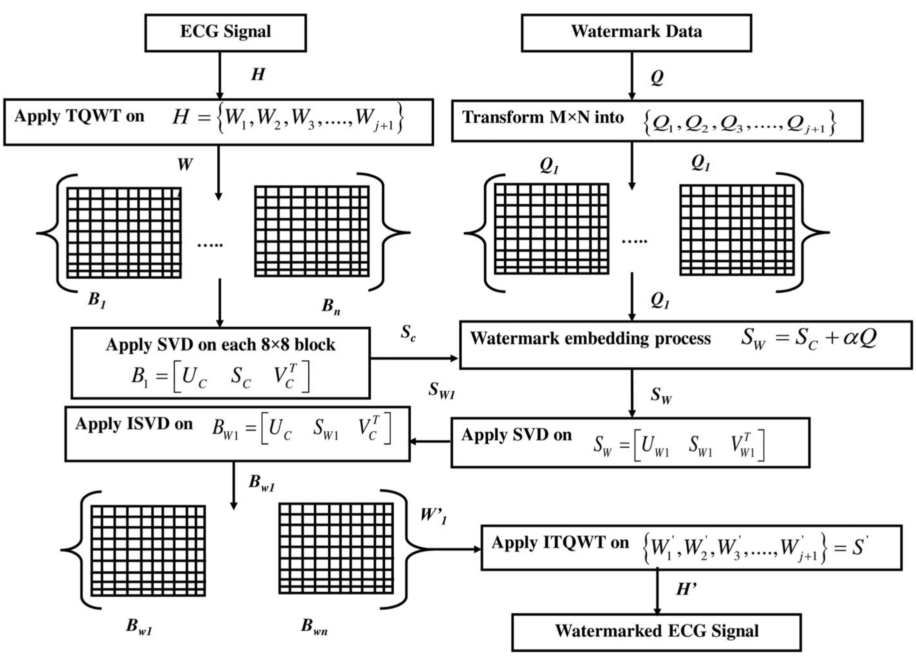


FIGURE 2 TQWT-SVD based ECG steganography scheme

Step 6: Obtain the modified singular values using the quantization embedding process as specified in Equation (9)

$$\{S_{wk}\} = \{S_{ck}\} + \alpha \times \{Q_k\} \tag{9}$$

Step 7: Perform SVD on the singular value $\{S_{wk}\}$ as given in Equation (10)

$$\{S_{wk}\} = \left[\{U_{ek}\}\{S_{ek}\}\{V_{ek}{}^{T}\}\right] \tag{10}$$

Step 8: Obtain watermark sub-band block $\{B'_k\}$ by using Equation (11)

$$\left[\{U_{ck}\}\{S_{ek}\}\{V_{ck}{}^{T}\}\right] = \{B'_k\} \tag{11}$$

Step 9: Reconstruct watermarked ECG signal (H_w) with ITQWT as given in Equation (12)

$$\begin{gathered}\left\{W'_{1(1\times M)}\right\} = \left\{\left\{B'_{1(8\times 8)}\right\},\left\{B'_{2(8\times 8)}\right\},\ldots\left\{B'_{M(8\times 8)}\right\}\right\} \\ [H'(1,x)] = ITQWT \quad \{W_1, W_2, W_3 \ldots W_j, W_{j+1}\}\end{gathered} \tag{12}$$

3.2 | Watermark extraction process

Step 1: Decompose the watermarked ECG signal (H) using TQWT to obtain a sub-band of high frequency

$$\left\{W'_1,\ W'_2,\ W'_3 \ldots W'_j,\ W'_{j+1}\right\} = TQWT[H'(1,x)] \tag{13}$$

Step 2: The watermark high-frequency sub-band $\{W'_1\}$ with $1 \times N$ is transformed into a cell array of $(M \times 64)$.

Step 3: The higher-frequency watermark sub-band array of $M \times 64$ has been converted back to a cell array of $1 \times M$ size in which each row of cell array {W1} is converted into a cell of 8 × 8 in size.

$$\{W'_1\} = \left\{B'_{k\,(1\times M)}\right\} = \left\{\left\{B'_{1(8\times 8)}\right\},\left\{B'_{2(8\times 8)}\right\},\ldots\left\{B'_{M\,(8\times 8)}\right\}\right\} \tag{14}$$

where $\{B'_1\}$ to $\{B'_M\}$ are block cells with 8 × 8 in size.

Step 4: Apply SVD to each array block and obtain singular values for each array block $\{B'_{k(1\times M)}\}$

$$\{B'_k\} = \left[\{U'_{ck}\}\{S'_{ek}\}\left\{V'_{ck}{}^{T}\right\}\right] \tag{15}$$

where $k = 1, 2, 3,\ldots, M$ and $\{S'_{ek}\}$ are the singular values of high frequency sub-band.

Step 5: Obtain sub-band D by using Equation (16).

$$\left[\{U'_{ek}\}\{S'_{ek}\}\left\{V'_{ek}{}^{T}\right\}\right] = \{D_k\} \tag{16}$$

Step 6: Extract watermark from sub-band as given in Equation (17).

$$\{Q'\} = ((\{D_k\} - \{S_{ck}\})/\alpha) \tag{17}$$

Step 7: Calculate a threshold for the perfect reconstruction of watermark cell information with Equation (18).

$$\begin{gathered} Th = \mathrm{mean}(\mathrm{mean}(\{Q'\})) \\ Q_e = \begin{cases} 1 & Q' \geq Th \\ 0 & Q' < Th \end{cases}\end{gathered} \tag{18}$$

Step 8: Transform the watermark cell array into watermark information (Q_e) as shown in Figure 3.

3.3 | Performance analysis

Peak signal to noise ratio (PSNR) is a ratio between maximum value of cover signal and mean square value of cover and watermarked ECG signal which is represented in Equation (19). PSNR value is used to measure of peak error in watermarked signal that is expressed in terms of decibels (dB).[18-23,26-29]

$$\mathrm{PSNR} = 20\log \frac{\max(H)}{\sqrt{\frac{1}{N}\sum_{i-1}^{N}(H-H')^2}} \tag{19}$$

Percentage residual difference (PRD) is a relative square difference between cover and watermarked ECG signal which is presented in Equation (20). In general, lower PRD value results better perceptual quality of watermarked data.[18-23,26-29]

$$\mathrm{PRD} = \sqrt{\frac{\sum_{i=1}^{N}(H-H')^2}{\sum_{i=1}^{N}(H)^2}} \times 100 \tag{20}$$

where H is cover ECG signal, H' is watermarked ECG signal and N is total number of ECG samples.

Algorithm 1 Watermark embedding algorithm

Input: $q, r, J, \alpha, k = 1, r = 1, a = 1$

$H \leftarrow$ cover ECG signal

$Q \leftarrow$ watermark data

Output: $H' \leftarrow$ watermarked ECG signal

$N \leftarrow length(H)$;
$w \leftarrow tqwt(H,q,r,J)$;
$kx1 \leftarrow (w\{a\})$;
$w_1 \leftarrow w$;
$N \leftarrow length\ of\ w_1$
$[m_1\ n_1] = size\ of\ (Q)$;
for $p = 1$ **to** m_1 **do**
  for $q = 1$ **to** n_1 **do**
  $Q \leftarrow$ *convert watermark data of* $m_1 \times n_1$ *array into* $1 \times N$ (*where* $N = m \times n$)
  $r \leftarrow r + 1$
  end for
end for
for $i = 1$ **to** 64 **for** *N samples* **do**
  for $j = i$ **to** $i + 63$ **do**
  $Q \leftarrow$ *Segment* $1 \times N$ *watermark array into* $k \times 64$ *arrays*
  $B \leftarrow$ *Segment the high frequency coefficient* (w_1) *of* $1 \times N$ *into* $r \times 64$ *arrays*
  end for
end for
  $Q_{\{r \times \{8 \times 8)\}} \leftarrow$ *reshape each watermark array* (1×64) *into* 8×8
  $B_{\{r \times (8 \times 8)\}} \leftarrow$ *reshape each high frequency coefficient array* (1×64) *into* 8×8
for $i_1 = 1$ **to** m_1 **do**
  $[U,S,V] \leftarrow apply\ SVD(B\{i_1\})$
  $U_1\{i_1\} \leftarrow U$
  $S_1\{i_1\} \leftarrow S$
  $V_1\{i_1\} \leftarrow V$
  $SW\{i_1\} \leftarrow S_1\{i_3\} + (\alpha \times Q\{i_1\})$
  $[U_2,S_2,V_2] \leftarrow apply\ SVD(SW\{i_1\})$
  $U_3\{i_1\} \leftarrow U_2$
  $S_3\{i_4\} \leftarrow S_2$
  $V_3\{i_1\} \leftarrow V_2$
  $z\{i_1\} \leftarrow U_1\{i_1\} \times S_2\{i_1\} \times V_1\{i_1\}'$
end for
for $i_2 = 1$ **to** m_1 **do**
  $a_3 \leftarrow z\{i_2\}$;
  for $i_3 = 1$ **to** 8 **do**
    for $\mathrm{j}_3 = 1$ **to** 8 **do**
      $sigarray(1,k) \leftarrow a_3(j_3,i_3)$;
      $k \leftarrow k + 1$;
    end for
  end for
end for
$w'\{1\} \leftarrow sigarray$;
$H' \leftarrow itqwt(w',Q,r,N)$

Algorithm 2 Watermark extraction algorithm

Input : q, r, J, α, $r = 1$, $a = 1$, $kr = 1$;$mr = 1$; $nr = 1$; U_1; V_1; $e = 1$; m_1
$H' \leftarrow$ watermarked ECG signal

Output : $Q^* \leftarrow$ watermark data

$w_r \leftarrow$ *apply tqwt*(H',q,r,J);
$w_{r1} \leftarrow (w_r\{a\})$;
$L \leftarrow$ length(w_{r1});
for $i = 1$ **to 64** for L samples **do**
  for $j = i$ **to** $i + 63$ **do**
  $B' \leftarrow$ *Segment the high frequency coefficient* (w_{r1}) *of* $1 \times N$ *into* $r \times 64$ *arrays*
  $mr \leftarrow mr + 1$;
  end for
  $kr \leftarrow kr + 1$;
end for
$B'_{\{r \times (8 \times 8)\}} \leftarrow$ reshape each high frequency coefficient array (1×64) into 8×8
for $i_1 = 1$ **to** m_1 **do**
  $[U_r,S_r,V_r] \leftarrow$ *apply SVD*$(B'\{i_1\})$
  $U_{r1}\{i_1\} \leftarrow U_r$
  $S_{r1}\{i_1\} \leftarrow S_r$
  $V_{r1}\{i_1\} \leftarrow V_r$
  $Z_r\{i_1\} \leftarrow U_1\{i_1\} \times S_{r1}\{i_1\} \times V_1\{i_1\}'$
  $rQarray\{i_1\} \leftarrow (z_r\{i_1\} - S_1\{i_1\})/\alpha$
end for
for $i_2 = 1$ **to** m_1 **do**
  $a_e \leftarrow rQarray\{i_2\}$
  for $i = 1$ **to** 8 **do**
    for $j = 1$ **to** 8 **do**
      $eQarray(1,ek) \leftarrow a_e\,(j,i)$
      $e \leftarrow e+1$
    end for
  end for
end for
for $p = 1$ **to** m_1 **do**
  for $q = 1$ **to** 64 **do**
    $Q^* \leftarrow eQarray(1,r)$
    $r \leftarrow r + 1$
  end for
end for

Normalized cross correlation (NCC) is used to evaluate the robustness between original and extracted watermarked image as given in Equation (21).

$$\mathrm{NC} = \frac{\sum_{i=0}^{N}\sum_{j=0}^{M}[Q(i,j)Q_e(i,j)]}{\sum_{i=0}^{N}\sum_{j=0}^{M}[Q(i,j)]^2} \tag{21}$$

where Q and Q_e represent original image and extracted watermark image, respectively.

Structural similarity measure index (SSIM) is used to measure imperceptibility between cover and watermarked ECG signal as described in Equation (22).[25,30]

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{22}$$

where μ_x, μ_y, σ_x,σ_y, and σ_{xy} are mean, SD and cross-covariance value of the signal x, y, respectively. C_1 and C_2 are the regularization constants which are added to

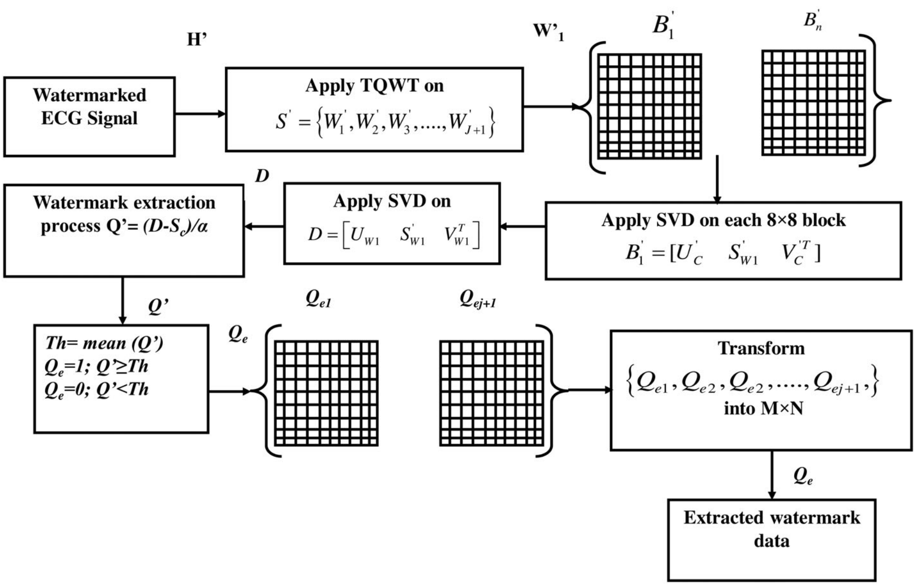


FIGURE 3 Data extraction process

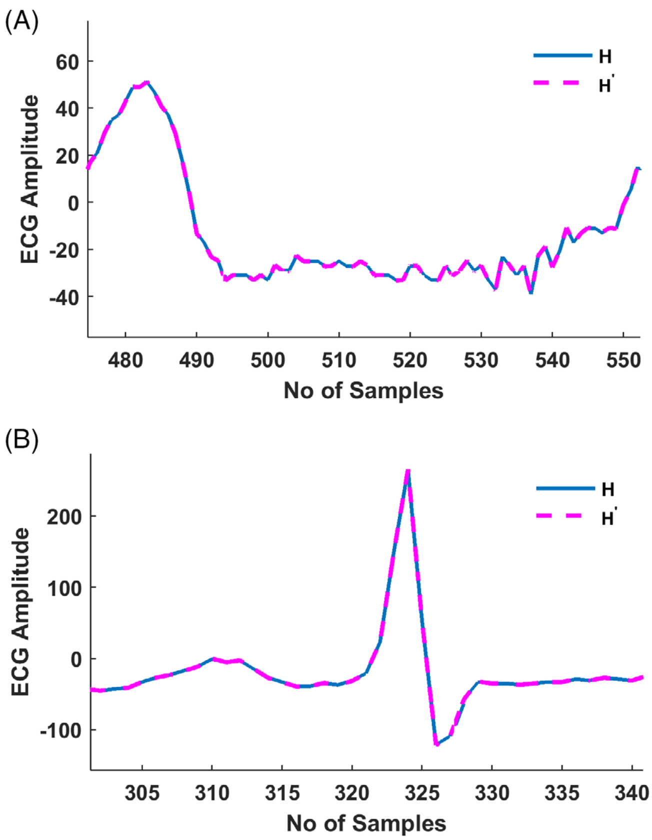


FIGURE 4 A,B, Cover and watermarked ECG signal [Color figure can be viewed at wileyonlinelibrary.com]

ensure numerical stability and also to accommodate perception of human visual system.

Further, value of extracted watermark information is measured by using bit error rate (BER) as described in Equation (23).[18,19,27,28]

$$\mathrm{BER} = \frac{\text{bits retrieved correctly}}{\text{total number of bits}} \times 100 \tag{23}$$

4 | RESULTS AND DISCUSSIONS

The proposed scheme considers 6400 samples of ECG signals from MIT-BIH normal and Arrhythmia databases. The length of the cover data determines the number of mark bits that may be inserted in an ECG signal. For example, a watermark bit of 100 × 64 size requires 6400 samples of ECG signals, that is, each ECG signal sample carries a watermark bit. In general, an ideal watermarking algorithm selectively identifies frequency band of cover signal where secret information is embedded into cover data. But the ECG cover signal gets disturbed due to data integration that may affect the watermark signal diagnosability.

The present study deals with the selection of ECG signal sub-band high-frequency coefficients to embed watermark data with minimal signal deterioration. The performance metrics, like PSNR, PRD, SSIM and BER are analyzed in order to prove robustness and imperceptibility of the proposed steganography scheme. The deviation between the cover and the watermarked ECG signal is found to be minimal and the difference is not apparent in the naked eye as shown in Figure 4A,B. The amount of signal distortion in the watermarked ECG signal is analyzed using the PSNR value. Increased PSNR results in a less distorted signal.

The ECG arrhythmia and normal database test performance is also analyzed by using the different scaling factor α and results are presented in Tables 1 and 2. It is found

TABLE 1 PSNR and PRD values of arrhythmia ECG signal

102-ECG arrhythmia signal												
Scaling factor	0.05			0.1			0.5			0.9		
Test image	PSNR	PRD	SSIM	PSNR	PRD	SSIM	PSNR	PRD	SSIM	PSNR	PRD	SSIM
Image1	88.35	0.0009	1	82.10	0.002	1	66.29	0.012	0.9999	59.82	0.026	0.9996
Image2	86.15	0.0012	1	79.97	0.0025	1	64.32	0.015	0.9999	57.98	0.032	0.9996
Image3	86.25	0.0012	1	80.08	0.0025	1	64.72	0.014	0.9999	58.40	0.030	0.9996
Image4	86.63	0.0012	1	80.35	0.0024	1	64.43	0.015	0.9999	58.11	0.031	0.9996
Image5	87.85	0.001	1	81.74	0.0021	1	67.01	0.011	0.9999	61.05	0.022	0.9998
Image6	88.74	0.0009	1	82.49	0.0019	1	66.80	0.011	0.9999	60.40	0.024	0.9997
Image7	86.26	0.0012	1	80.09	0.0025	1	64.56	0.014	0.9999	58.24	0.030	0.9996
Image8	85.26	0.0014	1	79.04	0.0028	1	63.14	0.017	0.9999	56.67	0.036	0.9994
Image9	85.92	0.0013	1	79.69	0.0026	1	63.71	0.016	0.9999	57.26	0.034	0.9995
Image10	86.05	0.0013	1	79.88	0.0025	1	64.30	0.015	0.9999	58.09	0.031	0.9995
Average	86.74	0.0011	1	80.54	0.0023	1	64.92	0.014	0.9999	58.60	0.029	0.9995

TABLE 2 PSNR and PRD values of normal ECG signal

16 420 m-ECG normal signal												
Scaling factor	0.05			0.1			0.5			0.9		
Test image	PSNR	PRD	SSIM	PSNR	PRD	SSIM	PSNR	PRD	SSIM	PSNR	PRD	SSIM
Image1	88.32	0.018	1	82.15	0.038	1	67.00	0.218	0.9991	61.06	0.433	0.9975
Image2	86.19	0.024	1	80.04	0.048	0.999	64.96	0.276	0.9988	59.08	0.543	0.9966
Image3	86.31	0.024	1	80.16	0.048	0.999	65.13	0.271	0.9986	59.12	0.541	0.9957
Image4	86.54	0.023	1	80.35	0.047	0.999	65.23	0.268	0.9986	59.37	0.526	0.996
Image5	87.95	0.019	1	81.84	0.039	1	67.18	0.214	0.9993	61.51	0.411	0.9979
Image6	88.63	0.018	1	82.42	0.037	0.999	67.32	0.210	0.9988	61.48	0.413	0.9972
Image7	86.34	0.024	1	80.21	0.047	0.999	65.26	0.267	0.999	59.37	0.526	0.9968
Image8	85.30	0.027	1	79.13	0.054	0.999	63.89	0.313	0.9987	57.91	0.623	0.9956
Image9	85.92	0.025	1	79.73	0.051	1	64.54	0.290	0.999	58.57	0.577	0.9965
Image10	86.08	0.024	1	79.92	0.049	1	64.85	0.280	0.9988	59.01	0.548	0.9963
Average	86.75	0.022	1	80.59	0.045	0.999	65.53	0.260	0.9988	59.64	0.514	0.9966

that the scaling factor α increases 9 times, the PSNR value decreases by 27%. From literature, it is found that an ideal PSNR of 30 dB should be met by a good steganography system. Tables 1 and 2 represent the PSNR values of the proposed steganography scheme, which are higher than the ideal value. The simulation results have showed that the watermarked ECG signal shows a minimum deterioration of the signal even for the greater value of the scaling factor α. The watermarked binary data is multiplied by scaling factor within range of 0.1 to 0.9 that is added to the sub-band coefficients of cover signal whose values are in order of 100. As a result, cover signal coefficient experiences minimum deviation and eventually insignificant signal deterioration as shown in the Figure 5. The quality of the output signal is also analyzed using the structural similarity measure index (SSIM).

In general, ideal SSIM values are near to 1 representing a minimum deteriorated ECG signal, and the study produces similar results as illustrated in Tables 1 and 2. To analyze the signal distortion, the PRD value of the watermarked ECG signal is evaluated. In general, ideal PRD value for watermarked signals should be 0% to 9%, to make the diagnosis easier. The results achieved in Tables 1 and 2 are observed to be within the ideal value. The results

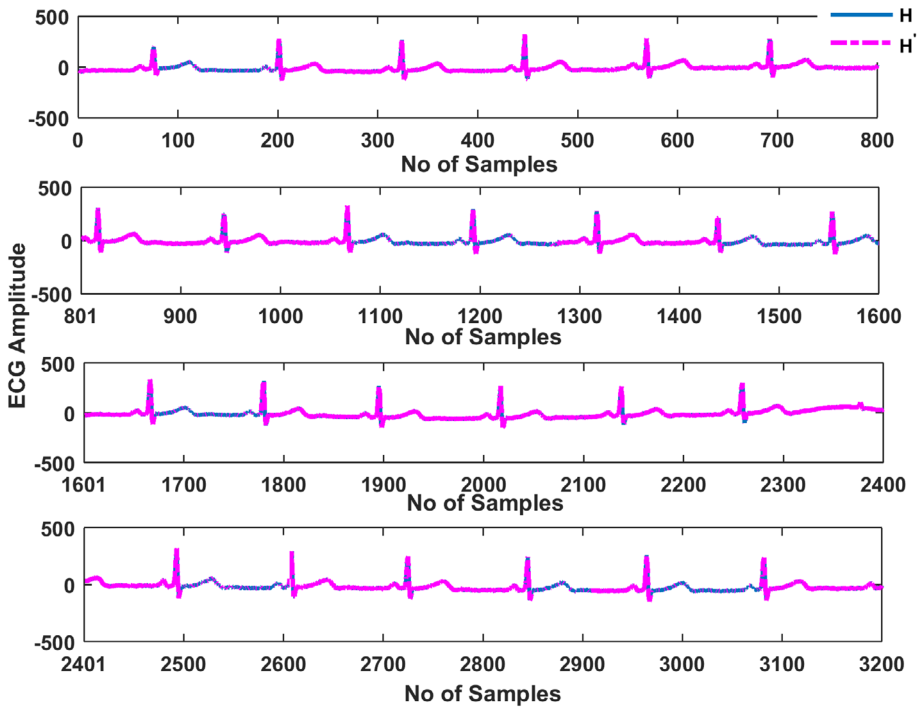


FIGURE 5 Cover and watermarked ECG signal [Color figure can be viewed at wileyonlinelibrary.com]

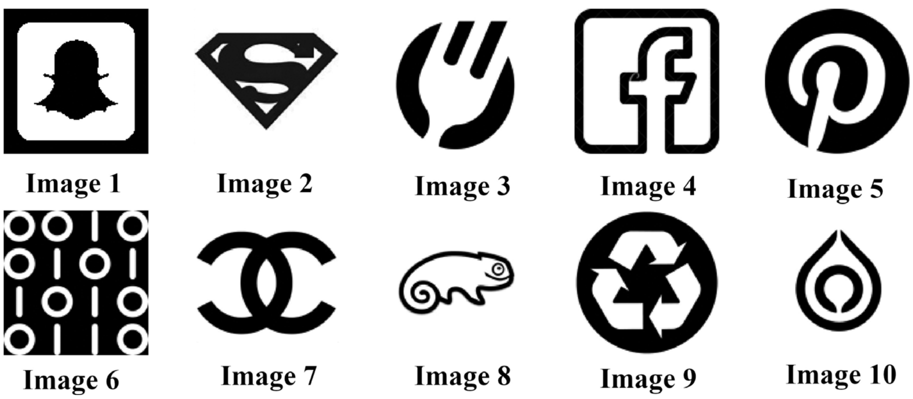


FIGURE 6 Ten different watermark image

TABLE 3 Represents normalized cross correlation value for different cover signal

NCC				
Signal	$\alpha = 0.05$	$\alpha = 0.1$	$\alpha = 0.5$	$\alpha = 0.9$
16 420 m	1	1	0.9998	0.9986
102 m	1	1	0.9988	0.9972

of the simulation confirm that the watermarked ECG signal have showed minimum distortion of the signal and its suitability for the diagnostic process. The scaling factor varies from 0.05 to 0.9 and the metric values are found to be ideal, as shown in Tables 1 and 2.

In addition, the proposed ECG steganography system is tested with signal numbers 16 272 m, 16 273 m, 16 420 m, 16 483 m, and 16 539 m from the normal database and 100 m, 101 m, 102 m, and 103 m from the database of arrhythmia. The proposed scheme also used 10 different watermark information as shown in Figure 6. Moreover, the scheme is analyzed for various scaling factors ranging from 0.05 to 0.9 and for different watermark sizes ranging from 4.1 kb to 64 kb. Imperceptibility and robustness are analyzed using normalized cross correlation values (NCC). In general, the value of NCC close to 1 is exactly the same as the value of original data.

NC value greater than 0.75 is accepted as normal from the literature. Table 3 shows the NC values obtained for different ECG signals and are found to be within the ideal value that demonstrates the robustness of the proposed scheme.

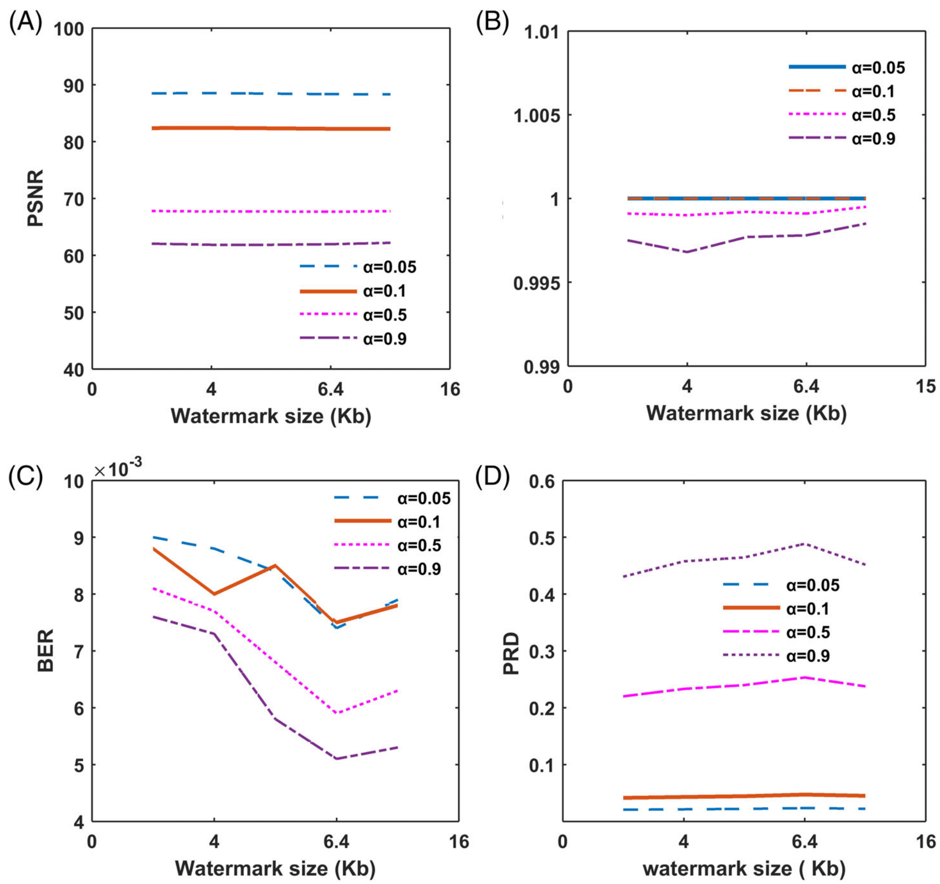


FIGURE 7 A-D, Performance metrics evaluation by varying watermark size and scaling factor (α) [Color figure can be viewed at wileyonlinelibrary.com]

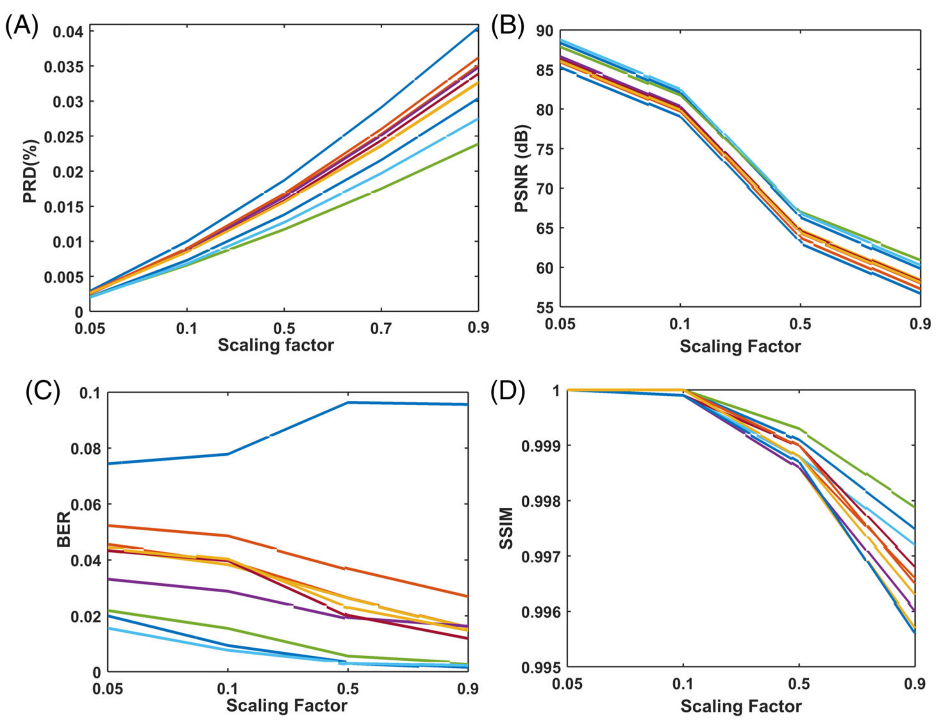


FIGURE 8 A-D, PSNR, PRD, SSIM, and BER value evaluated by varying 10 different watermark data and scaling factor [Color figure can be viewed at wileyonlinelibrary.com]

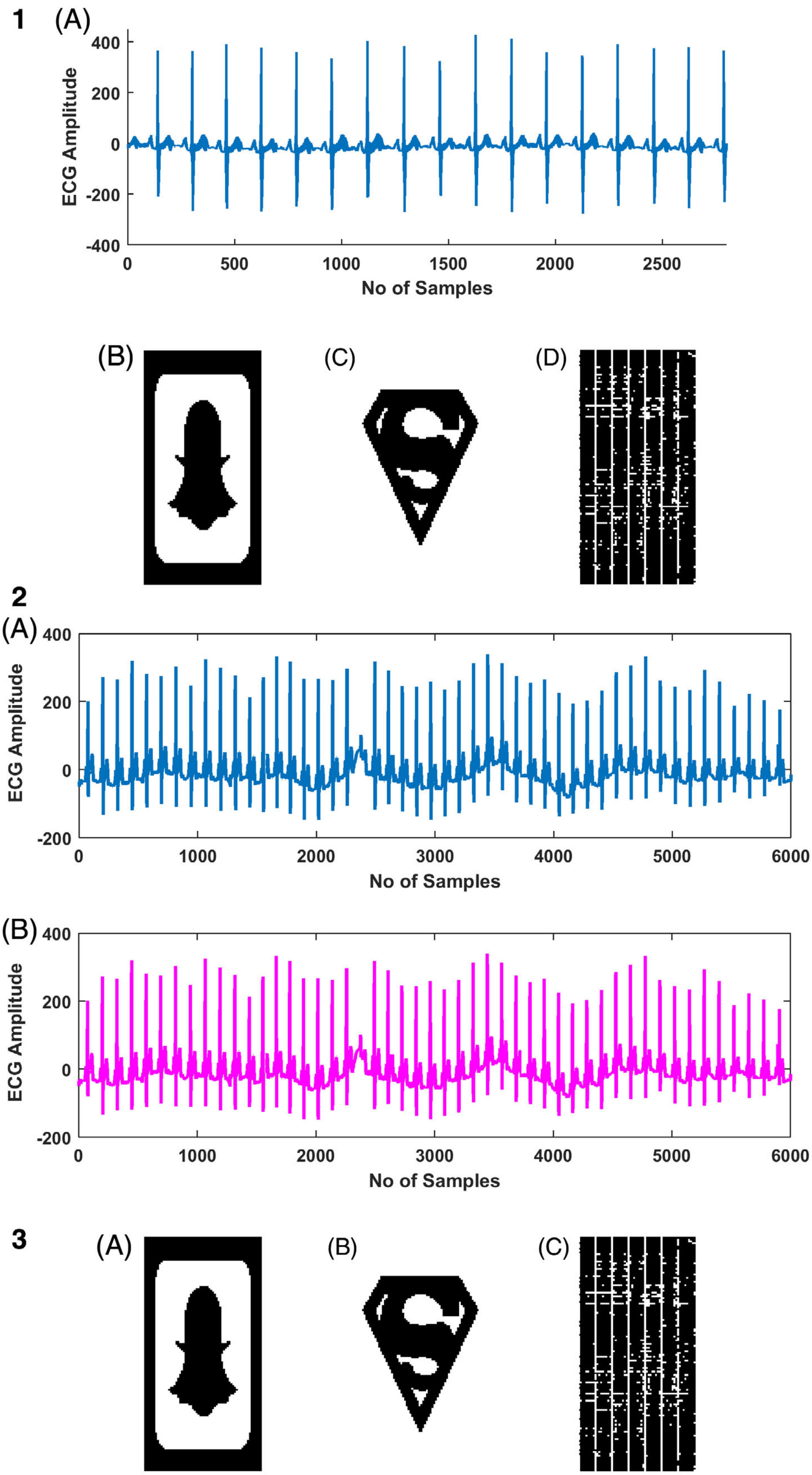
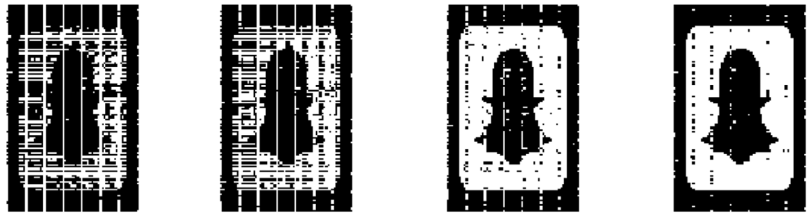


FIGURE 9 (1) The false positive detection problem, A, watermarked ECG signal; B, watermark information embedded in, A; C, watermarked image used for extraction; D, extracted watermarked information. (2) A, Watermarked ECG signal (H'). B, Watermarked ECG signal (H_1). (3) A-C, False positive attack analysis, A, watermark information Q; B, watermark information Q_1; C, extracted watermarked information by using U and V^T component and the secret key obtained during data embedded process H' [Color figure can be viewed at wileyonlinelibrary.com]

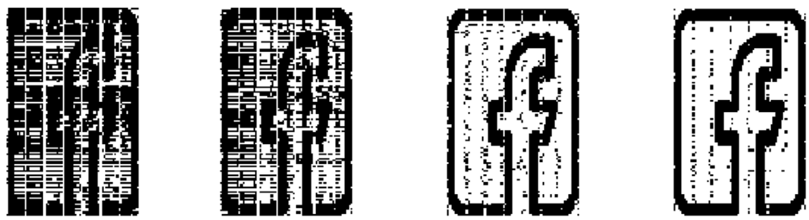
FIGURE 10 A-C, Extracted watermark information and its BER values for different noise attack

(A)



SNR	10	20	30	40
BER	0.2778	0.2027	0.0542	0.0192
NCC	0.1974	0.3281	0.7560	0.9478

(B)



SNR	10	20	30	40
BER	0.3823	0.2967	0.0667	0.032
NCC	0.2267	0.3976	0.7600	0.9392

(C)

SNR	10	20	30	40
BER	0.4522	0.3469	0.0939	0.0403
NCC	0.1929	0.3510	0.7312	0.9329

4.1 | Effect of scaling factor (α)

The scaling factor α plays an important role in determining imperceptibility of watermarked signal. The proposed steganography scheme is analyzed by varying scaling factor from 0.05 to 0.9 for 20 different watermarked data. The low value of the scaling factor results in a minimum signal distortion reflected in the values of PSNR, PRD and SSIM.[26] On the other hand, the value of the scaling factor closes to 1 result in poor PSNR, PRD and SSIM values, but the PRD value increases with the deterioration of the signal. Figure 7A-D shows performance metrics evaluated by varying watermark sizes and also scaling factor (α). The scaling factor value 0.05 has showed a larger error and a poor BER value. The BER value has been evaluated by the different scaling factor is shown in Figure 7B. The scaling factor of 0.05 is observed with a greater error in the retrieved information obtained with an increase in the BER value. The large error in the information obtained is mainly due to the fact that the signal value is reduced and sign changes in the steganography process[26] Figure 8A-D represents PSNR, PRD, SSIM and BER values, as evaluated by varying scaling factor ranges between 0.05 and 0.9 for 10 different watermark data. The PRD value increase as the scaling factor α increases, but the value of PSNR, BER, and SSIM decreases with the scaling factor α increase. Increased scaling factor will increase the deterioration of the signal and decrease PSNR, SSIM and BER.

4.2 | False positive detection analysis

4.2.1 | False positive test 1

It is understood from the literature that the SVD-based watermarking algorithm usually suffers from false positive detection, which can detect watermarks in watermarked data that are not actually embedded in them. Therefore, the reliability of the proposed scheme is tested. The watermarked ECG signal H' and the

TABLE 4 The comparative analysis of different steganography technique

Reference	Algorithm	Cover	Watermark	PSNR	Payload (bits)
Proposed	TQWT + SVD	ECG	Binary	59.64	64 000
Araghi et al[46]	DWT + 2D SVD	Image	Gray scale	46.95	Equal to cover size
Mathivanan et al[47]	DWT + location selection and pixel swapping method	ECG	Binary	45.63	21 000
Siddharth et al[48]	Deep ANN + ownership watermark and tampering localization	ECG	Binary	29.87	1199
Araghi et al[49]	DWT + 2D SVD	Image	Gray scale	46.69	64*64 and 8 bits for DS
Mathivanan et al[45]	DWT + quantization	ECG	Binary	51.4	229
Yang and Wang[28]	Coefficient alignment	ECG	Patient data	56.34	7500
Patil et al[50]	Curvelet Transform + Chaos	ECG	Binary image + Patient data	16.33	12bits/sample
Wang et al[29]	UES	ECG	Binary	—	56 000
Elshazly et al[23]	DWT + SVD	Audio	Binary image	50.81	1648
Jero et al[22]	DWT + SVD	ECG	Binary	50.44	4489
Jero et al[26]	Curvelet transform	ECG	Binary	43.44	4016
Jero et al[27]	CACO	ECG	Binary	34.43	24 560
Ibaida and Khalil's[14]	DWT	ECG	Patient data	48.47	19 200
Zhou et al[31]	DWT, APDCBT, and SVD	Image	Binary image	101.97	2048
Fazli and Moeini[32]	DWT-DCT-SVD	Image	Binary image	101.97	4096
Agarwal et al[33]	DWT–SVD and Firefly	Image	Gray scale	54.05	1024
Chih-Chin Lai[34]	Improved SVD	Image	Binary image	48.58	1024
Bai Ying Lei et al[35]	SVD–DCT	Audio	Binary image	32.53	256

TABLE 5 Test results of resampled signal

Resampling rate	101 m		102 m	
Metrics	BER	PSNR	BER	PSNR
100 Hz	0.0019	58.9513	0.0027	59.3354
200 Hz	0.0036	60.4321	0.0028	59.9254
300 Hz	0.0042	61.6219	0.0052	61.8884
500 Hz	0.0214	61.5398	0.0344	61.2325

watermark information Q are shown in Figure 9(1)A,B. Figure 9(1)C represents another watermark image Q_1 used for the watermark extraction. Figure 9(1)D shows clearly that the original watermark information Q cannot be extracted using an arbitrary reference image other than the original.

4.2.2 | False positive test 2

The ECG signal 16 272 m is used as cover data H and the watermark Q is embedded using proposed scheme to get watermarked ECG signal H'. Alternatively, the cover ECG signal H is embedded with another watermark data Q_1 to generate watermarked ECG signal of H_1. During data extraction process, the U and V^T component from the decomposed SVD and their respective secret key is used to extract watermark data Q and Q_1. In general, during data extraction process the secret key and U and V^T components of H_1 watermarked ECG signal is used to extract watermark data Q_1. The proposed scheme employs the secret key and U and V^T components of H_1 watermarked ECG signal is used to extract watermark data Q to test false positive attack. The decomposed SVD U and V^T component and secret key from H_1 watermarked ECG signal has failed to extract the watermark data Q that is embedded inside a watermarked ECG signal H. The secret key mismatch will halt the data extraction process as shown in Figure 9(2)A,B.

4.2.3 | False positive test 3

ECG signal 16 420 m is used as cover data H and the watermark information Q is embedded using proposed

TABLE 6 Obtained NCC value for different watermarked image by varying SNR value

NCC, $\alpha = .9$, 16 272 m-ECG normal signal				
Test image	**SNR = 10 dB**	**SNR = 20 dB**	**SNR = 30 dB**	**SNR = 40 dB**
Image1	0.9537	0.9948	0.9994	0.9999
Image2	0.9529	0.9946	0.9994	0.9999
Image3	0.9489	0.9949	0.9995	0.9999
Image4	0.9503	0.9948	0.9995	0.9999
Image5	0.9479	0.995	0.9995	0.9999
Image6	0.9505	0.9945	0.9994	0.9999
Image7	0.9512	0.9945	0.9995	0.9999
Image8	0.9489	0.995	0.9994	0.9999
Image9	0.9504	0.9947	0.9995	0.9999
Image10	0.9489	0.9947	0.9995	0.9999
Average	0.9503	0.9948	0.9995	0.9999

TABLE 7 Computation time analysis of proposed scheme with other traditional technique

Algorithm	Method	Computation time (sec)
Proposed	TQWT + SVD	1.79
Wang et al[29]	UES	10
Makbol Nasrin[24]	RDWT-SVD	3.23
Sangeetha and Anita[25]	DWT + SVD	1.73
Chen[51]	DCT	2.87

scheme to get watermarked ECG signal H_1. To test false positive attack, the watermarked ECG signal H_1 is again used as cover data to embedded watermark information Q_1 to generate watermarked ECG signal of H_2. During data extraction process, the U and V^T component of H_2 and the respective secret key is used to extract the watermark data Q_1. Similarly, the U and V^T component of H_1 and the individual secret key is used to extract the watermark data Q. Hence, to test the false positive attack the U and V^T components and the secret key of process H_1 is used extract watermark data Q_1. The attacker secret key mismatch will result in different watermark information as shown in Figure 9(3)A-C.

4.3 | Noise attack

The addition of noise is one of the most frequent attacks in steganography. The robustness of the proposed system is analyzed by adding Gaussian white noise with different SNR values. The Gaussian white noise is intentionally added to evaluate the robustness of the proposed scheme. The resultant watermarked image is corrupted by Gaussian white noise and is distributed over the entire spatial location of the cover signal. The quality of information obtained from watermarks is completely dependent on the noise density. If the noise density is lower, the watermark data extracted have minimal distortions and are reflected in the BER value. If the noise density is high, the information extracted results in greater distortion, with an increase in the BER value, as illustrated by Figure 10A-C. The results have shown a better resistance to noise than other conventional techniques.[31-45] The results of the proposed scheme are compared with other steganography techniques, as shown in Table 4. The method proposed shows that the PSNR and payload capacity are better than any other traditional scheme.[24,25,29,31-45,51]

Araghi et al[46,49] have proposed an image steganography technique using DWT and 2D SVD that has achieved an average PSNR value of 46 dB with variable payload capacity is found to be better than Siddharth et al[48] and Mathivanan et al.[45] Mathivanan et al[47] have proposed an ECG steganography using DWT and pixel swapping achieved a PSNR value of 45.63 dB with a payload efficiency of 21 k-bits which is observed to be better than Siddharth et al[48] and Mathivanan et al.[45] The proposed scheme described in this study considers the payload capacity of 64 k-bits, and the obtained results are found to be better than Siddharth et al[48] and Mathivanan et al.[45] Moreover, the imperceptibility of the proposed scheme is found to be good in comparison with Yang and Wang,[28] Siddharth et al,[48] Mathivanan et al,[47] Patil et al[50] and Mathivanan et al,[45] and is replicated in the PSNR value of 59.64 dB. Mathivanan et al and Yang and Wang[28] PSNR values are 51.4 dB and 56.34 dB which are found to be better than Siddharth et al,[48] Mathivanan et al[47] and Patil et al.[50] However, it considers a very low payload of 229 bits and 7500 bits compared to other traditional algorithms as shown in Table 4.

The CACO algorithm proposed by Jero et al[27] and the DWT steganography proposed by Ibaida and Khalil[14] have showed similar high payload capacity, but PSNR values decreased with an increase in payload capacity. In addition, the proposed scheme has a payload capacity of 64 k-bits with a PSNR of 59.64 dB, which is better than the Ibaida, Jero and Yang methods. Table 4 shows that the PSNR value of the proposed scheme is 19% higher than Jero et al[22] and 20% higher than Ibaida & Khalil[14] steganography schemes. Similarly, the proposed scheme's payload capacity is 2.6 and 3.3 times higher than Jero et al[27] and Jero et al.[14] As shown in Figure 5, the cover signal with an initial 128 Hz sample rate has been down sampled to 100 Hz and is up sampled to 500 Hz. With an increase in sample rate of ECG signal 101 m, 102 m, 103 m and 104 m, the values of BER and PSNR have increased as shown in Table 5. The four time increase in sample rate has increased BER by 2%, making the proposed system more robust against resample attacks.

Figure 10A-C shows the BER and NCC values of various watermark images. The study reflects increases in value of BER and NCC with increase in value of SNR. Form the literature, it is found that the BER value near zero has a minimum loss in extracted data and that the NCC value near to 1 shows that the extracted watermark data looks similar to the original data Low SNR value in the watermarked ECG signal will increase the amount of noise distribution, resulting in poor quality of the extracted watermark data. Alternatively, the values BER and NCC are considered good for higher SNR values. The obtained NCC values of the watermarked ECG signal (16 272 m) by varying 10 different watermark data and SNR between 10 dB and 40 dB that are shown in Table 6. The watermarked ECG signal looks exactly similar to the cover signal and its NCC values for the SNR value ranging from 10 to 40 dB are closed at ideal value 1. Accordingly, the proposed ECG steganography has minimum signal distortion for maximum noise distribution and it can be used for diagnose propose.

4.4 | Cost of computation

This proposal is implemented with a 32-bit Windows 7 Ultimate system using the MATLAB (R2015a), an Intel Core i3 processor with 2.40 GHz and 4 GB RAM. The calculation time for this scheme is better than other traditional techniques of steganography as shown in Table 7. The evaluation time of the proposed scheme is 5 times faster than the unified embedding scrambling (UES) algorithm.[29] In addition, the average working time is 1.6 times faster than other traditional methods.[24,25,29,31-45,51]

5 | CONCLUSIONS

In this article, a new ECG steganography is proposed to hide patient information in an ECG signal using TQWT and SVD. To achieve this, TQWT is used to decompose the original ECG signal into frequency sub-bands. The patient information is then embedded into singular value using a quantization embedding process. The main objective of the proposed scheme is to minimize signal deterioration, improve diagnosability and also to ensure better data retrieval capability. Metrics, such as PSNR, PRD, SSIM and BER are used to analyze the performance of the proposed approach. The number of errors in the patient information obtained is analyzed by BER. It is observed that 1.6 times increase in payload capacity increases BER values by 4%. Similarly, 1.6 times the increase in payload capacity decreases the PSNR value by 0.3% and the PRD value increases by 6%. Moreover, the simulation result of the proposed scheme has strong resistance to external attacks.

ORCID

P. Mathivanan https://orcid.org/0000-0002-0580-7757
A. Balaji Ganesh https://orcid.org/0000-0002-0897-3590

REFERENCES

1. Cox I, Miller M, Bloom J, Fridrich J, Kalker T. *Digital Watermarking and Steganography*. 2. San Francisco, CA: Morgan Kaufmann; 2007.
2. Phadikar A. *Data Hiding Techniques and Applications Specific Designs*. Saarbrucken: LAP LAMBERT Academic Publishing; 2012.
3. Ameen MA, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. *J Med Syst*. 2012;36:93-101.
4. Liu J, Tang G, Sun Y. BA secure steganography for privacy protection in healthcare system. *J Med Syst*. 2013;37:9918. https://doi.org/10.1007/s10916-012-9918-z.
5. Moody GB, Mark RG. The impact of the MIT-BIH arrhythmia database. *IEEE Eng Med Biol*. 2001;20:45-50.
6. Act, An., Health insurance portability and accountability act of 1996, Public Law 104 (1996) 191.
7. Pan J, Tompkins WJ. A real-time QRS detection algorithm. *IEEE Trans Bio-Med Eng*. 1985;32(3):230-236. https://doi.org/10.1109/TBME.1985.32553.
8. Nambakhsh MS, Ahmadian A, Ghavami M, Dilmaghani RS, Karimi-Fard S. A novel blind watermarking of ECG signals on medical images using EZW algorithm. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual*

International Conference of the IEEE (pp. 3274-3277). IEEE; 2006.

9. Zheng KM, Qian X. Reversible data hiding for electrocardiogram signal based on wavelet transforms. In *Proceedings of the 2008 International Conference on Computational Intelligence and Security (CIS2008)*, Suzhou, China, 13–17 December, pp. 295-299; 2008.
10. Zheng KM, Tang LW, Qian X. Watermarking technology for electrocardiogram signal certification. *Comput Eng Appl*. 2009; 45(20):231-233.
11. Kaur S, Farooq O, Singhal R, Ahuja BS. Digital watermarking of ECG data for secure wireless communication. In *Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (ITC2010)*, Kochi, Kerala, India, 12-13 March, pp. 140-144; 2010.
12. Ibaida A, Khalil I, Al-Shammary D. Embedding patients confidential data in ECG signal for healthcare information systems. *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*. IEEE; 2010.
13. Ibaida A, Khalil I, Schynde RV. A low complexity high capacity ECG signal watermark for wearable sensor-net health monitoring system. *Comput Cardiol*. 2011;38:393-396.
14. Ibaida A, Khalil I. Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. *IEEE Trans Biomed Eng*. 2013;60:3322-3330.
15. Loukhaoukha K, Chouinard JY, Taieb MH. Optimal image watermarking algorithm based on LWT-SVD via multiobjective ant colony optimization. *J Inf Hiding Multimedia Signal Process*. 2011;2(4):303-319.
16. Run RS, Horng SJ, Lai JL, Kao TW, Chen RJ. An improved SVD based watermarking technique for copyright protection. *Expert Syst Appl*. 2012;39(1):673-689. https://doi.org/10.1016/j.eswa.2011.07.059.
17. Ali M, Ahn CW. An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Process*. 2014;94:545-556.
18. Selesnick IW. Wavelet transform with tunable Q-factor. *IEEE Trans Signal Process*. 2011;59(8):3560-3575.
19. Patidar S, Pachori RB, Garg N. Automatic diagnosis of septal defects based on tunable-Q wavelet transform of cardiac sound signals. *Expert Syst Appl*. 2015;42(7):3315-3326.
20. Patidar S, Pachori RB. Classification of cardiac sound signals using constrained tunable-Q wavelet transform. *Expert Syst Appl*. 2014;41(16):7161-7170.
21. Lajnef T, Chaibi S, Eichenlaub JB, et al. Sleep spindle and K-complex detection using tunable Q-factor wavelet transform and morphological component analysis. *Front Hum Neurosci*. 2015;9:414.
22. Jero SE, Ramu P, Ramakrishnan S. Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission. *J Med Syst*. 2014; 38(10):132.
23. Elshazly AR, Nasr ME, Fouad MM, Abdel-Samie FS. High payload multi-channel dual audio watermarking algorithm based on discrete wavelet transform and singular value decomposition. *Int J Speech Technol*. 2017;20(4):951-958.
24. Makbol Nasrin M, Ee KB. Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *Int J Electron Commun (AEU)*. 2013;67:102-112.
25. Sangeetha N, Anita X. Linear weighted watermarking using normalized principal components. *Complex Intell Syst*. 2018;4(3):181-193. https://doi.org/10.1007/s40747-017-0065-5.
26. Jero SE, Ramu P, Ramakrishnan S. ECG steganography using curvelet transform. *Biomed Signal Process Control*. 2015;22: 161-169.
27. Ramu P, Swaminathan R. Imperceptibility—robustness tradeoff studies for ECG steganography using continuous ant colony optimization. *Expert Syst Appl*. 2016;49:123-135.
28. Yang CY, Wang WF. Effective electrocardiogram steganography based on coefficient alignment. *J Med Syst*. 2016;40(1):66.
29. Wang H, Zhang W, Yu N. Protecting patient confidential information based on ECG reversible data hiding. *Multimed Tools Appl*. 2016;75(21):13733-13747.
30. Vallathan G, Devi GG, Kannan AV. Enhanced data concealing technique to secure medical image in telemedicine applications. In *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 186–190). IEEE; 2016.
31. Zhou X, Zhang H, Wang C. A robust image watermarking technique based on DWT, APDCBT, and SVD. *Symmetry*. 2018;10 (3):77.
32. Fazli S, Moeini M. A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *Optik*. 2016;127:964-972.
33. Mishra A, Agarwal C, Sharma A, Bedi P. Optimized gray-scale image watermarking using DWT–SVD and Firefly algorithm. *Expert Syst Appl*. 2014;41(17):7858-7867.
34. Lai CC. An improved SVD-based watermarking scheme using human visual characteristics. *Opt Commun*. 2011;284(4): 938-944.
35. Lei BY, Soon Y, Li Z. Blind and robust audio watermarking scheme based on SVD–DCT. *Signal Process*. 2011;91(8):1973-1984.
36. Hussain M, Wahab AWA, Idris YIB, Ho AT, Jung KH. Image steganography in spatial domain: a survey. *Signal Process: Image Commun*. 2018;65:46-66.
37. Liao X, Qin Z, Ding L. Data embedding in digital images using critical functions. *Signal Process: Image Commun*. 2017;58: 146-156.
38. Shiu HJ, Lin BS, Huang CH, Chiang PY, Lei CL. Preserving privacy of online digital physiological signals using blind and reversible steganography. *Comput Methods Programs Biomed*. 2017;151:159-170.
39. El_Rahman SA. A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. *Comput Electr Eng*. 2018;70:380-399.
40. Subhedar MS, Mankar VH. Image steganography using redundant discrete wavelet transform and QR factorization. *Comput Electr Eng*. 2016;54:406-422.
41. Maheswari SU, Hemanth DJ. Frequency domain QR code based image steganography using Fresnelet transform. *AEU-Int J Electron Commun*. 2015;69(2):539-544.
42. Liao X, Yin J, Guo S, Li X, Sangaiah AK. Medical JPEG image steganography based on preserving inter-block dependencies. *Comput Electr Eng*. 2018;67:320-329.

43. Mathivanan P, Ganesh AB. QR code based color image cryptography for the secured transmission of ECG signal. *Multimed Tools Appl*. 2019;78(6):6763-6786.
44. Mathivanan P, Ganesh AB, Venkatesan R. QR code-based ECG signal encryption/decryption algorithm. *Cryptologia*. 2019;43(3):233-253.
45. Mathivanan P, Jero SE, Ramu P, Ganesh AB. QR code based patient data protection in ECG steganography. *Australas Phys Eng Sci Med*. 2018;41(4):1057-1068.
46. Araghi TK, Abd Manaf A. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Gener Comput Syst*. 2019;101:1223-1246.
47. Mathivanan P, Jero SE, Ganesh AB. QR code-based highly secure ECG steganography. In *International Conference on Intelligent Computing and Applications* (pp. 171-178). Singapore: Springer; 2019.
48. Bhalerao S, Ansari IA, Kumar A, Jain DK. A reversible and multipurpose ECG data hiding technique for telemedicine applications. *Pattern Recogn Lett*. 2019;125:463-473.
49. Araghi TK, Abd Manaf A, Araghi SK. A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. *Expert Syst Appl*. 2018;112:208-228.
50. Patil V, Patil M. Curvelet based ECG steganography for protection of data. In *Computational Vision and Bio Inspired Computing* (pp. 238-248). Cham, Springer; 2018.
51. Chen ST, Guo YJ, Huang HN, Kung WM, Tseng KK, Tu SY. Hiding patient's confidential data in the ECG signal via transform-domain quantization scheme. *J Med Syst*. 2014;38(6):54.

How to cite this article: Mathivanan P, Balaji Ganesh A. ECG steganography based on tunable Q-factor wavelet transform and singular value decomposition. *Int J Imaging Syst Technol*. 2020;1–18. https://doi.org/10.1002/ima.22477