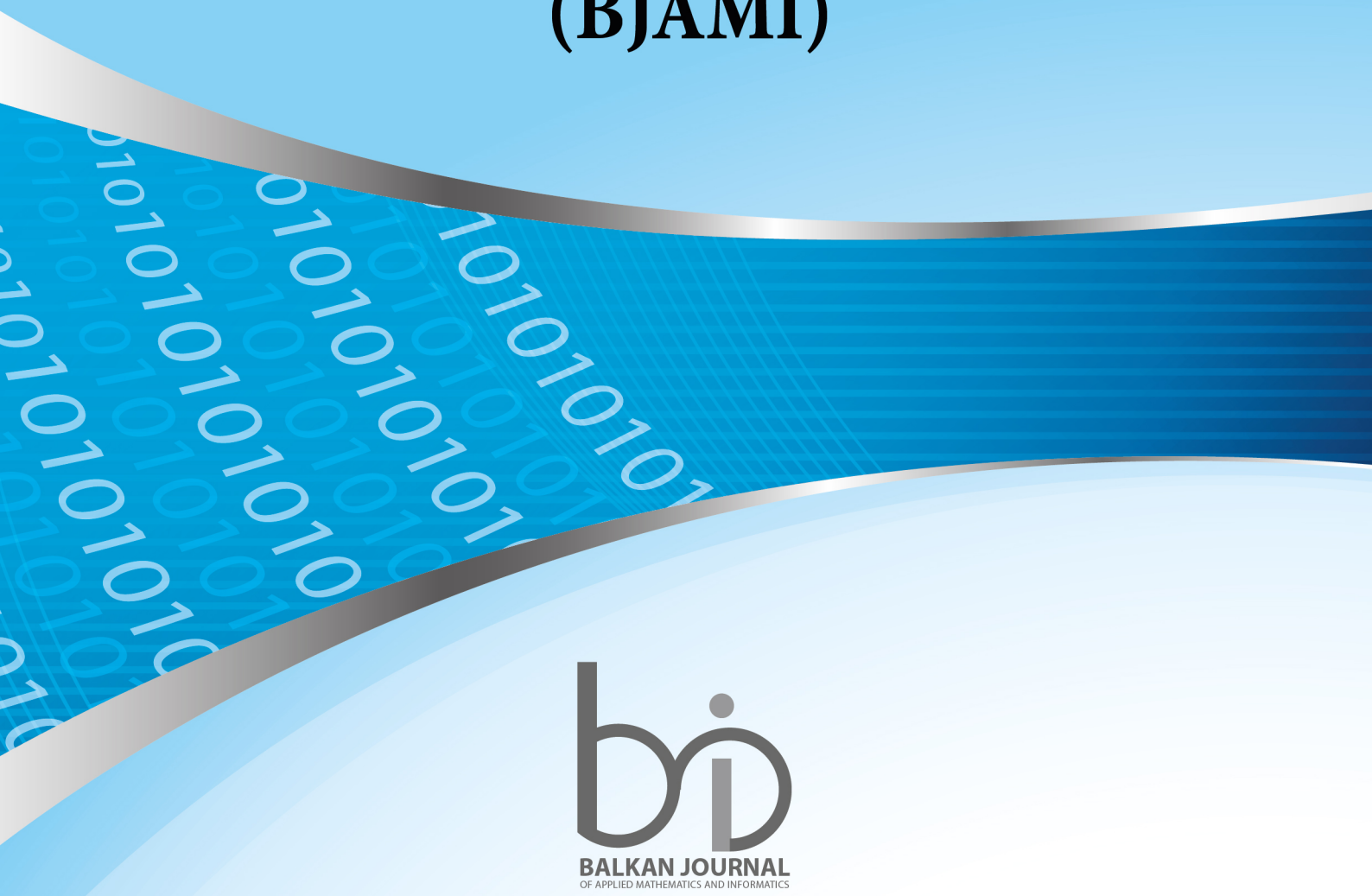
GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

ISSN 2545-4803 on line

BALKAN JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS (BJAMI)



YEAR 2021

VOLUME IV, Number 2

GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

ISSN 2545-4803 on line

BALKAN JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS

(BJAMI)

YEAR 2021 VOLUME IV, Number 2

AIMS AND SCOPE:
BJAMI publishes original research articles in the areas of applied mathematics and informatics.

Topics:
1. Computer science;
2. Computer and software engineering;
3. Information technology;
4. Computer security;
5. Electrical engineering;
6. Telecommunication;
7. Mathematics and its applications;
8. Articles of interdisciplinary of computer and information sciences with education, economics, environmental, health, and engineering.

Address of the editorial office
Goce Delcev University – Stip
Faculty of philology
Krste Misirkov 10-A
PO box 201, 2000 Štip,
Republic of North Macedonia

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS (BJAMI), Vol 3

ISSN 2545-4803 on line
Vol. 4, No. 1, Year 2021

EDITORIAL BOARD

CONTENT

UDC: 616.12-073.432.19:004.89.056.55

STATE-OF-THE-ART SURVEY OF DATA HIDING IN ECG SIGNAL

ALEKSANDAR VELINOV, IGOR STOJANOVIC AND VESNA DIMITROVA

Abstract. With the development of new communication technologies, the number of biomedical data that is transmitted is constantly increasing. This is sensitive data and therefore it is very important to preserve privacy when transmitting it. For this purpose, techniques for data hiding in biomedical signals are used. This is a comprehensive survey of research papers that covers the latest techniques for data hiding in ECG signal and old techniques that are not covered by the latest surveys. We show an overview of the methodology, robustness, and imperceptibility of the techniques.

1. Introduction

Biomedical signals are signals that we use to monitor physiological activities of organisms including neural and cardiac rhythms, blood glucose, oxygen saturation levels, blood pressure, etc. With biomedical signals processing, we can extract useful information from biomedical signals. This information can help to determine the actual state of the patient's health. This is also very important for continuous monitoring of the situation. This will allow a quick reaction in a patient who has a worsened condition. This emphasizes the importance of biomedical signals to humans.

In Figure 1, we can see the general procedure for the acquisition of a digital signal. Sensors are used to detect electrical signals. Transducers are used to convert nonelectric magnitudes into electric signals that can be stored, transmitted and treated [1]. In the next two steps of the procedure, the signal is amplified and filtered. This is done so that the signal meets the hardware requirements, to reduce noise and to compensate for some of the unwanted sensor characteristics. By using an A/D converter, the analog waveform is converted into a digital signal. The A/D conversion consists of two steps: a sampling process and a quantization procedure. The sampling process is used to convert the continuous signal into a discrete-time series. The elements of this process are named samples. The quantization procedure assigns the amplitude value of each sample within a set of determined discrete values [1] [2]. Finally, a digital signal is obtained, which can be further processed.

In medical applications it is often not enough just to get the signal. It is necessary to process the signal to obtain the appropriate information. Sometimes the signal is noisy and it needs to be cleaned or enhanced. Thomas in [3] introduces a method for compression and noise reduction of biomedical signals.

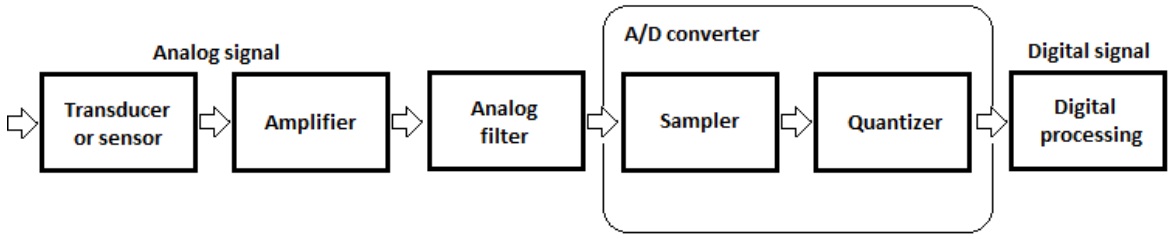


Figure 1. *Procedure for acquisition of digital signal*

Some of the well-known biomedical signals are: Electrocardiogram (ECG), Electroencephalogram (EEG) and Electromyogram (EMG). ECG is used to record the electrical activity of the heart. EEG is used to record the electrical activity of the brain. EMG is a monitoring method to record the electrical activity of the muscle.

Chang and Moura in [4] present a framework that treats data as random signals and with using Wiener filtering [5] or Kalman filtering [6] we can extract the desired signal components [7]. Relevant information may not be visible in the signal. Therefore, certain transformations are made to obtain the relevant information. Elgendi et al. in [8] present a six-steps high-level framework for biomedical signal processing (BSP).

In this section we will introduce some tools used for BSP. Vujović et al. in [9] present a virtual (software) instrument with a statistical analyzer for testing algorithms for biomedical signals. They implemented various reconstruction algorithms for different types of biomedical signals and different applications with under-sampled data. Cabrera at al. in [10] present a tool for training biomedical engineers in the BSP field. Different signal processing techniques are implemented with this tool. BioSig[1] is an open source software library for BSP [11]. BioSig can also be employed in neuro-informatics, brain-computer interfaces, neurophysiology, psychology, cardiovascular systems, etc. Bio-SP[2] is another tool for BSP. This tool is intended for assisting researchers in machine learning and pattern recognition to extract the feature matrix from biomedical signals [12].

The development of communication technologies has contributed to the transmission of biomedical data. During this period of Covid-19 pandemic, the number of biomedical data transmitted is quite high. Most often this is private and sensitive patient data. If third parties receive the data, the privacy of patients may be compromised. The authenticity and integrity should also be preserved. It is therefore important to provide secure communication channels for transmission. One way to achieve this is by data hiding in the biomedical signals. The areas of security that deal with this are: steganography and watermarking [18]. In the following sections, we will mention some of the steganography techniques used to hide data in the ECG signal.

[1] BioSig tool, https://github.com/dongzhenye/biosignal-tools

[2] Bio-SP, https://www.mathworks.com/matlabcentral/fileexchange/64013-biosignal-specific-processing-bio-sp-tool

There is still no comprehensive survey that provides an overview of the stenographic techniques methodologies used for data hiding in the ECG signal. Therefore, the need for this survey was imposed, which as novelties contains:

- Older data hiding techniques not mentioned in recent surveys
- New data hiding techniques that have been developed recently
- Data hiding techniques mentioned in older surveys but not related to appropriate biomedical signals

The paper is structured as follows: Section 2 covers the fundamentals of the ECG signal. Section 3 presents an overview of the techniques used for data hiding in the ECG signal. The last section is the conclusion of our work.

2. ECG fundamentals

An electrocardiogram (ECG) is a non-linear dynamic signal which is used for the diagnosis of heart diseases [13]. This signal tests the work of the heart by measuring its electrical activity. It is a small electrical impulse that spreads through the heart muscle. The ECG machine is used for detection of the ECG signal. In this process, the machine records the electrical activity of the heart and displays this data as a signal on a paper sheet [13]. The first ECG machine was invented in the early 1900s[3]. Numerous studies have led to the progress in this direction. Iskandar et al. in [14] present a prototype of a low-cost portable electrocardiogram (ECG) based on Arduino-Uno with Bluetooth feature. Bhuyan in [15] also presents a low-cost microcontroller-based ECG machine.

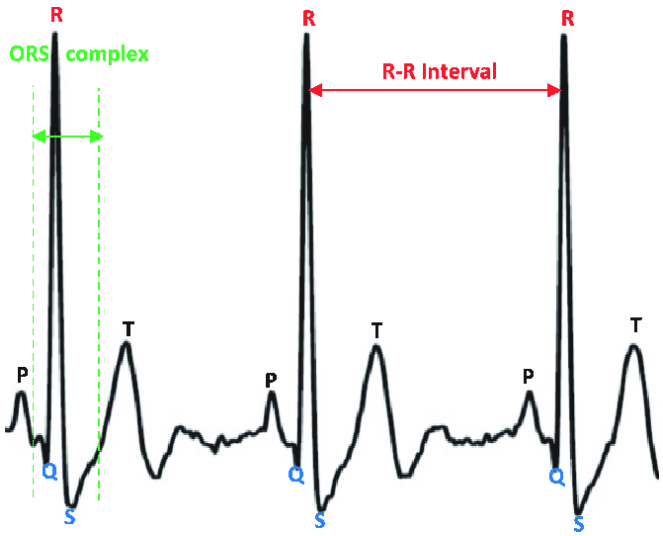


Figure 2. *An example of the ECG signal*[4]

[3] EKG Machine, http://www.madehow.com/Volume-3/EKG-Machine.html
[4] ECG signal, source: https://images.app.goo.gl/ZihBvGjRL4eqAeLfA

Figure 2 shows one example of the ECG signal [16]. The baseline of the ECG tracing is named as an isoelectric line, and it shows the resting membrane potentials. There are deflections from this line and they are denoted in alphabetical order.

The ECG signal is represented by P-QRS-T waves. The P wave, which is the first deflection, indicates depolarization of the atrial muscle cells. It does not show the contraction of the muscle. The amplitude of the P wave is usually between 0.1 and 0.2 mV and its duration is between 0.06 and 0.08s.

The QRS complex is a ventricular depolarization of an amplitude about 1mV and the duration time between 0.06 and 0.12s [17]. The Q part is the initial downward deflection, the R part is the initial upward deflection, and the S part is the return to the baseline, or to the isoelectric point [19]. Depolarization is often tis presented only as an "RX complex". It is assumed that the contraction will begin at the peak of the R part of the QRS complex. The T wave is the positive deflection after each QRS complex. It represents the rapid repolarization of contractile cells.

Table 1 shows all ECG electrical events [19].

Table 1. ECG electrical events

	Event	ECG Evidence
1	Sinoatrial node initiates impulse	Not visible
2	Depolarization of atrial muscle	P wave
3	Atrial contraction	Not visible
4	Depolarization of the AV node & Common Bundle	Not visible
5	Repolarization of the atrial muscle	Not visible
6	Depolarization of the ventricular muscle	QRS complex
7	Contraction of the ventricular muscle	Not visible
8	Repolarization of the ventricular muscle	T wave

When determining the activity of the heart, in addition to the ECG signal, it is necessary to know personal information about the person for whom the tests are performed. If this data is sent separately, it can be misused. It is therefore best to hide this data in the ECG signal.

3. Overview of the techniques for data hiding in ECG signal

Bhattacherjee et al. in [20] present a survey of steganographic methods for the ECG signal. They classify the data hiding techniques into two main categories: Frequency Domain Techniques (FDT) and Spatial Domain Techniques (SDT). FDT covers the following subcategories: Wavelet domain techniques, curvelet based ECG steganography and some others frequency domain techniques. SDT consists of LSB based methods and other techniques in spatial domain. They present only the papers related to data hiding in the ECG, but do not show the data for the methodologies, data embedding, robustness,

and imperceptibility. That is why we present a comprehensive survey of papers covering the steganography methods of data hiding in ECG. In addition, papers with references from 61 to 70 and 48 are not covered in [20].

Ibaida and Khalil in [21] present a wavelet-based steganography technique for data hiding in the ECG signal. Their technique consists of the following phases: Encryption, Wavelet Decomposition, Embedding operation, and Inverse Wavelet Recomposition.

- Encryption

For encryption of confidential patient information, they proposed the XOR ciphering technique.

- Wavelet Decomposition

In the second phase, they used the Wavelet transform. It is a process used for the decomposition of the given signal into coefficients that represent the frequency components of the signal at a given time. For this they proposed the Discrete Wavelet Transform (DWT) method. DWT is applied to the signal using band filters (high-pass filter and low-pass filter). The result of this operation are two different signals, one related to the high-frequency components and the other related to the low-frequency components of the given signal. The low-frequency signal represents the most important feature of the ECG signal. The high-frequency signal represents the noisily part of the ECG signal and it is called a detail signal. The high-pass filter gives the detail coefficients, and the low-pass filter gives the approximation coefficients. These coefficients are later used to hide data.

This DWT process can be repeated multiple times. It is known as the multilevel packet wavelet decomposition. In [21] they proposed a five-level wavelet packet decomposition. DWT is defined as follows:

$$W(i,j) = \sum_{i} \sum_{j} X(i)\Psi ij(\mathrm{n}) \tag{1}$$

In (1), W(i,j) are DWT coefficients, i and j are the scale and shift transform parameters and Ψij(n) is the wavelet basis time function with finite energy and decay.

- Embedding operation

In the third phase, for the embedding operation they used a scrambling operation using two parameters: a shared key and a scrambling matrix. This matrix is stored in the transmitter side and also in the receiver side. They proposed a 128 x 32 scrambling matrix (2), where s is the number between 1 and 32.

$$\mathrm{S} = \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,32} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,32} \\ \vdots & \vdots & \ddots & \vdots \\ s_{128,1} & s_{128,2} & \cdots & s_{128,32} \end{bmatrix} \tag{2}$$

The matrix must meet these conditions:

- The same row must not contain duplicate elements
- Rows must not be duplicates

First, the shared key is converted into ASCII codes. Each character is represented by a number from 1 to 128. Next, the scrambling sequence fetcher reads the corresponding row from the scrambling matrix, for each character code. One example of a fetched row is:

S_r = 30, 28, 6, 3, 16, 11, 32, 7, 22, 17, 14, 8, 5, 29, 21, 25, 31, 27, 26, 19, 15, 1, 23, 2, 4, 18, 24, 13, 9, 20, 10, 12

If the fetched row is as S_r, the bits embedding will start with reading the current wavelet coefficient in subband 30 and changing its LSB bits. Then, it will read the wavelet coefficient in subband 28, and changing its LSB bits, and so on. The steganography level is determined by the level vector. It contains information about how many LSB bits will be changed for each subband in the process of data embedding.

- Inverse Wavelet Recomposition

The last phase of this technique is Inverse Wavelet Recomposition (IWR). With IWR the resultant 32 subbands are recomposed. The final result is the new ECG recomposed signal.

The above methodology has been used in most of the papers we have reviewed. In the next sub-sections, we will show which techniques are most commonly used for encryption, which type of wavelet transformation is used, and which are the most common methods of data hiding.

3.1 Encryption techniques

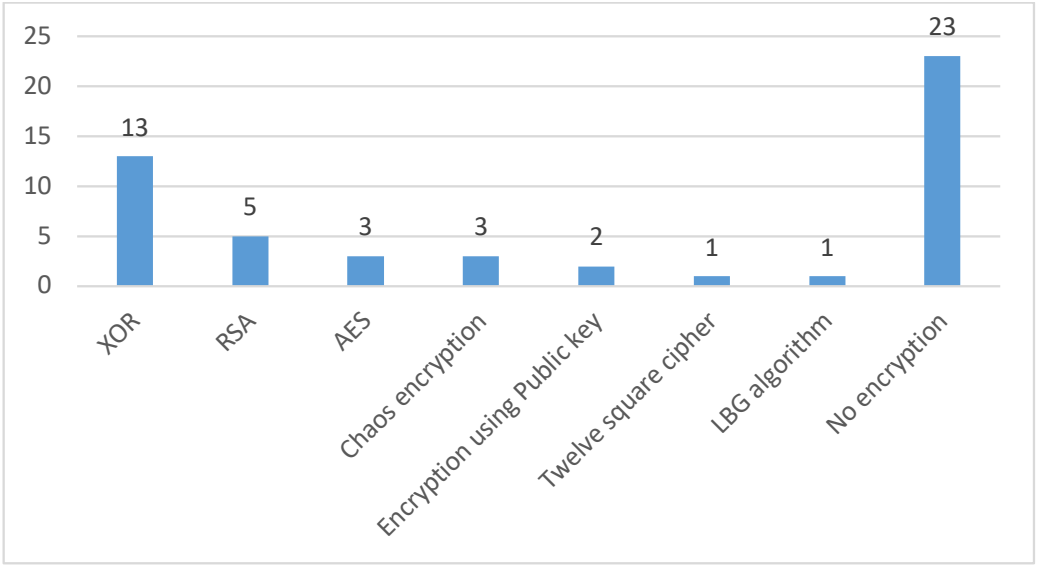


Figure 3. Encryption techniques proposed in papers

In Figure 3, we can see all techniques for encryption that are used in the papers. The XOR technique is the most used. Other techniques that are used are: RSA, AES, Chaos encryption, encryption with public key, twelve square cipher, and LBG algorithm. Some papers suggest more techniques. Most papers (23) do not use encryption of the data being transmitted. It is good to use encryption because in most cases it is sensitive data.

3.2 Wavelet Transformation

Regarding methodology, we have classified the papers into 5 categories: DWT-based techniques, DWT-based techniques with different approach, Integer Wavelet Transform (IWT)-based techniques, Haar Wavelet Transform (HWT)-based techniques and other techniques.

A. DWT-based techniques

Papers [25, 26, 30, 35, 36, 50, 53, 58, 62, 63], like [21], all use DWT. The only difference is that some of them use a different encryption algorithm such as RSA, AES or Chaos cryptography. The general formula for bit embedding for this technique is as follows:

$$\sum_{i=1}^{n} Coeff\_bits\_i \tag{3}$$

where, n is the total number of used coefficients and Coeff_bits_i is the bits that can be embedded in each coefficient. These papers basically do not present data for analysis of robustness and imperceptibility.

B. DWT-based techniques with different approach

Papers [22, 23, 27, 28, 29, 32, 38, 52, 59, 65] use DWT with a different approach for data hiding in the ECG signal. [23, 27, 29, 32] in addition also use the Pan-Tompkin's QRS detection algorithm. [22, 23, 27, 29, 32] proposed Singular Value Decomposition (SVD) for secret data embedding into the decomposed ECG signal. The authors in [27] present the Continuous Ant Colony Optimization Algorithm (CACO). This method is used to identify Multiple Scaling Factors (MSFs) that can provide a better tradeoff in comparison to the Uniform Single Scaling Factor (SSF). The optimal MSFs can improve the ECG steganography performance. For the embedding operation, the authors in [38] proposed the Unequal Steganography Embedding (USE) method. The authors in [52] proposed the Adaptive LSB Replacement method for embedding. Augustyniak in [59] shows that the analysis of the ECG bandwidth gap can be used as a possible carrier for the supplementary digital data. Boostani and Sabeti in [65] proposed a multi-channel steganography, which in addition uses a non-linear feedback shift register (NLFSR) method for input message bits shuffling.

C. IWT-based techniques

Papers [24, 37, 61, 68, 69, 70] use the Integer Wavelet Transform (IWT) technique. The presented techniques in [24] and [37] proposed similar methodologies as the DWT-based techniques. The only difference is that instead of DWT they use IWT. The techniques in [61] and [68] hide data bits in the host bundles of the low and high subbands of the IWT

coefficients. Sony et al. in [69] used modified LSB for data bits embedding and chaotic maps for security. The same authors in [70] additionally use the pixel inverted pixel value differencing (PI-PVD) technique to hide confidential data.

D. HWT-based techniques

Papers [34, 45, 47] use Haar Wavelet Transformation (HWT). Sivaranjani and Radha in [34] proposed the Arnold cat map technique that is used to scramble the encrypted data. They also use RSA for encryption and SVD for data bits embedding. Wu et al. in [45] proposed a histogram shifting and thresholding scheme and the LSB substitution method for private data embedding.

E. Other techniques

Sheeba et al. in [33] proposed a technique which used the Chaos crypto system for encryption, wavelet decomposition (Short Time Fourier Transform, Forward Lifting in IWT and Reverse Lifting Scheme in IWT) and LSB for bits embedding. Mathivanan et al. in [39] present a QR code-based highly secure ECG steganography. They proposed logistic chaotic encryption, transforming information into 2D binary matrix and data embedding using pixel permutation. Jero et al. in [40] and [41] proposed an ECG steganography technique which uses curvelet transform. Ibaida et al in [42] proposed a steganography technique that embeds confidential information of patients into specific locations (special range numbers) of the ECG host signal. Mai et. al in [43] proposed a method for the steganography-based access control to medical data that are hidden in ECG. Abuadbba and Khalil in [44] present a steganography technique that is based on Fast Walsh-Hadamard Transform. For encryption they proposed AES. They also provide coefficient shuffling. Vallathan et al. in [46] show an enhanced data concealing technique that uses the Contourlet transform, LSB for bits embedding and the LBG algorithm for encryption. Banerjee and Sigh in [48] present a new approach of ECG steganography and prediction using deep learning. This method uses the TP segment for data hiding. Pandey et al. in [49] present a technique that uses a chaotic map and a simple value difference model for ECG steganography and Orthogonal Frequency Division Multiplexing (OFDM) based secured patient information transmission. Duy et al. in [51] proposed a technique for data bits embedding only between the T-P wave of the ECG signal. Yang and Wang in [54] present an effective ECG steganography technique based on coefficient alignment. They present two types of data hiding methods: lossy and reversible ECG steganography. The same authors in [55] proposed data hiding in ECG based on smart offset coefficients. Shiu et al. in [56] show a blind and reversible steganography that uses error correcting code, matrix coding and decision code. Wang et al. in [57] also present a reversible ECG data hiding technique based on Local Linear Prediction (LLP), Prediction Error Expansion and threshold T. Mathivanan and Ganesh in [60] proposed a color image steganography using the XOR multi-bit embedding process. Yang et al. in [64] present an adaptive ECG steganography based on 2D approach with predetermined rules. Cheng and Yang in [66] proposed ECG steganography based on Fast Discrete Cosine Transform

(FDCT). Yang et al. in [67] present an efficient reversible ECG steganography by adaptive LSB approach based on 1D FDCT domain.

3.3 Bits embedding methods, databases used, robustness and imperceptibility

Most papers use LSB and SVD methods for bits embedding. In one of the papers a USE algorithm is proposed.

The MIT-BIH arrhythmia database is mostly used in the analysis and evaluation of the ECG data hiding techniques. Other databases used are: Physikalisch-Technische Bundesanstalt (PTB) database, MIT-BIH NSR database, BIDMC-CHF database, Mitdb, European ST-T, ptbdb database, and self-recorded database.

Some of the papers display information related to robustness and imperceptibility.

An overview of the methodology, robustness and imperceptibility of the data hiding methods in ECG is given in Table 2.

Table 2. Overview of the methodology, robustness and imperceptibility of the methods for data hiding in ECG

No	Ref no.	Methodology	Bits embedding	Robustness	Imperceptibility
1	[21]	1.Encryption (XOR) 2. DWT 3. Embedding operation (LSB) 4. Inverse Wavelet Decomposition (IWD)	$\sum_{i=1}^{n} Coeff\_bits\_i$ n- total number of used coefficients Coeff_bits_i – bits embedded in each coefficient	/	/
2	[22]	DWT SVD Inverse DWT	/	The robustness is successfully achieved	/
3	[23]	Pan and Tompkins QRS detection algorithm, DWT SVD	/	/	Yes
4	[24]	Encryption (XOR) Integer-to-Integer Wavelet Transform, Embedding operation (LSB), Inverse Wavelet Transform (IWT)	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
5	[25]	Encryption (XOR) DWT Embedding operation (LSB), IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
6	[26]	Encryption (XOR) DWT Embedding (LSB), IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
7	[27]	Pre-processing of the ECG signal using the Pan-Tompkin's QRS detection algorithm DWT SVD	/	Achieved respective robustness	Yes

		Continuous Ant Colony Optimization Algorithm (CACO)			
8	[28]	Encryption using Public Key DWT	/	/	/
9	[29]	Pan-Tompkin's QRS detection algorithm DWT SVD BCH error-correcting codes (for extraction)	/	Improved robustness using the BCH error-correcting codes	Yes
10	[30]	Encryption (RSA) Wavelet decomposition of the host ECG signals Embedding (LSB) IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
11	[31]	Encryption (RSA) DWT Embedding (LSB) IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
12	[32]	Encryption (XOR) Pan-Tompkin's QRS detection algorithm DWT SVD Inverse DWT	/	/	/
13	[33]	Encryption (Chaos crypto system) Wavelet Decomposition (Short Time Fourier Transform, Forward Lifting in IWT, Reverse Lifting scheme in IWT) Embedding (LSB)	$\sum_{i=1}^{n} Detail\_Coeff\_bits\_i$ n- total number of used detailed coefficients Detail_Coeff_bits_i – bits embedded in each coefficient	/	Yes
14	[34]	Encryption (RSA) HWT Arnold cat map technique (used to scramble the encrypted data) SVD	$\sum_{i=1}^{n} Detail\_Coeff\_bits\_i$	/	/
15	[35]	Encryption (RSA) DWT Embedding (LSB) IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$ n- total number of used coefficients Coeff_bits_i – bits embedded in each coefficient	/	/
16	[36]	Encryption (RSA) DWT Embedding (LSB) IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
17	[37]	Encryption (XOR) IWT Embedding (LSB) Inverse IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/

18	[38]	DWT Embedding (USE algorithm) Inverse Discrete Wavelet Transform (IDWT)	$c^{m}_{detail_{new}}$ -total modified coefficients	The proposed technique is robust	/
19	[39]	DWT Patient data is transformed into a 2D binary matrix (QR code) Swapping method Inverse DWT	$\sum_{i=1}^{n} S\_Coeff\_bits\_i$ Where n is the number of swapped coefficients	/	Yes
20	[40]	Convert 1D ECG signal into 2D ECG image (Tompkins algorithm) Curvelet Transform (Fast Fourier Transform – FFT and Fast Discrete Curvelet Transform -FDCT)	Data hiding capacity depends on the ECG signal size and number of bits stored per an ECG sample	/	/
21	[41]	Convert 1D ECG signal into 2D ECG image (Tompkins algorithm) Curvelet Transform Threshold selection algorithm Quantization method Inverse Curvelet Transform	/	/	Yes
22	[42]	ECG Signal Preprocessing Shift Special Range Transform Data Hiding ECG Signal Scaling and Level Correction	Embed the secret bits using the shifted value as a host according to the equation: Mn = $\begin{cases} M_o + (R\_\max - S) & if\ B = 1 \\ M_o - (S - R_{min}) & if\ B = 0 \end{cases}$ Where, Mn – new resultant value of the new data Rmin – minimum value of the selected special range Rmax – maximum value B – secret bit	/	Yes
23	[43]	ECG Signal Preprocessing Shift Special Range Transform Data Hiding ECG Signal Scaling and Level Correction	Embed the secret bits using the shifted value as a host according to the equation: Mn = $\begin{cases} M_o + (R\_\max - S) & if\ B = 1 \\ M_o - (S - R_{min}) & if\ B = 0 \end{cases}$ Where, Mn – new resultant value of the new data Rmin – minimum value of the selected special range Rmax – maximum value B – secret bit	/	Yes
24	[44]	Fast Walsh-Hadamard Transform (FWHT) Encryption (AES) Coefficients shuffling Key-Driven Random Order Inverse Walsh-Hadamard Re-transform	b= $\sum_{i=1}^{n}\left((R\ x\ C\ x\ D) - hc\right)\ x\ S$ where, b - highest embedded bits n - biomedical signal's samples R, C and D - dimensions of the reshaped 3D template after	The proposed technique is robust	Yes

			implementing FWHT transformation hc - less-significant sequence coefficients S - stego scale per value.		
25	[45]	Invertible Integer-to-Integer HWT Histogram Shifting and Thresholding Scheme Overflow and Underflow Detection Embedding (LSB) Inverse Haar DWT	/	/	/
26	[46]	Encryption (LBG algorithm) Contourlet Transform Embedding (LSB)	/	/	/
27	[47]	Signal transformation technique (Haar Wavelets) Encryption (Security Key) Embedding (LSB) Haar Wavelet recomposition	/	/	Yes
28	[48]	The method uses only the TP-segment of entire ECG Long Short-Term Memory Recurrent Neural Network (LSTM RNN) (method used after decryption)	1 bit per sample of TP-segment	/	/
29	[49]	Chaotic map based embedding location generation Sample value difference method based secret data embedding	The resulting absolute difference and a predefined dyadic range table determine the number of bits to be embedded in the given sample pair.	/	Yes
30	[50]	DWT Encryption (XOR or AES) Embedding (LSB) Inverse Wavelet Re-composition (IWR)	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
31	[51]	Identify waveforms (detect T and P wave) Encryption (SHA3 and AES-192) Embedding operation (LSB matching algorithm)	Embedding three data bits m1, m2 and m3 into three ECG signals x_1, x_2 and x_3 that form three output samples y_1, y_2 and y_3: $f^3_{emb}(x,m) = \{y \in Ax : (x_1+2x_2+3x_3) \bmod 8 = m\}$ where $x = (x_1,x_2,x_3)$ $m = 4m_1 + 2m_2 + m_3 = \{0,1,2,3,4,5,6,7\}$ $A_x = \{(x_1,x_2,x_3),(x_1\pm1,x_2,x_3),(x_1,x_2\pm1,x_3),(x_1,x_2,x_3\pm1),(x_1\pm1,x_2,x_3\pm1)\}$	/	Yes
32	[52]	DWT	A variable number of LSBs would be utilized for embedding secret message bits.	/	/

		Encryption (Twelve Square Cipher) Embedding operation (Adaptive LSB Replacement)	For example: - If the value of the pixel (vi) is in the range 240 ≤ vi ≤255, then 4 bits of secret data will be embedded into the 4 LSBs of the pixel value. - If 224 ≤ vi ≤239, then 3 bits of secret data will be embedded into the 3 LSB's of the pixel.		
33	[53]	Encryption (Chaos Cryptography) DWT Embedding operation (LSB) IWR	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
34	[54]	Reversible ECG steganography: Embedding secret bits in the predefined bundles of the host ECG (LSB substitution) (Note: The paper also presents Lossy ECG steganography methods)	$\sum_{i=1}^{n} Bundles\_bits\_i$ n- bundle size (it is not fixed) Bundles_bits_i – bits embedded in each bundle	This method has a certain degree of robustness	/
35	[55]	Embedding secret bits in the predefined bundles of the host ECG (LSB substitution)	$\sum_{i=1}^{n} Bundles\_bits\_i$ Bundles_bits_i – bits embedded in each bundle (They proposed 2 bits)	This method has a certain degree of robustness	/
36	[56]	Error Correcting code (Hamming codes) Matrix coding Decision code	Position to be changed=$m \oplus H_x$ Where x – cover bit vector m- secret bits H_x - it is given	The (31,26)-Hamming code exhibits the best robustness	/
37	[57]	Local Liner Prediction (LLP) Prediction Error Expansion Data embedding (Original value, predicted value, prediction error and threshold T are given)	Threshold T controls the embedding capacity (from the experiments about 7 bits per sample)	/	/
38	[58]	Encryption (XOR) DWT Embedding (LSB) Inverse Wavelet Re-Composition	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
39	[59]	Heartbeat detection Delimitation of selected wave borders DWT Bandwidth gap analysis Coding the message Inverse DWT	$\sum_{i=1}^{n} Coeff\_bits\_i$	/	/
40	[60]	Signal Pre-processing XOR Coding Modulo Division Process Data Embedding	$I'_{WC} = I'_{CC} \oplus Q$ Where, I'_{WC} – image component with embedded data	To increase the robustness of the proposed method,	Yes

			I'$_{CC}$ – selected location from image component Q – quotients obtained from modulo division process $T = \sum_{i=1}^{3} I'wc_i$ T - Total embedded bits I'wc$_i$ – Embedded bits in image components	the encrypted information is given to the modulo division process, and the location selection process using threshold value is used.	
41	[61]	IWT Hiding data in the ECG hot bundle Inverse IWT	In host bundle of size n (n-1) bits	The larger values of control integer, the better robustness performance obtained by the proposed method	Yes
42	[62]	Chaos encryption, DWT, LSB replacement algorithm IWR	$\sum_{i=1}^{n} Detail\_Coeff\_bits\_i$	/	/
43	[63]	Encryption (XOR) DWT Embedding (LSB) IWD	$\sum_{i=1}^{n} Coeff\_bits\_i$	Because the ECG signal is denoised, the noise cannot affect the covert data.	/
44	[64]	Two-dimensional (2D) bit-embedding/-extraction approach Hiding data in the ECG host bundles	(n-1) x n bits in a host bundle at a time	The proposed method with the larger τ (control integer) provides better robustness performance than that with the smaller τ.	/
45	[65]	Encryption (XOR), Nonlinear feedback shift register (NLFSR), DWT- NLFSR, DCT- NLFSR, DWT with LSB or DWT-SVD Inverse Wavelet Transfom	For ASCII: DCT-NLFSR and NLFSR: 7 times of the length of the ECG signal (non-QRS parts) DWT-NLFSR: 7 times of the half length of non-QRS length of ECG signal DWT-SVD and evolutionary-based DWT-SVD: 7 times of the half length of nonQRS length of ECG signals.	/	/
46	[66]	Fast Discrete Cosine Transform (FDCT) Hiding secret data in host bundle Inverse FDCT	(Size of host ECG data / Size of DCT bundle) x ϕ	The proposed method has a certain degree of robustness	/
47	[67]	1D FDCT Adaptive LSB technique	$\{sji\}_{i=0}^{n-2}$ bits,	The proposed method has a degree of robustness that is	/

			where s_{ij} are series of non-overlapping jth bundles of size n taken from 1D FDCT coefficients	rarely seen in the traditional reversible ECG steganography. The method is robust against attacks such as noise addition, inversion, truncation, translations, etc.	
48	[68]	IWT Hiding data in the ECG host bundle Inverse IWT	Precondition: host bundle of size 3 If criteria-1: $\|s_{j0}-s_{j1}\| \leq \tau$ And If criteria-2: $\left\|\frac{sj0+sj1}{2}-sj2\right\| \leq \tau$ are satisfied then: 2 bits in host bundle If the conditions are not satisfied: 1 bit in bundle	The proposed method provides robustness performance better than the existing techniques	/
49	[69]	Encryption (XOR) IWT Chaotic maps for additional security Modified LSB Inverse IWT	$\sum_{i=1}^{n} Approx\_Coeff\_bits\_i$ n- total number of used coefficients Approx_Coeff_bits_i – bits embedded in each approximate coefficient	The robustness is duly ensured as the confidential data is encrypted prior to embedding into the ECG signal	/
50	[70]	Encryption (XOR) IWT Modified LSB, Pixel Inverted Pixel Value Differencing (PI-PVD) Chaotic maps for security Inverse IWT	$\sum_{i=1}^{n} Approx\_Coeff\_bits\_i$	Robustness is successfully achieved	Yes

Conclusion

The amount of medical data being transmitted is constantly increasing. These are sensitive data for which privacy and integrity should be preserved. In this context, techniques for data hiding in medical signals are used. In this paper, we have presented a comprehensive survey of all the techniques for data hiding in the ECG signal. In our next research, we will focus on discovering new techniques.

References

[1] Bronzino, J. D., & Peterson, D. R. (Eds.). (2014). Biomedical signals, imaging, and informatics. CRC Press, book.

[2] Johansson, H. (2014). Sampling and quantization. In Academic Press Library in Signal Processing (Vol. 1, pp. 169-244). Elsevier.

[3] Schanze, T. (2018). Compression and noise reduction of biomedical signals by singular value decomposition. IFAC-PapersOnLine, 51(2), 361-366.

[4] Chang, H, Moura, J (2010). Biomedical Engineering and Design Handbook: McGraw Hill, a chapter of the book.

[5] Chen, J., Benesty, J., Huang, Y., & Doclo, S. (2006). New insights into the noise reduction Wiener filter. IEEE Transactions on audio, speech, and language processing, 14(4), 1218-1234.

[6] Oikonomou, V. P., Tzallas, A. T., Konitsiotis, S., Tsalikakis, D. G., & Fotiadis, D. I. (2009). The use of Kalman filter in biomedical signal processing. Kalman Filter: Recent Advances and Applications.

[7] Manju, B. R., & Sneha, M. R. (2020). ECG Denoising using Wiener filter and Kalman filter. Procedia Computer Science, 171, 273-281.

[8] Elgendi, M., Howard, N., Lovell, N., Cichocki, A., Brearley, M., Abbott, D., & Adatia, I. (2016). A six-step framework on biomedical signal analysis for tackling noncommunicable diseases: Current and future perspectives. JMIR Biomedical Engineering, 1(1), e1.

[9] Vujović, S., Draganić, A., Lakičević Žarić, M., Orović, I., Daković, M., Beko, M., & Stanković, S. (2020). Sparse analyzer tool for biomedical signals. Sensors, 20(9), 2602.

[10] Cabrera, J., Alonso-Hernández, J. B., & Travieso-González, C. M. (2015). Tool for biomedical signals processing.

[11] Vidaurre, C., Sander, T. H., & Schlögl, A. (2011). BioSig: the free and open source software library for biomedical signal processing. Computational intelligence and neuroscience, 2011.

[12] Sarah Ostadabbas (2021). Biosignal-Specific Processing (Bio-SP) Tool (https://www.mathworks.com/matlabcentral/fileexchange/64013-biosignal-specific-processing-bio-sp-tool), MATLAB Central File Exchange. Retrieved January 26, 2021.

[13] Taha, Taha & El-Sayed, Ayman & Rafat, Salma. (2016). A Survey on Classification of ECG Signal Study. Communications on Applied Electronics (CAE). 6. 11. 10.5120/cae2016652467.

[14] Iskandar, W. J., Roihan, I., & Koestoer, R. A. (2019, December). Prototype low-cost portable electrocardiogram (ECG) based on Arduino-Uno with Bluetooth feature. In AIP Conference Proceedings (Vol. 2193, No. 1, p. 050019). AIP Publishing LLC.

[15] Bhuyan, M. H., Hasan, M. T., & Iskander, H. (2020). Low Cost Microcontroller Based ECG Machine. International Journal of Biomedical and Biological Engineering, 14(7), 192-199.

[16] Ben Slama, Amine & Lentka, Łukasz & Mouelhi, Aymen & Diouani, Mohamed Fethi & Sayadi, Mounir & Smulko, Janusz. (2018). Application of statistical features and multilayer neural network to automatic diagnosis of arrhythmia by ECG signals. Metrology and Measurement Systems. 25. 10.24425/118163.

[17] Slama, A. B., Lentka, Ł., Mouelhi, A., Diouani, M. F., Sayadi, M., & Smulko, J. (2018). Application of statistical features and multilayer neural network to automatic diagnosis of arrhythmia by ECG signals. Metrology and Measurement Systems, 25(1).

[18] Fkirin, Alaa & Attiya, Gamal & El-Sayed, Ayman. (2016). Steganography Literature Survey, Classification and Comparative Study. Communications on Applied Electronics. 5. 13-22. 10.5120/cae2016652384.

[19] Becker, D. E. (2006). Fundamentals of electrocardiography interpretation. Anesthesia progress, 53(2), 53-64.

[20] Bhattacherjee, P., Ganguly, D., & Chatterjee, K. (2021). A Brief Survey of Steganographic methods for ECG Signal. In Proceedings of International Conference on Frontiers in Computing and Systems (pp. 35-43). Springer, Singapore.

[21] Ibaida, A., & Khalil, I. (2013). Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. IEEE Transactions on biomedical engineering, 60(12), 3322-3330.

[22] Jero, S. E., Ramu, P., & Ramakrishnan, S. (2014). Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission. Journal of medical systems, 38(10), 1-11.
[23] Jero, S. E., Ramu, P., & Ramakrishnan, S. (2015). Steganography in arrhythmic electrocardiogram si3nal. In 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (pp. 1409-1412). IEEE.
[24] Liji, C. A., Indiradevi, K. P., & Babu, K. A. (2016). Integer-to-integer wavelet transform based ECG steganography for securing patient confidential information. Procedia Technology, 24, 1039-1047.
[25] Awasthi, D., & Madhe, S. (2015, February). Analysis of encrypted ECG signal in steganography using wavelet transforms. In 2015 2nd international conference on electronics and communication systems (ICECS) (pp. 718-723). IEEE.
[26] Dilip, P. K., & Raskar, V. B. (2015). Hiding patient confidential information in ECG signal using DWT technique. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 4(2).
[27] Ramu, P., & Swaminathan, R. (2016). Imperceptibility—robustness tradeoff studies for ECG steganography using continuous ant colony optimization. Expert Systems with Applications, 49, 123-135.
[28] Sankari, V., & Nandhini, K. (2014, February). Steganography technique to secure patient confidential information using ECG signal. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-7). IEEE.
[29] Jero, S. E., & Ramu, P. (2016). A robust ECG steganography method. In 2016 10th International Symposium on Medical Information and Communication Technology (ISMICT) (pp. 1-3). IEEE.
[30] Devi, A., & ShivaKumar, K. B. (2016). Novel audio steganography technique for ECG signals in point of care systems (NASTPOCS). In 2016 IEEE international conference on cloud computing in emerging markets (CCEM) (pp. 101-106). IEEE.
[31] Asha, N. S., Anithadevi, M. D., Shivakumar, K. B., & Kurian, M. Z. (2016, May). ECG signal steganography using wavelet transforms. In Int. J. Adv. Netw. Appl.(IJANA) In: Proceedings of the 1st International Conference on Innovations in Computing & Networking (ICICN16), CSE, RRCE (pp. 355-359).
[32] Meghani, D., & Geetha, S. (2016, March). ECG steganography to secure patient data in an E-healthcare system. In Proceedings of the ACM Symposium on Women in Research 2016 (pp. 66-70).
[33] Sheeba, G., Anju, M. I., Priya, K. H., Monisha, V., & Banu, M. S. (2015). Secure crypto and ECG steganography based data communication for wireless body sensor network. Int. J. Innovative Res. Comput. Commun. Eng, 3(3).
[34] Sivaranjani, B., & Radha, N. (2017, October). Securing patient's confidiential information using ECG steganography. In 2017 2nd International Conference on Communication and Electronics Systems (ICCES) (pp. 540-544). IEEE.
[35] Marakarkandy, B., & Tiwari, M. R. (2015). Secure Steganography, Compression and Transmission of ECG signal for Protecting Patient Confidential Information in Point-of-Care Systems. Int. J. Appl. Innovation Eng. Manag.(IJAIEM), 4(7), 94-99.
[36] Awasarmol, S. P., Ashtekar, S., & Chintawar, A. (2017, August). Securely data hiding and transmission in an ECG signal using DWT. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 2850-2854). IEEE.
[37] PremChandran, K., & Krishnakumar, K. P. (2015, January). ECG steganography using Integer Wavelet transform. In 2015 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.
[38] Sahu, N., Peng, D., & Sharif, H. (2017, May). Unequal steganography with unequal error protection for wireless physiological signal transmission. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
[39] Mathivanan, P., Jero, S. E., & Ganesh, A. B. (2019). QR code-based highly secure ECG steganography. In International Conference on Intelligent Computing and Applications (pp. 171-178). Springer, Singapore.

[40] Jero, S. E., Ramu, P., & Ramakrishnan, S. (2015). ECG steganography using curvelet transform. Biomedical Signal Processing and Control, 22, 161-169.
[41] Jero, S. E., & Ramu, P. (2016). Curvelets-based ECG steganography for data security. Electronics Letters, 52(4), 283-285.
[42] Ibaida, A., Khalil, I., & Al-Shammary, D. (2010, August). Embedding patients' confidential data in ECG signal for healthcare information systems. In 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology (pp. 3891-3894). IEEE.
[43] Mai, V., Khalil, I., & Ibaida, A. (2013, July). Steganography-based access control to medical data hidden in electrocardiogram. In 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (pp. 1302-1305). IEEE.
[44] Abuadbba, A., & Khalil, I. (2016). Walsh–Hadamard-based 3-D steganography for protecting sensitive information in point-of-care. IEEE Transactions on Biomedical Engineering, 64(9), 2186-2195.
[45] Wu, W., Liu, B., Zhang, W., & Chen, C. (2015, May). Reversible data hiding in ECG signals based on histogram shifting and thresholding. In 2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech) (pp. 1-5). IEEE.
[46] Vallathan, G., Devi, G. G., & Kannan, A. V. (2016, March). Enhanced data concealing technique to secure medical image in telemedicine applications. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 186-190). IEEE.
[47] Premarathne, U., Abuadbba, A., Alabdulatif, A., Khalil, I., Tari, Z., Zomaya, A., & Buyya, R. (2016). Hybrid cryptographic access control for cloud-based EHR systems. IEEE Cloud Computing, 3(4), 58-64.
[48] Banerjee, S., & Singh, G. K. (2021). A new approach of ECG steganography and prediction using deep learning. Biomedical Signal Processing and Control, 64, 102151.
[49] Pandey, A., Saini, B. S., Singh, B., & Sood, N. (2017). An integrated approach using chaotic map & sample value difference method for electrocardiogram steganography and OFDM based secured patient information transmission. Journal of medical systems, 41(12), 1-20.
[50] Shekhawat, A. S., Jain, A., & Patil, D. (2014). A study of ECG steganography for securing patient's confidential data based on wavelet transformation. Int. J. Comput. App, 105, 12-16.
[51] Duy, L. D., Minh, T. N. T., & Thanh, T. H. (2017, November). Adaptive steganography technique to secure patient confidential information using ECG signal. In 2017 4th NAFOSTED Conference on Information and Computer Science (pp. 336-340). IEEE.
[52] Neela, S., & Vijaykumar, V. R. (2015). ECG steganography and hash function-based privacy protection of patients medical information. Int. J. Trends Eng. Technol, 5(2), 236-241.
[53] Kumar, P. P., & Raj, E. B. (2016). An enhanced cryptography for ECG steganography to satisfy HIPAA privacy and security regulation for bio-medical datas. Biomedical and Pharmacology Journal, 9(3), 1087-1094.
[54] Yang, C. Y., & Wang, W. F. (2016). Effective electrocardiogram steganography based on coefficient alignment. Journal of medical systems, 40(3), 66.
[55] Yang, C. Y., & Wang, W. F. (2017, August). High-capacity ECG steganography with smart offset coefficients. In International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 129-136). Springer, Cham.
[56] Shiu, H. J., Lin, B. S., Huang, C. H., Chiang, P. Y., & Lei, C. L. (2017). Preserving privacy of online digital physiological signals using blind and reversible steganography. Computer methods and programs in biomedicine, 151, 159-170.
[57] Wang, H., Zhang, W., & Yu, N. (2016). Protecting patient confidential information based on ECG reversible data hiding. Multimedia Tools and Applications, 75(21), 13733-13747.
[58] Khandare, M., Ladhake, S. A., & Ghate, U. S. (2016). An approach of ECG steganography to secure the patient's confidential information. Int. Res. J. Eng. Technol.(IRJET), 3(03), 1867-1871.
[59] Augustyniak, P. (2012, September). Analysis of ECG bandwidth gap as a possible carrier for supplementary digital data. In 2012 Computing in Cardiology (pp. 73-76). IEEE.
[60] Mathivanan, P., & Ganesh, A. B. (2017, August). Colour image steganography using XOR multi-bit embedding process. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 1980-1988). IEEE.

[61] Yang, C. Y., & Wang, W. F. (2020). Progressive Data Hiding in Integer Wavelet Transform of Electrocardiogram by Using Simple Decision Rule and Coefficient Calibration. Revue d'Intelligence Artificielle, 34(1), 11-20.
[62] Bhatia, G. M. V. S (2015). ECG Steganography based Privacy Protection of Medical Data Utilizing Chaos Encryption. IJISET - International Journal of Innovative Science, Engineering & Technology, 2(11), 818-822.
[63] Davis, J., Pu, R. (2017). Empirical Mode Decomposition and Data Hiding In ECG Signal. International Research Journal of Engineering and Technology (IRJET), 4(7), 2464-2467.
[64] Yang, C. Y., Lai, C.-M., Lin, H.-C., Lin, T.-Y., & Lu, R.-L. (2020). Adaptive Electrocardiogram Steganography Based on 2D Approach with Predetermined Rules. Asian Journal of Computer and Information Systems, 8(1). https://doi.org/10.24203/ajcis.v8i1.6059
[65] Boostani, R., & Sabeti, M. (2018). Multi-Channel ECG-based Steganography. Biomedical Engineering: Applications, Basis and Communications, 30(06), 1850046.
[66] Cheng, L., Yang, C. (2018). 'High Performance Electrocardiogram Steganography Based on Fast Discrete Cosine Transform'. World Academy of Science, Engineering and Technology, Open Science Index 139, International Journal of Computer and Information Engineering, 12(7), 509 - 514.
[67] Yang, C. Y., Cheng, L. T., & Wang, W. F. (2020). An efficient reversible ECG steganography by adaptive LSB approach based on 1D FDCT domain. Multimedia Tools and Applications, 79(33), 24449-24462.
[68] Yang, C. Y., Wang, W. F., & Lai, C. M. (2020). Adaptive Data-hiding in Electrocardiogram Based on Integer Wavelet Transform Domain and Incremental Approach. In 2020 9th International Conference on Industrial Technology and Management (ICITM) (pp. 285-290). IEEE.
[69] Soni, N., Saini, I., & Singh, B. (2020). Integer Wavelet Transform-Based ECG Steganography for Hiding Patients' Confidential Information in e-Healthcare Systems. In Soft Computing: Theories and Applications (pp. 513-525). Springer, Singapore.
[70] Soni, N., Saini, I., & Singh, B. (2020). An integer wavelet transform and pixel value differencing based feature specific hybrid technique for 2D ECG steganography with high payload capacity. Multimedia Tools and Applications, 1-36.

Aleksandar Velinov
University of Goce Delchev,
Faculty of Computer Science, „Krste
Misirkov" 10-A,
Macedonia
aleksandar.velinov@ugd.edu.mk

Igor Stojanovic
University of Goce Delchev,
Faculty of Computer Science, „Krste
Misirkov" 10-A,
Macedonia
igor.stojanovik@ugd.edu.mk

Vesna Dimitrova
Ss. Cyril and Methodius University,
Faculty of Computer Science and
Engineering, „Ruger Boskovik" 16,
Macedonia
vesna.dimitrova@finki.ukim.mk