mathematics

MDPI

Article

Mathematically Based Assessment of the Accuracy of Protection of Cardiac Data Realized with the Help of Cryptography and Steganography

Galya Georgieva-Tsaneva [1,*], Galina Bogdanova [2] and Evgeniya Gospodinova [1]

[1] Institute of Robotics, Bulgarian Academy of Science, 1113 Sofia, Bulgaria; jenigospodinova@abv.bg
[2] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria; g.bogdanova@gmail.com
* Correspondence: galitsaneva@abv.bg

Abstract: This paper describes the application of cryptography and steganography in the protection of cardiac databases. The original cardiac data studied were transformed using a Daubechies wavelet transform. The next step is to conduct Energy Packing Efficiency-based compression. A watermark is added to the received data to protect against unauthorized access, before hybrid cryptography is performed using a suitably selected encryption algorithm. The presented and analyzed algorithm includes protection using public and symmetric key cryptography. The proposed software algorithm is performed on real electrocardiographic, photoplethysmographic, and Holter cardio data. We have evaluated the effectiveness of the applied approach and concluded that a sufficient level of protection of the studied data has been achieved, with methods of authentication and accuracy applied to the users.

Keywords: cryptography; watermarking; cardio data; wavelet analysis; Daubechies basis

Citation: Georgieva-Tsaneva, G.; Bogdanova, G.; Gospodinova, E. Mathematically Based Assessment of the Accuracy of Protection of Cardiac Data Realized with the Help of Cryptography and Steganography. *Mathematics* **2022**, *10*, 390. https://doi.org/10.3390/math10030390

Academic Editor: Angel Martín-del-Rey

Received: 25 December 2021
Accepted: 23 January 2022
Published: 27 January 2022

1. Introduction

Ensuring the protection and security of several real signals used in people's daily lives from malicious interference, unauthorized access, forgery, and severe attacks is possible today thanks to the creation of mathematically based software solutions. Cryptography [1] is a basic mathematical method for providing confidentiality (directly related to the protection of individuals' personal data) and the authentication of data and objects, as well as non-repudiation. Today, telemedicine, based on the latest advances in information and communication technologies, offers the opportunity for the remote continuous monitoring of patients, during which they perform their daily activities. Healthcare services are increasingly being used to ensure that health care is provided to each individual according to his or her needs, anytime, anywhere in the world. This enables each person to be part of their usual social community, while at the same time providing them with appropriate medical supervision and, if necessary, contact with their healthcare provider. Such an approach enables doctors to care for a larger number of patients while consuming fewer resources and providing appropriate health care at the right time. The security of data must be ensured when transmitting recorded medical information and personal data. The use of encryption technology is one of the most effective ways to maintain the security of biomedical signals. For this reason, issues related to authentication and confidentiality are at stake in telemedicine, ensuring that only authorized users should have access to patients' medical and personal data. At the same time, the quality of the original signals must be preserved to the extent necessary so as not to impair the data's diagnostic properties. In the implementation of information systems in health care, it is necessary to ensure reliability, safety, and security.

Questions about the use of encryption remain on the agenda. In December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy identified encryption as a key method of protecting individual rights and ensuring the security of individuals [2].

The application of cryptographic algorithms regardless of the specific method of implementation (public key, secret key, or hybrid algorithms) is very important for the security of transmitted information. The use of key exchange protocols, digital signatures, and watermark embedding are effective tools for the protection of data, signals, and images.

The choice of the most appropriate encryption algorithm has an essential role in the process of designing the scheme of protection of transmitted information. The choice of the key used is extremely important, as in practice almost every key can be broken (including from a brute-force attack) by using a rough attack [3] if high computing power is used and enough time is allocated to search for the key.

1.1. Background

The choice of certain encryption algorithms is determined by their application and the goals that are set. When implementing protection through an encryption procedure with a public asymmetric key, the mathematical method of the Rivest-Shamir-Adleman algorithm (RSA) is very often used [4]. This method remains highly valued to this day and is often used to ensure the encryption and integrity of the transmitted information, and verification of the originality of the data. Implementation of RSA keys to prevent cryptographic attacks when using smart cards on multiple devices is discussed in [5]. In [6], Michael Wiener analyzes a cryptanalytic attack on the use of short RSA secret exponents. The presented algorithm is based on continuous fractions and seeks to find sufficiently short secret exponents in polynomial time. When the secret degree increases in size beyond a certain maximum, the time required to find the secret exponent increases rapidly (exponentially). The decomposition of prime numbers has been the subject of much research looking for fast and simple techniques [7,8], including the creation of polynomials generating sums of squares with a targeted application in cryptography [9,10]. The authors of [11] propose a new method for realizing a semisimple factorization based on the properties of Pythagorean triplets, proposing a new mathematical model based on the binary approach for the greatest common divisor with simple arithmetic operations to find the sum of two squares of one or both prime factors.

Another commonly used mathematical method for the encryption process is elliptic curve cryptography, an approach to provide public key encryption that is based on the algebraic structure of elliptic curves on finite fields [12]. Security encryption systems based on public key cryptography, such as RSA systems, use semiprime factorization [11], an important numerical method. Elliptic curve cryptography uses smaller-length keys to implement the same level of security as the RSA algorithm [13].

The authors of [14] present a new cryptographic algorithm with a public key, using a matrix model to improve the efficiency and speed of encryption. The authors include several unknown quantities and one additional sub-equation during the encrypting process. The execution time of the algorithm proposed by the authors was found to be faster when compared with the RSA and elliptic curve cryptography algorithms.

The use of cryptography in biomedical applications is a popular and well-functioning method for ensuring the confidentiality of medical research and the personal data of individuals. A symmetric encryption algorithm [15] based on the double chaotic layer encryption method was proposed and tested on electroencephalograms. This algorithm's intended usage is electroencephalograms, electrocardiograms, and blood pressure data and it is oriented for telemedical applications. The data used in the research were taken from the public database of PhysioBank [16].

The authors of [17] propose the use of the RSA algorithm in medical imaging, using watermark and Discrete Wavelet Transform of Daubechies with two coefficients (Db2) and two levels of decomposition. The proposed watermark procedure (the watermark is

encrypted with a key generated by the RSA algorithm) was tested on three types of images (MRI, CT, and US). The proposed scheme shows a good degree of protection against alleged attacks before transmitting medical images through communication channels.

In [18], the authors explore the issue of maintaining the integrity and confidentiality of patient's medical information when transmitted wirelessly, via Wireless Body Area Networks (BANs).

A 128-bit secret key generation using an electrocardiographic (ECG) signal to protect communications via wireless BANs is proposed by the authors of [19]. The paper presents a scheme for creating the secret key, which uses the parameters of the patient's ECG signal. The obtained results show the effectiveness of this solution for generating a unique key and a key agreement for the protection of transmitted information.

1.2. The Purpose of This Article

The purpose of this article is to present a method for the application of cryptography to protect three types of cardio data: ECG, photoplethysmographic signal (PPG), and Holter. The encryption procedure is performed after compression of the studied data and performing a wavelet transform (WT) on the resulting sequence. The proposed encryption procedure aims to offer good protection of the three types of cardio signals when creating an archive of the used ECG, PPG, and Holter records, obtained in the study of cardio records from patients with various cardiovascular diseases and a healthy control group. The created algorithm is implemented in software in a Microsoft Visual C++ programming environment as a standard software application. Mathematical analyses of the conducted researches have been made and evaluation characteristics have been determined.

This study analyzes the effectiveness of the individual steps in implementing the applied cardio data protection procedure (using parameters to evaluate the effectiveness of the algorithms used in the procedure) and to compare the values of the parameters of the output signal with those of the input signal for all three types of cardio data.

Another research task of the article is to make an analysis of the influence of the length of the watermark, the choice of specific wavelet basis (Haar, Db4, Db8, Db12, and Db16 wavelet basis were studied), and the choice of method for processing threshold coefficients on the estimating parameters of the output-transformed cardio signal. The results of the research are presented parametrically and graphically.

The rest of this paper is organized as follows. Section 2 presents the technology used in this study and the proposed method for protecting cardiac data from possible attacks and attempts at unauthorized access. Section 3 shows the results obtained by applying the described method on three types of cardio data and presents the comparative analyses. Finally, Sections 4 and 5 provide the final remarks in the form of discussion and conclusions, respectively.

2. Materials and Methods

Cryptography is a mathematically based technology that implements cryptographic algorithms, codes, and protocols to ensure the protection of information, data, messages, communications, and methods and tools for their implementation. Cryptographic software is an algorithm for encrypting, namely, converting original data and information into incomprehensible strings of characters (transmitted through communication channels) so that this form cannot be used by persons without authorized access [20]. The second stage (decryption) consists of the correct inverse transformation (through the application of mathematical functions and security parameters) of the encrypted data. On the other hand, cryptanalysis aims to compromise the security that is achieved through cryptography.

Another aspect of cryptography is the authentication [21] of the transmitted message to the two parties involved, the process-sender and recipient. This ensures the integrity of the transmitted message and its rejection/non-rejection.

Some of the parameters used in encryption, called keys, do not change over time. The cryptographic code used can be likened to a dictionary of correspondence of the entered meaning of the words used and can result in unreadable, or without logic or

meaning expressions, data, and signs. Cryptographic protocols used in practice are rules and agreements of action for the practical implementation of cryptographic algorithms and codes. A practical cryptosystem consists of a cryptographic algorithm or code and a cryptographic protocol. Cryptographic methods and tools are sets of cryptographic mechanisms, the key elements of which are cryptographic algorithms [22], specifically responsible for the implementation of the necessary security and protection of information.

2.1. Cardio Data Protection Methods

Modern means of data protection are becoming more and more common due to the daily need to transmit medical records (ECG, PPG, blood pressure, etc.) through communication channels and ensure their integrity and resistance to various types of attacks. The advantage of protecting cardio signals is that they are relatively less susceptible to fraud due to their unique nature. On the other hand, ECG and PPG sensors generate a constantly large number of reports that need to be processed in real time.

Electrocardiography and photoplethysmography are modern non-challenging tools for studying the health status of subjects, providing information about the state of the cardiovascular system, the activity of the autonomic nervous system, and others. This paper presents the results attached to three types of cardio data: PPG (Figure 1), ECG (Figure 2), and Holter records. The waveform of the cardio signal recorded by a Holter device is identical to that of the ECG signals recorded with an electrocardiograph; the difference is that the Holter device is designed to record continuous ECG data (24 h, 72 h, and more) All data on which the tests are applied are obtained cardio records, which is especially important for the reality of the results. Preliminary processing was applied to the three types of study data, which includes the reduction of interference [23], detection of the maximum deviations in the signals (QRS complexes are Q, R, S-characteristic points in the ECG signal, with a maximum deviation of the amplitude at the R point [24]), and localization of the P peak at the PPG signal.

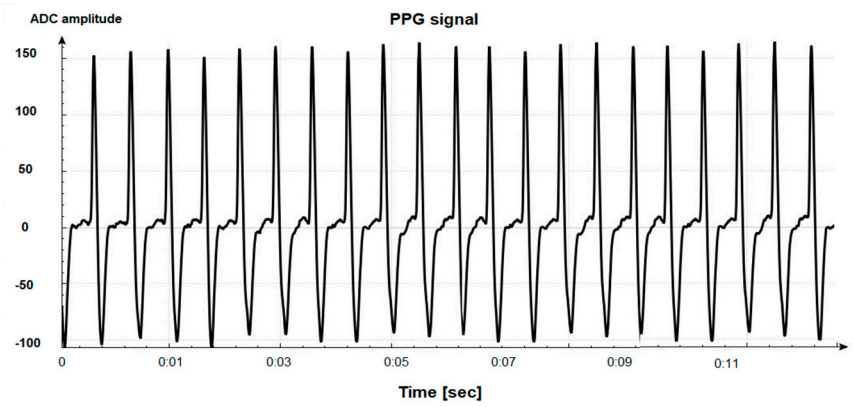

Figure 1. Graph of a real PPG signal.

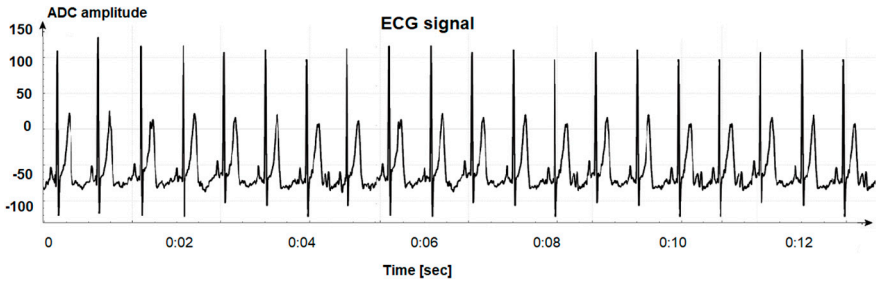

Figure 2. Graph of a real ECG signal.

2.2. Cardio Data Protection Procedure

The cardio data protection mathematically based method proposed and researched in this paper (Figure 3) consists of the following steps:

- Applying the Discrete Wavelet Transform with Daubechies basis with four coefficients to the studied cardio data;
- Application of optimized Energy Packing Efficiency-based compression of the obtained sequence;
- Watermark embedding in the reduced WT coefficients;
- Encryption procedure using a hybrid cryptography algorithm;
- Applying the Inverse Discrete Wavelet Transform of the obtained sequence;
- Determination of the studied parameters for evaluation of the used algorithms.

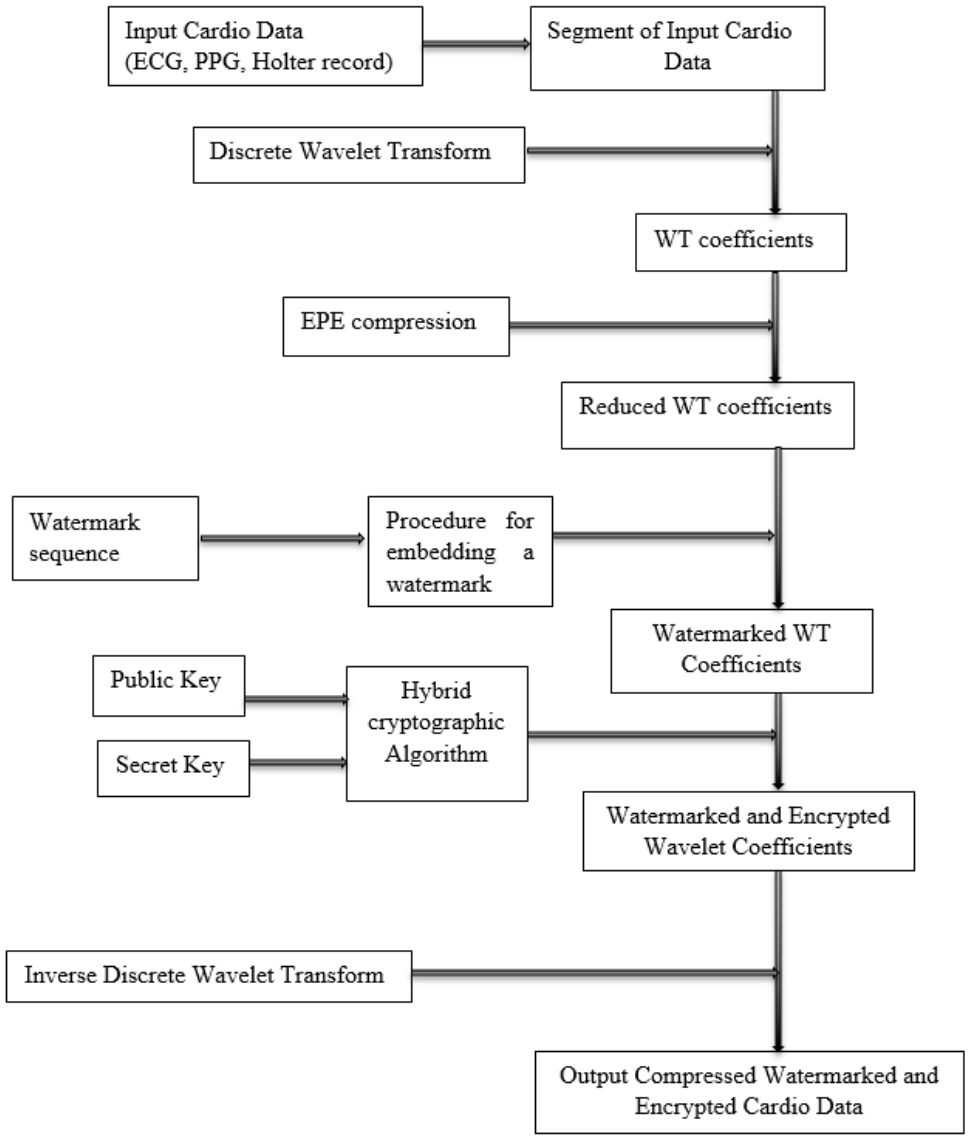

Figure 3. Block diagram of the presented method.

2.2.1. Discrete Wavelet Transform

Discrete Wavelet Transform, based on the concept of Multi-Resolution Analysis, can be applied to each signal examined. The studied input (ECG, PPG, Holter) signal can be represented by a wavelet function $\varphi_{i,\,j}$ and scaling function $\psi_{i,n}$ [25]:

$$\varphi_{i,j}(t) = 2^{-i/2}\varphi_0\left(2^{-i}t - j\right),\ j \in Z; \tag{1}$$

$$\psi_{i,j}(t) = 2^{-i/2}\psi_0\left(2^{-i}t - j\right),\ j \in Z. \tag{2}$$

In the implementation of the wavelet transform, the digital signal $x(t) \in L^2(R)$ is represented as the sum of orthogonal scaling functions and wavelets collection of details and a low-resolution approximation [26]:

$$\begin{array}{c} x(t) = approx_N(t) + \sum_{i=1}^{N} detail_i(t) = \\ \sum\limits_j a_x(N,j)\varphi_{N,j}(t) + \sum_{i=1}^{N}\sum\limits_j d_x(N,j)\varphi_{N,j}(t). \end{array} \tag{3}$$

In this paper, Daubechies wavelet transform is implemented. Wavelet transforms are suitable for studying the properties of cardio signals (which are non-stationary and dynamic in nature) because in their application they provide information about the signal in both the frequency and time domains. The classical Fourier transform provides good information about the frequency distribution of the signal but does not provide information about the exact moment at which a frequency component appears. The Daubechies discrete WT used in this study has a compactly maintained orthonormal basis. A Daubechies transform with four wavelet coefficients (Db4) and four levels of decomposition is chosen.

2.2.2. Compression

The next step in the cardio data encryption procedure involves the application of optimized compression based on the Energy Packing Efficiency (EPE) method [27]. The chosen method of compression requires preliminary data processing (normalization of the studied sequence is carried out): first by amplitude and then by period. After this input processing, the EPE-based threshold processing itself takes place. At each subsequent level i of the wave decomposition of the data, the corresponding signal energy is calculated, using the current values of the detailed coefficients $D(i, j)$, total K for the respective level:

$$E_{Di} = \sum_{j=1}^{K}(D(i,j))^2. \tag{4}$$

Compression based on the Energy Packaging Efficiency processing method reduces any excess information in the signal (but it does not remove the diagnostic properties of the signal) when processing the signal threshold, setting a zero value of insignificant wavelet coefficients (their presence in the studied sequence does not significantly affect the significance of the signal).

2.2.3. Digital Watermarking

The incorporation of a watermark in cardiac signals and data, as well as in the header of the compact record in which personal information about a particular patient is transmitted, is used to protect the continuity of personal data and the medical research of individuals. Cardio signals must be stored and transmitted with sufficient accuracy to ensure that their most important property, namely their ability to carry diagnostic information, is preserved. To this end, it is important to preserve them without changing the form of the basic waveforms of the cardio signals, which must not be influenced by the embedded watermark. Digital encryption of watermarks by quantizing cardiac data was used in this work.

Embedding

In this work, the watermark is embedded in cardiac data after a Db4 wavelet transform with four levels of decomposition. The watermark (sequence Mr) was embedded in the lowest frequency, to ensure its resilience to attacks. The sequence Mr with cardio data information $\{cd_i\}$ is added to coefficient c_i whereby the transformed coefficient c_i' is obtained at the lowest fourth decomposition level by the formula [28]:

$$c_i' = \begin{cases} \left\lfloor \frac{c_i}{Mr} \right\rfloor \cdot Mr + \frac{3}{4}Mr, \ if \ cd_i = 1; \\ \left\lfloor \frac{c_i}{Mr} \right\rfloor \cdot Mr + \frac{1}{4}Mr, \ if \ cd_i = 0. \end{cases} \quad (5)$$

Extraction

Extraction is implemented through this rule, where c_i^* is the WT coefficient of the lowest-frequency sub-band and cd_i^* is the embedded watermark sequence [28]:

$$cd_i' = \begin{cases} 1, \ if \ c_i^* - \left\lfloor \frac{c_i^*}{Mr} \right\rfloor \cdot Mr \geq \frac{1}{2}Mr; \\ 0, \ if \ c_i^* - \left\lfloor \frac{c_i^*}{Mr} \right\rfloor \cdot Mr < \frac{1}{2}Mr. \end{cases} \quad (6)$$

This presented embedding/extraction method is stable and resistant to compression, filtration, and geometric transformations.

Encryption

In this work for the encryption of cardio records (ECG, Holter, PPG), the cryptographic hybrid algorithm is applied and analyzed. The presented hybrid crypto algorithm used two keys: a public key and a private key. The algorithm uses the RSA algorithm to encrypt the public key, with most of the work on encrypting/decrypting cardio records performed through a more efficient AES algorithm using a symmetric key.

RSA was one of the first public-key cryptosystems, being first published in 1977. Created as a revolutionary technology for encryption and decryption, RSA is able to provide sufficient security for data and today's information systems. RSA technology is based on an encryption procedure using a public key; authentication of the sender with a digital signature. The technology is difficult to break because it is based on decomposing numbers that have a very high total number of digits (for example, 200 or more) into prime factors. The technology provides a method for generating through simple calculations of two prime numbers and also generates through calculations and two keys needed for the process of transmitting information. Bit multiplication and modular multiplication are the simple arithmetic operations on which the algorithm is based. The data is initially divided into segments in order to implement the process of their encryption.

Applied algorithm implementation steps for key generation:

- Software generation of two large prime numbers (d and z, so $d \neq z$);
- The remainder of the product of the public key and private key determination ($p = d * z$);
- Euler's totient function determination according to the formula:

$$\varphi(p) = (d-1) * (z-1); \quad (7)$$

- Software integer (k) generation, with the integer within the range $(1, \ \varphi(p))$, where k and $\varphi(p)$ are relatively prime;
- For decryption purposes, the number q is calculated, so $q = k^{-1} mod \ \varphi(p)$;
- The public key (k, p) used in encryption algorithm determination;
- The private key (q) formation.

Advantage of RSA algorithm: The issue of key sharing as an asymmetric key pair (public and private key) is easy to solve.

Disadvantages of RSA algorithm: The implementation of the algorithm requires a lot of buffer memory, so it is not suitable for encrypting medical data such as ECG, PPG, or

Holter cardio records, as they generate a large number of values per unit of time. It is slow and insufficiently resistant to attacks.

The AES algorithm (the Rijndael algorithm) is a symmetric encryption algorithm having the same encryption/decryption keys with a length of 128, 192, or 256 bits according to AES technology.

The AES algorithm has four stages:

1. Key Expansions—during this first step in the algorithm, the creation of round keys from the cipher key are performed;
2. Initial Round during which the process of adding the round keys are made—each byte of the state is bitwise XOR-ed using this received round key;
3. Rounds includes the following steps:
   - The non-linear substitution procedure (each byte is replaced by another according to a rule set in tabular form);
   - Transposition (of the last three rows) of the state is performed cyclically, according to a certain number of steps;
   - The mixing operation procedure is performed by multiplying (each state column with a polynomial expression);
   - In this step, the added round key is the initial round key.
4. Final Round: Sub-Bytes, Shift-Rows, and finally the implementation of Round-Key.

Advantages of AES: Fast and suitable for encrypting large data, such as medical cardio signals. It can easily maintain a large key size and is less open to attack.

Disadvantages of AES: The implementation of key exchange can be a problem, as the same key is used for encryption/decryption, while there is no good resistance to interpolation attacks.

In the implementation of the presented procedure, we used 12 rounds for a 192-bit key.

3. Results

3.1. The Cardio Database Used for the Study

The encryption algorithm was applied based on real cardio data ECG and FIG signals, obtained using a specially designed PPG device by the authors, allowing for the simultaneous recording of two PPG signals and one ECG signal. In parallel, a Holter recording was made, using a Holter monitoring device placed on the studied individual. Holter can continuously record cardiac data for up to 72 h. This study involved the three types of cardio recordings performed simultaneously with a duration of 2 h, with the same sampling rate. A parallel recording of 24 separate triples of signals (ECG, PPG, Holter) was made, and each received triplet of signals was analyzed to match its main parameters relevant to the diagnostic process (detection of maximum amplitude deviations, formation of time series constituting the intervals of successive heartbeats, etc.).

3.2. Evaluation of Presented Algorithms

An assessment of the presented data protection procedure was made in the paper. The evaluation of the algorithms involved in the procedure was made by calculating appropriate parameters for the evaluation of cardio data:

1. The Euclidean error-distance parameter (Percentage Residual Difference) accurately estimates the distortion in the decrypted data relative to the initial cardio input data [29]:

$$\mathrm{PRD} = \sqrt{\frac{\sum_{i=1}^{L}(x_{ori}(i) - x_{tr}(i))^2}{\sum_{i=1}^{L}(x_{ori}(i))^2}} \cdot 100[\%], \tag{8}$$

   where:

   x_{ori} is the original initial cardio signal,
   x_{tr} is the converted cardio signal,
   L is the length of the investigated signal.

2. The parameter Signal to Noise Ratio (SNR) is:

$$\mathrm{SNR} = 10 \cdot log_{10} \frac{\sum_{i=1}^{L} (x_{ori}(i) - x_{tr}(i))^2}{\sum_{i=1}^{L} (x_{ori}(i))^2}. \quad (9)$$

3. The parameter Peak Signal to Noise Ratio (PSNR) is the ratio of the maximum value of the converted cardio signal to the mean squared deviation of the original, initial cardio signal (where max is the maximum value from the original ECG signal) [30]:

$$\mathrm{PSNR} = 10 \cdot log_{10} \frac{max^2}{\frac{1}{L} \sum_{i=1}^{L} (x_{ori}(i) - x_{tr}(i))^2}. \quad (10)$$

4. The parameter Mean Square Error (MSE) is used to quantify the reconstruction error [31]:

$$\mathrm{MSE} = \frac{1}{L} \sum_{i=1}^{L} .(x_{ori}(i) - x_{tr}(i))^2 \quad (11)$$

5. The parameter Root Mean Square Error (RMSE) [32] is:

$$\mathrm{RMSE} = \sqrt{\frac{1}{L} \sum_{i=1}^{L} (x_{or}(i) - x_{tr}(i))^2}. \quad (12)$$

6. The parameter Mean Absolute Percentage Error (MAPE) [32] is:

$$\mathrm{MAPE} = \frac{1}{L} \sum_{i=1}^{L} \left(\frac{|x_{or}(i) - x_{tr}(i)|}{x_{or}} \right) \cdot 100\%. \quad (13)$$

7. The parameter Bit Error Rate (BER) [33] is:

$$\mathrm{BER} = \frac{\sum_i x_{or} \oplus x_{tr}}{L}. \quad (14)$$

8. The parameter evaluating the relative entropy Kullback–Leibler divergence (KLD) [34] is:

$$\mathrm{KLD}(p_{or}, p_{tr}) = \int p_{or}(x) log \frac{p_{tr}(x)}{p_{or}(x)} dx.$$

3.3. Evaluation of Compressed Algorithm

The Energy Packing Efficiency-based compressed algorithm used in this paper was assessed by the Euclidean error-distance parameter and compression ratio, determined by the formula [29]:

$$\mathrm{CR} = \frac{NS_{in}}{NS_{out}}. \quad (15)$$

where:

NS_{in} is the length of the initial cardio signal,
NS_{out} is the length of the output cardio signal.

Estimates were made using the parameters of PRD and compression ratio on the three types of examined cardio signals. The tables below (Tables 1–3) show the obtained parameters for the EPE-based method of reduction of the WT coefficients for the studied ECG, Holter, and PPG signals.

Table 1. CR and PRD values for ECG records (N = 24).

Parameters						**Value**
Approximating Coefficients with EPE 99%						**99%**
Detailed coefficients		99%	95%	90%	80%	75%
Block length	CR [mean ± std]	3.92 ± 0.84	3.98 ± 0.81	4.14 ± 0.91	4.49 ± 0.93	4.73 ± 0.97
1024 samples	PRD (%)	1.26 ± 0.12	1.88 ± 0.13	2.32 ± 0.15	2.47 ± 0.16	2.51 ± 0.18
Block length	CR [mean ± std]	3.94 ± 0.86	4.08 ± 0.81	4.17 ± 0.93	4.53 ± 0.94	4.81 ± 0.99
2048 samples	PRD (%)	1.32 ± 0.13	1.98 ± 0.14	2.44 ± 0.17	2.49 ± 0.16	2.58 ± 0.19
Block length	CR [mean ± std]	3.98 ± 0.11	4.14 ± 0.13	4.19 ± 0.9	4.38 ± 0.91	4.83 ± 0.98
4096 samples	PRD (%)	1.34 ± 0.12	1.98 ± 0.17	2.48 ± 0.19	2.57 ± 0.18	2.62 ± 0.17

Table 2. CR and PRD values for Holter records (N = 24).

Parameters						**Value**
Approximating Coefficients with EPE 99%						**99%**
Detailed coefficients		99%	95%	90%	80%	75%
Block length	CR [mean ± std]	4.06 ± 0.71	4.23 ± 0.8	4.29 ± 0.82	4.81 ± 0.79	4.98 ± 0.85
1024 samples	PRD (%)	1.18 ± 0.11	2.02 ± 0.13	2.28 ± 0.09	2.37 ± 0.41	2.48 ± 0.32
Block length	CR [mean ± std]	4.14 ± 0.69	4.28 ± 0.7	4.37 ± 0.83	4.84 ± 0.81	5.04 ± 0.88
2048 samples	PRD (%)	1.22 ± 0.14	1.85 ± 0.11	2.32 ± 0.13	2.4 ± 0.39	2.54 ± 0.36
Block length	CR [mean ± std]	4.17 ± 0.13	4.31 ± 0.22	4.42 ± 0.12	4.89 ± 0.14	5.07 ± 0.17
4096 samples	PRD (%)	1.23 ± 0.12	2.03 ± 0.17	2.35 ± 0.14	2.59 ± 0.28	2.68 ± 0.39

Table 3. CR and PRD values for PPG records (N = 24).

Parameters						**Value**
Approximating Coefficients with EPE 99%						**99%**
Detailed coefficients		99%	95%	90%	80%	75%
Block length	CR [mean ± std]	3.87 ± 0.98	3.98 ± 0.88	4.06 ± 0.63	4.36 ± 0.58	4.54 ± 0.8
1024 samples	PRD (%)	1.24 ± 0.09	1.78 ± 0.11	2.25 ± 0.12	2.51 ± 0.16	2.64 ± 0.17
Block length	CR [mean ± std]	3.92 ± 0.97	4.06 ± 0.77	4.11 ± 0.67	4.44 ± 0.78	4.58 ± 0.83
2048 samples	PRD (%)	1.31 ± 0.11	1.88 ± 0.13	2.27 ± 0.14	2.6 ± 0.17	2.71 ± 0.21
Block length	CR [mean ± std]	3.96 ± 1.03	4.06 ± 0.99	4.14 ± 0.65	4.55 ± 0.69	4.61 ± 0.91
4096 samples	PRD (%)	1.33 ± 0.16	1.78 ± 0.25	2.29 ± 0.13	2.63 ± 0.18	2.77 ± 0.19

The results are shown for the tests performed on the three types of signals (ECG, Table 1; Holter, Table 2; PPG, Table 3). The compression ratio, according to the studies conducted based on 24 triples, simultaneously recorded different ECG, Holter, and PPG signals, ranging from 3.87 (for PPG) to 5.07 (for Holter). Increasing the degree of data compression resulted in an increase in the PRD parameter, which indicates that there are changes in the data compared to the original input data. The advantage of cardio signals is that they are recorded with many reports per unit time and contain a lot of redundant information that can be compressed without a significant loss of information. On the other hand, it is extremely important to preserve the shapes and amplitudes of the main waves in the signal that carry diagnostic information. An appropriate ratio between PRD and CR can be selected for each specific application, with the main goal being to preserve the diagnostic properties of the compressed cardio signal. Studies on the size of the block, into which the time cardio series is divided in order to perform compression, show an increase in the compression ratio with increasing block length. The parameter prd, measuring the quality of the received signal and its similarity to the original signal, also reduces some of the increase, which is not essential. The EPE-based algorithm has the ability to control the compression ratio according to the needs of different cardiac applications. The results presented below were obtained by establishing EPE values equal to 0.99% for all levels of decomposition. The EPE-based algorithm has the ability to control the compression ratio

according to the needs of different cardiac applications. The results presented below were obtained by establishing EPE values equal to 0.99% for all levels of decomposition.

3.4. Evaluation of Watermarked Algorithm

The evaluation of the procedure for embedding the watermark is performed on the obtained cardio data sequence from the previously performed steps: compression and watermarked WT cardio coefficients. The evaluation parameters are PRD and PSNR. The obtained values of these parameters for PPG signals are shown in Table 4. At higher values of the PSNR indicator, the transformations performed on the studied signals have a higher quality.

Table 4. Values of PRD and PSNR for PPG signals.

Cardio Record №	PRD [%]	PSNR [dB]
1	0.2014	53.11
2	0.1911	52.03
3	0.1805	46.38
4	0.2502	48.44
5	0.1611	51.08
6	0.1173	44.37
7	0.1239	48.55
8	0.1386	44.07
9	0.1604	49.75
10	0.2091	54.98
11	0.1035	44.09
12	0.1357	52.47

3.5. Evaluation of Encryption Algorithm

The evaluation of the encryption procedure is based on the transformation of PPG signals, with the calculated values shown in Table 5. The table shows the determined values of PRD and SNR for 12 PPG signals before encryption and after decryption. The calculated values can be used to estimate the magnitude of the differences between the values of the studied signals. The studied parameters show that there are no large differences between the original and the decrypted signals, and therefore the considered procedures are suitable for application in cardiac information, as they retain their diagnostic capabilities. The Signal to Ratio varies from 31.83 to 46.37, which are good parameter values showing a sufficient degree of preservation of the quality of the converted signal.

Table 5. Values of PRD and SNR for PPG signals.

Cardio Record №	PRD [%]	SNR [dB]
1	0.0372	34.89
2	0.1497	46.37
3	0.1023	31.83
4	0.1132	36.06
5	0.0656	32.88
6	0.0944	32.14
7	0.1633	38.56
8	0.1948	32.58
9	0.1408	36.37
10	0.1012	41.07
11	0.1167	41.28
12	0.0683	32.64

3.6. Evaluation of Proposed Cardio Data Protection Procedure

An evaluation of the proposed procedure for encryption of cardio signals in the implementation of different lengths of the built-in watermark has been made (Table 6). The results were obtained by applying the procedure on the PPG data.

Table 6. Evaluation parameters for different watermark lengths.

Watermark Length	32	64	128	256	512
PSNR [db]	45.33	44.44	43.62	42.33	41.51
MSE	0.043	0.047	0.051	0.058	0.063
PRD [%]	5.14	5.86	6.31	6.87	6.99
RMSE	0.2074	0.2168	0.2258	0.2408	0.251
MAPE [%]	0.0041 ± 0.001	0.0046 ± 0.002	0.013 ± 0.002	0.11 ± 0.003	0.21 ± 0.007
BER	0.005	0.08	0.11	0.18	0.22
KLD	0.002	0.006	0.014	0.06	0.08

The parameters in Table 7 were obtained from evaluating 24 PPG signals (each signal represented 2 h of recording). The results in Table 7 show a high degree of compression when using the Haar transformation, but worsened values for the other estimation parameters. The application of the Db4 transformation in the implementation of the presented method proved to be the most optimal in terms of the obtained values of the studied parameters (almost the same results are obtained with Db8). The application of Daubechies wavelet transform with more coefficients than eight leads to a deterioration of the studied parameters.

Table 7. Estimation parameters for different wavelet basis.

Wavelet Basis	Db2 (Haar)	Db4	Db8	Db12	Db16
PSNR [db]	14.81 ± 1.19	52.03 ± 0.81	51.16 ± 0.47	45.32 ± 0.31	44.65 ± 0.88
MSE	0.91 ± 0.08	0.022 ± 0.001	0.024 ± 0.002	0.043 ± 0.02	0.046 ± 0.001
PRD [%]	16.88 ± 3.74	5.91 ± 0.99	6.12 ± 1.02	6.82 ± 1.11	6.94 ± 1.03
RMSE	0.956 ± 0.11	0.1483 ± 0.03	0.1549 ± 0.04	0.2047 ± 0.07	0.2145 ± 0.07
MAPE [%]	0.33 ± 0.04	0.0047 ± 0.0008	0.0051 ± 0.001	0.0054 ± 0.01	0.062 ± 0.03
BER	0.41 ± 0.1	0.011 ± 0.03	0.014 ± 0.08	0.017 ± 0.09	0.024 ± 0.01
KLD	0.36 ± 0.01	0.006 ± 0.01	0.014 ± 0.002	0.011 ± 0.02	0.06 ± 0.003
CR	6.68 ± 0.84	4.18 ± 0.53	4.16 ± 0.72	3.99 ± 0.32	3.81 ± 0.41

The dependence of MSE on the selected algorithm of threshold processing of the coefficients in the compression step of the proposed method was studied. The initial ECG data examined are shown in Figure 4, while Figure 5 shows a graph of the reconstructed data.

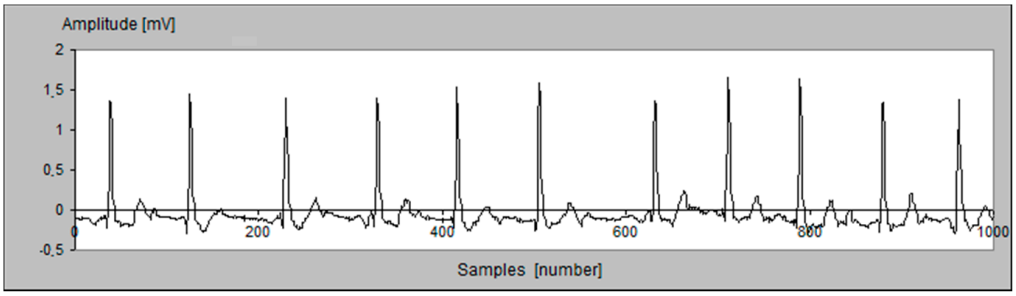

Figure 4. Graph of original ECG signal.

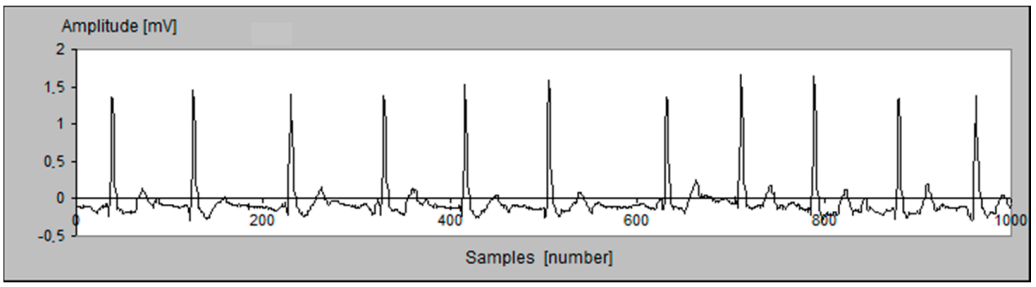

Figure 5. Graph of received (transformed) ECG signal.

Figures 6 and 7 present the MSE obtained from the reconstruction of the ECG signal data (shown in Figure 4). The calculations were performed on the basis of the initial input ECG signal and the received output ECG signal. The research aims to demonstrate both the values of the obtained MSE between the input and output signal and the differences in the MSE (graphically represented) using the amplitude method of reduction of the coefficients (Figure 6) and the EPE method (Figure 7). The comparison between the two graphs shows significantly lower MSE values when using the EPE method.

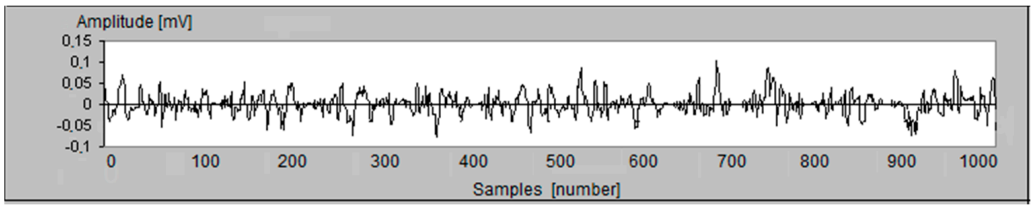

Figure 6. MSE in data reconstruction (amplitude compression method, Db4 wavelet basis, 32 bits watermark length).

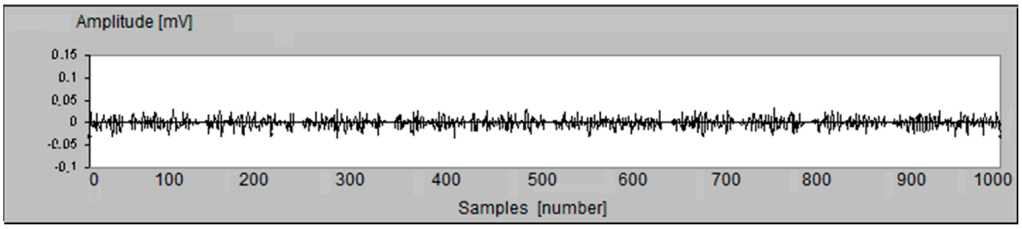

Figure 7. MSE in data reconstruction (EPE-based compression method, Db4 wavelet basis, 32 bits watermark length).

It is worth discussing the analysis of the PRD parameter for different methods of threshold processing. Figure 8 shows a graph of the dependence of the PRD parameter (determined in the output-transformed signal) and the compression ratio when using the amplitude method of threshold processing. The graphs show a significant increase in PRD at compression ratios greater than 5, leading to distortions in the values of the reconstructed cardio data (PPG, ECG, and Holter). In threshold processing using the EPE-based method, the PRD values were significantly lower (Figure 9), which is an indication of a better identity of the reconstructed data compared to the input. This allows for the realization of high degrees of compression in the implementation of the cardio data protection procedure, with the achievement of good identity between the submitted and received cardio data.

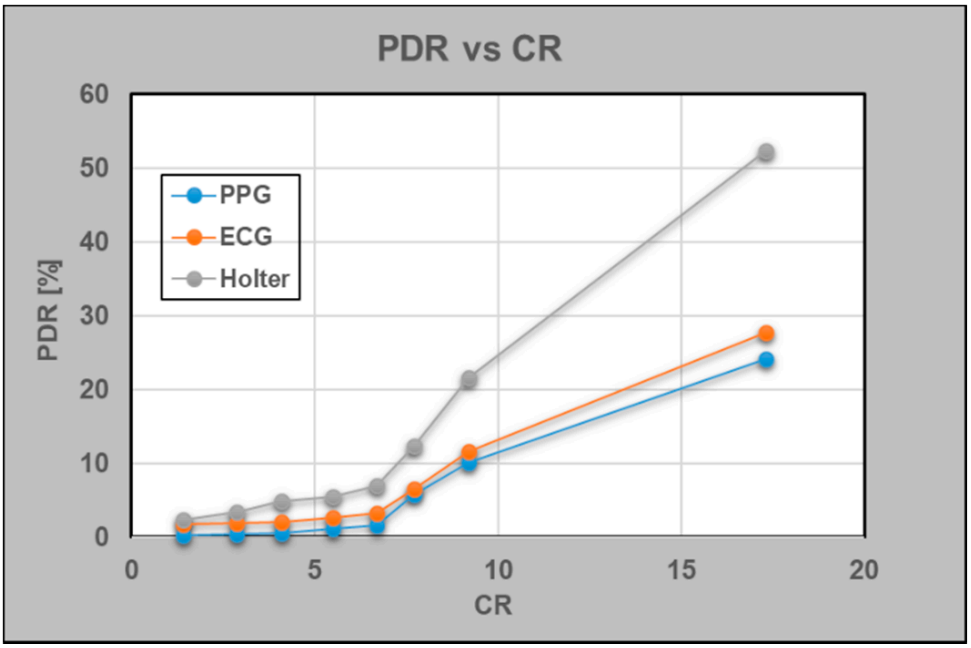

Figure 8. Dependence of PRD on the compression ratio for different types of cardio data (amplitude method of threshold processing).

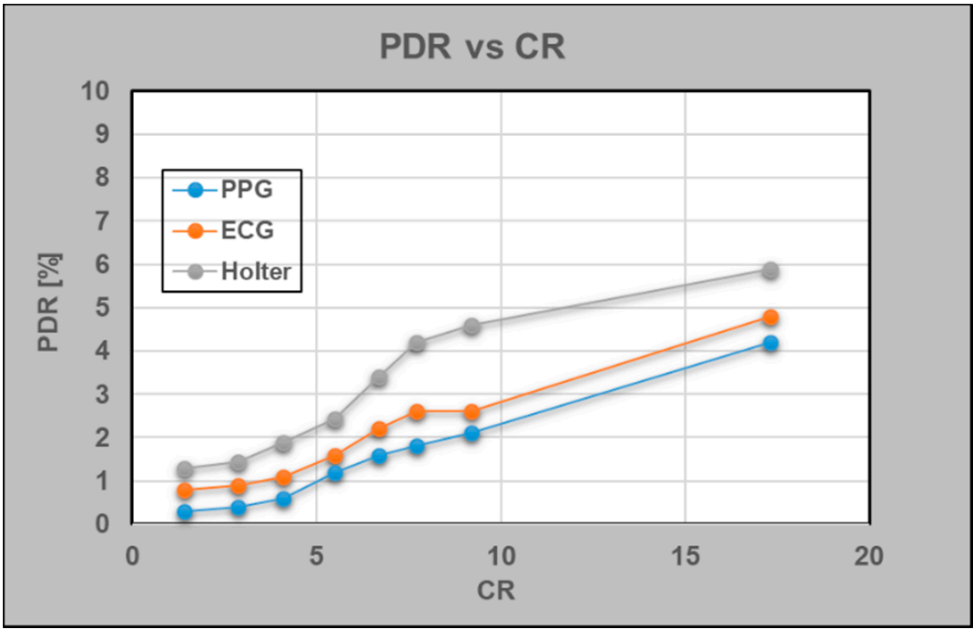

Figure 9. Dependence of PRD on the compression ratio for different types of cardio data (EPE-based threshold processing method).

Implementations of the cardio data protection procedure with different wavelet bases affect the dependence of PRD on BER (Figure 10). Using Db4 and Db8, more optimal ratios of the studied parameters were obtained. When using the wavelet bases Db12 and Db16 with an increase in BER above 0.03, a significant increase in PRD values was observed. The results were obtained in studies on PPG.

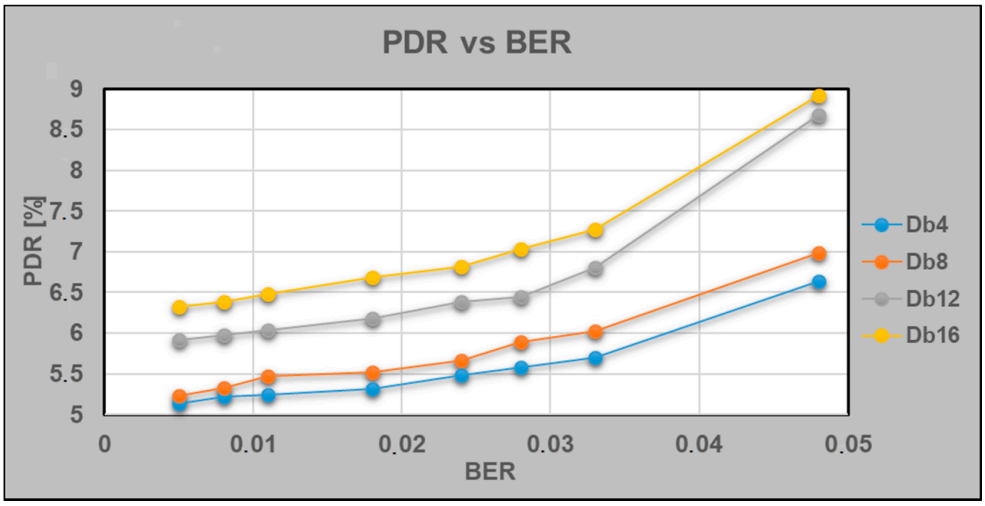

Figure 10. Dependence of the PRD coefficient on BER in the implementation of cardio data protection procedure with different wavelet basis.

The results of the Signal to Noise ratio in the output cardio signal to the input signal are shown in Figure 11. Daubechies wavelet realizations with four and eight coefficients achieved a higher Signal to Noise ratio in the output signal compared to the input signal studied. The results were obtained in studies on PPG.

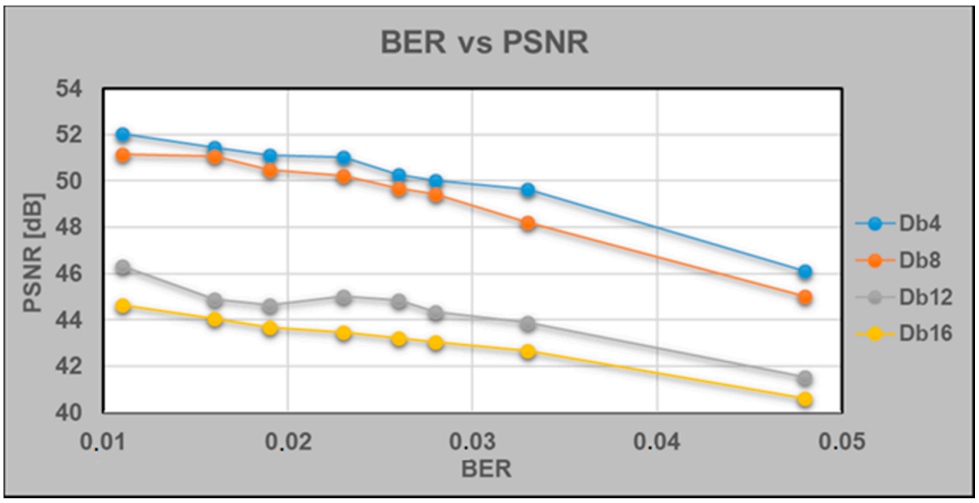

Figure 11. Dependence of the PSNR coefficient on BER in the implementation of cardio data protection procedure with different wavelet basis.

All results were obtained in research conducted through a software program in the MATLAB environment and all showed the effectiveness, security, stability, and potential use of the proposed scheme in telemedicine.

4. Discussion

The authors are about to apply the proposed procedure for the protection of cardio data on a larger number of real cardio data (ECG, PPG, and Holter), which are currently still being collected and will be organized, stored, and protected. Access will be authorized through an information platform in a database of cardio records. The application of the proposed procedure for the protection of cardio data will provide an opportunity to highlight all the strengths and possible weaknesses of the protection procedure. Real ECG, PPG, and Holter records are currently being collected from patients with various

heart conditions and healthy volunteers. In some cardiac diseases, deviations from the standard form of cardio signals are observed. Testing the proposed procedure with such data will allow for wider use of the discussed encryption method. The authors envisage the application and analysis of evaluation parameters in the application of other cryptographic methods of protection (e.g., adaptive Humming Bird method and others).

5. Conclusions

The purpose of cryptography is to protect data from unauthorized use. The cryptographic method offers a secure change of transmission data with different procedures; after acceptance in the opposite environment, the data is decrypted and restored to its original appearance. Cryptography can solve problems related to network data protection, as well as its successful implementation enabling the protection of applications and data on communication channels, cloud computing, etc.

This paper aims to provide an effective cryptographic solution that is sufficient to address issues related to the challenges of transmitting biomedical signals and data (providing protection, preserving the integrity of data, and the confidentiality of patients' personal information). The proposed protection procedure is applied to three types of cardio data: ECG, PPG, and Holter records. All tested signals are real and received with either a PPG device (ECG and PPG) or Holter, which are created or purchased under a research project "Investigation of the application of new mathematical methods for the analysis of cardiac data" in which the authors of the paper participated. The implementation of the proposed procedure is implemented in the Microsoft Visual C++ software application. All steps of the procedure have been studied: EPE-based compression algorithm, performing a wavelet transform based on Daubechies, embedding a watermark in the wavelet coefficients obtained at the lowest level of reconstruction, and hybrid algorithm encryption. From the study of algorithmic methods with evaluation parameters, it can be concluded that cardio data (ECG, PPG, and Holter records) that is decrypted and transformed with inverse wavelet transform retain their diagnostic characteristics, having sufficient accuracy compared to the original data.

The proposed encryption procedure achieves a good degree of compression, ranging from 3.87 (PPG) to 4.98 (Holter). The Signal to Noise Ratio was examined after applying the encryption algorithm step. The SNR values ranged from 31.83 to 46.37, which is an indicator of the quality of the transmitted signal having been retained.

The integrated mathematical approach proposed and researched can be used in the implementation of the protection of the information base from real ECG, PPG, and Holter cardio records, obtained during the authors' work on the research project. The protection of medical signals and patients' personal data can be applied in the transmission of information via communication channels between medical institutions in which records of cardio data are kept and the center for processing and storage of the cardio database.

The encryption procedure proposed in this paper will be applied specifically in creating protection for the three types of ECG, PPG, and Holter signals. It involved the implementation of an archive that was processed and tested using mathematical analysis cardio signals obtained in the study of patients with various cardiovascular diseases and a healthy control group.

Author Contributions: Conceptualization and design, G.B. and G.G.-T.; Data curation and reviews for correctness, G.G.-T. and E.G.; Conceptualization and methodology for protection of archive from cardio data, G.B.; Investigation, G.G.-T.; Software creation for mathematical analysis of cardio data, G.G.-T.; Performed experiments, G.G.-T.; Writing—manuscript, G.G.-T.; Manuscript review and contribution to final version, E.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Science Fund of Bulgaria (scientific project "Investigation of the application of new mathematical methods for the analysis of cardiac data"), Grant Number KP-06-N22/5, 7 December 2018.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Research Ethics Committee at Medical University—Varna, Bulgaria., Protocol/Decision No. 82, 28 March 2019.

Informed Consent Statement: All participants were informed in advance of the research that would be done to them. Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The cardio data we processed for the research purposes of this paper were obtained from the Medical University of Varna, Bulgaria (available on http://hrvdata.vtlab.eu/, accessed on 7 December 2018).

Conflicts of Interest: All authors declare no conflict of interest.

References

1. Limniotis, K. Cryptography as the Means to Protect Fundamental Human Rights. *Cryptography* **2021**, *5*, 34. [CrossRef]
2. European Union. The EU's Cybersecurity Strategy for the Digital Decade. Available online: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (accessed on 4 January 2022).
3. Kh-Madhloom, J.; Abd Ghani, M.K.; Baharon, M.R. ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing. *Intell. Autom. Soft Comput.* **2021**, *28*, 498–512. [CrossRef]
4. Aryanti, A.; Mekongga, I. Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher in Web Based Information System. *E3S Web Conf.* **2018**, *31*, 10007. [CrossRef]
5. Nemec, M.; Sys, M.; Svenda, P.; Klinec, D.; Matyas, V. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, 30 October–3 November 2017; pp. 1631–1648.
6. Wiener, M. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inf. Theory* **1990**, *160*, 553–558. [CrossRef]
7. Northshield, S. A Short Proof of Fermat's Two-square Theorem. *Am. Math. Mon.* **2020**, *127*, 638.
8. Dickson, L.E. *History of the Theory of Numbers: Diophantine Analysis*, 2nd ed.; Dover Publications: New York, NY, USA, 2005.
9. Christopher, A.D. A partition-theoretic proof of Fermat's Two Squares Theorem. *Discret. Math.* **2016**, *339*, 1410–1411. [CrossRef]
10. Hiary, G.A. A Deterministic Algorithm for Integer Factorization. *Math. Comput.* **2016**, *85*, 2065–2069. [CrossRef]
11. Overmars, A.; Venkatraman, S. New Semi-Prime Factorization and Application in Large RSA Key Attacks. *J. Cybersecur. Priv.* **2021**, *1*, 660–674. [CrossRef]
12. Verri Lucca, A.; Mariano Sborz, G.A.; Leithardt, V.R.Q.; Beko, M.; Albenes Zeferino, C.; Parreira, W.D. A Review of Techniques for Implementing Elliptic Curve Point Multiplication on Hardware. *J. Sens. Actuator Netw.* **2021**, *10*, 3. [CrossRef]
13. Cheung, D.; Maslov, D.; Mathew, J.; Pradhan, D.K. On the Design and Optimization of a Quantum Polynomial-Time Attack on Elliptic Curve Cryptography. In *Workshop on Quantum Computation, Communication, and Cryptography*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 96–104. [CrossRef]
14. Shin, S.-H.; Yoo, W.-S.; Choi, H. Development of Public Key Cryptographic Algorithm Using Matrix Pattern for Tele-Ultrasound Applications. *Mathematics* **2019**, *7*, 752. [CrossRef]
15. Murillo-Escobar, M.; Cardoza-Avendaño, L.; López-Gutiérrez, R.; Cruz-Hernández, C. A Double Chaotic Layer Encryption Algorithm for Clinical Signals in Telemedicine. *J. Med. Syst.* **2017**, *41*, 59. [CrossRef] [PubMed]
16. Moody, G.B.; Mark, R.G.; Goldberger, A.L. PhysioNet: A Web-Based Resource for the Study of Physiologic Signals. *IEEE Eng. Med. Biol. Mag.* **2001**, *20*, 70–75. [CrossRef] [PubMed]
17. Kishore, P.; Venkatram, N.; Sarvya, C.; Reddy, L. Medical Image Watermarking Using RSA Encryption in Wavelet Domain. In Proceedings of the 2014 First International Conference on Networks & Soft Computing, Guntur, India, 19–20 August 2014; pp. 258–262. [CrossRef]
18. Zhang, Z.; Wang, H.; Vasilakos, A.V.; Fang, H. ECG-Cryptography and Authentication in Body Area Networks. *IEEE Trans. Inf. Technol. Biomed.* **2012**, *16*, 1070–1078. [CrossRef] [PubMed]
19. Karthikeyan, M.V.; Manickam, J.M.L. ECG-Signal Based Secret Key Generation (ESKG) Scheme for WBAN and Hardware Implementation. *Wireless Pers. Commun.* **2019**, *106*, 2037–2052. [CrossRef]
20. Ogiela, L.; Ogiela, M.R. Bio-Inspired Cryptographic Techniques in Information Management Applications. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 1059–1063. [CrossRef]
21. Ogiela, M.R.; Ogiela, L. Cognitive cryptography techniques for intelligent information management. *Int. J. Inf. Manag.* **2018**, *40*, 21–27. [CrossRef]
22. Beimel, A.; Farràs, O.; Mintz, Y. Secret-Sharing Schemes for Very Dense Graphs. *J. Cryptol.* **2016**, *29*, 336–362. [CrossRef]
23. Georgieva-Tsaneva, G. Wavelet Based Interval Varying Algorithm for Optimal Non-Stationary Signal Denoising. In Proceedings of the 20th International Conference on Computer Systems and Technologies, Ruse, Bulgaria, 21–22 June 2019; pp. 200–206. [CrossRef]
24. Georgieva-Tsaneva, G. Wavelet Based method for Non-Stationary Time Series Processing. In Proceedings of the 21st International Conference on Computer Systems and Technologies' 20, Ruse, Bulgaria, 19–20 June 2020; pp. 122–128. [CrossRef]

25. Georgieva-Tsaneva, G.; Gospodinov, M.; Gospodinova, E. Simulation of Heart Rate Variability Data with Methods of Wavelet Transform. In Proceedings of the 2012 Conference on Computer Systems and Technologies, Ruse, Bulgaria, 22–23 June 2012; Volume 630, pp. 306–312.
26. Mallat, S. A theory for multiresolution signal decomposition: The wavelet representation. *IEEE Trans. Pattern Anal. Mach. Intell.* **1989**, *11*, 674–693. [CrossRef]
27. Gospodinov, M.; Georgieva-Tsaneva, G. Optimization algorithm for EPE-based wavelet compression for ECG signals. In Proceedings of the International Conference on Automatics and Informatics, Sofia, Bulgaria, 3–7 October 2011; pp. B299–B302.
28. Tseng, K.-K.; He, X.; Kung, W.-M.; Chen, S.-T.; Liao, M.; Huang, H.-N. Wavelet-Based Watermarking and Compression for ECG Signals with Verification Evaluation. *Sensors* **2014**, *14*, 3721–3736. [CrossRef]
29. Ibaida, A.; Khalil, I.; Schyndel, R. A Low Complexity High Capacity ECG Signal Watermark for Wearable Sensor-net Health Monitoring System. *Comput. Cardiol.* **2011**, *38*, 393–396.
30. Daoui, A.; Karmouni, H.; Sayyouri, M.; Qjidaa, H. Efficient Methods for Signal Processing Using Charlier Moments and Artificial Bee Colony Algorithm. *Circuits Syst Signal Process* **2022**, *41*, 166–195. [CrossRef]
31. Ouali, M.; Tinouna, A.; Ghanai, M.; Chafaa, K. Electrocardiogram Signal Denoising by Hilbert Transform and Synchronous Detection. *Int. J. Bioautom.* **2020**, *24*, 323–336. [CrossRef]
32. Hamayel, M.J.; Owda, A.Y. A Novel Cryptocurrency Price Prediction Model Using GRU, LSTM and bi-LSTM Machine Learning Algorithms. *Artif. Intell.* **2021**, *2*, 477–496. [CrossRef]
33. Almehmadi, F.S.; Chatterjee, M.R. Secure chaotic transmission of electrocardiography signals with acousto-optic modulation under profiled beam propagation. *Appl. Opt.* **2015**, *54*, 195–203. [CrossRef] [PubMed]
34. Samawi, H.M.; Yin, J.; Zhang, X.; Yu, L.; Rochani, H.; Vogel, R.; Chen, M. Kullback-Leibler Divergence for Medical Diagnostics Accuracy and Cut-point Selection Criterion: How it is related to the Youden Index. *J. Appl. Bioinform. Comput. Biol.* **2020**, *9*, 2. [CrossRef]