International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I2P118

Volume 72 Issue 2, 163-177, February 2024

Original Article

Deep Learning-Based Anomaly Detection of ECG Signals for Telemedicine Applications

Akhila N. S[1], Sabeena Beevi. K[2], Bejoy Abraham[3]

[1,2]*Department of Electrical and Electronics Engineering, TKM College of Engineering, Kerala, India.*
[3]*Department of Computer Science and Engineering, College of Engineering Muttathara, Kerala, India.*

[2]*Corresponding Author : sabeena3000@tkmce.ac.in*

Received: 25 August 2023 Revised: 23 November 2023 Accepted: 23 January 2024 Published: 03 February 2024

Abstract *- The growing global emphasis on healthcare and protection issues underscores the importance of point-of-care (POC) technologies. These technologies play a crucial role in delivering cost-effective solutions for telemedicine, further emphasizing their significance in the healthcare landscape. Although POC has clear benefits, it does not provide a primary patient diagnosis. Hence, this study focuses on the primary diagnosis of cardiac diseases by detecting abnormalities in the Electrocardiogram (ECG) on the patient's side itself. Achieving accurate diagnosis necessitates access to patients' confidential data. However, transmitting this sensitive information across a public network may lead to numerous security concerns. Additionally, serious privacy issues could arise since personal health information might be revealed to unauthorized individuals. This paper proposes a novel long, short-term based deep-learning technique for detecting the abnormality of ECG signals. The conveyed data's secrecy, security, and privacy are reinforced by employing a steganographic technique reliant on the Fast Walsh Hadamard transform. Features like spectral entropy and instantaneous frequency are used to increase the LSTM network's accuracy. Diverse transforms and their corresponding reconstruction methods are analysed, and it was observed that Walsh-Hadamard transforms are particularly well-suited for this specific application. This is primarily attributed to their compression capabilities, which effectively reduce the storage space needed for the data. The method being suggested is evaluated against traditional approaches outlined in the current literature.*

Keywords *- Electrocardiogram, Long short-term memory network, Telemedicine, POC.*

1. Introduction

Point of Care technology (POC) refers to medical devices and technologies used at the bedside or near the patient to provide immediate diagnostic and monitoring results. These technologies are designed to facilitate efficient and convenient healthcare delivery, enabling healthcare providers to make quick patient care decisions without sending samples to a laboratory. Telemedicine refers to providing healthcare services and medical information from a distance through telecommunication technology. It allows healthcare professionals to interact with patients who are located in different geographic locations, providing consultation, diagnosis, treatment, and monitoring remotely [1]. These systems primarily function by exchanging biomedical signals, video, and audio-based data over a suitable communication medium, such as the internet. Compared to other industries, the healthcare industry has been hesitant to embrace new technologies due to stringent regulations and the sensitive nature of medical data. However, POC systems have emerged as a promising healthcare solution [1]. Their key advantages are rapid access to test results, facilitating prompt medical assessments, and appropriate interventions.

Also, diagnosing patients at their homes can significantly reduce the rising traffic at hospitals and medical aids. Globally, Cardiovascular Diseases (CVD) rank first among the leading causes of death, accounting for more deaths each year than any other factor [9]. Systems at the point of care can significantly improve CVD outcomes as well. Point-of-care cardiac diagnostic testing provides immediate results, emphasizing the significance of monitoring Electrocardiograms (ECGs) and enabling automatic diagnosis.

Integration of PoC systems into healthcare has enhanced patient care and delivered quicker results. However, it is important to note that these systems generally do not include primary heart disease diagnosis as part of their capabilities. The majority of the research in this area has primarily focused on the spectral analysis of ECG signals, which involves a number of steps like feature extraction and classification [2], as well as preprocessing of the electrocardiogram data. Additionally, within POC, the need for patients' private and confidential data for in-depth analysis of cardiovascular diseases raises numerous security apprehensions.

Established techniques like encryption-decryption, watermarking, and wavelet-based methods for secure transmission of ECG signals have demonstrated vulnerabilities to potential attacks. Considering these challenges, this paper presents a pioneering system that tackles several key objectives. It aims to empower primary diagnosis at the patient's location, guarantee comprehensive patient privacy protection at both ends and uphold robust data security measures.

Long Short-Term Memory Network (LSTM), a sort of Recurrent Neural Network (RNN), is used to do the initial diagnostic of an ECG at the patient's side. In the event of any abnormalities, the signal is relayed to the medical professionals for additional examination and treatment. Time-dependent features are utilised to enhance the performance of the LSTM network. To ensure precise disease diagnosis, the ECG signals are transmitted alongside the patient's personal information (name, age, gender, etc.) and diagnostic data (temperature, oxygen saturation, blood pressure, etc.). Concealing this data involves employing a steganography-based technique. The paper is organized such that Section 2 of the paper presents a synopsis of recent literature concerning anomaly detection and methods based on steganography. Following this, Section 3 elaborates on the proposed approach. Section 4 contains the experimental findings, discussions, and comparisons. The paper's conclusion is outlined in section 5.

2. Literature Review

The most important waveform in an electrocardiogram is the QRS complex. Because it depicts the electrical activity within the heart during ventricular contraction, the timing and pattern of its presence offer substantial insights into the heart's present condition. It acts as the basis for automatically determining heart rate and serves as the initial reference for categorizing the cardiac cycle because of its unique form. Additionally, it finds application in ECG data compression algorithms. The cornerstone of nearly all automated ECG analysis algorithms is the detection of QRS complexes. Because of this, the majority of early anomaly detection techniques relied on this QRS detection [2].

This approach is carried out in two steps: first, the signal is subjected to a wavelet transform filtering, and next, a maximum detection and peak classification algorithm is used to localize the QRS complex. Numerous algorithms have been proposed to categorize ECG heartbeat patterns by extracting characteristics from the ECG data. One commonly used method is Fourier transform analysis, which reveals the range of frequency amplitudes present in the signal. However, it only offers the spectral components only, not their temporal correlations. The wavelet transform was then used to extract features. This technique begins by removing noise through either a soft or hard thresholding method. Then, the characteristics of the ECG wave are segmented into coefficient vectors using the most effective wavelet transformation. The set of orthogonal and bi-orthogonal wavelet filter banks, which show the strongest correlation with the ECG signal, was employed to establish the mother wavelet transform. After analysing the ECG signal, the coefficients for the QRS complex, T wave, and P wave are separated, summed, and utilized for feature extraction. Following this, methods based on neural networks [12] were introduced, such as the Back Propagation Neural Network (BPNN) and Support Vector Machine (SVM) classifier [6]. They utilized the discrete wavelet transform to extract features, integrating these with time interval features for neural network training purposes.

All of these techniques initially require denoising the signal. Various features are used for the right categorization and detection of the anomaly. Every information protection solution should be carefully evaluated in terms of security, effectiveness, and capacity [17]. The majority of currently offered solutions, however, do not adequately balance these three aspects. The Health Insurance Portability and Accountability Act (HIPAA) [7] encompasses two vital necessities crucial for safeguarding healthcare privacy. Enacted by the US government in 1996, HIPAA outlines privacy and security regulations. These laws set boundaries on health information usage and disclosure, ensuring patients exercise greater control over their information.

The security regulations outline the safeguards put in place to protect data availability, confidentiality, and integrity. As a result, clearly defined cryptographic methods such as digital signatures, encryption, and key recovery mechanisms [4] came into play. In this instance, the patient data is stored on a smart card. Smart card usage has limitations even though it safeguards confidentiality and integrity. Additionally, the efficiency of the classical encryption techniques utilized here is inadequate since every time the data is needed, it must first be decrypted. Due to significant advancements in information and communication technology, there have been substantial transformations in healthcare delivery and the handling of medical data. Digital images can be transferred over the internet freely on a regular basis. As a result, biometric image authentication emerged as a significant research trend. To safeguard intellectual property rights and validate the host biometric photos, digital watermarking techniques can be used to insert confidential information. A wavelet-based electrocardiogram (ECG) signal watermarking technique with good data-hiding capacity has been devised [8]. Most of the energy in an ECG signal resides within the QRS complex waves.Consequently, selecting wavelet coefficients for concealment should aim to avoid significant distortion of these QRS complex waves. Reversibility refers to the ability to extract the original, lossless digital media from marked media and restore it. This technique uses the original ECG signal to apply the B-spline wavelet transform to find the QRS complex.

After identifying the R waves, the original ECG signal undergoes another round of Haar lifting wavelet transformation. Subsequently, non-QRS high-frequency wavelet coefficients are selected by employing index subscript mapping and comparison. The watermark is integrated by shifting the chosen coefficients one bit to the left. Eventually, the ECG signal is restored using the inverse Haar lifting wavelet transform.

Additionally, Arnold transform is used to scramble the watermark prior to embedding it. As it only shifts one bit, this approach has a limited capacity. As a result, each ECG sample value can only be kept in 1 bit. Additionally, the security of this technique relies entirely on the algorithm itself without using a user-defined key. The algorithm is designed based on a typical ECG signal that includes a detectable QRS complex. However, it may not function effectively for abnormal signals where the QRS complex cannot be detected.

Healthcare expenditures could be reduced, and easy and quick access to medical professionals made possible by the interchange of medical data. Large amounts of a patient's important information, such as biosignals, are therefore frequently exchanged along with medical photographs during exchange procedures between healthcare providers. The benefits of data authentication and memory usage can be combined when patient information is added to digital content, such as photos. The fact that the data is delivered across an insecure network, like the internet, could result in unauthorised access to patient data. Watermarking is thus employed here as a fix [7]. In this case, an integer wavelet transform is applied for lossless watermarking. The initial signal undergoes division into a series of coefficients through the integer wavelet transform. Data embedding is done by shifting the peak and zero points identified by the histogram approach [8,9]. But this also mainly focuses on authenticity.

Outsourcing medical analysis presents challenges with regard to data protection. While utilising encryption techniques to secure transmission routes is a possibility, protecting the data while doing analyses is challenging because it frequently entails processing steps on the raw data. The primary use of this data is to conduct DNA searches, and it should be given to the cloud provider for processing. Bloom filters are employed for DNA analysis. Homomorphic cryptography [10] is also utilised here, allowing third parties to view the material without compromising privacy. Utilising homomorphic encryption aimed to find a balance between security and efficacy. Despite this attempt, its intricate nature makes this non-conventional cryptography impractical for real-world applications.The central concerns revolve around ensuring the security and privacy of data transmitted from point-of-care systems. Body sensors are used to gather physiological data and patient biological information. Following this, the signals are forwarded to the patient's device for further analysis or diagnosis.

Subsequently, these signals, along with sensitive patient information, diagnosis reports, and urgent alerts, are transmitted via the internet to the central hospital computers. Doctors may access such biological signals from anywhere using any device, analyse them, and potentially make a decision in an emergency. Relying on the internet as your main communication channel exposes you to heightened security and privacy risks, alongside potential challenges regarding data integration.

In order to provide a secure transfer of patient personal information along with physiological measurements from body sensors, a new security mechanism [17] is suggested. This approach merges steganography techniques to hide patient-specific information within the biological signals of the patient. Moreover, the proposed approach utilizes an encryption-centered model to restrict access to the concealed data solely to authorized individuals. Within this research, the patient's ECG signal acts as the primary signal, carrying not only various sensor measurements such as temperature, glucose, location, and blood pressure but also the patient's confidential information.

Since most healthcare systems will gather ECG data, the ECG signal is employed in this instance. In addition, the ECG signal is significant in comparison to other types of data. It will, therefore, be appropriate to house other small-scale sensitive information. In this study, the wavelet transform is employed to decompose the signal, and steganography techniques are utilized to embed data into the host signal.

While this approach offers advantages regarding privacy and security, the complexity arises from the multiplication and convolution processes involved. Previous methods for analysing ECG signals involved traditional approaches such as detecting PQRST values. Subsequently, neural network-based methods such as BPNN, KNN, and SVM were introduced, but these techniques require manual feature engineering. Various cryptography and watermarking techniques have been introduced to address the need for data confidentiality. However, these methods do not guarantee the complete secrecy or confidentiality of the data.

Moreover, these methods often incur higher computational costs, impacting the system's efficiency. In an attempt to address data security concerns, some approaches rely on cryptographic techniques where medical records are encrypted using a password. The fundamental premise is that solely authorized individuals possessing the correct password can access the encrypted data. Nonetheless, encrypted data remains susceptible to security breaches by unauthorized entities that might decrypt private information like patient records, prescription histories, and so forth. Here, Deep LSTM neural networks are utilised to detect aberrant behaviour in a predicted manner. This approach offers several advantages over traditional methods.

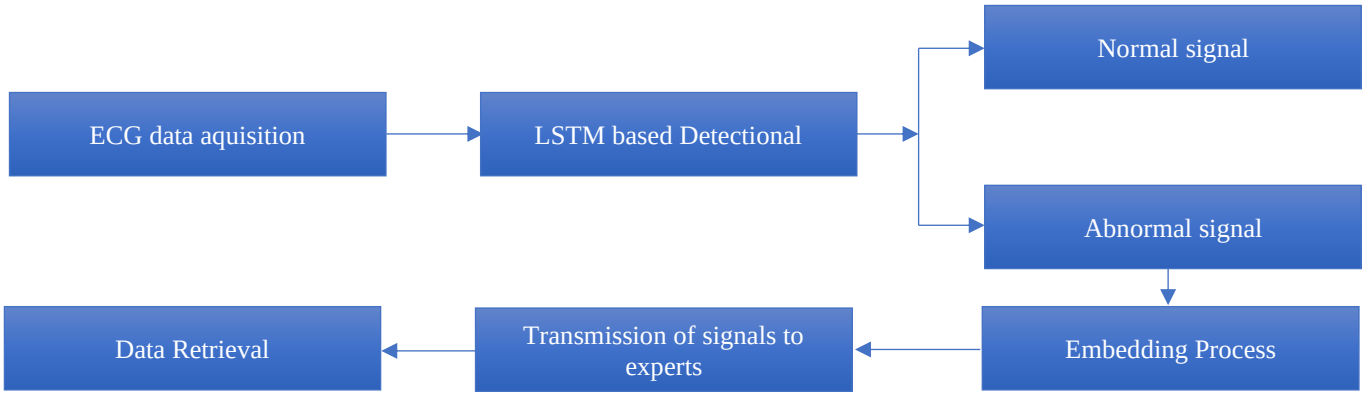

Fig. 1 Data flow diagram

Firstly, it requires minimal or no preprocessing of the data, allowing for a more streamlined analysis process. Secondly, it operates directly on the raw signals without needing hand-coded features, which can be time-consuming and subjective. Lastly, it does not rely on prior knowledge of anomalies, making it adaptable to different scenarios.To enhance data security, a 3D order Walsh-Hadamard-based steganography method is employed. This technique ensures faster and easier computations while securely embedding confidential information within the biomedical ECG signals. By transmitting these signals to hospital authorities, they can access and analyze the data, potentially making critical decisions in emergency situations. This method ensures the confidentiality of patient's medical data while also honoring the obligations of healthcare professionals to secure sensitive information.

3. Materials and Methods

This paper strikes the right balance between the two main issues raised by [17]: (1) the need to accurately identify ECG signal anomalies in order to provide growing cardiac diseases with faster treatments, and (2) the need to provide security and protect patient private information on both ends as well as the biomedical signal.

Figure 1 depicts a straightforward data flow of the technique. ECG information is obtained via PhysioNet, and patient information is manually entered. Within this strategy, two categories of data exist: standard biomedical signals like ECG and extremely sensitive information encompassing personal particulars and diagnostic data.

The first step is to analyze the biomedical signal, such as ECG, using LSTM networks to detect any abnormalities or anomalies. The LSTM networks are trained to recognize patterns and deviations from normal behavior in the signal. Further action can be taken if an abnormality is detected, such as notifying healthcare professionals or triggering an alert.

A steganographic algorithm is applied to ensure the privacy and security of the confidential information. This algorithm conceals private data within the biomedical ECG signals, making it imperceptible to unauthorized individuals. By embedding the confidential information into the ECG signal, it remains protected during transmission and storage.

By combining abnormality detection using LSTM networks and steganography techniques, this approach provides a comprehensive solution for analyzing biomedical signals, detecting abnormalities, and securing confidential information within the signals. The internet is used to send stego signals, or ECG signals with embedded sensitive information, to remote health authorities.

In the proposed approach, the stego signals, which are the biomedical signals embedded with confidential information, are managed by health authorities. To boost the signal's concealment capability, the Fast Walsh Hadamard transform is employed [12]. This transformation improves the signal's capacity to hide a greater volume of data. To preserve the original signal with minimal distortion, solely the least significant values are utilized to embed the patient's confidential information. This approach helps maintain the integrity and quality of the biomedical signal while incorporating confidential data. To enhance the security of the private information, a security key is employed. This key is combined with personal data, further strengthening the protection of the individual's information.

Additionally, the security key is automatically rotated to mitigate the risk of unauthorized access or attacks. By periodically changing the key, the system becomes more resilient against unauthorized individuals attempting to access the private data. By integrating the Fast Walsh Hadamard transform, using the least significant values for embedding, and implementing a rotating security key, the proposed method strives to guarantee the privacy and security of the patient's personal and diagnostic information within the biomedical signals. The host signal is transformed into a three-dimensional order using this rotated key. Others can only access the stego signals, while those with the key will be able to extract the information.

3.1. Anomaly Detection of ECG Signals

The analysis and classification of ECG data can be done using a variety of conventional machine-learning approaches. Integrating the primary limitations of conventional machine learning techniques lies in their dependence on manually selected features, constraining their capacity to effectively capture intricate patterns in data. Moreover, attaining high classification accuracy frequently demands a substantial number of features, resulting in complexity and computational expense.

On the other hand, deep learning architectures offer a solution to these challenges. They belong to a broader family of machine learning methods known as Artificial Neural Networks (ANNs). Deep learning models can directly analyze raw data, such as biomedical signals, without requiring manual feature extraction. This allows them to automatically learn intricate patterns and representations from the data itself.

Recurrent Neural Networks (RNNs) represent a prevalent category of deep neural networks tailored for managing sequential inputs with diverse lengths. Uniquely structured to accommodate sequential data, they integrate feedback connections, enabling the retention of information across distinct time steps. The structure of an RNN typically consists of a tanh layer and a series of repeated neural network modules. These components, commonly known as RNN cells, retain a concealed state encompassing information from prior time steps, continually refreshing it with new input at each subsequent step.

The hidden state serves as a memory that retains relevant information about the sequence as it progresses [25]. The present condition of a basic RNN can be computed through the following equation:

$$h_t = \tanh(W_h * h_{t-1} + W_x * x_t) \quad (1)$$

Here ht signifies the current state, ht-1 denotes the preceding state, xt represents the input at the current time step, and wh, along with wx symbols, symbolizes weight matrices capturing the relationships between the hidden state and the input.

The output state of a simple RNN is determined by:

$$y_t = W_y * h_t \quad (2)$$

Additionally, yt represents the output at the current time step, and Wy stands for a weight matrix linking the hidden state to the output.These equations highlight how the hidden state of an RNN evolves over time, capturing information from past inputs and influencing future outputs. The inherent recurrent structure enables RNNs to adeptly represent and scrutinize sequential data, rendering them suitable for diverse assignments such as natural language processing, speech recognition, and time series analysis. However, conventional RNNs may encounter challenges in capturing prolonged temporal relationships due to the vanishing gradient issue, where gradients dwindle exponentially as they traverse backward through time. This limitation hinders the ability of RNNs to effectively capture and retain information over long sequences. A specialized form of RNN known as Long Short-Term Memory(LSTM) was introduced to tackle this challenge. LSTM networks employ memory cells capable of preserving information for extended durations, enabling them to overcome the vanishing gradient issue and capture prolonged dependencies.

These networks incorporate distinct units like input gates, forget gates, and output gates alongside the conventional hidden units found in typical RNNS. These gates manage the information flow within the network, allowing selective updates and removal of data stored in memory cells. The input gate determines which input parts are stored, the forget gate regulates what information to discard, and the output gate controls the output based on the memory cell's current state.

By integrating memory cells and gate mechanisms, LSTM networks effectively retain and update information across extended sequences, making them ideal for tasks involving long-term dependencies such as language modelling, speech recognition, and sentiment analysis. The design of LSTM networks has shown success in mitigating the vanishing gradient problem, enabling the modelling of prolonged dependencies, and improving performance across various sequential data tasks.

3.2. Embedding Process

Once a signal's normality or abnormality is identified, typical ECG signals undergo the Fast Walsh Hadamard transform(FWHT). The personal data, in conjunction with a security key and rotation factor, is utilized to convert the FWHT values into a 3D-ordered matrix.

This matrix is integrated into the ECG signal, forming a stego signal. This stego signal, housing the encrypted personal data, is transmitted to health authorities. Access to the embedded personal information at the receiver's end is solely possible for authorized users possessing the key.

The original ECG signal, including the embedded personal data, is reconstructed using the inverse Walsh Hadamard transform, guaranteeing the restoration of the initial signal. Here are the various stages of the embedding process:

3.2.1. Walsh Hadamard Transform

The Walsh Hadamard Transform (WHT) represents an orthogonal conversion that dissects a signal into a series of orthogonal and rectangular waveforms called Walsh or Hadamard functions [13]. Distinguished from other transformations, the FWHT operates without multiplication processes and remains real-valued.

This is because the amplitude of the Walsh or Hadamard functions is limited to two values: +1 or -1.In the proposed scheme, the FWHT is employed for encryption and decryption purposes. The coefficients of the FWHT are calculated using equation (3). The formula used to compute the FWHT coefficients (cn) incorporates the sampled values of the ECG signal (si) and the transformation matrix (w(n,i)). This equation facilitates the transformation of the initial signal into the Walsh or Hadamard domain.

$$c_n = \frac{1}{M}\sum_{i=0}^{M-1} s_i w(n,i), n = 1,2.....M-1 \quad (3)$$

The selection of values in the matrix can be customized according to the specific application requirements.The Walsh-Hadamard transform is known for its suitability in signal analysis applications. It offers a good compression ratio, which means that the transformed signal requires less storage space compared to the original signal. Additionally, it enables rapid signal reconstruction, making it efficient for various signal-processing tasks.

3.2.2. Patient Data Encryption

The Advanced Encryption Standard (AES) stands as a prevalent cryptographic method for securing personal data. Functioning as a block cipher, AES encrypts data in standardized block sizes rather than individual bits. It employs a symmetric key approach, wherein the identical key serves for both encryption and decryption purposes. Additionally, AES supports various key lengths: 128, 192, and 256 bits. AES-128 utilizes a 128-bit key, AES-192 uses a 192-bit key, and AES-256 employs a 256-bit key.

The key length determines the level of security provided by the encryption algorithm. Generally, a longer key length offers stronger encryption and is harder to break using brute force attacks. The AES encryption process involves multiple transformation rounds, including substitution, permutation, and mixing operations, to scramble the plaintext and produce the ciphertext.

The same process is reversed during decryption using the same key. Using AES encryption protects and secures personal data, ensuring confidentiality and integrity during transmission or storage. Figure 2 illustrates a single round of the AES algorithm. AES-128 is employed to combine the diagnostic and patient data. Equation (4) [13] denotes the encrypted representation (Ec) of the personal information [19].

$$E_c \Leftarrow D_e(K, S_c) \quad (4)$$

The AES algorithm, represented by De, utilizes a key (K) to combine the original patient confidential information (Sc). AES is designed as a substitution-permutation network. The number of transformation rounds in AES depends on the key size, and for AES-128, ten rounds are performed.

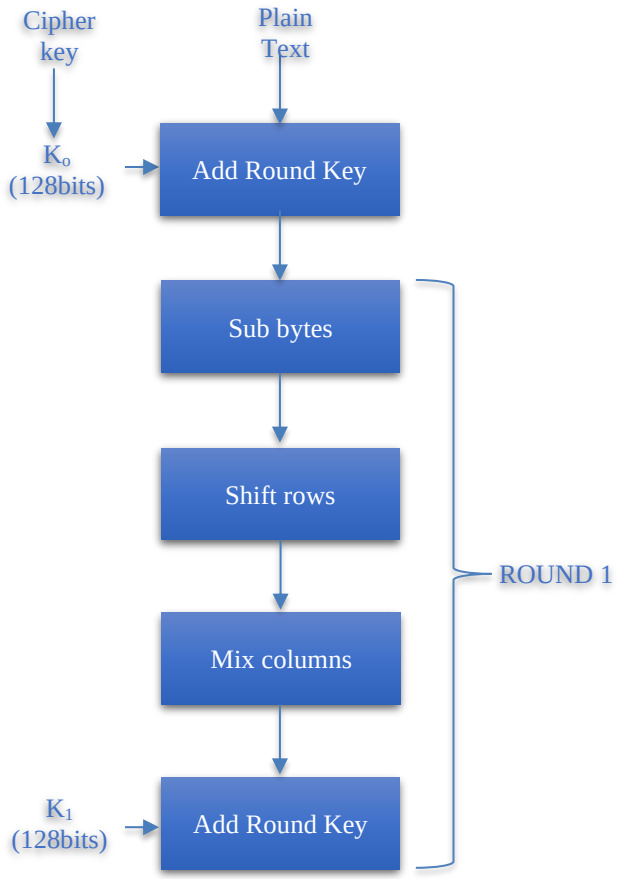

Fig. 2 One round of AES-128[26]

The encryption process involves several iterations, each comprising the following steps as shown: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key. The final step in this process involves combining the output of the preceding three steps with four words from the key schedule using XOR.Conversely, the decryption process follows a comparable structure but features distinct steps for each round: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, and 4) Inverse mix columns. Similar to encryption, the third step in decryption involves XOR-ing the output of the previous two steps with four words from the key schedule. Notably, the last round of encryption and decryption excludes the mix column and inverse mix column steps, respectively.

3.2.3. Patient Data Embedding

After encryption, the key is used to reconfigure the physiological signal into a three-dimensional structure to embed the encrypted patient data. Initially, the key undergoes rotation based on a rotation factor determined by tallying the number of ones in its binary form. Then, the key is rearranged randomly, both in ascending and descending orders, leading to the restructuring of the signal into a three-dimensional sequence. From this sequence, one array of dimensions X × Y × Z is extracted to facilitate the incorporation of the encrypted data, subsequently transmitted to authorized individuals.

3.2.4. Retrieving the Signal and Personal Data

Upon reception, the reverse embedding process is initiated to retrieve both the personal data and the original ECG signal. Initially, the signal is reconverted from its vector format. Subsequently, AES decryption is employed to retrieve the original ECG signal. Furthermore, the Inverse Fast Walsh Hadamard Transform (IFWHT) is executed on the ECG signal to restore it to its initial state. This reverse sequence ensures the recovery of both the personal data and the original ECG signal at the receiver's end.

3.2.5. Inverse Walsh Hadamard Transform

To restore the original signal and the personal data, the embedded signal must be reconfigured from its 3D structure into a vector format. This is followed by reversing the embedding process by applying the Inverse Fast Walsh Hadamard Transform (IFWHT) for signal decomposition.

It's worth emphasizing that the stego biomedical signal retains its utility for diagnostic purposes, offering crucial information for medical analysis. However, retrieving the patient's personal information is only possible by authorized individuals who possess the secret key, ensuring that access to sensitive data is restricted to legitimate authorities. The re-composition of the signal using the Inverse Fast Walsh Hadamard Transform (IFWHT) can be represented by Eq. (5) [19]:

$$si = \sum(cn * w(n,i)) \quad (5)$$

In this equation, cn represents the FWHT coefficients, si represents the sampled value of the ECG signal, and w(n,i) represents the transformation matrix used in the FWHT. By applying this equation, the original ECG signal can be reconstructed from its transformed coefficients.

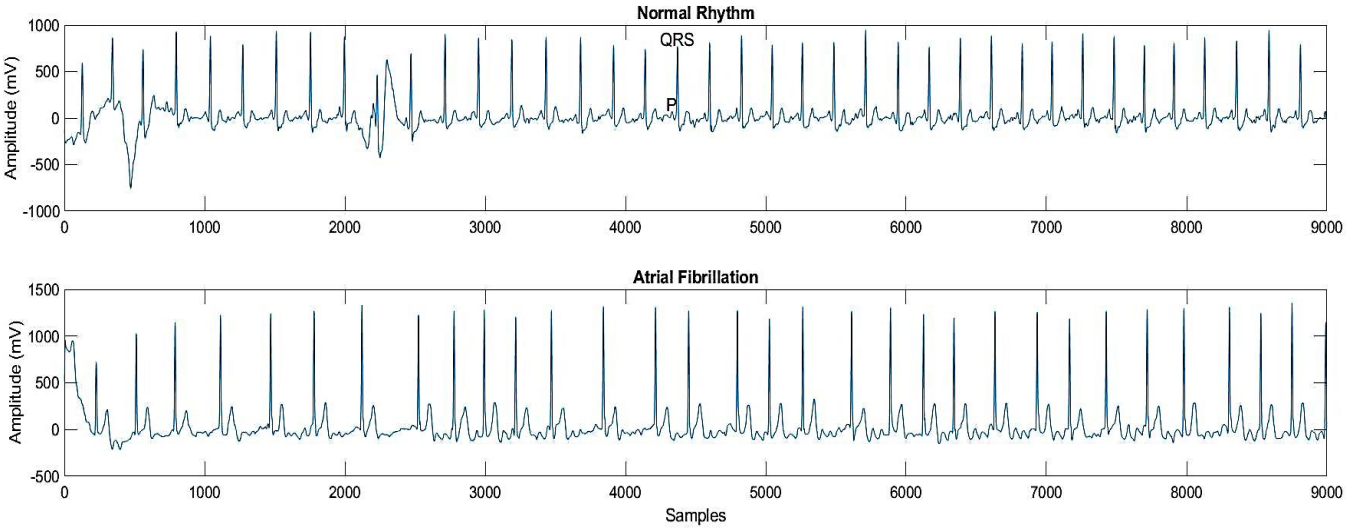

Fig. 3 Normal and abnormal signal

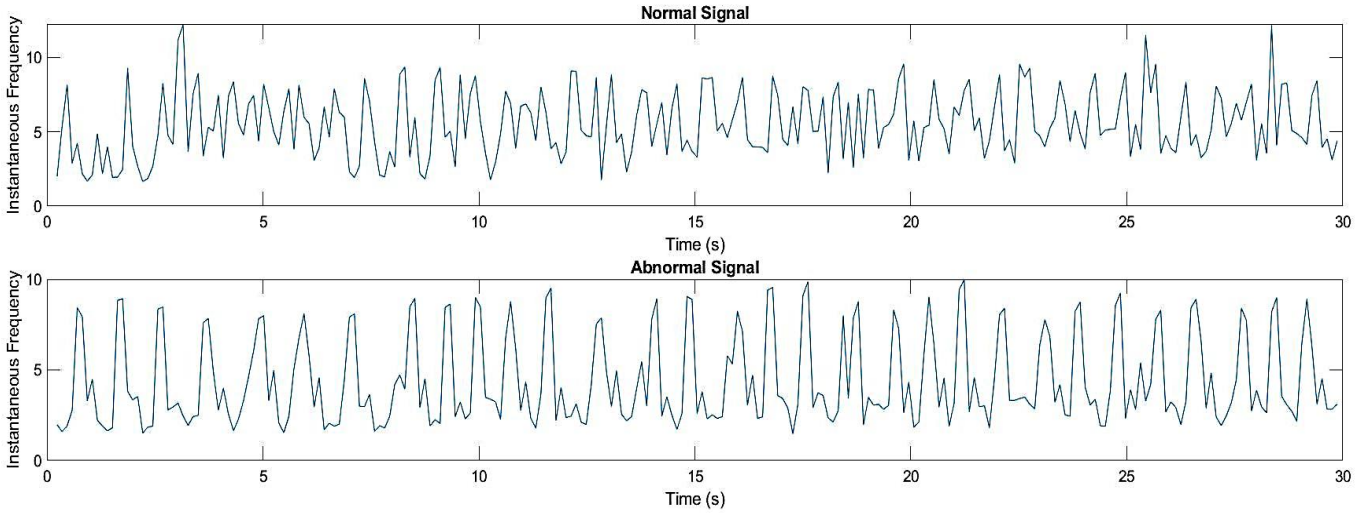

Fig. 4 Instantaneous frequency of normal and abnormal signal

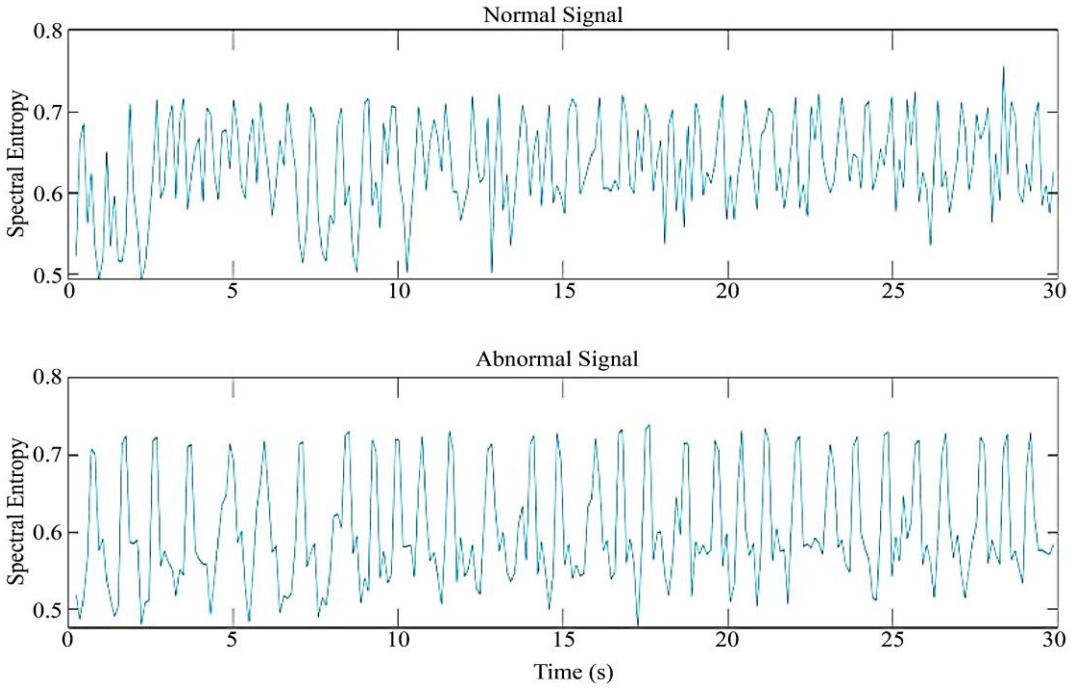

Fig. 5 Spectral entropy of normal and abnormal signal

4. Results and Discussion

4.1. Dataset

The dataset comprises a collection of ECG signals sampled at a rate of 300 Hz. These signals are obtained from ECG lead recordings, with varying lengths ranging from 30 seconds to 60 seconds. Every dataset within the repository comprises 9000 samples. Figure 3 provides an instance displaying both a typical and an irregular ECG signal.

4.2. Anomaly Detection

The ECG signal exhibits distinct P, QRS, and T waves, each representing a specific heartbeat phase. The P-wave signifies atrial depolarization, the QRS complex represents ventricular depolarization, and the T-wave indicates ventricular repolarization. Analysing these waves' duration, shape, and amplitude serves as a crucial aspect of time domain analysis.This study's analysis involves estimating the instantaneous frequency and spectral entropy. Figures 4 and 5 depict the instantaneous frequency and spectral entropy of both normal and abnormal ECG signals. The dataset utilized comprises 738 normal signals and 5050 abnormal signals. The dataset comprises 9000 samples per signal, segregated into a 70% training set and a 30% testing set. The model is trained over 10 epochs, configured with a learning rate 0.01.

4.3. Performance Measures

4.3.1. Accuracy

Accuracy signifies the ratio of accurately predicted observations to the total number of observations, serving as an overall indicator of the model's ability to predict both positive and negative cases.

4.3.2. Precision

Precision quantifies the ratio of correctly predicted positive observations to the total number of predicted positive observations, denoting the model's precision in predicting positive cases.

4.3.3. Recall (Sensitivity)

Recall depicts the ratio of correctly predicted positive observations to the total number of actual positive observations, gauging the model's proficiency in identifying positive cases. Equations 6 to 10 provide the specific values of these performance measures using LSTM networks.

$$\text{Sensitivity} = \frac{N_{TP}}{N_{TP}+N_{FN}} \times 100 \quad (6)$$

$$\text{Precision} = \frac{N_{TP}}{N_{TP}+N_{FP}} \times 100 \quad (7)$$

$$\text{F-Score} = 2 \times \frac{Sensitivity \times Precision}{Sensitivity + Precision} \times 100 \quad (8)$$

$$\text{Accuracy} = \frac{N_{TP}+N_{TN}}{N_{TP}+N_{TN}+N_{FP}+N_{FN}} \times 100 \quad (9)$$

$$\text{Specificity} = \frac{N_{TN}}{N_{FP}+N_{TN}} \times 100 \quad (10)$$

4.3.4. True Positive (TP)

True Positive (TP) signifies the instances where the model accurately predicts the positive class. True Negative (TN) indicates the instances where the model accurately predicts the negative class. False Positive (FP) represents the instances where the model incorrectly predicts the positive class.

4.3.5. False Negative (FN)

False Negative (FN) represents the instances where the model inaccurately predicts the negative class.It is indicated that LSTM achieves high values for accuracy, precision, sensitivity, and F-score, suggesting that the proposed method performs well in terms of overall accuracy, precise positive predictions, correct identification of positive cases, and a balanced measure of precision and recall.

4.3.6. F-score

The F-score computes the weighted average of precision and recall, offering a balanced measure considering both precision and recall.

4.3.7. Specificity (True Negative Rate)

Specificity evaluates the ratio of actual negatives correctly identified as negatives. It complements sensitivity and focuses on correctly identifying negative cases.

4.4. Embedding Process

In Fig.6, an ECG signal and its corresponding changes after applying the FWHT are depicted. The figure illustrates that the obtained FWHT coefficients can be categorized into two groups:

Low coefficient values: These coefficients represent the important parts crucial for accurately rebuilding the signal. Higher coefficient values: These coefficients have less impact on signal reconstruction and can be considered less significant.

Based on this observation, in Fig.6, it is shown that the crucial coefficients lie between 0 and <2000, while the coefficients with higher values are considered less significant. As a result, all coefficient values after >2000 are removed. The ECG signal is then rebuilt using the remaining lower coefficients, which contain the essential information for signal reconstruction.

It demonstrates the capability of the proposed method to classify abnormal signals accurately. The reconstructed signal maintains the essential information while minimizing distortion.

By utilizing a small percentage of the FWHT coefficients, the genuine signal can be reconstructed, highlighting the capacity and flexibility of the approach. The restored abnormal signal offers crucial insights to healthcare professionals, aiding in diagnostic processes and medical decision-making.

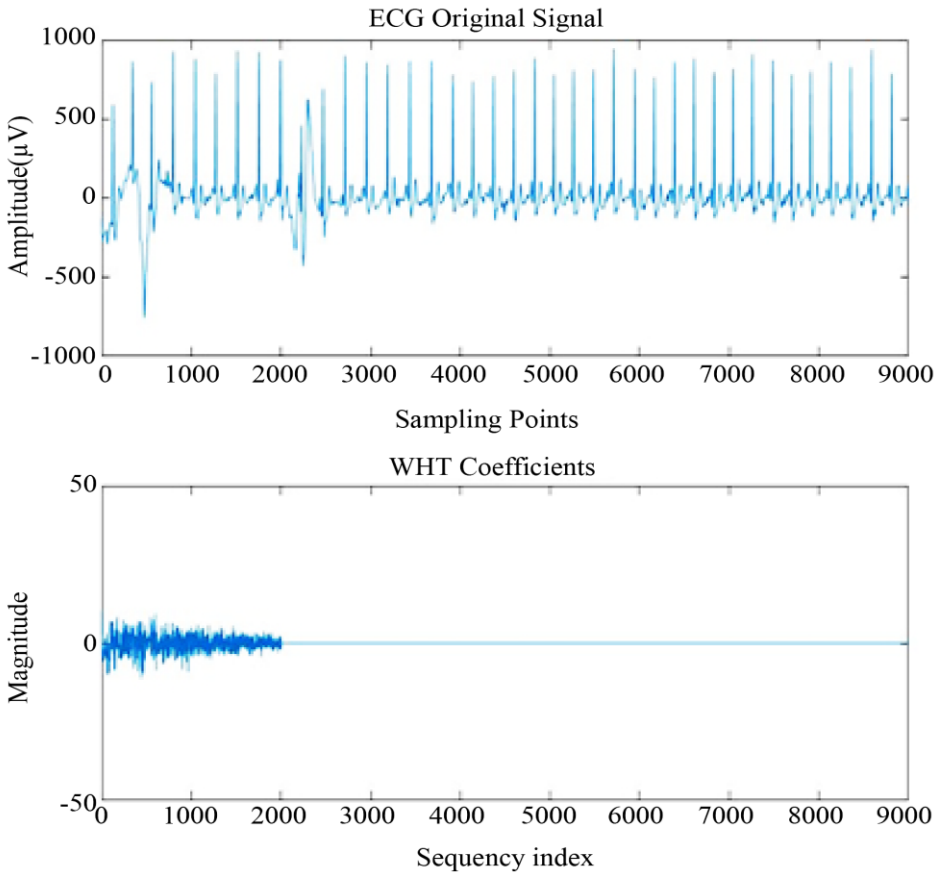

Fig. 6 WHT is applied to the ECG signal.

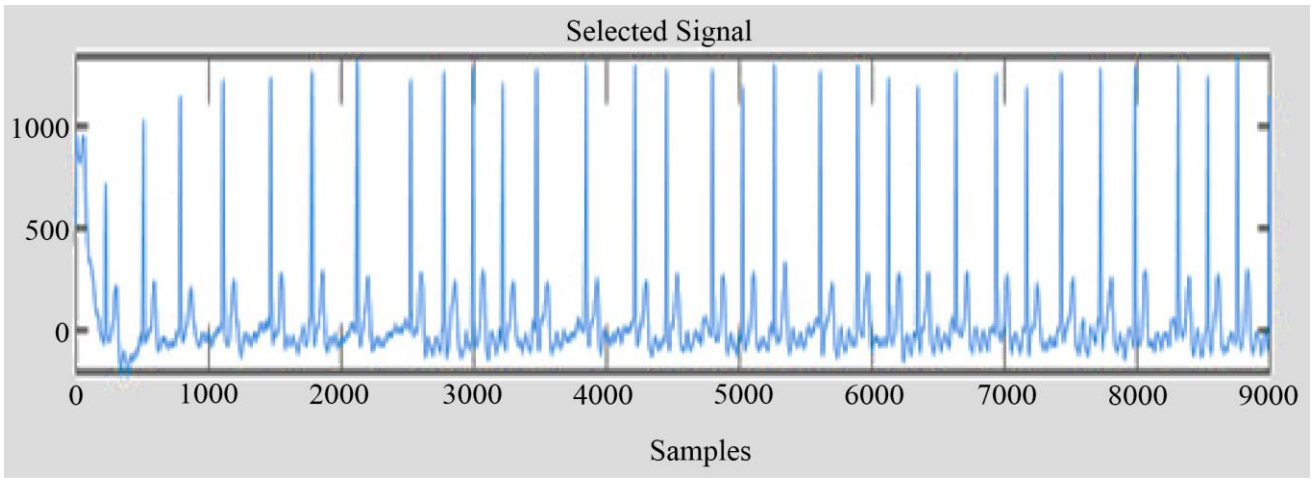

Fig. 7 Abnormal signal for embedding

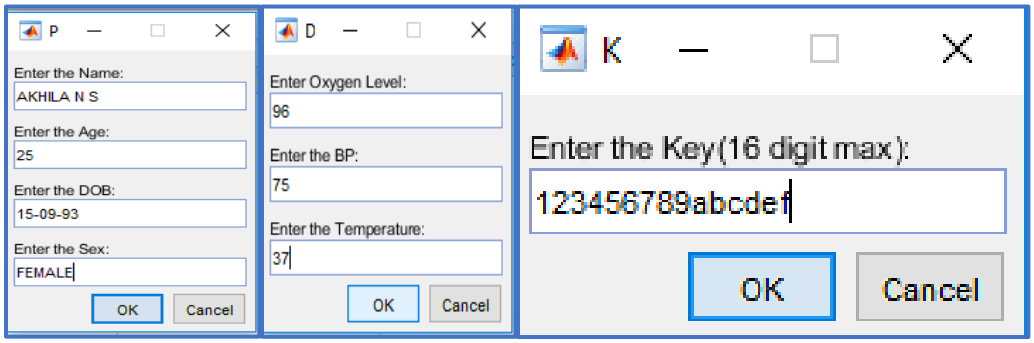

Fig. 8 Personal data and key

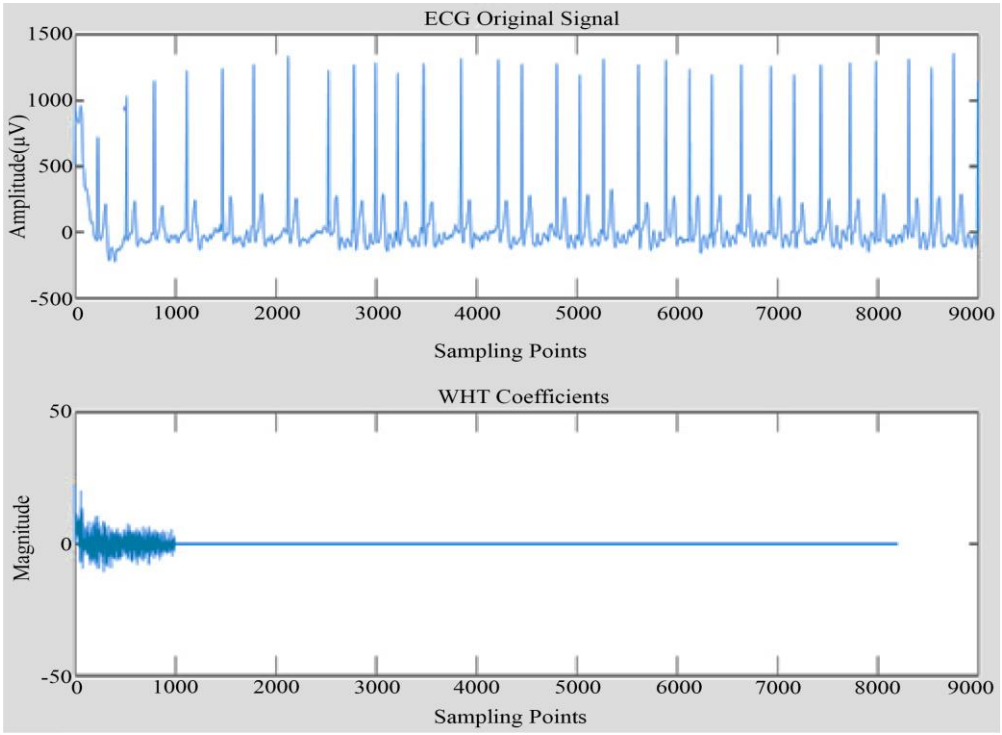

Fig. 9 FWHT applied on selected signal

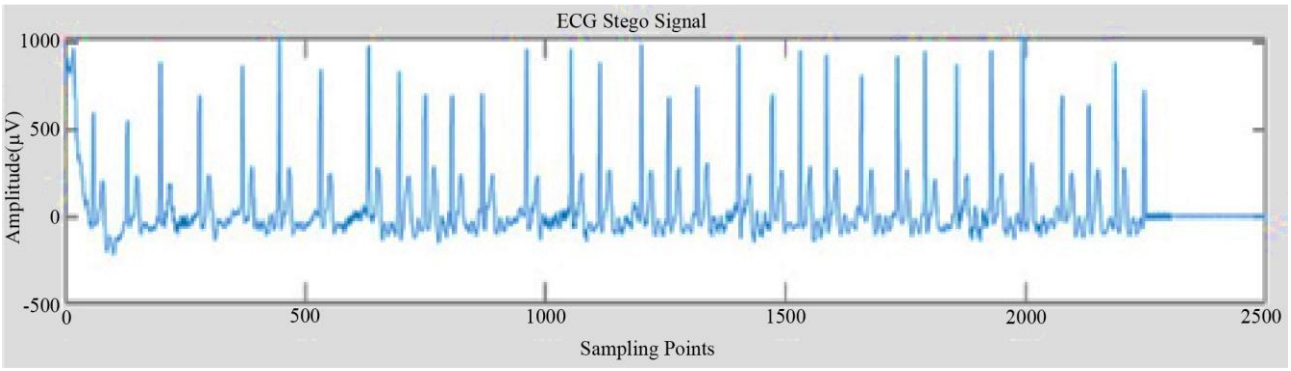

Fig. 10 Signal after embedding

Within this project, apart from the ECG signal, sensitive patient details, including name, age, gender, date of birth, and physiological metrics like temperature, blood pressure, and oxygen levels, are manually inputted. These additional details are essential for a comprehensive analysis and diagnosis of the disease. By integrating this personal information, healthcare providers can enhance their comprehension of the patient's overall health status, facilitating more precise and tailored medical care.

Figure 7 shows an anomalous ECG signal that necessitates additional examination by medical professionals. Figure 8 showcases the inputted personal information, encompassing the patient's details and the user-defined 16-byte key. Subsequently, the chosen signal undergoes FWHT for data embedding.

The result of FWHT on the selected signal is depicted in Figure 9. In this illustration, the removal of higher coefficients is executed, considering their lower significance in the signal reconstruction process. Eliminating these higher coefficients not only augments the signal's embedding capacity but also ensures the preserved fundamental characteristics of the reconstructed data. Fig.10 illustrates the stego signal, which represents the signal after embedding the personal data and physiological readings. Upon comparing it with the original signal, it is apparent that there is minimal variation. This indicates that the embedding process has been performed effectively, as the stego signal closely resembles the original signal regarding its waveform and characteristics. The minimal variation ensures that the diagnostic information contained in the signal remains intact and can be utilized for further analysis without significant distortion.

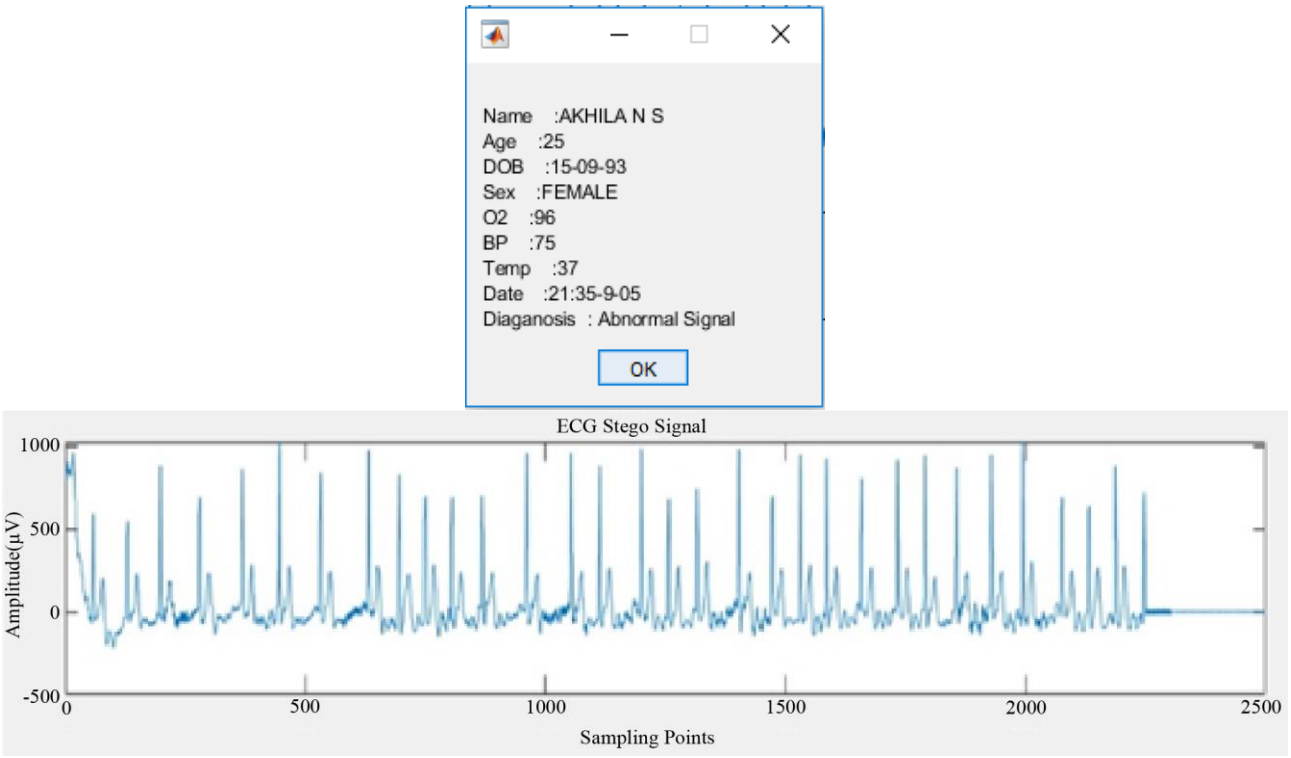

Fig. 11 Reconstructed original signal and personal data

4.5. Retrieval of Confidential Information

Fig.11 visually demonstrates the successful retrieval of the patient's private data. The confidential data contains delicate information, encompassing personal particulars and diagnostic details like temperature, blood pressure, and glucose levels.

In the figure, these data have been converted into bits and embedded within the transferred biomedical signal. Furthermore, the primary diagnosis of the ECG signal is showcased alongside the personal data. This indicates that the embedded personal data has been accurately extracted from the stego signal, allowing the authorized recipient to access the patient's private information and perform a comprehensive analysis for diagnosis and treatment purposes

4.6. Performance Comparison

The performance of the proposed method is evaluated by comparing it with two traditional classification methods: BPNN (Backpropagation Neural Network) and SVM (Support Vector Machine). Both BPNN and SVM are widely used supervised machine learning algorithms for classification tasks. In this evaluation, eight different features, including mean and standard deviation, are used as input for both BPNN and SVM classifiers. The results presented in Table 1 indicate that the BPNN and SVM classifiers show lower performance values compared to the LSTM classifier. The LSTM classifier achieves a high accuracy of 94.87%, outperforming the other two methods.

Table 1. Performance evaluation of different techniques

	LSTM	BPNN	SVM
Accuracy	94.87	80.53	87.73
Precision	94.80	80	87.86
Sensitivity	94	81	86.6
Specificity	94.79	81.42	87
F-score	94.8	80.49	87.65

The maximum PRD values measured were found to be 0.7%. This indicates that the difference between the stego and extracted signals is very small, always below 1%. Despite the biomedical signals' varying sample ranges and characteristics, the PRDs remain consistently low. This underscores that the proposed model exerts a negligible and consistent influence on the genuine transmitted biomedical signals. Furthermore, the model offers a robust solution for safeguarding the confidentiality of patient's private information and ensuring the authenticity of regularly collected signals.

The Bit Error Rate (BER) is also computed to evaluate the reliability of the extracted signal, affirming the model's effectiveness in upholding the integrity of the transmitted data. Equation (11) presents the PRD measure, where x represents the original signal, and y represents the stego or extracted signal.

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N} x_i^{\,2}}} \qquad (11)$$

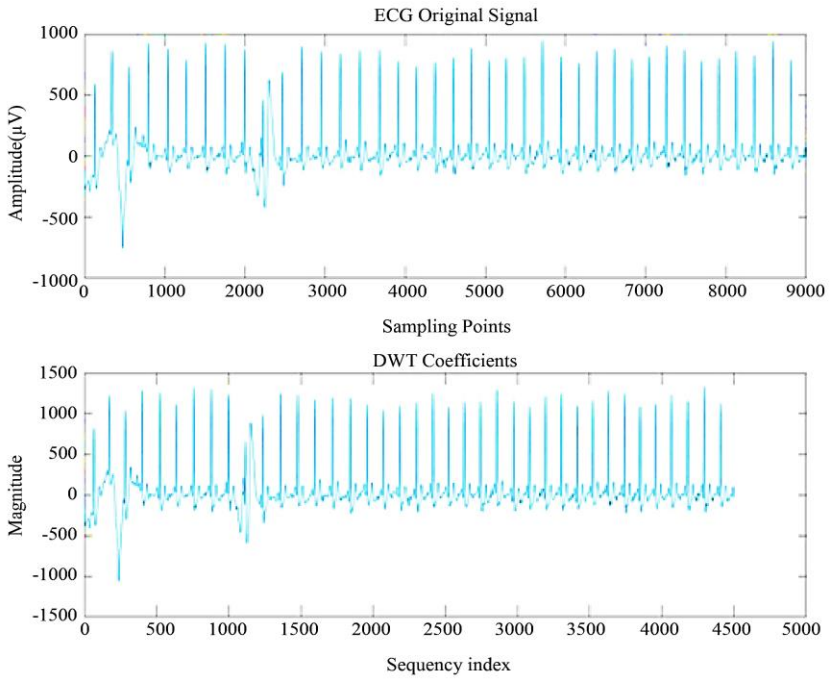

Fig. 12 DWT transform of the ECG signal

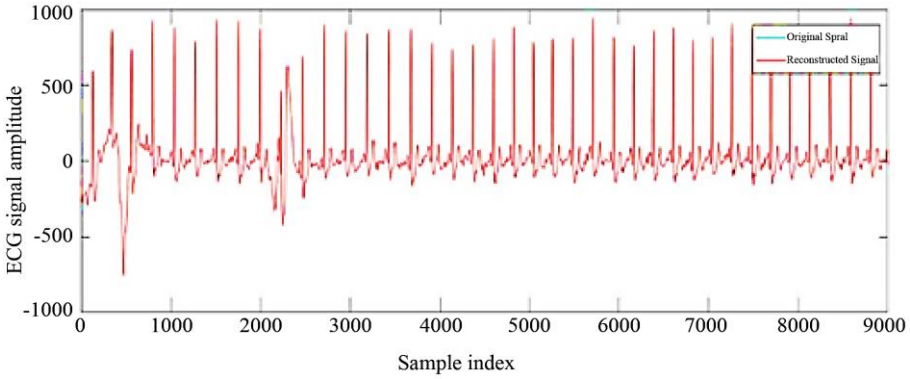

Fig. 13 Reconstruction of DWT transform

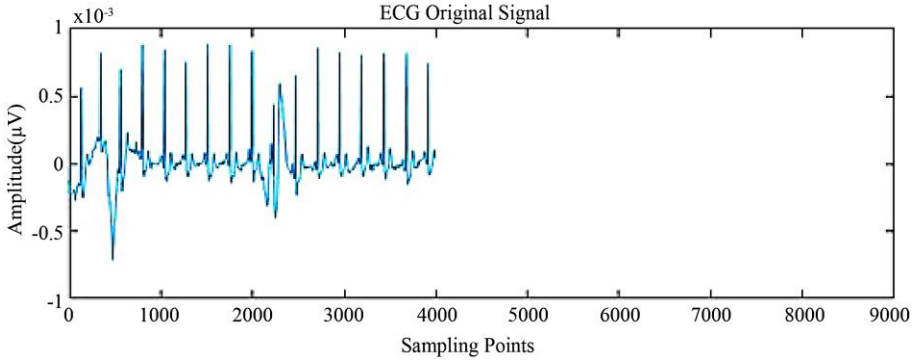

Fig. 14 Extracted signal after transmission using DWT transform

Comparisons were made between different types of transforms and their reconstruction methods. ECG signals, being large in size, often require efficient storage for future analysis and retrieval. Walsh-Hadamard transforms were found to be well-suited for this application due to their compression capabilities, which reduce storage space requirements. Furthermore, only less significant coefficients are employed within this algorithm during the embedding procedure. Additionally, Walsh-Hadamard transforms allow for rapid signal reconstruction. In contrast, wavelet transforms have some drawbacks despite their advantages. They are relatively expensive regarding both time (quadratic complexity) and operations (involving multiplications). Meanwhile, Fourier transforms concentrate the coefficients in a single value, and wavelet transforms retain the signal as it is. The average PRD results of wavelet transforms were found to be 0.93%, making them less suitable for this particular application. Fig.12 and Fig.13 depict the DWT transform and its reconstruction, while Fig.14 represents the extracted signal after the transmission process.

5. Conclusion

Nowadays, Point of Care (PoC) systems are becoming increasingly prevalent, and among the various biological signals used in healthcare, the electrocardiogram (ECG) stands out as the most widely used. ECG records the heart rate by detecting small electrical changes with the help of electrodes. Analyzing ECG signals plays a crucial role in diagnosing, understanding, and predicting cardiovascular disorders, which are responsible for a significant percentage of global deaths. However, diagnosing issues in ECG signals is a challenging task. A deep learning approach is applied to directly classify ECG signals at the patient's end to tackle this issue. Moreover, a unique and resilient 3D steganographic-based Walsh-Hadamard algorithm is employed to safeguard patients' confidential data within Point-of-Care (PoC) systems. This algorithm utilizes a key to convert FWHT values into a 3D order and integrates the private data within the biomedical signal. The embedding procedure strives for maximal capacity by utilizing FWHT to convert the signals into frequency-based coefficients and selectively employing less significant coefficients to reduce distortion. The key is employed to selectively encrypt the private information, rearrange the FWHT values into a random 3D template, and generate a dynamic hiding sequence in 3D to enhance security. The LSTM model demonstrates a high accuracy of 94.85%, surpassing the performance of SVM and BPNN. PRD results further confirm that FWHT outperforms Fourier and wavelet transforms in terms of preserving signal integrity. Extensive literature reviews and comparisons have been conducted to validate the proposed method. As a future scope of this work, the developed approach can be extended to other physiological signals, such as Photoplethysmogram (PPG) and Electroencephalogram (EEG) signals, opening up possibilities for broader application and research.

References

[1] Paul Yager, Gonzalo J. Domingo, and John Gerdes, "Point-of-Care Diagnostics for Global Health," *Annual Review of Biomedical Engineering*, vol. 10, pp. 107-144, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[2] B. Castro, D. Kogan, Amir B. Geva, "ECG Feature Extraction Using Optimal Mother Wavelet," *21st IEEE Convention of the Electrical and Electronic Engineers in Israel*, Tel-Aviv, Israel, pp. 346-350, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[3] Amjed Al-Fahoum, "Quality Assessment of ECG Compression Techniques Using a Wavelet-Based Diagnostic Measure," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 1, pp. 182-191, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[4] D.S. Venkateswarlu, K.S. Verma, and K.S.R.A. Murthy, "e Health Networking to Cater to Rural Health Care and Health Care for the Aged," *2007 9th International Conference on e-Health Networking, Application and Services*, Taipei, Taiwan, pp. 273-276, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[5] Wei-Bin Lee, and Chien-Ding Lee, "A Cryptographic Key Management Solution for Hipaa Privacy/Security Regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34-41, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[6] Farid Melgani, and Yakoub Bazi, "Classification of Electrocardiogram Signals with Support Vector Machines and Particle Swarm Optimization," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 5, pp. 667-677, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[7] Kai-mei Zheng, and Xu Qian, "Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms," *2008 International Conference on Computational Intelligence and Security*, Suzhou, China, pp. 295-299, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[8] Hêmin Golpîra, and Habibollah Danyali, "Reversible Blind Watermarking for Medical Images Based on Wavelet Histogram Shifting," *2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Ajman, United Arab Emirates, pp. 31-36, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] M. Natarajan, and Gayas Makhdumi., "Safeguarding the Digital Contents: Digital Watermarking," *DESIDOC Journal of Library Information Technology*, vol. 29, no. 3, pp. 29-35, 2009.[Google Scholar] [Publisher Link]

[10] Honggang Wang et al., "Resource-Aware Secure ECG Healthcare Monitoring through Body Sensor Network," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 12-19, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[11] Suneet Kaur et al., "Digital Watermarking of ECG Data for Secure Wireless Communication," *2010 International Conference on Recent Trends in Information, Telecommunication and Computing*, Kerala, India, pp. 140-144, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[12] Ayman Ibaida, Ibrahim Khalil, and Fahim Sufi, "Cardiac Abnormalities Detection from Compressed ECG in Wireless Telemonitoring Using Principal Components Analysis (PCA)," *2009 International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Melbourne, VIC, Australia, pp. 207-212, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[13] Shanxiao Yang, and Guangying Yang, "ECG Pattern Recognition Based on Wavelet Transform and BP Neural Network," *Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10)* pp. 246-249, 2010. [Google Scholar]

[14] V. Vijaya, K. Kishan Rao, and V. Rama, "Arrhythmia Detection through ECG Feature Extraction Using Wavelet Analysis," *European Journal of Scientific Research*, vol. 66, no. 3, pp. 441-448, 2011. [Google Scholar] [Publisher Link]

[15] Henning Perl et al., "Fast Confidential Search for Bio-Medical Data Using Bloom Filters and Homomorphic Cryptography," *2012 IEEE 8th International Conference on E-Science*, Chicago, IL, USA, pp. 1-8, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ming Li et al., "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131-143, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ayman Ibaida, and Ibrahim Khalil, "Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems," *IEEE Transactions on Bio-Medical Engineering*, vol. 60, no. 12, pp. 3322-3330, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[18] Alsharif Abuadbba, Ibrahim Khalil, and Mohammed Atiquzzaman, "Robust Privacy Preservation and Authenticity of the Collected Data in Cognitive Radi Network Walsh-Hadamard Based Steganographic Approach," *Pervasive and Mobile Computing*, vol. 22, pp. 58-70, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[19] Alsharif Abuadbba, and Ibrahim Khalil, "Walsh-Hadamard-Based 3-D Steganography for Protecting Sensitive Information in Point-of-Care," *IEEE Transactions on Bio-Medical Engineering*, vol. 64, no. 9, pp. 2186-2195, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[20] Ary L. Goldberger et al., "PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals," *American Heart Association*, vol. 101, no. 23, pp. 215-220, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[21] Gari D. Clifford et al., "AF Classification from a Short Single Lead ECG Recording: The PhysioNet/Computing in Cardiology Challenge 2017," *2017 Computing in Cardiology (CinC)*, Rennes, France, pp. 1-4, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[22] Bosun Hwang et al., "Deep ECGNet: An Optimal Deep Learning Framework for Monitoring Mental Stress Using Ultra Short-Term ECG Signals," *Telemedicine Journal and e-Health*, vol. 24, no. 10, pp. 753-772, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[23] Pranav Rajpurkar et al., "Cardiologist-Level Arrythmia Detection with Convolutional Neural Networks," *arXiv*, pp. 1-9, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[24] Kaiming He et al., "Deep Residual Learning for Image Recognition," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 770-778, 2016. [Google Scholar] [Publisher Link]

[25] Alex Graves, and Jürgen Schmidhuber, "Classification with Bidirectional LSTM and Other Neural Network Architectures," *Neural Networks*, vol. 18, no. 5-6, pp. 602-610, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[26] Nitish Srivastava et al., "Dropout: A Simple Way to Prevent Neural Networks from Overfitting," *Journal of Machine Learning Research*, pp. 1929-1958, 2014. [Google Scholar] [Publisher Link]

[27] Shuto Nagai, Daisuke Anzai, and Jianqing Wang, "Motion Artefact Removals for Wearable ECG Using Stationary Wavelet Transform," *Healthcare Technology Letters*, vol. 4, no. 4, pp. 138-141, 2017. [CrossRef] [Google Scholar] [Publisher Link]