IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 1, February, 2025, pp. 557-568
Journal homepage: http://iieta.org/journals/ts

An ECG Signal Encryption and Classification Using Sparse Autoencoder and Optimized Neural Network Techniques

Sumathi Shanmugasundaram*, Murukesh Chinnasamy, Lakshmi Sangeetha Annaman

Department of ECE, Velammal Engineering College, Chennai 600066, India

Corresponding Author Email: sumathiapece@gmail.com

https://doi.org/10.18280/ts.420147

Received: 8 May 2024
Revised: 2 August 2024
Accepted: 14 January 2025
Available online: 28 February 2025

Keywords:
healthcare data security, encryption, classification, deep learning, CNN, autoencoder, optimization

ABSTRACT

Secure transmission of patient diagnostic information is crucial in healthcare monitoring due to the inclusion of private user details. Electrocardiogram (ECG) signal is one of the most important medical signals that represents the vital signs of patients and immediate medications are provided by physicians based on the observation of ECG signals. Altering or tampering with such data leads to serious issues so it is essential to introduce proper security measures to enhance the data security. Encryption is one of the efficient approaches which is widely used for data security in various domains. However, the features of encryption methodologies are less explored in raw medical data applications. This research work introduces a novel method for encrypting and decrypting ECG signals by utilizing a sparse autoencoder combined with Chaotic Logistic Mapping to enhance data security. The classification module in this research employs a convolutional neural network to efficiently extract features and an optimized artificial neural network to classify the data. Experimental verification of proposed approach attains better classification accuracy of 96.6% which is much better than the existing classification techniques.

1. INTRODUCTION

The advancement of healthcare systems in the digital era incorporates numerous technical innovations, aiming to improve patient care through enhanced data security measures and reducing the frequency of conventional one to one diagnosis and treatment practices. Telecommunication systems, telemedicine systems are introduced to get suggestions from physicians even from remote locations. People can access the specialists in the particular field by simply sitting in home and transmitting their medical data through internet. Healthcare devices are equipped to collect and consolidate the samples at a periodic interval and provide the same to physicians at the time of analysis. However, the data transmission in telecommunication channels introduces serious security threats which is a major concern in the present situation. Healthcare data, which includes personal and private information, should only be accessible to physicians and not to unauthorized individuals.

The electrocardiography is an important element in healthcare systems to detect abnormalities in patients. The worldwide diagnostic procedure for electrocardiography is similar and securing Electrocardiogram (ECG) signals gains more attention specifically after implementation of EU general data protection regulation (GDPR). ECG signals include user sensitive information also it can be used as a biometric. ECG features can be used as a cryptographic key in a few applications like pseudo-random number generators, shift generators [1], etc. These sensitive data should be accessed only the authorized persons and to achieve this privacy preserving methods should be adapted before transmitting the information in the communication channel. Researchers are increasingly focusing on securing healthcare data by introducing various security measures, including authentication, access controls [2], and watermarking [3], etc. However, these authentication and access control practices can be compromised if the cryptographic key is discovered or guessed. So, to bring an extra effort to secure the data before transmission, encryption procedures are introduced so that even the access controls are known to intruder, they cannot able to retrieve the encrypted message.

Recent methods for encrypting ECG signals include the Advanced Encryption Standard (AES) [4, 5], Dynamic AES [6], Selective Encryption (SE) [7], Chaos-based encryption [8], Wavelet and Chaotically Huffman Code [9], Logistic mapping-based stream encryption [10], Lightweight selective encryption (LWSE) [11], etc. However, the research towards identifying potential encryption model for ECG signal encryption is still in progress. The major objective of this research work is to bring an efficient and secure ECG signal encryption using deep learning technique. Since the feature merits of deep learning techniques are observed in various domains for feature extraction and classification and it is less explored in the encryption process. Specifically, the autoencoder in the deep learning model is mostly used for image-based applications, and limited works have evolved for signal processing. Specifically, healthcare signal processing is not explored using autoencoders which is the novelty of this proposed research work.

In addition to encryption, classification is also performed in

this research work using optimized neural network. Various machine learning based ECG signal classification approaches are evolved which include support vector machines, random forests, decision trees, etc. [12, 13]. However, the feature extraction procedures adopted in those models lag in performance while selecting essential features. Similarly, if the classification model parameters are optimized then the performance of the classification models might get improvements. Considering these observations, in this research work for feature extraction, features of deep learning are utilized. Convolutional Neural Network (CNN) extracts the essential features from ECG signals. The extracted signals are processed using an optimized artificial neural network to categorize the patient status into normal, abnormal, Myocardial Infarction (MI), and History of MI. The major contribution of this research work is summarized as follows.

•We have presented a secure ECG encryption procedure for healthcare data transmission using a sparse auto-encoder with Chaotic Logistic Mapping.

•We have presented a classification model to detect the patient status from ECG signals using an optimized artificial neural network. The classification model incorporated the deep learning technique -CNN for efficient feature selection.

•We have presented an intense experimental analysis of the proposed encryption and classification model using a benchmark dataset

•We have presented a performance analysis of the proposed model with existing models to demonstrate better performance.

The remaining part of the article is structured as follows. A vast literature analysis is presented in section 2 by discussing the existing encryption and classification procedures in ECG signal analysis. The proposed encryption and classification model are presented in section 3. Experimental results and their relevant discussion are presented in section 4, and finally, the observations are concluded in section 5.

2. RELATED WORKS

An ECG signal encryption is performed along with compression to ensure data privacy as well as data quality. A singular value decomposition technique-based data compression is reported by Liu et al. [14] enhances the compression efficiency. In the encryption process, singular value decomposition is used to generate the orthogonal key matrix and it is multiplied with the ECG matrix. In such a way, the data has been secured through encryption and the quality has been improved through compression using the singular value decomposition technique. An asymmetric cryptographic technique reported by Chen et al. [15] protects the privacy of information in ECG signals using a hybrid entropy encoder. The presented hardware model includes a lossless compression and an encryption encoder along with an error correction coding unit, and QRS complexity detector. The complex information is calculated through a complexity detector and it is encrypted using a hybrid entropy encoder before compression. Further the compressed data is transmitted with enhanced security features.

Similar encryption and compression procedure for ECG signals are reported by Hameed et al. [16] includes discrete wavelet transform, Huffman coding for compression process, and cipher block chaining advanced encryption standard technique is presented for the encryption process. The presented approach enhances the data quality and secures the data from passive monitoring attacks and eavesdropping. The system uses the QRS complex in the ECG signal as an encryption element to secure information in body area networks [17]. The complexities are used to obtain the initial key and then a linear feedback shift register is used to obtain the keystream for the data encryption process. Minimum energy consumption and dynamic key updates are the observed features of the presented research work.

An ECG signal classification model [18] utilizes the abstract features of heartbeat, clustering algorithm, and a rule-based classifier for efficient signal analysis. The rhythm and morphological features are selected and then QRS clustering is employed to minimize the errors in the classification of arrhythmia diseases. A similar parametric feature-based ECG signal classification model [19] considers the amplitude, time duration, and interval features from the ECG adopting a clustering-based feature extraction procedure. The extracted features are classified using classifiers like KNN, SVM, and artificial neural network and identified that support vector machine provides better accuracy than other models. The feature extraction procedure [20] includes principal component analysis along with dynamic time warping to enhance the ECG signal classification process. The morphological and segment features are obtained through the combined approach and classified using support vector machine to classify four classes of arrhythmias supraventricular, ventricular, fusion of ventricular, and normal and normal beats. Improved sensitivity and positive predictivity are the merits of the presented approach.

The ECG classification model [21] includes two delta-sigma modulators and a random forest algorithm for feature extraction and classification. The essential features are extracted at a sampling rate of 250 Hz and classified using the random forest to detect two types of arrhythmias supraventricular ectopic beats and ventricular ectopic beats. Compared to other machine learning models, the presented approach attains better performance with minimum computation complexity and memory utilization. The reduce the latency and increase the processing speed of ECG signal classification using machine learning algorithms, a delayed error normalized LMS adaptive filter is presented in reference [22]. The presented filtering technique removes the unwanted white noises in the signal so that better features are extracted while applying Heart Rate Variability (HRV) based feature extraction process. Compared to other machine learning algorithms the performance of the support vector machine is satisfactory in the ECG signal analysis.

An ensemble multi-label classification model [23] classifies the ECG signals to detect cardiovascular disease. Classifiers such as binary relevance, multi-label KNN, multi-label twin support vector machine, multi-label hierarchical adaptive resonance associative map, classifier chain, Label Space Partitioning classifiers are incorporated as an ensemble model to classify the ECG signals. However, the threshold value used in the classification process affects the classification accuracy. To overcome this, a genetic algorithm is incorporated in the presented work to obtain the optimal threshold. A multilabel feature selection model [24] incorporates kernelized fuzzy rough sets to select the optimal features. The multi-objective optimization-based classification model classifies the optimal features based on sparsity constraints. The relation between the signal features and diseases is correlated in the classification process to attain maximum classification

accuracy. A multimodal fusion framework [25] converts the raw ECG signal into three images using recurrence plot, Gramian angular field, and Markov transition field. The obtained images are fused and provided as input to convolutional neural network model to extract the essential features. The obtained optimal features are classified using support vector machine to detect different distinct arrythmia conditions.

A probabilistic process neural network model [26] performs multichannel signal classification of ECG signals to detect ten types of diseases. The network model includes an input layer that handles the dynamic signals and these signals are aggregated in the hidden layer as a Spatio-temporal aggregation process finally the probabilistic outputs are obtained as classification results. The probabilistic classification is performed by the SoftMax classifier so that better classification results are obtained by the presented approach with minimum computation parameters. The ECG signal classification model [27] presents a parallel recurrent neural network for efficient signal analysis. The basic information processing is performed using gated recurrent units and finally, the features are classified using SoftMax classifier. Independent feature extraction and efficient classification with minimum loss is the observed merits of the presented research model.

Deep learning-based ECG signal classification [28] extracts the essential features from the signal through deep layers and performs classification using a fully connected feedforward neural network [29]. The presented model evaluates the arrhythmia database and attains better sensitivity and specificity than the existing state of art of techniques. A two-dimensional deep convolutional neural network model [30] classifies ECG signals to detect arrhythmia. The time-domain ECG signals considered for analysis include normal beat, left and right bundle branch block beat, and contraction beats of ventricular and atrial. Using short-time Fourier transform the signals are converted into spectrograms so that classification is performed based on the features obtained from the convolutional neural network. Improved accuracy without any preprocessing steps is the observed merit of the presented research model.

Other than conventional convolutional neural networks, few other versions of CNN models are incorporated for ECG signal analysis such as time-spatial convolutional neural networks [31],

Multi-perspective convolutional neural network (MPCNN) [32] to improve the classification performance and minimize the training parameters. Bidirectional long short-term memory (BiLSTM) is used as a classifier in references [33, 34] for ECG signal classification. To improve the performance of the classifier model, convolution layers are stacked with BiLSTM so that better accuracy is obtained in the classification process. Improved sensitivity, specificity, and F1-score are the feature merits of the presented research model.

From the above literature analysis, the following research gaps are identified.

•It is observed that encryption models rely on conventional procedures which increases the computation complexity.

•The traditional solutions which address encryption without considering data compression. Handling large volume of ECG data requires efficient data compression so that a better balance between encryption and data quality can be provided. But traditional methods fail to establish such balance due to negligence of data compression.

•Similarly, the most of the ECG signal analysis performed using machine learning algorithms. The performance metrics of conventional machine learning based models can be enhanced if optimal parameters are obtained for the classifier.

•Various encryption methods are utilized in ECG signals security however the utilization of deep learning techniques for ECG signal encryption is not explored fully. The cryptography methods that are used in recent times increase the computational complexity and not fully utilize the potential of deep learning algorithms.

•There is a huge gap in developing an integrated approach that handles both encryption as well as classification. Most of the existing studies mainly focus either on encryption or classification without optimizing the other.

•There is a lack of integrated approaches that handle both encryption and classification efficiently in one streamlined workflow. Most studies focus on one aspect without optimizing the other in the context of secure ECG data transmission.

Considering these research gaps, an encryption model that combines a sparse autoencoder with Chaotic Logistic Mapping is presented in this research work to secure ECG data. Additionally, an optimized classification model is proposed to enhance the ECG signal analysis accuracy. This integrated approach aims to provide strong data security and attain superior classification performance.

3. PROPOSED WORK

The proposed ECG signal analysis is presented in this section in two phases. In the first phase, the encryption model is presented and the optimized classification model is presented in the second phase. Techniques like sparse autoencoder and Chaotic Logistic Mapping are used in the encryption process. The use of sparse autoencoders for ECG signal encryption is relatively novel as sparse autoencoders are typically employed in image processing or noise reduction tasks. However, their application in encrypting ECG signals represents its uniqueness from standard encryption techniques like AES or RSA. Similarly, the integration of chaotic logistic mapping in the proposed work provides improved security features through its dynamic encryption which is sensitive to initial conditions. This makes the method highly resistant to standard cryptography attacks. The classification process of the proposed model includes the genetic algorithm and artificial neural network to classify ECG signals to detect the current status of the patient. The application of optimization techniques specifically genetic algorithms to fine-tune the parameters of an artificial neural network (ANN) for ECG signal classification is novel and it not only improves accuracy but also ensures that the model generalizes well on unseen data by preventing overfitting.

Figure 1 depicts the overview of the proposed encryption model, and Figure 2 shows the classification model.

The proposed model integrates both encryption and classification process in ECG signal analysis to ensure better signal security and accurate diagnosis of patient's conditions. The ECG signals are initially encrypted using sparse autoencoder which is combined with chaotic logistic mapping. This encrypted data protects the sensitive information of patients during transmission. In the classification phase, the encrypted data are initially decrypted and preprocessed to ensure the signal integrity and remove noise factors which

introduced in signals during transmission process. The preprocessed signals are then fed into convolutional neural network for feature extraction and then classified using an optimized neural network. This combines process ensures the better transition of data between decryption and classification, also it provides reliable diagnostic results without compromising the security.

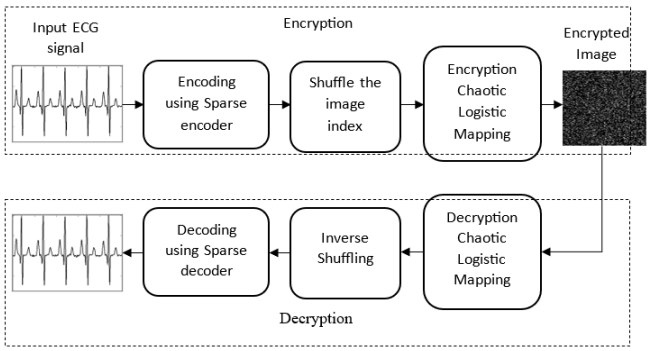

Figure 1. Overview of the proposed encryption process

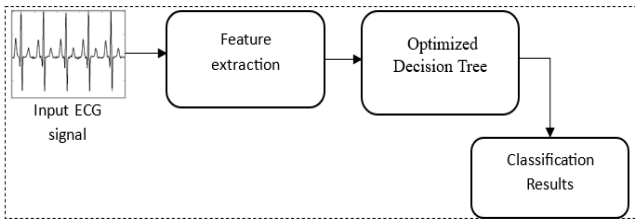

Figure 2. Overview of the proposed classification process

3.1 Encryption using sparse autoencoder and chaotic logistic mapping

The ECG signal encryption starts by encoding the input signal using sparse autoencoder. Generally, autoencoders are unsupervised learning algorithms which has the ability to handle and represent the large amount of unlabeled data. The encoding refers to the representation of middle layer with respect to the actual data as the input. The middle-hidden layers are used to decode the intermediate layer features so that actual input can be obtained at the output layer. The autoencoder reconstructs the signal considering the reconstruction error in the encoding and decoding process. Autoencoders reconstruct the signal without any supervisory measure since the features of the data can be learned automatically which avoids additional processing elements. The general structure of autoencoder is similar to feed-forward neural network so that the network is trained to learn the input features and produce the corresponding outputs rather than producing classification outputs.

The sparse autoencoder (SAE) in the research helps to reduce data redundancy and enhancing the efficiency when managing complex datasets. In the sparse autoencoder the majority of the hidden layer neurons will be inactive. This is because of the feasibly saturated condition of the neurons for most of the inputs. This results in the sparsity of features so that most of the elements of the features are considered as close to zero or zero. The sparsity is accomplished by the penalty term to mention the sparsity value. To obtain better clarity about sparse autoencoder the mathematical model is summarized in this section. Figure 3 depicts an illustration of sparse autoencoder with input, hidden and output layers.

Consider the input vector $n \in x^{D_n}$ and it is mapped by the autoencoder as a new vector $m \in x^{D^{(1)}}$. The new vector is expressed in terms of weight matrix and bias factors as follows.

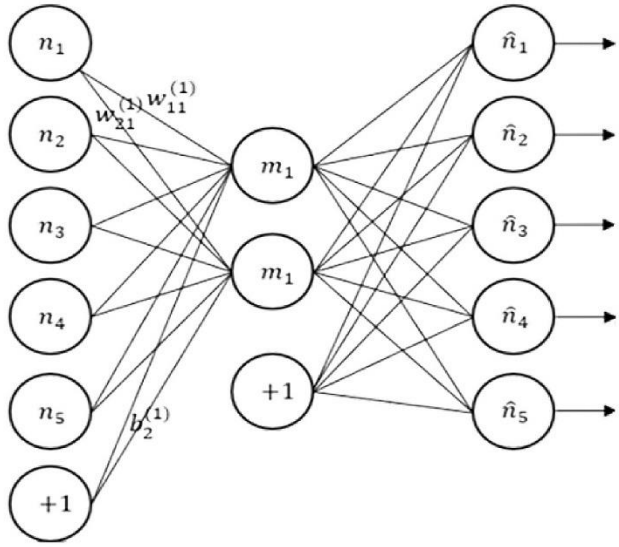

Figure 3. Sparse autoencoder

$$m^{(1)} = k^{(1)}\left(w^{(1)}n + \beta^{(1)}\right) \tag{1}$$

where, $k^{(1)}: x^{D^{(1)}} \rightarrow x^{D^{(1)}}$ represents the transfer function, the weight matrix is represented as $w^{(1)} \in x^{D^{(1)}}$ and the bias vector is represented as $\beta^{(1)} \in x^{D^{(1)}}$. The first layer of the autoencoder is represented using the superscript (1). In the next step the encoded representation m is transferred to reconstruct the input n by the decoder as per the following formulation.

$$\hat{n} = k^{(2)}\left(w^{(2)}n + \beta^{(1)}\right) \tag{2}$$

where, $k^{(2)}: x^{D^{(2)}} \rightarrow x^{D^{(2)}}$ represents the transfer function, the weight matrix is represented as $w^{(2)} \in x^{D^{(2)}}$ and the bias vector is represented as $\beta^{(2)} \in x^{D^{(2)}}$. The second layer of the autoencoder is represented using the superscript (2). In this stage, an adapted cost function is included in the autoencoder in the form of a regularization term to introduce the sparsity in the autoencoder. The activation functions are averaged to estimate the regularization term for each neuron i and it is expressed as:

$$\hat{\sigma}_i = \frac{1}{l}\sum_{j=1}^{l} m_i^{(1)}(n_j) \tag{3}$$

$$\hat{\sigma}_i = \frac{1}{l}\sum_{j=1}^{l} k\left(w_i^{(1)T} n_j + \beta_i^{(1)}\right) \tag{4}$$

where, the total number of training samples is represented as l, n_j indicates the input training sample, $w_i^{(1)T}$ represents the weight matrix of the first layer in transpose form, $\beta_i^{(1)}$

represents the neural network bias vector. For high output activation function the neuron will be fired however for low activation value, only small number of input samples will be processed by the neuron which motivates the autoencoder to learn the features. So, in this stage, a limitation term is included with the activation function output that encourages the neuron to learn from the limited features. Similarly, the other neurons are motivated to learn from the small features so that every neuron will be responsible for individual features of the inputs. In order to measure the relativity of the targeted activation function σ and the actual activation function $\hat{\sigma}$ a sparsity regularize value is introduced. The Kullback-Leibler divergence function that defines the difference between the distributions are formulated as:

$$\Omega_{Spars} = \sum_{i=1}^{D^{(1)}} KL(\sigma \parallel \hat{\sigma}_i) \tag{5}$$

$$\Omega_{Spars} = \sum_{i=1}^{D^{(1)}} \sigma \log \frac{\sigma}{\hat{\sigma}_i} + (1-\sigma) \log \left(\frac{1-\sigma}{1-\hat{\sigma}_i}\right) \tag{6}$$

where, KL represents the divergence function and σ represents the activation function. In order to make the distribution close to each other the cost function is decreased and it is expressed using mean square error as follows:

$$E = \frac{1}{L} \sum_{l=1}^{L} \sum_{v=1}^{V} \left[\left(N_{vl} + \hat{N}_{vl}\right)^2\right] + [\rho * \Omega_w] + \left[B * \Omega_{Spars}\right] \tag{7}$$

where, the first element in the equation indicates the mean square error, the second element indicates the layer regularization term added to the cost function and the third element indicates the sparse regularization. The layer regularization value is added to avoid the sparsity regularization value being small in the training process when there is an increase in weight and decrease in mapped vector m and it is expressed as:

$$\Omega_w = \frac{1}{2} \sum_{h}^{H} \sum_{j}^{l} \sum_{i}^{v} \left(w_{ij}^{(1)}\right)^2 \tag{8}$$

where, the hidden layers are represented as H, the total number of input samples is represented as L, the number of classes is represented as V.

The encoded input is shuffled in the next step as scrambling and shuffling are the basic and primary steps of encryption process. The encryption process can involve one or more actions like scrambling the data, shuffling it, or using a combination of both to enhance security. However, instead of scrambling, the row-column shuffling is widely preferred as it is simple, fast, and efficient. While shuffling the row-column, the input is considered as a matrix function with j rows and k columns. The secret key is generated by selecting two tables in which one table is used for shuffling the rows and another table is used for shuffling the columns. Based on the shuffle table the rows and columns are shuffled. Similarly, for column shuffling is also performed. A simple pseudo random number generator is used to explain the shuffling process as the attack is irrespective to the shuffling table and the function is mathematically expressed as:

$$x_{i+1} = x_i^2 + x_i + S \ (mod\ n) \text{ for } i = 0,1,2 \ldots \tag{9}$$

where, the random initial seed is represented as S, n indicates the large number. The row shuffling table for is mathematically formulated as:

$$a = x_i (mod\ h) \tag{10}$$

$$T_r(i) = a + z \tag{11}$$

where, T_r represents the row shuffling table, minimum non-negative integer is represented as z. As per Eq. (11), shuffling is performed for row i for the values $0,1,2..h-1$. Similarly, the column shuffle is also performed to enhance the security of the encryption process. Further, the shuffled data is encrypted using Chaotic Logistic Mapping. The mathematics behind the chaotic theory considers the dynamic behavior of the sensitive systems. Chaos theory defines that a minor variation in the initial condition will introduce serious uncorrelation in the final sequence. When it is applied for the encryption process the entire sequence will be unpredictable if a suitable bifurcation parameter is selected for the encryption. Compared to other encryption procedures, the chaotic theory is simple, impregnable, and computationally faster. The logistic map which produces two-dimensional chaotic sequences that are non-periodic is mathematically expressed as:

$$p_{(n+1)} = \mu p_n (1 - p_n) \tag{12}$$

where, the bifurcation parameter is represented as u and its range is from $1 < \mu < 4$ and the initial value is represented as $p_0$and the generated sequence elements are $\{p_1, p_2, p_3 \ldots p_n\}$. Generally, the bifurcation range is selected between $3.56 < \mu \leq 4$ to obtain a better chaotic nature. In a completely chaotic state, the logistic map can be used as a pseudo-random number generator. The methods of probability and statistics can also be used to understand the characteristics of chaotic sequences.

The doubling of sequences completes when the value $\mu = 3.569$ and the system becomes chaotic. For a small range of μ values the system exhibits periodic behavior and this region is called a periodic window.

In the periodic window, an intermittency property is exhibited by the logistic map which is similar to periodic behavior interrupted by the chaotic bursts. Lyapunov exponent method is used to determine the chaotic nature and it is explained using the following formulation:

$$\mathcal{L} = \frac{1}{n}\left(\ln\left|f'_\mu(p_1)\right| + \ln\left|f'_\mu(p_2)\right| + \cdots + \ln\left|f'_\mu(p_n)\right|\right) \tag{13}$$

where, the differentiation function of p is represented as f'_μ and the successive iterations are given as $p_1, p_2, \ldots, p_n$. The exponent function can be computed from the samples obtained from the near points. Bifurcation occurs in a system when the average Lyapunov exponent is zero. The encryption process using chaotic logistic mapping considers the image dimension and layers. Let us consider an image $I(x, y, \ell)$ in which x indicates the number of rows and y indicates the number of columns and the layer is represented as ℓ. A permutation process is applied in the encryption process followed by the

diffusion process. The diffusion process is illustrated in Figure 4. The image pixels are rearranged in the permutation process as follows:

$$p_i = [p \times 10^3] \, mod \, x \tag{14}$$

$$q_i = [q \times 10^3] \, mod \, y \tag{15}$$

where, p_i and q_i are the vectors which are obtained based on the condition given in Eq. (12). In the permutation process, the image exchanges its pixel with the vectors p_i and q_i. For the diffusion process, Eq. (12) is modified as follows to obtain the vector p_k and it is given as:

$$p_k = [p \times 10^{10}] \, mod \, 256 \tag{16}$$

where, the vector p_k and permutated matrix are processed to obtain the final results.

The results obtained from the diffusion process are stored in C_k. The process starts with the input vector $p_k$and matrix M_k with mod 256. The results are recombined with XOR along with the delay function D^{-2} and D^{-3}. The final expression is given as:

$$C_k = p_k Xor \big((M_k + p_k) mod 256\big) \ldots Xor C_k(D^{-3}) Xor C_k(D^{-2}) \tag{17}$$

The encryption process increases the diffusion level which increases the data security against cryptographic attacks.

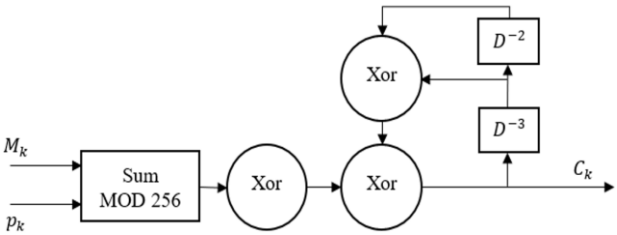

Figure 4. Diffusion process

3.2 Classification using optimized artificial neural network

The classification model presented in the proposed work includes Cat Swarm Optimization (CS) and Modified Decision Tree (MDT) Classifier for efficient classification. The parameters of DT are optimized by the CS to attain maximum classification accuracy and minimum loss. Before classification, the features are extracted using convolutional neural network so that optimal features are processed by the classification model to attain better performance.

3.2.1 Feature extraction using convolutional neural network (CNN)

Convolutional neural network (CNN) is a familiar deep learning architecture that includes an automated feature extraction process and a fully connected network for classification process. In this research work, the essential features are obtained using CNN and classified using genetic optimized artificial neural network instead of fully connected network to obtain maximum accuracy. Before feature extraction, the ECG signals are preprocessed since the data is collected generally from different environments which include frequency interference, EMG interference baseline drift, etc., So, it is essential to denoise the signal before classification. Generally, filters are used in the preprocessing steps to remove the noises. In this research work a wavelet transform approach is adopted before filtering. The wavelet transform decomposes the nonstationary signal into different frequency bands. Then an adaptive threshold filter is employed to select the wavelet function. These simple preprocessing steps are enough for the classification models as the essential features are directly extracted by the CNN model.

The convolutional neural network model used in the proposed work includes an input layer, three convolution layer and 3 pooling layer and a fully connected layer with a classifier. The convolution and pooling layer extract and maps the features from input to enhance the learning speed and avoids data overfitting. An average pooling layer is preferred in the proposed architecture instead of max-pooling to preserve the input data features. The architecture of the proposed CNN model used for feature extraction is depicted in Figure 5. The convolutional kernel convolutes the feature map which is obtained from the previous layer. Offsetting the convolution kernel and transferring it as a non-linear activation function the output of the convolution layer is obtained as follows:

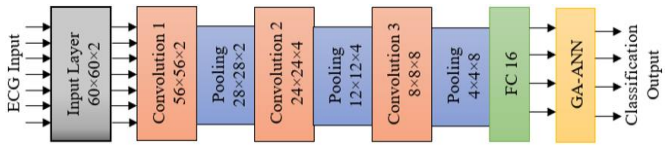

Figure 5. CNN architecture

$$y_i^{m,n} = f\left(b_i^{m,n} + \sum_{h=1}^{H} w_{h,i}^{m,n} * k_{i+h-1}^{m-1,n}\right) \tag{18}$$

where, the output of the i^{th} neuron in layer m is represented as $y_i^{m,n}$, the function $f()$ indicates the activation function. The offset of the neuron for layer m is represented as $b_i^{m,n}$ and the output of the neuron for layer $m-1$ is represented as $k_{i+h-1}^{m-1,n}$. The convolution kernel for m^{th} layer is represented as $w_{h,i}^{m,n}$.

The pooling layer in the proposed architecture included next to the convolution layer and it reduces the convolution layer output data dimension. This helps to reduce the network complexity and avoids overfitting. The pooling layer function is mathematically expressed as:

$$O_i^{m,n} = f\left(\delta_i^{m,n} pool\left(k_i^{m-1,n}\right) + b_i^{m,n}\right) \tag{19}$$

where, the i^{th} neuron output for layer m is represented as $O_i^{m,n}$, the function $f()$ indicates the activation function. The offset of the neuron for layer m is represented as $b_i^{m,n}$ and the sampling weight coefficient is represented as $\delta_i^{m,n}$. The pooling function is represented as $pool()$ and the output of the $m-1$ is represented as $k_i^{m-1,n}$. Generally, a dropout layer is included before the fully connected layer. Based on the probability in the CNN training process, few neurons will be disconnected in the dropout layer. This dropout prevents data overfitting and enhance the network generalization ability. The layer details of proposed CNN architecture are depicted in Table 1.

Further, the obtained features are classified using genetic optimized artificial neural network for maximum accuracy.

Table 1. Layer details of CNN model

Layers	Type	Parameters	Stride
Layer 1	Input layer	60×60×2	-
Layer 2	Conv 1	56×56×2	1
Layer 3	Pool 1	28×28×2	1
Layer 4	Conv 2	24×24×4	1
Layer 5	Pool 2	12×12×4	1
Layer 6	Conv 3	8×8×8	1
Layer 7	Pool 3	4×4×8	1
Layer 8	FC1	16	-

3.2.2 Genetic optimized artificial neural network

The feature benefits of artificial intelligence technique like artificial neural networks are explored by various researchers. Though ANN solves complex problems, the slow learning rate and local minima are the major demerits observed. In this research work, to overcome this optimization models are incorporated so that the weight and bias conditions of artificial neural networks are adjusted to obtain optimal performance. Figure 6 depicts the process flow of optimized Neural Network for ECG signal classification.

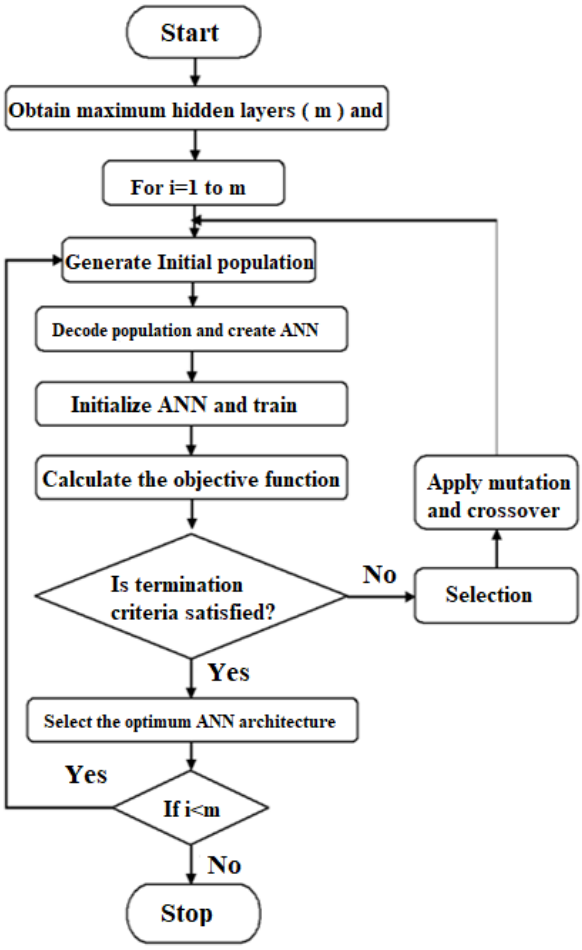

Figure 6. Process flow of proposed optimized ANN

So, an objective function or fitness function should be obtained. Here the reason for introducing optimization in the classification process is to obtain minimum cost network which should provide better performance with minimum computational parameters. Mean square error (MSE) is generally used as network objective function. The error function which controls the ANN performances are training error (e_{train}) and generalization error (e_{gen}). Along with these error function, architecture criterion ($\mathcal{A}_c$), solution consistency ($\mathcal{S}_c$) and learning time constants (L_t) are considered to obtain the objective function for the optimized ANN model. Mathematically the objective function is formulated as:

$$f_{obj} = \left[e_{train} + e_{gen}\right] * [\mathcal{A}_c] * [\mathcal{S}_c] * [L_t] \tag{20}$$

The training error (e_{train}) defines the memorization ability of the network. In the training process the learning progress of the network is measured and it is formulated as:

$$e_{train} = \frac{\sum_{i=1}^{n} |(y_{ti} - y_{ri})/y_{ti}|}{n} \tag{21}$$

where, the absolute relative error average is represented as e_{train} and the training data vector target value is represented as y_{ti}. The network response to the training data is represented as y_{ri} and the total number of training data samples is represented as n. The generalization error is the measure that defines the response-ability of the network. The response of the network for similar but not identical samples is defined in terms of generalization error. Mathematically the generalization error is formulated as:

$$e_{gen} = \frac{\sum_{i=1}^{m} |(y_{ti} - y_{ri})/y_{ti}|}{m} \tag{22}$$

where, the generalization error is represented as e_{gen} and the testing data vector target value is represented as y_{ti}. The network response to the testing data is represented as y_{ri} and the total number of training data samples is represented as m. The architecture criteria define the architecture through the penalty function. Since smaller architectures avoid data overfitting the training phase and increase the generalization ability. With minimum neurons and weight factors, the training process can be accelerated better than a conventional setup. So, in the architecture criteria, the weights and biases are considered and it is expressed as an exponential function as follows:

$$\mathcal{A}_c = \alpha e^{f(k)} \tag{23}$$

where, the total number of biases (k) and weights are represented as a function $f(k)$ and α is constant factor and its value is 1. The value of $f(k) = 0.01 \times k$. Though the generalization error is essential but it is not sufficient to persuade the network. since the generalization error provides the mean for all testing data. However, there may be a chance for low generalization error for special cases when the network prediction accuracy is lesser than the desired accuracy. To handle this situation a solution criterion is introduced in the objective function which computes the prediction error for the test data. When outlier cases are observed a penalty is applied which produces a high prediction error and based on that the network model is redirected to obtain accurate solutions using solution criteria. Mathematically the solution criteria are formulated as:

$$\mathcal{S}_c = 1 + \psi x + \varrho y \tag{24}$$

where, the test case average quality prediction is represented as x and the unacceptable quality prediction is represented as y. Two adjustment factors are used to define the attributes such

as ψ and ϱ and its values are considered as 0.33 and 1 respectively. The learning time constants are introduced considering the total epochs which required for training. This function is expressed as:

$$L_t = a * e + b \tag{25}$$

where, a and b are the linear function constants and its values are 2×10^{-5} and 1 respectively and the total training epoch is represented as e.

4. RESULTS AND DISCUSSION

MIT-BIH Arrythmia Database, open-source databases including Arrythmia Database, QT Database, and MIT-BIH Supraventricular Arrhythmia Database were used in this work. These databases are different in classes of beats, the volume of the dataset, number of individual volunteers. These databases consist of 2-lead recordings. Above all, they all have annotations for every single beat including the type of each beat. The proposed encryption and classification of ECG signal analysis performance is verified through simulation performed in MATLAB 2019 installed in an intel i5 processor 2.40 GHz with memory of 8GB. The simulation parameters for sparse autoencoder convolution neural network and artificial neural network are collectively presented in Table 2.

Table 2. Simulation parameter

Algorithm	Parameters	Range/Value
Sparse Autoencoder	Number of convolution layers	3
	Number of pooling layers	1-2
	Number of Hidden layers	1
	Total number of Neurons, Kernel size	256 & [3 3]
	Activation function	Log sigmoid
CNN	Number of convolution layers	3
	Number of pooling layers	3
	Number of Hidden layers	1-2
	Total number of Neurons, Kernel size	1,23,018 & [7 7]
	Activation function	ReLU
ANN	Number of convolution layers	5-10
	Number of pooling layers	2-4
	Number of Hidden layers	2 to requirement
	Total number of Neurons, Kernel size	1,22,000 & [5 5]
	Activation function	ReLU

The outputs obtained in the encryption process are depicted in Figure 7 which includes the encoded output, shuffled output, and encrypted output. The original ECG signal is encoded using the autoencoder and shuffled using row-column image shuffling.

Finally using chaotic logistic mapping, the shuffled image is encrypted. Results indicate that the encrypted image is looks like a noisy image which could not be decrypted by others without a proper authentication key.

The encrypted signal is decrypted by reversing the encryption procedure. Initially, decryption is performed using chaotic logistic mapping and the decrypted image is again shuffled through row-column shuffling procedure to obtain the encoded image. Finally, the decoding is performed using sparse autoencoder unit and the actual signal is retrieved without any losses. The decrypted output is depicted in Figure 8.

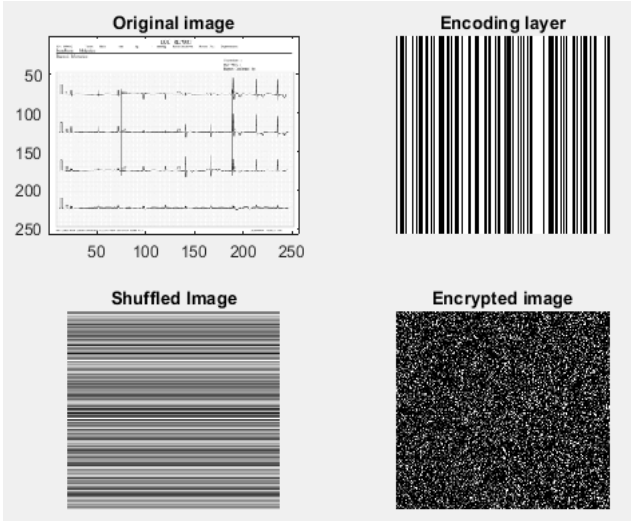

Figure 7. ECG signal encryption

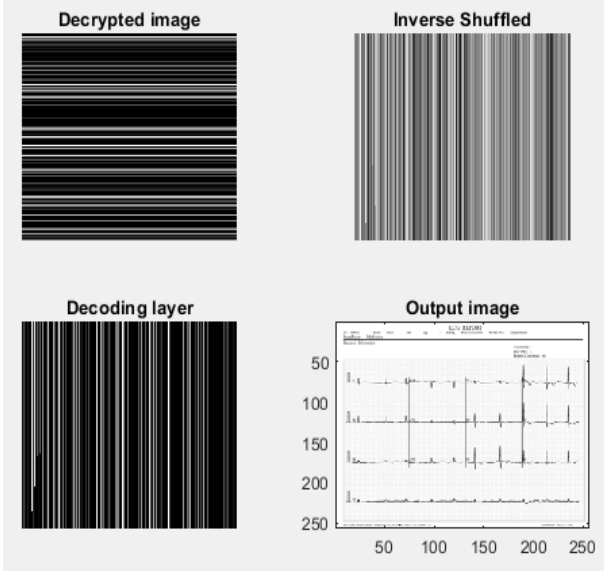

Figure 8. ECG signal decryption

The proposed encryption model performance is compared with the existing reversible data Hiding technique in terms of a number of changing pixel rate ($NPCR$), Structural Similarity Index (SSIM), and Peak to Signal to Noise Ratio (PSNR). The mathematical formulation used to calculate the above parameters is given as follows:

$$NPCR = \frac{\sum_{ij} D(i,j)}{m \times n} \times 100\% \tag{26}$$

$$SSIM(x,y) = \frac{(\mu_x\mu_y + s_1)(2\sigma_{xy} + s_2)}{(\mu_x^2 + \mu_y^2 + s_1)(\sigma_x^2 + \sigma_y^2 + s_2)} \tag{27}$$

$$PSNR = 10\log_{10}\left(\frac{255}{\sqrt{MSE}}\right)(\text{dB}) \tag{28}$$

$$MSE = \frac{1}{mn}\sum_{y=1}^{m}\sum_{x=1}^{n}\left(I(x,y) - I'(x,y)\right)^2 \quad (29)$$

where, m, n are the dimensions, $I(x,y)$ indicates the normal image, $I'(x,y)$ indicates the approximated version, the average of x and y is represented as μ_x and μ_y respectively. The variance of x and y is represented as σ_x^2 and σ_y^2. σ_{xy} represents the covariance factor and the stabilization factor is represented as s_1 and s_2.

The classification results of the proposed model using a genetically optimized artificial neural network is depicted in Figure 9. The proposed classification model is aimed to classify the ECG signal into four classes such as 'Patients that have abnormal heartbeat', 'Myocardial Infarction Patients heartbeat', 'Normal heartbeat', and 'Patients that have History of MI'.

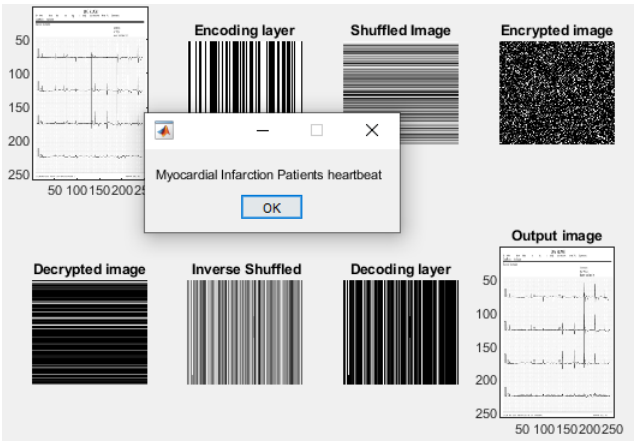

Figure 9. ECG signal classification

The experimentation is performed with 120 instances and the respective results are plotted in terms of confusion matrix. The actual and predicted classes for the four classes are depicted in Figure 10. For simple observation, class 1 is assigned for patients that have abnormal heartbeat', class 2 is assigned for 'Myocardial Infarction patient heartbeat', class 3 is assigned for 'Normal heartbeat' and class 4 is assigned for 'Patient that have a History of MI'.

		Predicted value			
		Class 1	Class 2	Class 3	Class 4
Actual value	Class 1	28	2	0	0
	Class 2	0	30	0	0
	Class 3	0	1	29	0
	Class 4	0	0	1	29

Figure 10. Confusion matrix

From the obtained values the parameters such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) values are summarized and depicted as a multi-class confusion matrix in Figure 11.

		TP	FP	FN	TN
Actual value	Class 1	28	0	2	90
	Class 2	30	3	0	87
	Class 3	29	1	1	89
	Class 4	29	0	1	90

Figure 11. Multi-class confusion matrix

Based on the parameters obtained the performance of the proposed classification model is evaluated in terms of accuracy, sensitivity, specificity, precision, and F1-score. The mathematical formulations for the classification parameters are given as follows.

$$\text{Accuracy } (Acc) = \frac{True\ Positive + True\ Negative}{Sum\ of\ all\ values} \quad (30)$$

$$\text{Sensitivity} = \frac{True\ Positive}{True\ Positive + False\ negative} \quad (31)$$

$$\text{Specificity} = \frac{True\ Negative}{True\ Negative\ + False\ Positive} \quad (32)$$

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (33)$$

$$\text{F1} - \text{score} = 2 \times \frac{Precision * Recall}{Precision + Recall} \quad (34)$$

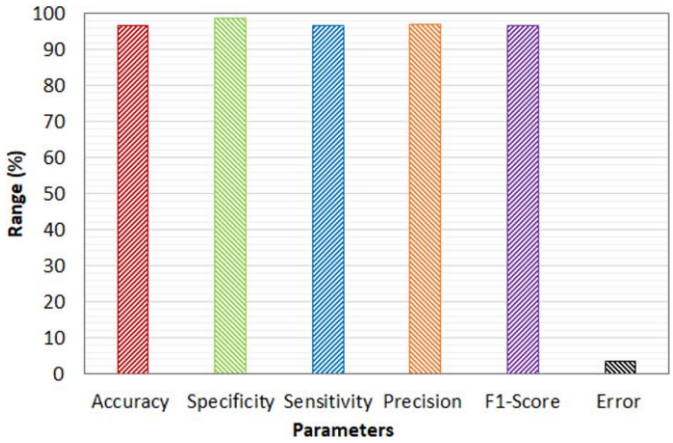

Figure 12. Performance metrics

The values obtained for the above parameters in the proposed model experimentation are depicted in Figure 12. It is observed from the figure maximum accuracy of 96.6% is obtained in the classification process which indicates that the proposed model effectively classifies the ECG signal and identifies the correct status. However, the loss in accuracy is due to the variations in the input signal.

The error percentage obtained by the proposed model is 0.033 which is 3.3%. The specificity and sensitivity obtained by the proposed model are 98.8% and 96.66% respectively. Similarly, the obtained precision and F1-score are 96.89% and 96.69% respectively. Results indicate the performance of the proposed model is quite better in terms of all the parameters.

Table 3 depicts the performance comparative analysis of the proposed model with existing models like support vector machine, K-Nearest Neighbor, Random Forest, LSTM, Ensemble SVM, Genetic with ELM. The results are obtained from the research works of Pandey et al. [35] and Diker et al. [36]. The results clearly depict the proposed optimized artificial neural network (ANN) model's better performance over traditional models in ECG signal classification. With a better sensitivity of 96.66% and specificity of 98.88% the proposed model outperforms existing Support Vector Machines which obtain 54.42% as sensitivity and 91.12% as specificity. Similarly, when compared to Random Forests which attained 53.28% as sensitivity, and 90.45% as

specificity the proposed model highlights its superior ability in correctly identify true positives and true negatives. When compared with advanced models like Ensemble SVM which attains 65.26% as sensitivity and 93.25% as specificity the proposed model performs better. In the case of LSTM which attained 48.09% as sensitivity and 87.95% as specificity the proposed ANN exhibits its higher performances by reducing false positives and negatives.

The precision and F1-score of the proposed optimized ANN exhibited in Table 3 highlight the maximum performances as 96.89% and 96.69% respectively which is significantly better than the existing methods. The existing SVM model attained precision of 51.26% and an F1-score of 52.82% while Random Forests model exhibited 56.24% precision and 53.15% as F1-score which is lesser than the proposed optimized ANN. Similarly, the advanced models like Ensemble SVM which attains 69.11% as precision, 66.24% as F1-score, and LSTM which attains 59.81% as precision and 53.31 as F1-score is lesser than the proposed model. The Genetic with ELM model attained results 93.72% as precision and 96.77% as F1-score, yet it is lesser than the proposed mode. From the results given in Table 3, it can be observed that the proposed classification model exhibits the maximum performance in terms of accuracy compared to all the other conventional classification models. Specifically, the proposed model's accuracy of 96.6% highlights its better classification performance over existing models like kNN, and SVM which attain lower accuracies like 72.56% and 90.09%. The accuracies of LSTM, RF, Ensemble SVM, and Genetic with ELM are 92.16%, 93.45%, 94.40%, and 95.0% which is approximately 5%, 4%, 3% and 2% lesser than the proposed model. The optimized ANN in the proposed model not only increases accuracy but also enhances the model's ability to generalize across different ECG signal types without overfitting.

Table 3. Performance comparative analysis with existing works

Algorithms	Sensitivity (%)	Specificity (%)	Precision (%)	F1-score (%)	Accuracy (%)
Support vector machine	54.42	91.12	51.26	52.82	90.09
K-Nearest Neighbor	49.09	83.96	37.58	39.16	72.56
Random Forest	53.28	90.45	56.24	53.15	93.45
LSTM	48.09	87.95	59.81	53.31	92.16
Ensemble SVM	65.26	93.25	69.11	66.24	94.40
Genetic with ELM	100	80.00	93.72	96.77	95.00
Proposed optimized ANN	96.66	98.88	96.89	96.69	96.66

5. CONCLUSION

This research work presents a novel encryption and classification of ECG signal using a sparse autoencoder, chaotic logistic mapping and genetically optimized artificial neural network. The proposed encryption procedure includes the deep features through a sparse autoencoder which enhances the encryption efficiency. The chaotic logistic mapping encrypts the shuffled sparse encoded ECG signal and the genetically optimized artificial neural network efficiently classifies the signal into four classes. The experimental results of the proposed model demonstrate better performance in terms NPCR and PSNR for encryption and accuracy for the classification process. Conventional reversible data hiding is compared with the proposed encryption model to validate the superior performance similarly proposed genetically optimized artificial neural network performance is compared with existing state of art techniques to validate the superior performances. Future work could explore hybrid encryption algorithms to potentially improve the security performance demonstrated in this study.

REFERENCES

[1] Moosavi, S.R., Nigussie, E., Levorato, M., Virtanen, S., Isoaho, J. (2017). Low-latency approach for secure ECG feature based cryptographic key generation. IEEE Access, 6: 428-442. https://doi.org/10.1109/ACCESS.2017.2766523

[2] Camara, C., Peris-Lopez, P., De Fuentes, J.M., Marchal, S. (2020). Access control for implantable medical devices. IEEE Transactions on Emerging Topics in Computing, 9(3): 1126-1138. https://doi.org/10.1109/TETC.2020.2982461

[3] Bhardwaj, R. (2022). Hiding patient information in medical images: An encrypted dual image reversible and secure patient data hiding algorithm for E-healthcare. Multimedia Tools and Applications, 81: 1125-1152. https://doi.org/10.1007/s11042-021-11445-3

[4] Arul Murugan, C., KarthigaiKumar, P. (2023). Survey on image encryption schemes, bio cryptography and efficient encryption algorithms. Mobile Networks and Applications, 28(4): 1385-1390. https://link.springer.com/article/10.1007/s11036-018-1058-3

[5] Pawar, K., Naiknaware, D. (2018). AES encrypted wavelet based ECG steganography. International Journal of Engineering and Techniques, 4(3): 23-29.

[6] Xu, H., Hua, K. (2016). Secured ECG signal transmission for human emotional stress classification in wireless body area networks. EURASIP Journal on Information Security, 2016: 5. https://doi.org/10.1186/s13635-015-0024-x

[7] Qiu, H., Qiu, M., Lu, Z. (2020). Selective encryption on ECG data in body sensor network based on supervised machine learning. Information Fusion, 55: 59-67. https://doi.org/10.1016/j.inffus.2019.07.012

[8] Mboupda Pone, J.R., Çiçek, S., Takougang Kingni, S., Tiedeu, A., Kom, M. (2020). Passive–active integrators chaotic oscillator with anti-parallel diodes: Analysis and its chaos-based encryption application to protect electrocardiogram signals. Analog Integrated Circuits and Signal Processing, 103: 1-15. https://doi.org/10.1007/s10470-019-01557-0

[9] Raeiatibanadkooki, M., Quchani, S.R., KhalilZade, M., Bahaadinbeigy, K. (2016). Compression and encryption of ECG signal using wavelet and chaotically Huffman code in telemedicine application. Journal of medical systems, 40: 73. https://doi.org/10.1007/s10916-016-

0433-5
[10] Wang, J., Han, K., Fan, S., Zhang, Y., et al. (2020). A logistic mapping-based encryption scheme for wireless body area networks. Future Generation Computer Systems, 110: 57-67. https://doi.org/10.1016/j.future.2020.04.002
[11] Sivasangari, A., Bhowal, S., Subhashini, R. (2019). Secure encryption in wireless body sensor networks. Emerging Technologies in Data Mining and Information Security, 3: 679-686. https://doi.org/10.1007/978-981-13-1501-5_60
[12] Wasimuddin, M., Elleithy, K., Abuzneid, A.S., Faezipour, M., Abuzaghleh, O. (2020). Stages-based ECG signal analysis from traditional signal processing to machine learning approaches: A survey. IEEE Access, 8: 177782-177803. https://doi.org/10.1109/ACCESS.2020.3026968
[13] Satija, U., Ramkumar, B., Manikandan, M.S. (2017). Automated ECG noise detection and classification system for unsupervised healthcare monitoring. IEEE Journal of Biomedical and Health Informatics, 22(3): 722-732. https://doi.org/10.1109/jbhi.2017.2686436
[14] Liu, T.Y., Lin, K.J., Wu, H.C. (2017). ECG data encryption then compression using singular value decomposition. IEEE Journal of Biomedical and Health Informatics, 22(3): 707-713. https://doi.org/10.1109/jbhi.2017.2698498
[15] Chen, S.L., Tuan, M.C., Lee, H.Y., Lin, T.L. (2017). VLSI implementation of a cost-efficient micro control unit with an asymmetric encryption for wireless body sensor networks. IEEE Access, 5: 4077-4086. https://doi.org/10.1109/ACCESS.2017.2679123
[16] Hameed, M.E., Ibrahim, M.M., Abd Manap, N., Mohammed, A.A. (2020). A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES. Future generation computer systems, 111: 829-840. https://doi.org/10.1016/j.future.2019.10.010
[17] Bai, T., Lin, J., Li, G., Wang, H., et al. (2019). A lightweight method of data encryption in BANs using electrocardiogram signal. Future Generation Computer Systems, 92: 800-811. https://doi.org/10.1016/j.future.2018.01.031
[18] Teijeiro, T., Félix, P., Presedo, J., Castro, D. (2016). Heartbeat classification using abstract features from the abductive interpretation of the ECG. IEEE Journal of Biomedical and Health Informatics, 22(2): 409-420. https://doi.org/10.1109/jbhi.2016.2631247
[19] Yang, H., Wei, Z. (2020). Arrhythmia recognition and classification using combined parametric and visual pattern features of ECG morphology. IEEE Access, 8: 47103-47117. https://doi.org/10.1109/ACCESS.2020.2979256
[20] Chen, X., Wang, Y., Wang, L. (2018). Arrhythmia recognition and classification using ECG morphology and segment feature analysis. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 16(1): 131-138. https://doi.org/10.1109/tcbb.2018.2846611
[21] Kung, B.H., Hu, P.Y., Huang, C.C., Lee, C.C., Yao, C.Y., Kuan, C.H. (2020). An efficient ECG classification system using resource-saving architecture and random forest. IEEE Journal of Biomedical and Health Informatics, 25(6): 1904-1914. https://doi.org/10.1109/jbhi.2020.3035191
[22] Venkatesan, C., Karthigaikumar, P., Paul, A., Satheeskumaran, S., Kumar, R. (2018). ECG signal preprocessing and SVM classifier-based abnormality detection in remote healthcare applications. IEEE Access, 6: 9767-9773. https://doi.org/10.1109/ACCESS.2018.2794346
[23] Sun, Z., Wang, C., Zhao, Y., Yan, C. (2020). Multi-label ECG signal classification based on ensemble classifier. IEEE Access, 8: 117986-117996. https://doi.org/10.1109/ACCESS.2020.3004908
[24] Li, Y., Zhang, Z., Zhou, F., Xing, Y., Li, J., Liu, C. (2021). Multi-label classification of arrhythmia for long-term electrocardiogram signals with feature learning. IEEE Transactions on Instrumentation and Measurement, 70: 2512611. https://doi.org/10.1109/TIM.2021.3077667
[25] Ahmad, Z., Tabassum, A., Guan, L., Khan, N.M. (2021). ECG heartbeat classification using multimodal fusion. IEEE Access, 9: 100615-100626. https://doi.org/10.1109/ACCESS.2021.3097614
[26] Feng, N., Xu, S., Liang, Y., Liu, K. (2019). A probabilistic process neural network and its application in ECG classification. IEEE Access, 7: 50431-50439. https://doi.org/10.1109/ACCESS.2019.2910880
[27] Xu, S., Li, J., Liu, K., Wu, L. (2019). A parallel GRU recurrent network model and its application to multi-channel time-varying signal classification. IEEE Access, 7: 118739-118748. https://doi.org/10.1109/ACCESS.2019.2936516
[28] Xu, S.S., Mak, M.W., Cheung, C.C. (2018). Towards end-to-end ECG classification with raw signal extraction and deep neural networks. IEEE Journal of Biomedical and Health Informatics, 23(4): 1574-1584. https://doi.org/10.1109/jbhi.2018.2871510
[29] Zhai, X., Tin, C. (2018). Automated ECG classification using dual heartbeat coupling based on convolutional neural network. IEEE Access, 6: 27465-27472. https://doi.org/10.1109/ACCESS.2018.2833841
[30] Huang, J., Chen, B., Yao, B., He, W. (2019). ECG arrhythmia classification using STFT-based spectrogram and convolutional neural network. IEEE Access, 7: 92871-92880. https://doi.org/10.1109/ACCESS.2019.2928017
[31] Meng, L., Ge, K., Song, Y., Yang, D., Lin, Z. (2021). Long-term wearable electrocardiogram signal monitoring and analysis based on convolutional neural network. IEEE Transactions on Instrumentation and Measurement, 70: 2507711. https://doi.org/10.1109/TIM.2021.3072144
[32] Niu, J., Tang, Y., Sun, Z., Zhang, W. (2019). Inter-patient ECG classification with symbolic representations and multi-perspective convolutional neural networks. IEEE Journal of Biomedical and Health Informatics, 24(5): 1321-1332. https://doi.org/10.1109/jbhi.2019.2942938
[33] Nurmaini, S., Darmawahyuni, A., Rachmatullah, M.N., Effendi, J., Sapitri, A.I., Firdaus, F., Tutuko, B. (2021). Beat-to-beat electrocardiogram waveform classification based on a stacked convolutional and bidirectional long short-term memory. IEEE Access, 9: 92600-92613. https://doi.org/10.1109/ACCESS.2021.3092631
[34] Altuve, M., Hernández, F. (2021). Multiclass classification of cardiac rhythms on short single lead ECG recordings using bidirectional long short-term

memory networks. IEEE Latin America Transactions, 19(7): 1207-1216. https://doi.org/10.1109/TLA.2021.9461850
[35] Pandey, S.K., Janghel, R.R., Vani, V. (2020). Patient specific machine learning models for ECG signal classification. Procedia Computer Science, 167: 2181-2190. https://doi.org/10.1016/j.procs.2020.03.269
[36] Diker, A., Avci, D., Avci, E., Gedikpinar, M. (2019). A new technique for ECG signal classification genetic algorithm Wavelet Kernel extreme learning machine. Optik, 180: 46-55. https://doi.org/10.1016/j.ijleo.2018.11.065