

Article

Versatile Machine Learning-Based Authentications by Using Enhanced Time-Sliced Electrocardiograms

Yi Zhao  and Song-Kyoo Kim * 

Faculty of Applied Sciences, Macao Polytechnic University, Macao SAR, China

* Correspondence: amang@mpu.edu.mo

Abstract: This paper addresses the enhancement of modern security through the integration of electrocardiograms (ECGs) into biometric authentication systems. As technology advances, the demand for reliable identity authentication systems has grown, given the rise in breaches associated with traditional techniques that rely on unique biological and behavioral traits. These techniques are emerging as more reliable alternatives. Among the biological features used for authentication, ECGs offer unique advantages, including resistance to forgery, real-time detection, and continuous identification ability. A key contribution of this work is the introduction of a variant of the ECG time-slicing technique that outperforms existing ECG-based authentication methods. By leveraging machine learning algorithms and tailor-made compact data learning techniques, this research presents a more robust, reliable biometric authentication system. The findings could lead to significant advancements in network information security, with potential applications across various internet and mobile services.

Keywords: authentication; biomedical signal processing; electrocardiogram (ECG); identification; machine learning; statistical learning; compact data learning



Citation: Zhao, Y.; Kim, S.-K.

Versatile Machine Learning-Based Authentications by Using Enhanced Time-Sliced Electrocardiograms.

Information **2024**, *15*, 187. <https://doi.org/10.3390/info15040187>

Academic Editors: Gholamreza Anbarjafari (Shahab) and Zahir M. Hussain

Received: 9 February 2024

Revised: 26 March 2024

Accepted: 27 March 2024

Published: 29 March 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Amid the swift advancement of internet technology, the prominence of network information security has surged. Predominant concerns within the sphere of information security encompass identity theft, privacy violations, false identities, and fraudulent transactions [1]. As a result, the exploration into dependable identity authentication systems has escalated in significance. Such systems can be broadly deployed across internet and mobile services to fortify user information and data security [2]. Identity authentication constitutes a vital component of security infrastructure development, encompassing the verification of identity, devices, or other characteristics of system user access, which is a fundamental requirement for system resource access [3,4]. Conventional authentication systems commonly utilize techniques like passwords, PIN codes, and tokens [5]. Yet, these methods are vulnerable to breaches and theft by hackers. Upon successful infiltration of the authentication via stolen passwords or tokens, intruders gain full access to system resources, presenting a considerable risk to system security [6]. In the contemporary internet landscape, conventional authentication methods fall short of fulfilling system security needs. Consequently, biometric-based authentication systems are progressively supplanting traditional ones. Biometric technology leverages the analysis of unique biological traits to autonomously authenticate and confirm personal identity [2,6]. Personal biometric indicators can be classified into biological and behavioral traits [7,8]. Physiological attributes encompass technologies associated with biological features like facial recognition, fingerprints, palm prints, DNA, and electrocardiograms (ECG) [6–9]. Behavioral attributes incorporate technologies related to human behavioral traits, including voice recognition, signature recognition, and gait analysis [6–8]. Given their uniqueness to each individual, biometric attributes serve as an effective and ideal authentication technology.

Biometric authentication systems typically use biological features such as fingerprints, irises, and faces for identity authentication [10,11]. Although these biological features are unique and stable, they also have technical applicability and robustness issues against spoofing attacks [10]. Fingerprint and face recognition are the most widely used identification technologies in biometric identification, but these biological features are also relatively easy to replicate [7–10]. For example, technologies such as silicone fingerprints, facial photos, and face masks can be used to deceive biometric identification systems [10]. Iris recognition is a safe and reliable biometric identification technology, but due to the manufacturer's consideration of the cost of identification equipment, the iris recognition device detection threshold is low and cannot reach a high enough security level [11]. Moreover, the iris recognition process is considered invasive and uncomfortable [10]. With the rapid development of artificial intelligence technology, the weaknesses of these biological features are more exposed, making the identification system more vulnerable to spoofing attacks [9]. Therefore, applying continuous biometric authentication methods to biometric authentication systems for identity authentication has been considered [9,12]. The electrocardiogram (ECG) has received widespread attention as a continuous biological feature and has gradually been applied to biometric authentication systems [9,10,13]. The ECG signal traces the electrical changes that occur in the heart during the cardiac cycle by placing a non-invasive sensor outside the heart [9,10,13,14]. Compared with other biological authentication features such as fingerprints, faces, and irises, the ECG has unique advantages in terms of being difficult to fake, offering real-time detection of living bodies, and having a continuous identification ability [9,15,16]. The scope of this research encompasses the selection of the optimal machine learning (ML) algorithm from several ML algorithms via an evaluation. Additionally, an enhanced time-slicing technique for ECG signals is newly suggested and its performance was assessed through comparison with previous studies [15,17,18]. This research is a novel and practical expansion of the tailor-made compact learning (CDL) approach [19,20], which is particularly relevant for the design of innovative ML-based biometric authentication systems.

The remainder of this article is segmented into five sections. Section 2 delves into the theoretical underpinnings, including tailor-made compact data, potential machine learning (ML) algorithms, and ML performance measures for assessing authentication systems. Section 3 introduces a use case for a specific authentication scenario [15]. This section also outlines the fundamentals of ECG authentication systems, which are based on a variety of ML algorithms and tailor-made compact data learning techniques. The optimal ML algorithm for the ECG-based authentication system is chosen from several candidate ML algorithms in Section 4. Section 5 showcases the crux of this research: a variant of the ECG time-slicing technique that outperforms other existing ML-based ECG authentication methods. Finally, the novel authentication system and its contributions are encapsulated in Section 6.

2. Theoretical Background

This section provides readers with a comprehensive understanding of the theoretical background that forms the backbone of this innovative system. The fundamentals of this research rest on three pillars: tailor-made compact data learning, candidate machine learning methods, and machine learning performance measures. The base of tailor-made compact data learning is introduced as the first pillar. The second pillar represents the candidate machine learning algorithms to apply the time-slicing techniques. The final pillar comprises the performance measures that serve as the key indicators of system performance and overall efficacy.

2.1. Tailor-Made Compact Data Learning

Compact data learning (CDL) presents an innovative and practical structure to improve classification systems by shrinking the size of machine learning training data [19]. The creation of compact data for machine learning involves the generation of an optimized

training dataset that sustains an equivalent machine learning accuracy while reducing the data volume [19]. This tailor-made compact data should encapsulate maximum knowledge patterns on a microscopic scale, facilitating the effective and customized use of massive data systems [20]. Massive datasets have captured the interest of virtually every industry, with leaders worldwide seeking advice, but these massive datasets still contain data complexity, noise, and data dependence. The tailor-made compact data represent the refined data for optimizing the data management process for machine learning training. Compact data are an optimized dataset that offers optimal benefits without the need to handle complex, massive data [20]. Numerous tailor-made CDL methods have been employed across a broad spectrum of data-driven research arenas, including machine learning-based biometrics [15,17,18,21] and ML-adapted civil engineering analysis [22]. As reported in previous studies [20,23], there is no established framework for tailor-made CDL. Any methods that can optimize the size of the training dataset may be regarded as tailor-made compact data. Notably, ECG time-slicing techniques, including time-sliced (TS) ECG [15,17] and RR-interval-framed (RRIF) ECG [18,21], exemplify the practical applications of tailor-made compact data learning in the creation of ML-based biometric authentication systems. These ECG slicing techniques, which embody the tailor-made CDL approach, have the capacity to produce sufficient ECG training datasets even with a limited number of ECG signal samples. By facilitating the use of minimal training data, tailor-made CDL expedites the training process, making it viable for machines to be trained within performance-constrained devices such as smartwatches or other IoT sensor devices.

2.2. Support Vector Machine Algorithm

Machine learning is a crucial field in contemporary computer research, enabling computers to learn autonomously without explicit programming [24]. Different algorithms are employed in machine learning to tackle diverse data types, as there is no universal algorithm capable of solving all problems [25]. Consequently, when designing a system, it is essential to select the most appropriate machine learning algorithm based on the problem type and data type and quantity to construct an effective model. Machine learning techniques have found extensive application in ECG research. Therefore, we opted for four widely used machine learning algorithms (e.g., KNN, SVM, CNN, and LSTM) to develop models for training and testing purposes because these ML algorithms are currently the most widely utilized. This particular section provides an in-depth account of the machine learning algorithm that we chose, guided by the results of our comprehensive experimental procedures. This algorithm is identified as the support vector machine (SVM) and we selected it due to its superior performance in terms of accuracy and training speed. The SVM is a binary classifier that sorts data through supervised learning. Let us consider the training samples and their label (x_i, y_i) , $y_i \in \{0, 1\}$; then, the two category classification hyperplane can be expressed as follows:

$$w^T x + b = 0, \quad (1)$$

where b is the displacement term and w is the normal vector. Then, a nonlinear support vector machine can be described as follows:

$$\text{Min} \left(\frac{1}{2} \|w\|^2 + C \sum_{i=1}^n \varepsilon_i \right). \quad (2)$$

After transforming the constrained problem of soft interval maximization into an unconstrained problem using the Lagrangian Function and into an equivalent pairwise form [26], the decision boundary is determined by maximizing the distance between the support vectors and the hyperplane. Let X be a low-dimensional space and the input

variable $x_i, x_j \in X$, then the nonlinear support vector machine optimization problem is transformed as follows:

$$\text{Max} \left(\sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \alpha_i \alpha_j y_i y_j K(x_i, x_j) \right), \quad (3)$$

Subject to

$$\sum_{i=1}^n \alpha_i y_i = 0, 0 \leq \alpha_i \leq C, i = 1, \dots, n,$$

where

$$K(x_i, x_j) = \exp \left(-\frac{\|x_i - x_j\|^2}{2\gamma^2} \right). \quad (4)$$

which is the kernel function. The penalty factor C in the context of support vector machine learning and prediction needs to be appropriately determined. A larger C results in fewer misclassified sample points and diminished empirical risk, but concurrently increases the structural risk, potentially culminating in overfitting. Conversely, a smaller C leads to a higher number of misclassified sample points and a simpler model structure, thereby increasing the likelihood of underfitting. As for γ , a smaller value results in more specific classifications and may cause overfitting, while a larger γ leads to more indistinct classifications and potentially results in underfitting. Consequently, the correct definition of C and γ values is crucial to enhance the classification performance of the SVM. According to our experiments, the SVM was selected for adapting the new time-slicing technique and the selection of the best algorithms was based on experimental results in Section 4.

2.3. Machine Learning Performance Measures

To assess machine learning models and select the optimal algorithm, we selected four evaluation measures to gauge their performance in handling multi-class classification tasks [27,28]. These four crucial performance measures, namely, accuracy, recall, precision, and F1-score, were utilized to evaluate the performance of each authentication system. Let us consider a 2-by-2 matrix Φ , which represents a confusion matrix as follows:

$$\Phi := \begin{bmatrix} \phi_{00} & \phi_{01} \\ \phi_{10} & \phi_{11} \end{bmatrix}, \quad (5)$$

where

ϕ_{00} = the number of the true negative;

ϕ_{01} = the number of the false negative;

ϕ_{10} = the number of the false positive;

ϕ_{11} = the number of the true positive.

The accuracy ρ is the percentage of correct classifications that a trained machine learning model achieves. The recall ω calculates the ratio of true positive samples correctly identified from all positive samples, and the precision ς estimates the ratio of true positive samples to predicted positive samples. From (1), the accuracy is defined as follows:

$$\rho = \frac{\phi_{00} + \phi_{11}}{N}, N = \sum_{\phi_{ij} \in \Phi} \phi_{ij}. \quad (6)$$

and the recall ω and the precision ς are as follows:

$$\omega = \frac{\phi_{11}}{\phi_{01} + \phi_{11}}, \quad (7)$$

$$\varsigma = \frac{\phi_{11}}{\phi_{10} + \phi_{11}}, \quad (8)$$

and the F1-score f^1 , which is a weighted average of the precision and recall, is defined as follows:

$$f^1 = \frac{2\omega\zeta}{\omega + \zeta}. \quad (9)$$

Let us assume that the confusion matrix of the multi-classification machine learning result is as follows:

$$\mathbb{A} = \begin{bmatrix} a_{00} & a_{01} & \cdots & \cdots & a_{0n-2} & a_{0n-1} & a_{0n} \\ a_{10} & a_{11} & a_{12} & \cdots & \cdots & a_{1n-1} & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{k0} & a_{k1} & \cdots & a_{kk} & \cdots & a_{kn-1} & a_{kn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1,0} & a_{n-1,1} & a_{n-1,2} & \cdots & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ a_{n,0} & a_{n,1} & \cdots & \cdots & a_{n,n-2} & a_{n,n-1} & a_{n,n} \end{bmatrix} \quad (10)$$

where $a_{ij}, i, j = 0, \dots, n$ are the elements of the confusion matrix $\mathbb{A}$. The binary confusion matrix Φ for evaluating the performance measures could be constructed as follows:

$$\phi_{00} = a_{00}, \quad (11)$$

$$\phi_{01} = \sum_{i=1}^n a_{i,0}, \quad (12)$$

$$\phi_{11} = \sum_{i=1}^n a_{i,i}. \quad (13)$$

$$\phi_{10} = \left(\sum_{i=1}^n \sum_{j=1}^n a_{i,j} \right) - \phi_{11}. \quad (14)$$

After constructing the the binary confusion matrix Φ from (11)–(14), all performance measures including the accuracy ρ , the recall ω , the precision ζ , and the F1-score f^1 could be easily calculated from (6)–(9).

3. Preliminary ECG Authentication Systems

This section presents the design of a time-slice-based ECG authentication system. The system is divided into three core components: data pre-processing, and the application of ECG dataset construction and machine learning models. Data pre-processing involves adjusting the ECG signal data using signal processing techniques to improve the accuracy of authentication. Therefore, three processing methods were introduced: baseline adjustment, power line interference (PLI) noise removal, and flipping signal [15]. Dataset construction utilizes time-slice techniques to segment the pre-processed dataset, creating a flexible and large number of data samples.

3.1. Use Case of ECG Authentication

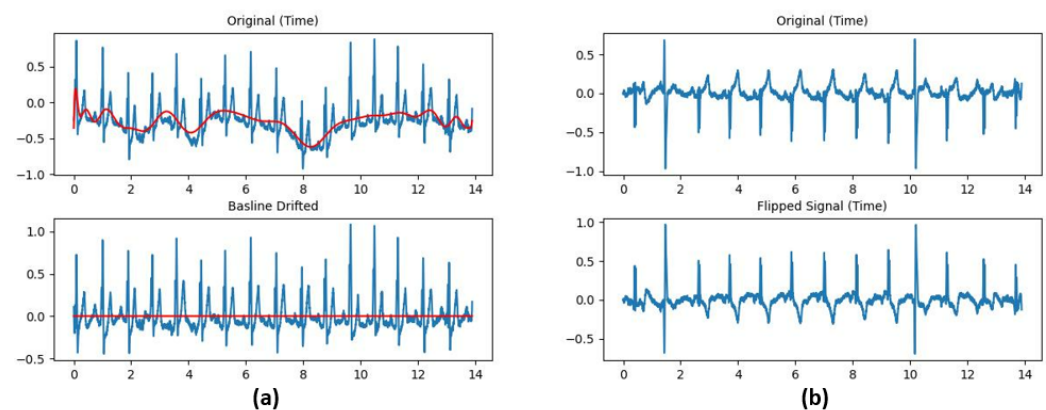
A use case offers an exhaustive illustration of how users will interact with a future system. Use case analysis assists in determining system requirements during the design phase and in elucidating key information for system procedures [15,29]. Diverse use cases can be sorted through use case analysis. By employing this analysis technique to envisage application scenarios for ECG-based user authentication, three unique authentication categories were identified (see Table 1): hospital patients (HOS), identity verification at building entrances (SCK), and continuous authentication for personal use (WD). It is paramount to recognize that system performance requirements, in terms of the authentication speed and accuracy rate vary among each category and are dependent on the intended application systems [15]. The particular user environments and assumptions for this study are outlined in Section 4.

Table 1. Categories for ECG-based authentications [15].

Category Type	Description	Known ID	Unknown ID	Personal Status
HOS	Identifying patients in a hospital before a patient takes their heart test.	O	X	X
SCK	Using ECG data in a security check.	O	O	X
WD	Identifying ownership for using personal wearable devices.	X	O	O

3.2. Pre-Processes for ECG Signal Enhancement

Prior to feeding data into a machine learning model, it is essential to pre-process them to boost classification accuracy. ECG signals are captured via electrodes placed on the body surface in the cardiac area. Nonetheless, the respiratory interference, muscle contractions, and low-frequency noise can corrupt the gathered ECG signals, leading to a baseline drift issue [30]. To tackle this problem, we utilize curve fitting techniques to adjust the baseline and remove the low-frequency component of ECG signals [31]. The use of curve fitting techniques eliminates the need for prior knowledge of the cutoff frequency when using high-pass filters to manage baseline drift. The baseline adjustment is depicted in Figure 1a. A small segment of the ECG signal data are selected and the average value is computed to determine whether the ECG is in an inverted state. Upon detection of an inverted state, the data are processed to revert them to the normal state. The ECG flip is illustrated in Figure 1b.

**Figure 1.** Various pre-processes for ECG signals I: (a) baseline drift adjustment; (b) flipping ECG signals [15].

While collecting ECG data, several varieties of noise interference can manifest, with power line interference (PLI) being a prevalent and challenging noise source [32]. The devices used for signal detection are notably vulnerable to PLI noise resulting from power line interference. To counteract the PLI noise, we employ Fourier transform to pinpoint abnormal peak points in the frequency domain that are 50 to 100 times the average value, subsequently eliminating these peak points. The process of removing power line interference noise is depicted in Figure 2. Incorrect electrode placement during ECG signal acquisition can lead to the collected ECG signals being inverted in comparison to normal signals [15]. Fourier Transform can effectively eliminate specific frequencies associated with noise. Typically, power line interference (PLI) is characterized by the occurrence of the 50 Hz frequency, while baseline wander is associated with the occurrence of the 1 Hz frequency. Consequently, the application of Fourier Transform can enhance ECG data by eliminating these frequencies after the transform, even without employing additional filters.

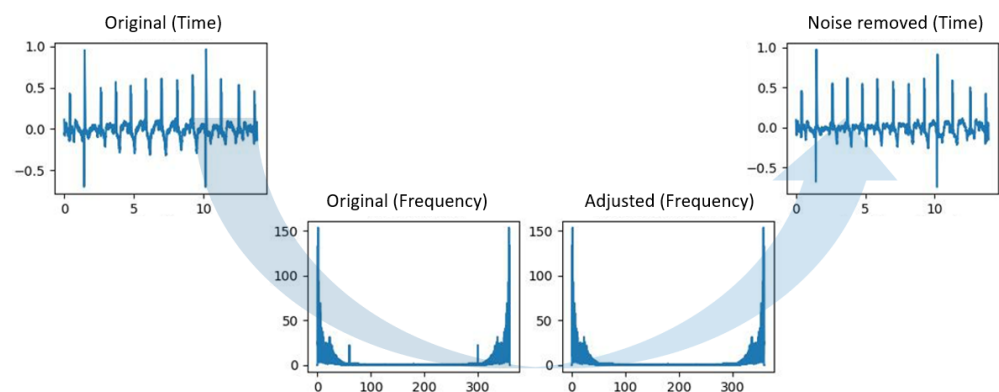


Figure 2. Various pre-processes for ECG signals II: PLI noise removal [15].

3.3. ECG Time-Slicing Techniques

We utilize a technique known as time-slicing [15,17,18,21] to handle the pre-processed ECG data. An ECG signal encompasses various wave forms, including the P wave, QRS complex, and T wave [33]. The QRS complex, within a single cardiac cycle, comprises three defining points, with the R peak representing the maximum amplitude [34]. Consequently, we opted to center the QRS complex around the R-peak. Through the application of the time-slice (TS) technique, we initiate from the R-peak moment and divide the ECG signal into smaller segments within a predetermined time window, at specific time intervals. These signal segments are subsequently layered with respect to the R-peak. The time-sliced (TS) data corresponding to the R-peak are depicted in Figures 3 and 4. We chose the average minimum heartbeat interval of 0.6 seconds, signifying a non-standard heart rate, as the slicing duration [15].

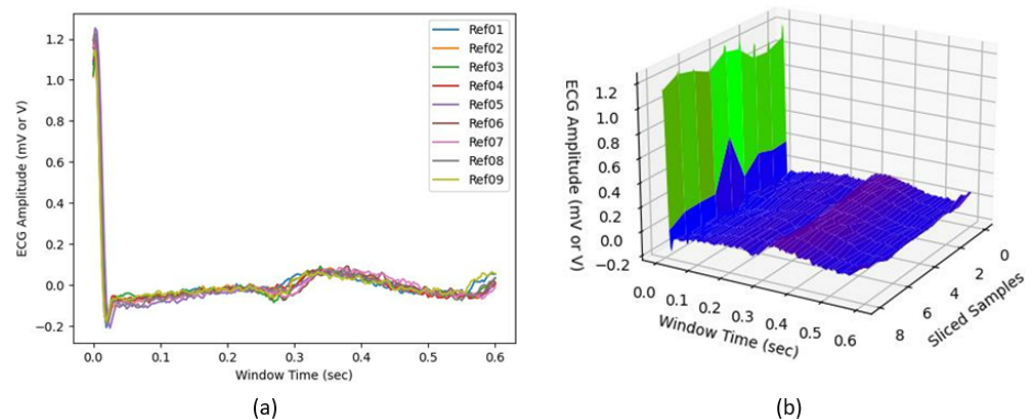


Figure 3. Time-sliced ECG signal samples [15,17]: (a) 2D visualization; (b) 3D visualization.

It is possible to slice ECG signals within their respective time intervals, resulting in the creation of a distinctive and adaptable dataset. Our proposed technique, known as the RR-interval frame (RRIF), emphasizes the RR-interval as a crucial feature of ECG signals, representing the duration between consecutive R-wave peaks [18,35,36]. The time-slice technique mentioned earlier involves constructing the dataset by anchoring it around the R-peaks.

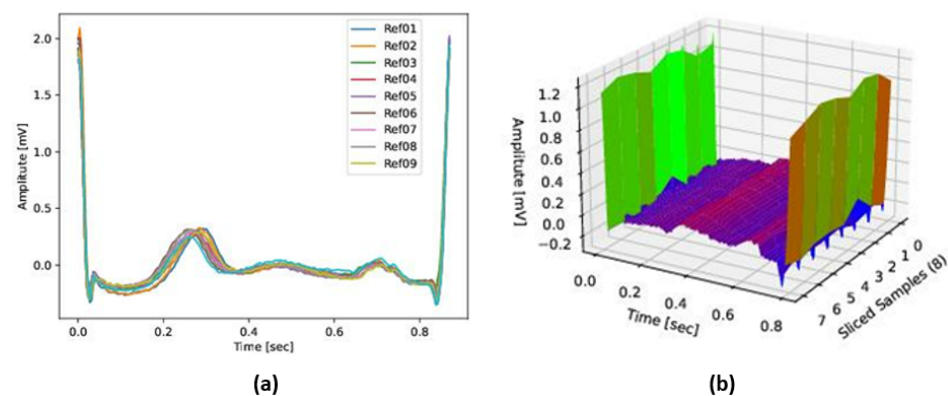


Figure 4. RR-interval-framed (RRIF) ECG signal samples [18]: (a) 2D visualization; (b) 3D visualization.

4. Robust Optimization for ML Model Selection

This research focuses on an ECG-based authentication system designed for the security check use case (SCK) [15,16]. As indicated in the table, this use case utilizes user ECG data for security checks at building entrances and, if necessary, room entrances. Security checkpoints are commonly employed by companies to verify the identities of employees and visitors. With the availability of portable ECG detection devices or sensors, ECG-based biometric authentication systems are poised to become a viable option alongside fingerprint scanning, facial recognition, voice identification, iris recognition, and retina scans for security checkpoints. In the SCK use case, the ECG-based authentication system can identify both registered regular employees and unknown individuals [15–17]. The underlying assumption is that authorized employees have previously registered their identities and historical ECG data in the ECG authentication system. Additionally, it is presumed that the measured ECG signals from the same employee exhibit sufficient stability for both the registration and inference phases. During the inference phase, the sampling time period is relatively short, lasting less than 30 s. Within this brief interval, the system can identify unknown entities [17]. After constructing the dataset, multiple machine learning models are selected and applied to the framework for training and testing, in order to compare and determine the optimal machine learning model. The system design model is shown in Figure 5.

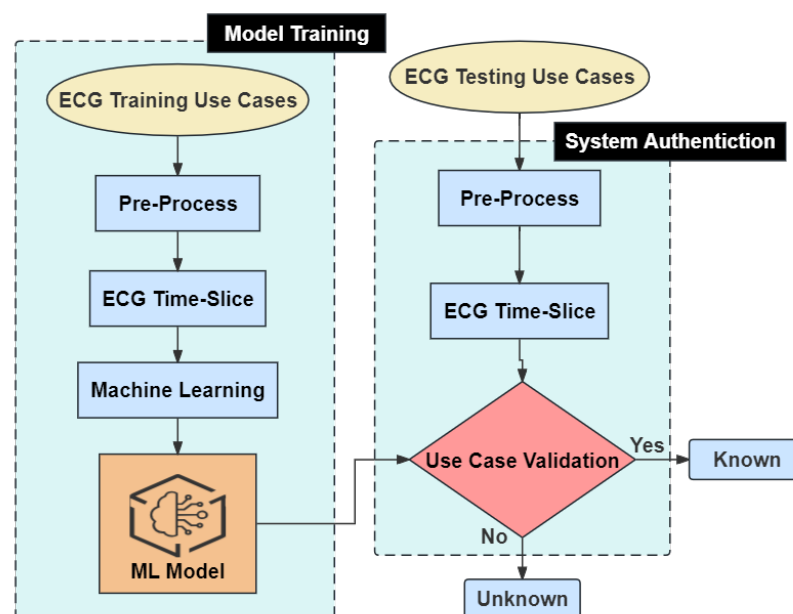


Figure 5. ECG authentication system based on time-sliced (only) ECG signals [17].

4.1. Experimental Setup

This section introduces the evaluation process for our ML-based authentication systems and the details of the ECG datasets for our experiments. This section is focused on the selection of the best ML algorithm for adapting a time-sliced ECG-based authentication system. The ML evaluation process for time-sliced ECG authentication (TS only) could be constructed as follows:

- **Data acquisition:** The dataset was gathered from PhysioNet [37], which is a free repository of a medical research database. This database provides multiple open-source biomedical data, including heartbeats (ECG) and brain waves (EEG; electroencephalogram);
- **Data pre-process:** to improve the quality of the ECG signals, we performed a series of pre-process operations on the acquired dataset, including baseline adjustment, signal removes noise, and signal flip [15,17,18];
- **Dataset construction:** This is the core part of our research. Various time-slicing techniques were applied for the SCK use case, which is defined on Table 1. The original time-slicing (TS) [15] and the combined time-slicing with the RR-interval framing [18] techniques were applied for reconstructing the training and testing ECG datasets;
- **Model training:** To obtain a fast and efficient authentication system, we needed to constantly adjust and optimize the hyperparameters of the ML models [38]. We input the constructed training set into five different machine learning algorithms (KNN, SVM, RF, CNN, and LSTM), and trained corresponding models;
- **System verification:** We used four common machine learning model evaluation metrics (accuracy, recall, precision, and F1-score) to verify the model's effectiveness. We input the constructed testing data into the trained models, obtained the model's test results, and determined the best model.

Although we provide the verification process for specific ML systems, this process gives a general framework for selecting a suitable ML algorithm in any ML-adapted systems.

This study employed two new sets based on the various ECG datasets from PhysioNet [37]. The normal data from MIT-BIH [39,40] and the data from the ECG-ID [41] were randomly selected for the primary ECG dataset. In total, 20 individual samples were selected and each individual sample was collected from two different time slots to make the training and testing datasets. For the assembly of the training datasets, 20 individuals from both ECG datasets [39,41] were randomly selected with their ECG data serving as the machine learning training datasets. The open-source Waveform Database software package (WFDB) [42] enabled reading 30 s of data records from each case for the training datasets. Similarly, the same 20 normal individuals but with different time slots, augmented by an additional 10 randomly selected individuals, were used as the test datasets. To maintain dataset variation, an extra 30 s of data records were read from each individual data point for the test datasets.

4.2. Robust Optimization for Selecting Machine Learning Models

This investigation primarily centers on ECG data processing techniques, and hence, we developed a relatively straightforward machine learning model. Recognizing the versatility of different machine learning algorithms for ECG data authentication, we constructed four prevalent models: CNN, LSTM, KNN, SVM, and RF for ECG data training and testing. CNN and LSTM are neural network algorithms, with common hyperparameters inclusive of the loss function, learning rate, optimization algorithm, dropout, hidden layer count, and epoch [43]. Each ML algorithm was assessed several times to find these hyperparameters and to pinpoint the optimal configuration. The specifics of the CNN and LSTM model hyperparameters are detailed in Table 2. Employing the cross-entropy error as the loss function for both the CNN and LSTM models, the CNN model utilizes the Adam algorithm with a learning rate of 0.003, while the LSTM model adopts the same algorithm with a learning rate of 0.002. Training occurs over 50 epochs for the CNN model and 100 epochs for the LSTM model, with the hidden layer count being 7 for the former and 4 for the latter.

Table 2. Hyperparameter setup for CNN and LSTM.

Parameters	CNN	LSTM
Learning Rate	0.003	0.002
Optimizer	Adam	Adam
Loss Function	Cross-entropy	Cross-entropy
Dropout	0.5	0.3
Number of hidden layers	7	4
Epoch	50	100

Compared to neural network algorithms, other machine learning (ML) algorithms such as K-nearest neighbors (KNN), support vector machines (SVM), and random forest (RF) necessitate fewer hyperparameters to be optimized and offer different options for hyperparameter settings [44]. We used a method combining random search and grid search to determine the optimal hyperparameters: we used random search to narrow the range of hyperparameters, and determined the optimal hyperparameters through grid search. The implementation of KNN, SVM, and RF models was carried out using the widely adopted scikit-learn open-source machine learning library [45]. For these three algorithms, five key hyperparameters were optimized and configured for model building. In the case of KNN, the parameters configured were n neighbors, weights, algorithm, leaf size, and metric [43,44,46]. For SVM, five commonly used hyperparameters, namely, C , kernel, probability, gamma, and decision function shape, were considered [43,44,46]. Similarly, for RF, five crucial hyperparameters were set: criterion, splitter, maximum depth, minimum samples leaf, and random state [43,44,46]. Table 3 presents the hyperparameters configured for the KNN. Specifically, n neighbors was set to 31, distance weights were used, the KDTree algorithm was implemented, the leaf size was assigned as 30, and the Euclidean distance metric was employed. The hyperparameter configurations for the SVM are also displayed in Table 3. Here, C was set to 13, the Gaussian kernel (RBF) was implemented, gamma was set to Scale, probability estimation was activated, and the one-vs-one (ovo) decision function shape (DFS) was utilized. Similarly, the hyperparameters set for RF are shown in Table 3, with Gini as the criterion, the number of estimation was 50, the maximum depth was set to 15, and the random state was set to 10.

Table 3. Hyperparameter setup for KNN, SVM, and RF.

Parameters	KNN	Parameters	SVM	Parameters	RF
Neighbors	31	C	13	Criterion	Gini
Weights	Distance	Kernel	RBF	n -estimators	50
Algorithm	Kd-tree	Probability	True	Random state	10
Leaf size	30	Gamma	Scale	Max. depth	15
Metric	Euclidean	DFS	OVO	OOB score	True
P	2	Shrinking	True		

While creating these models, each algorithm possesses typical parameters that are auto-learned during the training process and hyperparameters that need to be optimized before training [38]. For hyperparameter optimization, we used the grid search method, which optimizes the model by traversing the given hyperparameter combinations [38,43]. Grid search trains and evaluates the model for each hyperparameter combination, thus finding the best performing hyperparameter combination [38,43]. However, when facing unknown data validation, the best model obtained from model training may not necessarily achieve the optimal results. Therefore, we narrowed down the hyperparameter combinations by using the optimal hyperparameter combination and traversed them again to obtain the best hyperparameter combination. The optimization of these hyperparameters can augment the training speed and model accuracy [47]. It is noted that the hyperparameter optimization methods employed for the above machine learning algorithms are both robust and consider

the underlying data dependencies. Conversely, users have the option to utilize default parameters, which are automatically selected by the Python programming language.

4.3. Experimental Result

The efficiency of system authentication was evaluated through four metrics delineated in the previous sections (e.g., Sections 4.1 and 4.2). A performance analysis was conducted using a test dataset composed of 30 cases and 4964 data samples, which included 10 unknown cases. Machine learning models often misclassify unknown categories as known, so the class of each sample was determined by setting the maximum probability value. The four assessment metrics were used to analyze performance and pinpoint the optimal Reject rate, incrementally raised from 0 by 5×10^{-4} until it reached 0.3. Four machine learning algorithms and initial parameter settings were employed to generate the predicted probability matrix for each sample's class in the test dataset, which measured 4964×20 . The four metrics were calculated and compared based on the escalating Reject rate to discern the optimal Reject rate. The analysis of Table 4 facilitated a comparison of the four evaluation metrics: accuracy, precision, recall, and F1-score, at their respective training times. KNN and LSTM exhibited accuracy, precision, and recall values between 80% and 90%, with F1-score values spanning from 0.8 to 0.9. LSTM showed slightly lower performance compared to the KNN. The CNN, SVM, and RF models all exhibited accuracy, precision, and recall values surpassing 90%, with F1-score values exceeding 0.9. The CNN yielded the lowest values for all four evaluation metrics. Compared to other ML algorithms, the SVM, RF and CNN displayed a more balanced performance across all metrics. The SVM reached the apex of accuracy and precision values, at 92.43% and 96.18%.

Table 4. Performance results of various ML models for the time-sliced ECG (TS only).

Model	Accuracy	Precision	Recall	F1-Score	Train Time (Sec)
SVM	92.43%	96.18%	91.99%	0.940	0.164
RF	92.12%	92.64%	95.64%	0.941	1.410
CNN	90.78%	89.80%	96.76%	0.932	67.281
LSTM	84.89%	87.64%	89.25%	0.884	83.655
KNN	85.32%	89.30%	87.92%	0.886	0.179

5. Machine Learning-Based Combined Time-Sliced ECG Authentication Systems

This section presents an ECG authentication system that combines the time-slicing technique with the RR-interval framing (RRIF) technique. The pre-process and design of the machine learning model in this system are consistent with the two experimental setups mentioned earlier, with the only difference being the construction of the ECG dataset after pre-processing. The integration of the RR-interval framing technique with the time-slicing technique enhances the versatility and flexibility of the time-slicing technique when used alone. The system architecture is shown in the Figure 6.

5.1. System Design for Enhanced ECG-Based Authentication System

Our recommendation is to merge the RR-interval frame-based dataset with the time-slice dataset, both constructed using the same R-peak timings. This combination enhances the time-slice dataset, which can be used for training and testing the system. The pre-processing techniques applied before the core processing flow, including baseline drift adjustment, PLI frequency removal, and ECG flip, remain consistent with the methods described in Section 3. The average value of the ECG grid is 220, indicating the average number of frames between RR intervals [48]. The number of frames per RR interval can be adjusted accordingly [17]. R-peaks are detected in the pre-process dataset to capture all the RR intervals within the input range. The initial frame count is then adjusted based on the average number of frames between RR intervals to obtain the RR-interval frame ECG dataset. Figure 3 presents a sample RRIF-based ECG. This study primarily focuses on

constructing the ECG dataset, so the machine learning model construction parameters for this system remain the same as those outlined in Section 3.

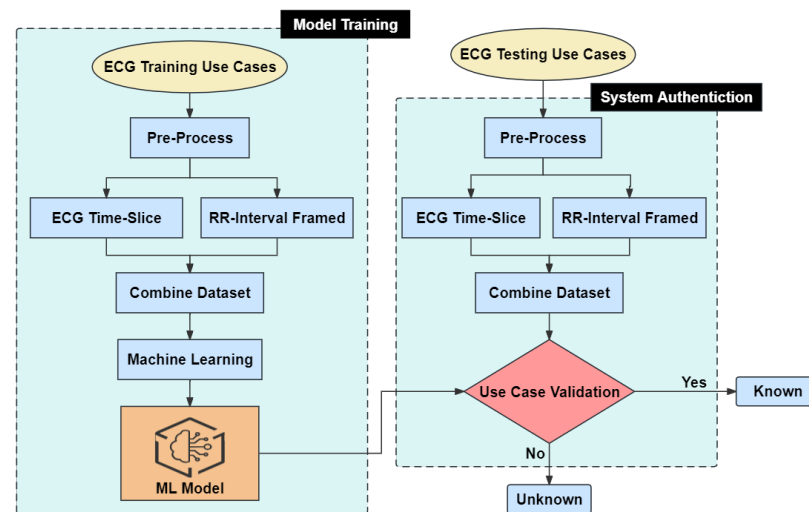


Figure 6. Enhanced combined time-sliced ECG authentication system (TS + RRIF).

5.2. Performance Result

A receiver operating characteristic curve (ROC) is a graphical plot that illustrates the performance of a binary classifier model at varying threshold values [23]. The Area Under ROC (AUC) is one of the most important evaluation metrics for measuring the performance of any classification model. It is a performance measurement for a classification problem at various thresholds settings. The performances of AUC for various ML algorithms for the combined time-sliced ECG authentication systems are shown in Figure 7. The ROC curve measures how accurately the model can distinguish between two things and AUC measures the entire two-dimensional area underneath the ROC curve. As you can see, the SVM gave the best AUC result for the combined time-sliced ECG authentication system.

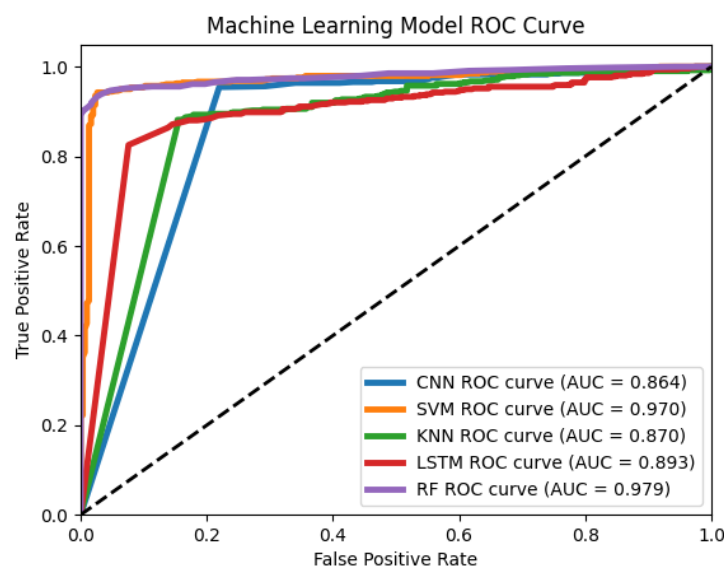


Figure 7. AUC performances of various ML algorithms.

Besides the AUC and the confusion matrix performance measures, other performance measures, including the accuracy, the precision, and the recall, were evaluated. From (11)–(14), all performance measures for various ML algorithms including the SVM could be calculated (see Table 5).

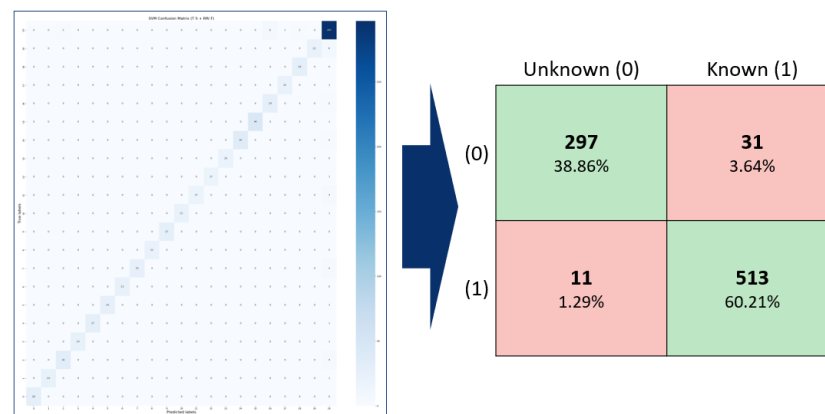
Table 5. Performance results of various ML models for the combined time-sliced ECG ($TS + RRIF$).

Model	Accuracy	Precision	Recall	F1-Score	Train Time (s)
SVM	95.07%	97.90%	94.30%	0.961	0.172
RF	94.90%	97.35%	94.67%	0.960	1.521
CNN	90.25%	91.37%	93.55%	0.924	123.864
KNN	87.19%	91.10%	88.58%	0.898	0.199
LSTM	86.45%	93.65%	84.47%	0.888	126.401

This score gives us a good idea of how well the classifier will perform. AUC is related to another evaluation metric: the confusion matrix Φ from 7. According to our ML evaluations, the SVM performed the best overall in terms of all measures and exhibited a 95% accuracy (see Figure 8). Specifically, this ML algorithm gave the best fit for our combined time-sliced ECG datasets. From (5) and (11)–(14), the confusion matrix could be constructed as follows:

$$\Phi = \begin{bmatrix} \phi_{00} & \phi_{01} \\ \phi_{10} & \phi_{11} \end{bmatrix} = \begin{bmatrix} 297 & 31 \\ 11 & 513 \end{bmatrix}, \quad (15)$$

and the major performance measures (i.e., ρ , ω , ζ , and f^1) of our innovative authentication system were easily calculated from (6)–(9). Figure 8 illustrates the transformation from a multi-class confusion matrix to a binary confusion matrix.

**Figure 8.** Confusion matrix for combined time-sliced ECG performance (SVM).

6. Conclusions

Biometric authentication systems have many advantages over traditional systems. However, the applications of ECG data depend on the particular use case and, thus, the nature of the authentication system could differ from other cases. A versatile time-slicing biometric authentication system, which uses a classification-based interpretable ML approach with various measures including a confusion matrix and an AUC graph, is proposed for the security check use case. In total, 4964 sliced ECG samples from 20 individuals were trained to build the ML-based authentication system and the SVM provided the best performances in terms of accuracy and training speed. In conclusion, using the optimized parameters of the SVM, the proposed authentication system was able to achieve up to a 95.1% accuracy. Besides accuracy, our experiments demonstrated that the support vector machine with the combined time-sliced ECG technique attained an AUC of 97% and an F1-score of 0.961, which indicates that the newly proposed time-slice technique is an improvement over prior studies. This research will lead to the development of compact and efficient ECG authentication systems based on machine learning, which could potentially be implemented on hardware with limited computing power, including portable ECG sensors and biometric IoT devices for enhancing their authentication security.

Author Contributions: Conceptualization, S.-K.K.; software, Y.Z.; writing—draft, Y.Z.; writing—revision, S.-K.K.; methodology, Y.Z. and S.-K.K.; supervision, S.-K.K.; project administration, S.-K.K.; review, S.-K.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Macao Polytechnic University (MPU), under Grant RP/FCA-04/2023.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not Applicable

Data Availability Statement: This study employed two new sets based on the various ECG datasets from PhysioNet [37].

Acknowledgments: This paper was revised using AI/ML-assisted tools. Special thanks to the reviewers who provided valuable advice for improving this paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Dharavath, K.; Talukdar, F.A.; Laskar, R.H. Study on biometric authentication systems, challenges and future trends: A review. In Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, India, 26–28 December 2013; IEEE: Danvers, MA, USA, 2013; pp. 1–7.
2. Rui, Z.; Yan, Z. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE Access* **2018**, *7*, 5994–6009. [\[CrossRef\]](#)
3. Velásquez, I.; Caro, A.; Rodríguez, A. Authentication schemes and methods: A systematic literature review. *Inf. Softw. Technol.* **2018**, *94*, 30–37. [\[CrossRef\]](#)
4. Barkadehi, M.H.; Nilashi, M.; Ibrahim, O.; Fardi, A.Z.; Samad, S. Authentication systems: A literature review and classification. *Telemat. Inform.* **2018**, *35*, 1491–1511. [\[CrossRef\]](#)
5. Sarkar, A.; Singh, B.K. A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimed. Tools Appl.* **2020**, *79*, 27721–27776. [\[CrossRef\]](#)
6. Alsaadi, I.M. Physiological biometric authentication systems, advantages, disadvantages and future development: A review. *Int. J. Sci. Technol. Res.* **2015**, *4*, 285–289.
7. Kataria, A.N.; Adhyaru, D.M.; Sharma, A.K.; Zaveri, T.H. A survey of automated biometric authentication techniques. In Proceedings of the 2013 Nirma university international conference on engineering (NUICONE), Ahmedabad, India, 28–30 November 2013; IEEE: Danvers, MA, USA, 2013; pp. 1–6.
8. Pahuja, G.; Nagabhushan, T. Biometric authentication & identification through behavioral biometrics: A survey. In Proceedings of the 2015 International Conference on Cognitive Computing and Information Processing (CCIP), Noida, India, 3–4 March 2015; IEEE: Danvers, MA, USA, 2015; pp. 1–7.
9. Ingale, M.; Cordeiro, R.; Thentu, S.; Park, Y.; Karimian, N. Ecg biometric authentication: A comparative analysis. *IEEE Access* **2020**, *8*, 117853–117866. [\[CrossRef\]](#)
10. Fratini, A.; Sansone, M.; Bifulco, P.; Cesarelli, M. Individual identification via electrocardiogram analysis. *Biomed. Eng. Online* **2015**, *14*, 1–23. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Bharadwaj, S.; Vatsa, M.; Singh, R. Biometric quality: A review of fingerprint, iris, and face. *EURASIP J. Image Video Process.* **2014**, *2014*, 34. [\[CrossRef\]](#)
12. Ryu, R.; Yeom, S.; Kim, S.H.; Herbert, D. Continuous multimodal biometric authentication schemes: A systematic review. *IEEE Access* **2021**, *9*, 34541–34557. [\[CrossRef\]](#)
13. Abdeldayem, S.S.; Bourlai, T. A novel approach for ECG-based human identification using spectral correlation and deep learning. *IEEE Trans. Biom. Behav. Identity Sci.* **2019**, *2*, 1–14. [\[CrossRef\]](#)
14. Merdjanovska, E.; Rashkovska, A. Comprehensive survey of computational ECG analysis: Databases, methods and applications. *Expert Syst. Appl.* **2022**, *203*, 117206. [\[CrossRef\]](#)
15. Kim, S.K.; Yeun, C.Y.; Damiani, E.; Lo, N.W. A machine learning framework for biometric authentication using electrocardiogram. *IEEE Access* **2019**, *7*, 94858–94868. [\[CrossRef\]](#)
16. Zhang, L.; Chen, S.; Lin, F.; Ren, W.; Choo, K.K.R.; Min, G. 1DIEN: Cross-Session Electrocardiogram Authentication Using 1D Integrated EfficientNet. *ACM Trans. Multimed. Comput. Commun. Appl.* **2023**, *20*, 1–17. [\[CrossRef\]](#)
17. Al Alkeem, E.; Kim, S.K.; Yeun, C.Y.; Zemerly, M.J.; Poon, K.F.; Gianini, G.; Yoo, P.D. An enhanced electrocardiogram biometric authentication system using machine learning. *IEEE Access* **2019**, *7*, 123069–123075. [\[CrossRef\]](#)
18. Kim, S.K.; Yeun, C.Y.; Yoo, P.D. An enhanced machine learning-based biometric authentication system using RR-interval framed electrocardiograms. *IEEE Access* **2019**, *7*, 168669–168674. [\[CrossRef\]](#)

19. Kim, S.K. Compact Data Learning For Machine Learning Classifications. *Axioms* **2024**, *3*, 137. [\[CrossRef\]](#)
20. Kim, S.K. Toward Compact Data from Big Data. In Proceedings of the 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 8–10 December 2020; IEEE: Danvers, MA, USA, 2020; pp. 1–5.
21. Kim, S.K.; Yeun, C.Y.; Yoo, P.D.; Lo, N.W.; Damiani, E. Deep Learning-Based Arrhythmia Detection Using RR-Interval Framed Electrocardiograms. In Proceedings of the Proceedings of Eighth International Congress on Information and Communication Technology, London, UK, 30 July 2023; Springer: Singapore, 2023; pp. 11–21.
22. Yoon, S.; Kim, S.K.; Cantwell, W.J.; Yeun, C.Y.; Cho, C.S.; Byon, Y.J.; Kim, T.Y. Defect detection in composites by deep learning using solitary waves. *Int. J. Mech. Sci.* **2023**, *239*, 107882. [\[CrossRef\]](#)
23. Fawcett, T. An introduction to ROC analysis. *Pattern Recognit. Lett.* **2006**, *27*, 861–874. [\[CrossRef\]](#)
24. Mahesh, B. Machine learning algorithms-a review. *Int. J. Sci. Res. (IJSR)* **2020**, *9*, 381–386.
25. Jordan, M.I.; Mitchell, T.M. Machine learning: Trends, perspectives, and prospects. *Science* **2015**, *349*, 255–260. [\[CrossRef\]](#)
26. Chen, K.; Yao, H.; Han, Z. Arithmetic optimization algorithm to optimize support vector machine for chip defect Identification. In Proceedings of the 2022 28th International Conference on Mechatronics and Machine Vision in Practice (M2VIP), Nanjing, China, 6–18 November 2022; IEEE: Danvers, MA, USA, 2022; pp. 1–5.
27. Kim, B.H.; Pyun, J.Y. ECG identification for personal authentication using LSTM-based deep recurrent neural networks. *Sensors* **2020**, *20*, 3069. [\[CrossRef\]](#) [\[PubMed\]](#)
28. Hossin, M.; Sulaiman, M.N. A review on evaluation metrics for data classification evaluations. *Int. J. Data Min. Knowl. Manag. Process* **2015**, *5*, 1.
29. Administration, U.G.S. Use Cases. 2019. Available online: <https://www.usability.gov/how-to-and-tools/methods/use-cases.html> (accessed on 16 November 2023).
30. Zhang, D. Wavelet approach for ECG baseline wander correction and noise reduction. In Proceedings of the 2005 IEEE engineering in medicine and biology 27th annual conference, Shanghai, China, 7–18 January 2006; IEEE: Danvers, MA, USA, 2006; pp. 1212–1215.
31. Arlinghaus, Sandra Lach; Arlinghaus, W.C. *Practical Handbook of Curve Fitting*; Crc Press: Boca Raton, FL, USA, 1994.
32. Kumar, P.; Sharma, V.K. Detection and classification of ECG noises using decomposition on mixed codebook for quality analysis. *Healthc. Technol. Lett.* **2020**, *7*, 18–24. [\[CrossRef\]](#) [\[PubMed\]](#)
33. Kaur, A.; Agarwal, A.; Agarwal, R.; Kumar, S. A novel approach to ECG R-peak detection. *Arab. J. Sci. Eng.* **2019**, *44*, 6679–6691. [\[CrossRef\]](#)
34. Sasikala, P.; Wahidabanu, R. Robust r peak and qrs detection in electrocardiogram using wavelet transform. *Int. J. Adv. Comput. Sci. Appl.* **2010**, *12*, 19638. [\[CrossRef\]](#)
35. Palaniappan, R.; Krishnan, S.M. Identifying individuals using ECG beats. In Proceedings of the 2004 International Conference on Signal Processing and Communications, 2004, SPCOM'04, Bangalore, India, 11–14 December 2004; IEEE: Danvers, MA, USA, 2004; pp. 569–572.
36. Faust, O.; Kareem, M.; Ali, A.; Ciaccio, E.J.; Acharya, U.R. Automated arrhythmia detection based on RR intervals. *Diagnostics* **2021**, *11*, 1446. [\[CrossRef\]](#) [\[PubMed\]](#)
37. Goldberger, A.L.; Amaral, L.A.; Glass, L.; Hausdorff, J.M.; Ivanov, P.C.; Mark, R.G.; Mietus, J.E.; Moody, G.B.; Peng, C.K.; Stanley, H.E. PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. *Circulation* **2000**, *101*, e215–e220. [\[CrossRef\]](#)
38. Luo, G. A review of automatic selection methods for machine learning algorithms and hyper-parameter values. *Netw. Model. Anal. Health Inform. Bioinform.* **2016**, *5*, 1–16. [\[CrossRef\]](#)
39. Moody, G.; Mark, R. The impact of the MIT-BIH Arrhythmia Database. *IEEE Eng. Med. Biol. Mag.* **2001**, *20*, 45–50. [\[CrossRef\]](#)
40. Apandi, Z.F.M.; Ikeura, R.; Hayakawa, S. Arrhythmia detection using MIT-BIH dataset: A review. In Proceedings of the 2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA), Kuching, Malaysia, 15–17 August 2018; IEEE: Danvers, MA, USA, 2018; pp. 1–5.
41. Lynn, H.M.; Yeom, S.; Kim, P. ECG-Based Biometric Human Identification Based on Backpropagation Neural Network. In Proceedings of the Proceedings of the 2018 Conference on Research in Adaptive and Convergent Systems, RACS '18, New York, NY, USA, 9–12 October 2018; pp. 6–10.
42. Xie, C.; McCullum, L.; Johnson, A.; Pollard, T.; Gow, B.; Moody, B. Waveform Database Software Package (wfdb) for Python. 2022. Available online: <https://physionet.org/> (accessed on 1 March 2024).
43. Yang, L.; Shami, A. On hyperparameter optimization of machine learning algorithms: Theory and practice. *Neurocomputing* **2020**, *415*, 295–316. [\[CrossRef\]](#)
44. Komer, B.; Bergstra, J.; Eliasmith, C. Hyperopt-sklearn: Automatic hyperparameter configuration for scikit-learn. In Proceedings of the ICML workshop on AutoML, Austin, TX, USA, 19 April 2014; Volume 9, p. 50.
45. Pedregosa, F.; Varoquaux, G.; Gramfort, A.; Michel, V.; Thirion, B.; Grisel, O.; Blondel, M.; Prettenhofer, P.; Weiss, R.; Dubourg, V.; et al. Scikit-learn: Machine learning in Python. *J. Mach. Learn. Res.* **2011**, *12*, 2825–2830.
46. Bergstra, J.; Komer, B.; Eliasmith, C.; Yamins, D.; Cox, D.D. Hyperopt: A python library for model selection and hyperparameter optimization. *Comput. Sci. Discov.* **2015**, *8*, 014008. [\[CrossRef\]](#)

47. Yu, T.; Zhu, H. Hyper-parameter optimization: A review of algorithms and applications. *arXiv* **2020**, arXiv:2003.05689.
48. Cadogan, M. PR Interval. 2021. Available online: <https://litfl.com/pr-interval-ecg-library/> (accessed on 30 December 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.