Разработка надежной системы биометрической аутентификации по ЭКГ с использованием глубокого обучения

Designing a Robust ECG Biometric Authentication System with Deep Learning

УДК 004.05
Получено: 17.01.2025 Одобрено: 21.02.2025 Опубликовано: 25.03.2025

Азаб Мохамед Абдалла Эльсайед
Аспирант, факультет безопасности информационных технологий
Факультет безопасности информационных технологий Университета ИТМО, г. Санкт-Петербург
e-mail: mohamed.a.azab@itmo.ru

Azab Mohamed Abdalla Elsayed
Postgraduate student, Faculty ofInformationTechnology Security
Faculty of Information Technology Security, ITMO University, St. Petersburg
e-mail: mohamed.a.azab@itmo.ru

Коржук В.М.
Доцент, факультет безопасности информационных технологий
Факультет безопасности информационных технологий Университета ИТМО, г. Санкт-Петербург
e-mail: vmkorzhuk@itmo.ru

Korzhuk V.M.
Associate Professor, Faculty of Information Technology Security,
Faculty of Information Technology Security, ITMO University, St. Petersburg
e-mail: vmkorzhuk@itmo.ru

Аннотация
Сегодня мы все чаще обращаемся к биометрическим системам аутентификации для защиты важной информации и ресурсов. Наш вклад в данной работе заключается в разработке надежной и инновационной системы биометрической аутентификации на основе сигналов ЭКГ, усиленной с использованием методов глубокого обучения. В предложенной системе применяется комплексная методология, включающая обработку сигналов, извлечение признаков, вейвлет-декомпозицию, детектирование QRS-комплекса, внутреннее моделирование, расчет расстояний и отклонений, усреднение пороговых значений, а также классификатор на основе искусственной нейронной сети (ИНС). Качество сигналов ЭКГ улучшается за счет предварительной обработки, после чего сигналы регистрируются. Уникальные характеристики формы сигнала ЭКГ извлекаются, а сам сигнал декомпозируется во временной и частотной областях с использованием вейвлет-преобразования. С помощью детектирования QRS-комплекса идентифицируются ключевые компоненты для биометрической аутентификации. Система строит внутреннее представление волн ЭКГ, вычисляет параметры, такие как расстояние и отклонение, и уточняет набор признаков для повышения устойчивости. Для повышения устойчивости к шуму и вариативности применяется усреднение пороговых значений. Наконец,

классификатор на основе ИНС, обученный на извлеченных признаках, выполняет аутентификацию. Система выводит результат аутентификации и подтвержденную личность индивидуума. Экстенсивное тестирование проводилось на известном наборе данных ЭКГ, достигнута точность 98%, что демонстрирует эффективность системы. Значение True Positive Rate (чувствительность) составило 95%, что указывает на высокую производительность в идентификации подлинных пользователей. При времени обработки 10 секунд система подходит для использования в реальном времени. Анализ ROC-кривой также показал отличную производительность в различении подлинных и неподлинных пользователей с площадью под кривой (AUC) 0,98. Предложенная система обеспечивает безопасную, надежную и адаптивную биометрическую аутентификацию на основе ЭКГ за счет интеграции сложных методов обработки сигналов и глубокого обучения для работы с реальными вариациями паттернов ЭКГ, что улучшает предыдущие разработки. Несмотря на высокую чувствительность и точность системы, в будущих исследованиях планируется улучшить селективность и снизить количество ложных срабатываний для повышения общей производительности.
Ключевые слова: глубокое обучение, сигнал ЭКГ, искусственная нейронная сеть (ИНС), безопасность, биометрическая аутентификация, обработка сигналов, QRS-комплекс, вейвлет-декомпозиция.

Abstract

Today, we are increasingly looking to biometric authentication systems to protect our crucial information and resources. Our contribution in this paper is a robust and novel biometric authentication system for ECG signals that are augmented using the deep learning techniques. A comprehensive methodology including signal processing, feature extraction, wavelet decomposition, QRS wave detection, internal modeling, distance and deviation calculations, and averaging threshold along with an artificial neural network (ANN) classifier are used in the proposed system. The quality of ECG signals is improved using preprocessing, and ECG signals are acquired. The ECG waveform features unique characteristics which are then extracted, and the signal is decomposed in both time and frequency domains using wavelet decomposition. Using QRS wave detection, critical components for biometric authentication are identified. The system constructs an internal representation of ECG waves, calculates parameters such as distance and deviation, and refines the feature set to improve robustness. An averaging threshold is applied to enhance resilience to noise and variability. Finally, an ANN classifier, trained on the extracted features, performs the authentication. The system outputs the authentication result and the verified identity of the individual. Extensive testing was conducted using a well-known ECG dataset, achieving an accuracy of 98%, demonstrating the system's effectiveness. The True Positive Rate (sensitivity) was 95%, indicating strong performance in identifying authentic individuals. With a processing time of 10 seconds the system would be appropriate for use in real-time applications. ROC curve analysis also demonstrated excellent performance in discriminating authentic from non-authentic individuals with an Area Under the Curve (AUC) of 0.98. Securing, dependable and adaptable ECG based biometric authentication system is provided with the integration of complicated signal processing and deep learning to deal with real ECG pattern variations, that improves on past work. Although the system is highly sensitive and accurate future work will be directed towards improving selectivity and decreasing false positives to improve performance as a whole.
Keywords: Deep learning, ECG Signal, Artificial Neural Network (ANN), Security, Biometric Authentication, Signal Processing, QRS Complex, Wavelet Decomposition.

Introduction

Biometric authentication is paramount in protecting sensitive information and resources [1]. ECG signals have unique and stable characteristics, and hence they have drawn much attention as some promising physiological signals for biometric identification. Patterns of the electrical activity of the heart, representing ECG signals, are an effective way of individual recognition. This study presents a novel biometric authentication system based on ECG signals and advanced deep learning approach. As such, the details of the proposed system here aim to enhance reliability and security by exploiting the complexities of ECG waveforms. Artificial Neural Networks (ANNs) are used to extract Individual Identification and a robust, accurate identification is performed. Current biometric methods are limited and this research tries to overcome the limitations of current biometric methods and offers secure access control methods. The fact is the need for secure, reliable authentication has increased dramatically as technology has penetrated every aspect of modern life. These include facial, voice and passwords, which are all becoming more and more useless because of the vulnerability involved: no facial data, twins can't be identified, voice recordings etc. They are a universal, robust, unique, stable, easy to collect and high-performance alternative to ECG signals [2]. ECG is the recording of the heart's electrical activity over time, revealing vital information about its rhythm and functionality. The electrocardiogram (ECG) is a graphical representation of the heart's electrical activity over time, recorded using electrodes placed on the body. An ECG signal is characterized by a repeating waveform that includes distinct components such as the P wave, QRS complex, and T wave, each corresponding to specific phases of the cardiac cycle: the P wave represents atrial depolarization, the QRS complex corresponds to ventricular depolarization, and the T wave indicates ventricular repolarization [3]. Fig. 1 shows these key components which offer very important understanding about the heart's condition and are crucial in looking at the heart's rhythm and functionality . These features have significantly different morphology, and temporal characteristics, between individuals, which are sufficiently unique between individuals, such that ECG signals are unique [4]. Evaluated through electrocardiographs, ECG signals also reflect variations in sensor placement, enabling enhanced waveform analysis. The standard 12-lead configuration categorizes signals into chest and limb leads, capturing periodic and recurrent patterns, with the QRS complex, encompassing the Q, R, and S waveforms, serving as the focal point of ECG analysis, typically represented in the sequence P-QRS-T [5].

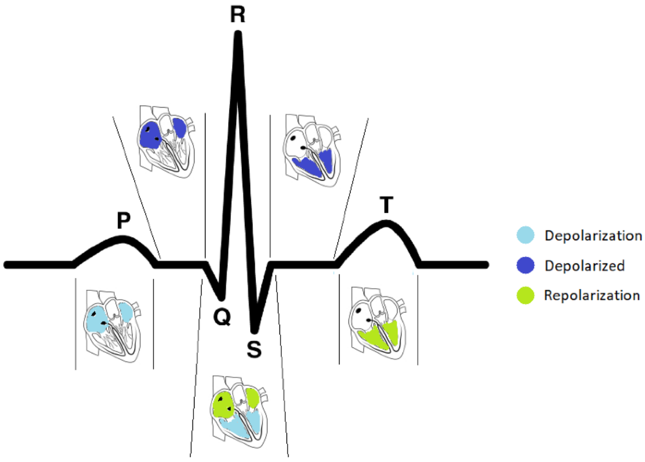

Fig. 1. Sequence of depolarization and repolarization events in the heart and their correlation to various heart beat wave forms in the ECG signal

The distinctiveness of ECG signals lies in their inter-individual variability, which reflects the anatomical and physiological differences between individuals. Moreover, studies have confirmed that while ECG signals exhibit some day-to-day variability, their long-term intra-individual characteristics remain stable and comparable [6]. This stability allows for reliable identification over extended periods, even with a time gap of more than a year between recordings. ECG signals, being involuntary and directly linked to the functioning of the heart, are difficult to replicate or manipulate, further enhancing their suitability for biometric authentication [7]. These unique characteristics have made ECG a popular and significant tool in the field of biometrics, with research dating back to the early 2000s.The organizational structure of this study is outlined as follows: Section 2 provides a detailed literature review to establish the context and relevance of the research and discusses the limitations of existing systems, while Section 3 elaborates on the methodologies of the proposed system. Section 4 presents and analyzes the results of the study, highlighting its effectiveness. Finally, Section 5 concludes the research and outlines potential directions for future work.

Background

H. Silvaet. Silvaet. Al. [8] "For safe healthcare systems like HIS, defining how people can use ECG biometrics to authorize access and show medical data is key. Confirming a patient's insurance and reviewing their health record are two tasks that need to be done right at the start as they form the basis for everything else. Today, biometrics is the main way to solve this issue, but regular ID check methods only confirm limited access - even though technology advances, we still need direct contact with readers confined to a single area. Current patient and doctor sign-in methods in Healthcare Information Systems aren't reliable enough and result in lower care quality since mismatched data from everywhere keeps causing errors. Study by Al. [6] explores the idea of employing the ECG heartbeat's shape and deadlines to tell people apart. These ECG readings, taken from 22 healthy participants' lead I channels during various states, help validate how well the system works by analyzing 550 test samples. The proposed method takes ECG recordings from beginning of QRS complex to T wave termination. In this paper, we developed plan for making ECG readings an essential biometric security element. Through tests on a group of 22 healthy recipients, three different access methods were created, and analysis confirmed ECG variations do offer real help in securing ECG signals as a biometric solution. Research shows that the QRS part of ECG stays constant regardless of heart rate and works well just to verify identity, making it a useful component for biological safety [9].

According to Y. Ho, Wang et. Al. [10], "Biometric Identification" identifies individuals through their unique physical and biological signal characteristics. This project looks at and assesses a way to study the ECG from one lead to tell different humans apart. When the first phase ends, the ECG data is broken down into several sections for processing, one window for each ECG heartbeat. Through identifying QRS correctly, our tool collects important data values to help with identifying who is who. Research work provides a biometric system for the structured study of a particular electrocardiogram of lead (ECG) of human authentication. The initial stage of such a system consists of a wide band-pass filter that used to noise removal as well as other artefacts produced from raw ECG signal. A. Krishnapuramet. Al. [11] "In the study "A Bayesian Method to Combined Feature Selection and Classifier Design", the authors propose using Bayesian analysis to determine the point when a classifier with fewer features becomes less accurate while also finding the most helpful factors to the classification task. The method uses high-profile importance to encourage sparsity in use of both theory capabilities and modules; such prior convictions assume the shape of regularizations for the possibility research which awards considerable clarity in the planning of knowledge. Researchers derive an expectation-maximization (EM) algorithm to effectively calculate the maximum a posteriori (MAP) point estimation of a various variables. The algorithm uses one of today's leading public algorithms that are essentially the same as support vector machine equivalents, but based on Bayesian theory. T. The author Jebaraet, man. Al. [12] developed two techniques for SVMs: selecting kernels to deal with multiple tasks and training individual SVMs on separate but connected datasets. A technique that is beneficial if several electronic classification methods and individually marked datasets occur against even a shared input space. Distinguishable datasets will typically reinforce the traditional choice of portraits or greatly strengthen with the classification techniques. A multi-task recognition learning technique using the very extreme entropy segregation formula is identified. The consequent convex algorithms retain the global solution objectives of support vector machines. Even then, in relation to several SVM classification and regression parameters, they often collectively calculate an optimum set of attributes and an optimal kernel combination. Tests are seen in simplified datasets. Andrea Bakker and her team showed how making separate regression tasks work together improved task modeling in their 2022 article [13]. To solve this in machine learning, we use a technique called multitask learning, where the network learns output from multiple related tasks at the same time. This is often achieved by a linear mixed effects model where there is a distinction between 'set effects, which are the same for all tasks,' and 'random effects, which can differ among tasks. In this paper, we will follow a Bayesian method in that few of the parameters are distributed (the same across all tasks) and few are very closely linked across a common probability distribution which can be derived from results. Throughout this manner, they try to incorporate the better aspects of both multi-level statistical approach as well as the neural network machinery. Article [14] "Geometrical dimensions of the differences of multi-lead ECG recordings. Electrocardiogram (ECG) is used as a clinical tool for evaluating or assistance a diagnosis in a cardiac patient ever since it was recorded in a man by Waller and then enhanced by Einthoven [15]. Normal ECG readings for healthy people show big differences between each person's heart patterns. These differences come from both the body's external structure and its internal electrical activity [16]. This study measures how much geometric factors influence the ECG's electrical signals. This study also details how to adjust for these elements. The study finds that most changes in ECG readings come from variations in how blood and tissues flow through your chest. Researchers have improved ECG-based biometric authentication methods, but there's still more to study and refine. Modern systems have problems with noise interference, struggle to handle differences in human responses, and require advanced ways to pull useful data from ECG signals [17]. The system we propose uses deep learning to solve these issues, making it more reliable and precise at verifying people [2] [18].

Method

Our proposed system combines multiple parts as shown in Fig. 2: signal processing, feature picking, wavelet analysis, and an Artificial Neural Network (ANN) biometric comparison tool. This deep learning method allows our system to uncover complex wave patterns in ECG signals, making it better at both recognizing and interpreting heart activity. The way the ECG signals are processed both inside the system and averaged out helps it detect heart issues better by ignoring unwanted background noise.

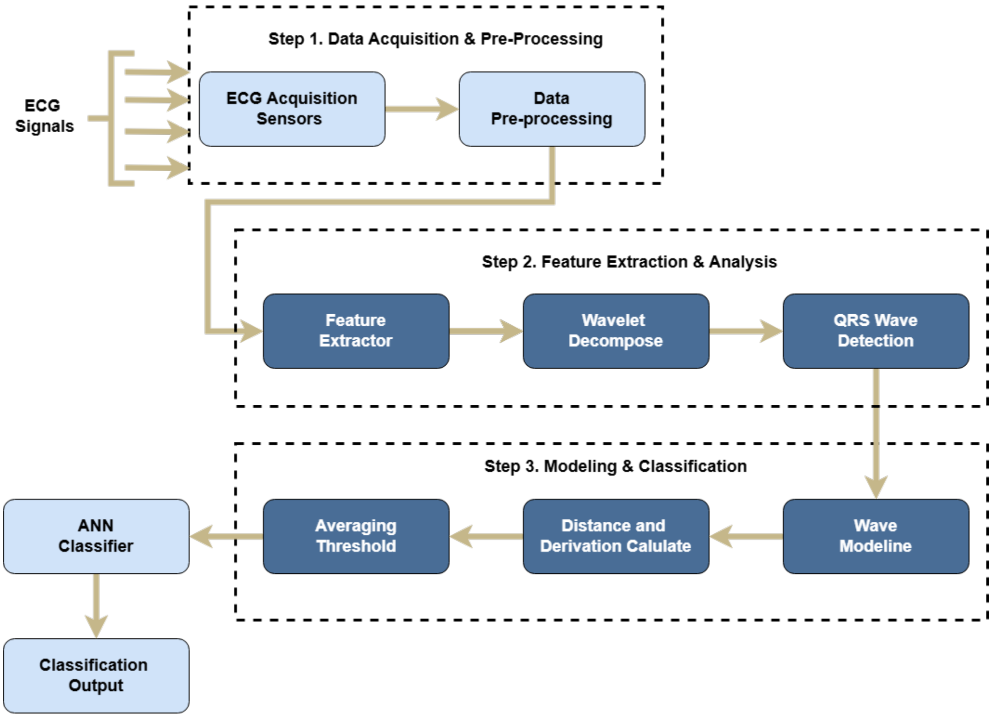

Fig. 2. Proposed block diagram.

Our System uses Deep learning methods to create unique biometric authentication systems that work for both one person and many people. This framework guides researchers and developers in making sure they gather enough ECG test data and collect it correctly, which helps them create effective ECG biometric identification solutions. We limit dataset boundaries by using use case analysis. We created three different ways to apply ECG authentication, depending on what kind of application needs it.

Materials and Methods

Data Acquisition

The ECG data used in this research was obtained from the ECG-ID dataset, a publicly available and widely recognized dataset for biometric authentication research. The dataset includes ECG signals from 90 subjects, providing a diverse and comprehensive range of signals for analysis. For this study, 40 subjects were selected, ensuring diversity in terms of age and gender to enhance the robustness and generalizability of the system. The ECG signals were recorded using a standard setup, focusing on Lead 1 for consistency. These signals were stored in a database for subsequent processing and analysis.

Signal Pre-Processing and Feature Extraction

The initial step in processing involved applying a median filter to the raw ECG signals to remove noise and artifacts, ensuring improved signal quality for further analysis. After pre-processing, key features such as the P-wave, QRS complex, and T-wave were extracted. These features, representing distinct phases of the cardiac cycle, serve as unique identifiers for distinguishing ECG signals among individuals. Wavelet decomposition was employed to analyze the signal in both time and frequency domains, isolating specific frequency bands to highlight relevant details for authentication.

Wave Analysis and Modelling

The QRS complex, being the most significant feature for authentication, was further analyzed through QRS wave detection, pinpointing its onset and offset. Internal calculations and wave modelling were then conducted to derive additional features, including the shape and amplitude of the QRS complex. To enhance the robustness of the system, distance and deviation calculations were performed to compare extracted features with a reference template. An averaging threshold was applied to increase resilience against noise and variability, ensuring consistent and reliable results.

Classification and Output Generation

The refined features were processed using an Artificial Neural Network (ANN) classifier, trained on a dataset of known ECG signals. The ANN utilized intricate patterns within the signals to authenticate individuals. The final system output provided a binary decision, indicating whether the input ECG signal was authentic or not. This decision was derived based on the results of the averaging threshold and ANN classification, showcasing the system's ability to deliver accurate and reliable biometric authentication.

Methodology

Fig. 3 shows the block diagram of the proposed approach. It consists of pre trained ANN classifier for the performance evaluation of ECG signal classification for person authentication. In the proposed methodology the steps as follows.

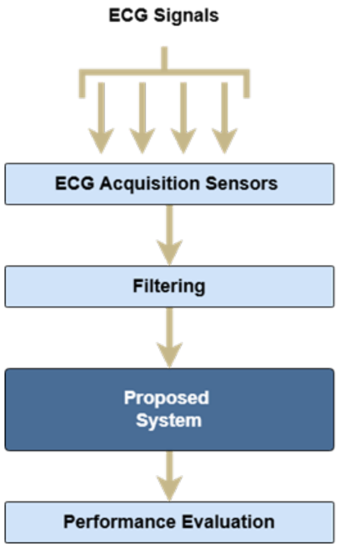

Fig. 3. Proposed methodology.

The collected ECG signals were retrieved from a pre-existing database and subjected to a series of pre-processing steps to enhance their quality. Initially, the signals were filtered to remove high-frequency noise and artifacts that could interfere with subsequent analysis. Pre-processing was carried out using a Band Pass Filter (BPF), which allows signals with frequencies below a specified cut-off to pass while attenuating those with higher frequencies. This technique ensures that only the relevant frequency range of the ECG signal is preserved for further processing. Following pre-processing, the filtered signals were prepared for input into the Artificial Neural Network (ANN) classifier. During this step, the layers of the ANN classifier were carefully configured, with all layers concatenated except for the first and the last three, optimizing the model's ability to analyze and classify the ECG signals effectively.

Results

Fig. 4 represents the raw ECG signal acquired from the individual. The ECG signal typically consists of P, Q, R, S, and T waves, each corresponding to different phases of the cardiac cycle. The irregularities and unique patterns in this signal form the basis for biometric authentication.

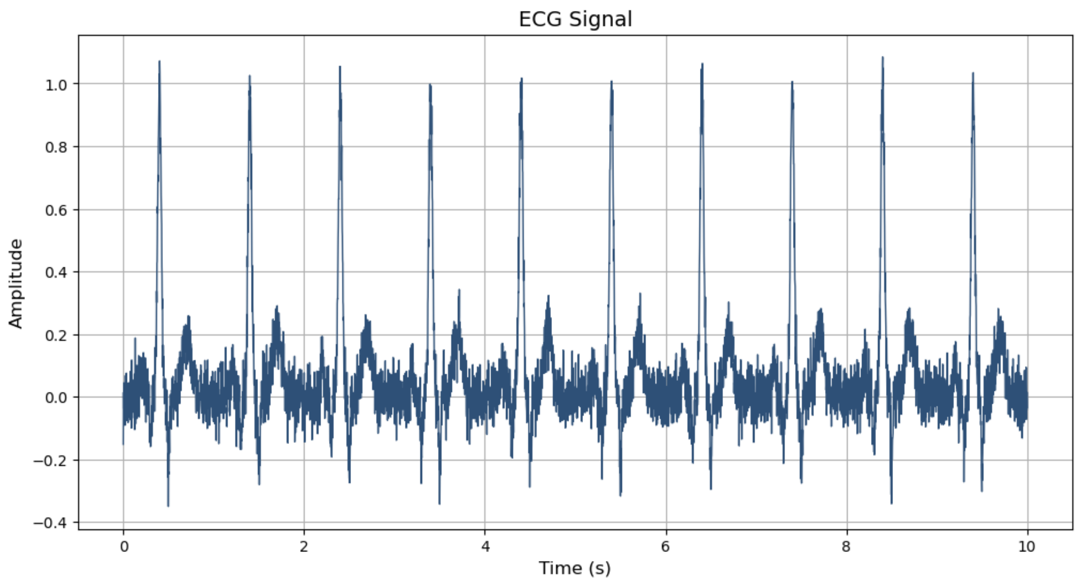

Fig. 4. Input ECG Signal.

During acquisition, the ECG signal is frequently contaminated by various types of noise. After removing unwanted noise from the ECG signal using Band pass filter (BPF), the ECG signal is displayed in Fig.5. It is this step that significantly improves the quality and accuracy of following signal processing and analysis.

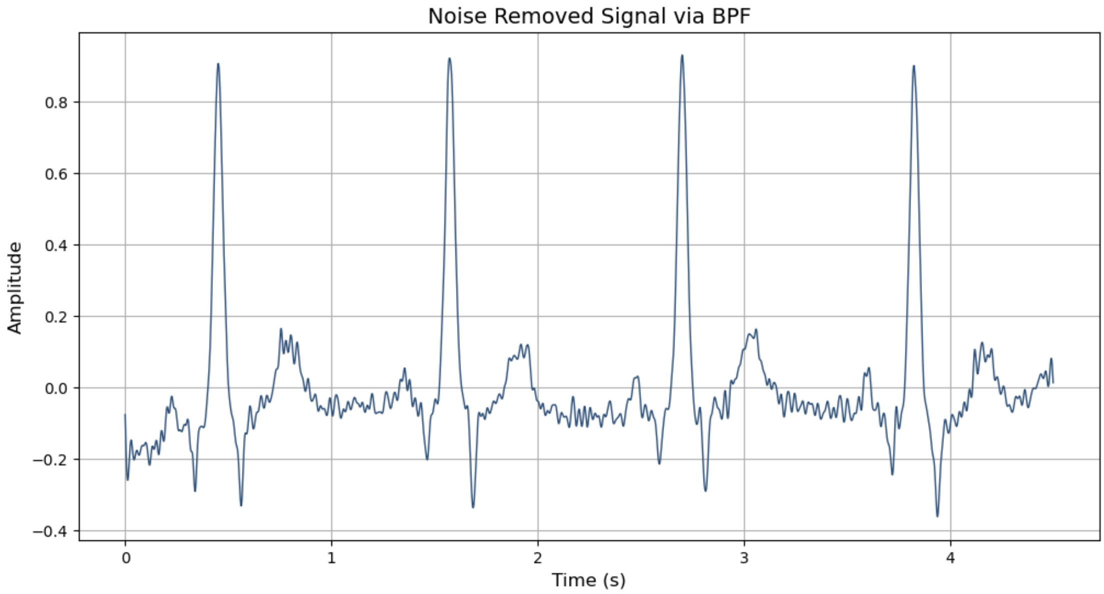

Fig. 5. Noise removed signal via BPF.

PQRS points represent the key landmarks in the ECG signal, namely the P-wave, QRS complex, and T-wave. Fig. 6 illustrates the identified PQRS points, providing a visual representation of the critical features used for subsequent analysis and feature extraction.

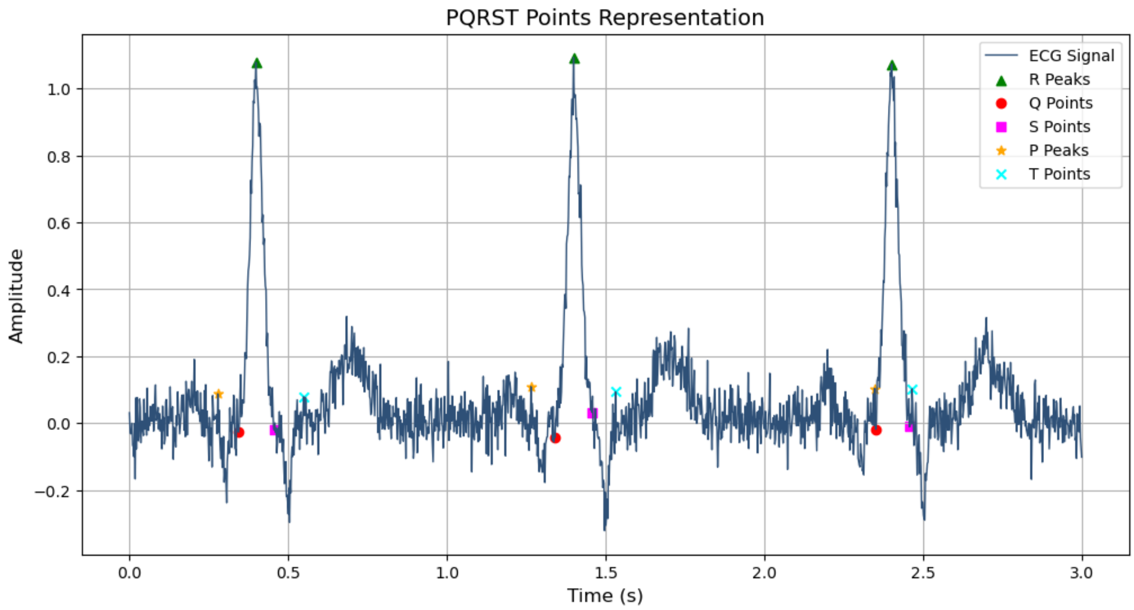

Fig. 6. PQRS points representation.

The accurate detection of R-peaks within the QRS complex is very important. Specifically detected R peaks in the ECG signal, representing a foundation for subsequent processing steps are shown in Fig. 7.

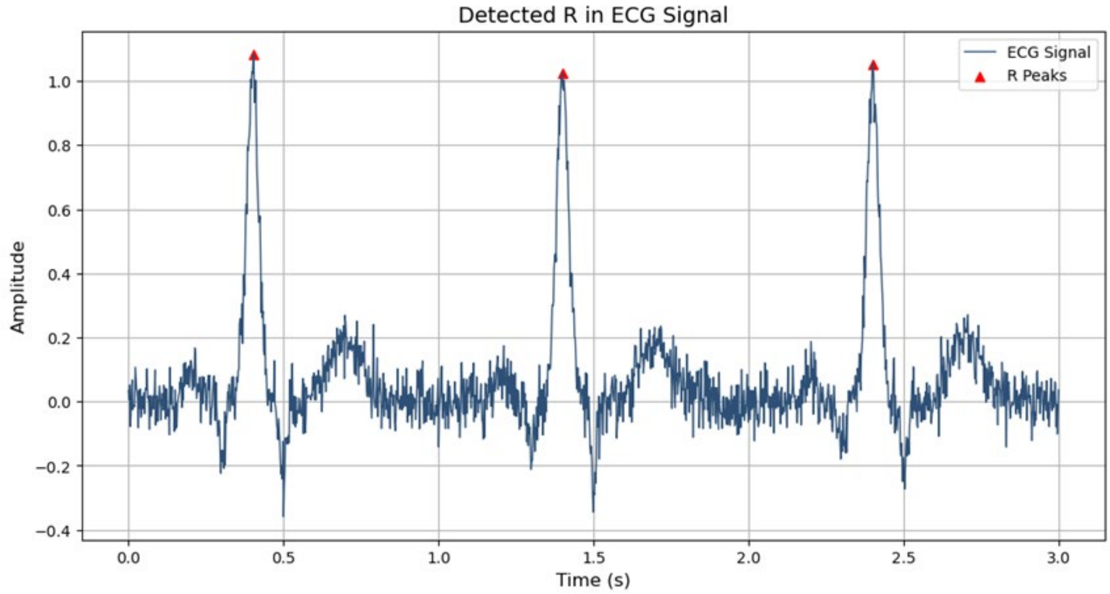

Fig. 7. Detected R in ECG Signal.

To mitigate the impact of noise and irregularities, a smoothing process is applied to the ECG signal. Fig. 8 shows the signal after smoothing, with a clearer underlying cardiac activity.

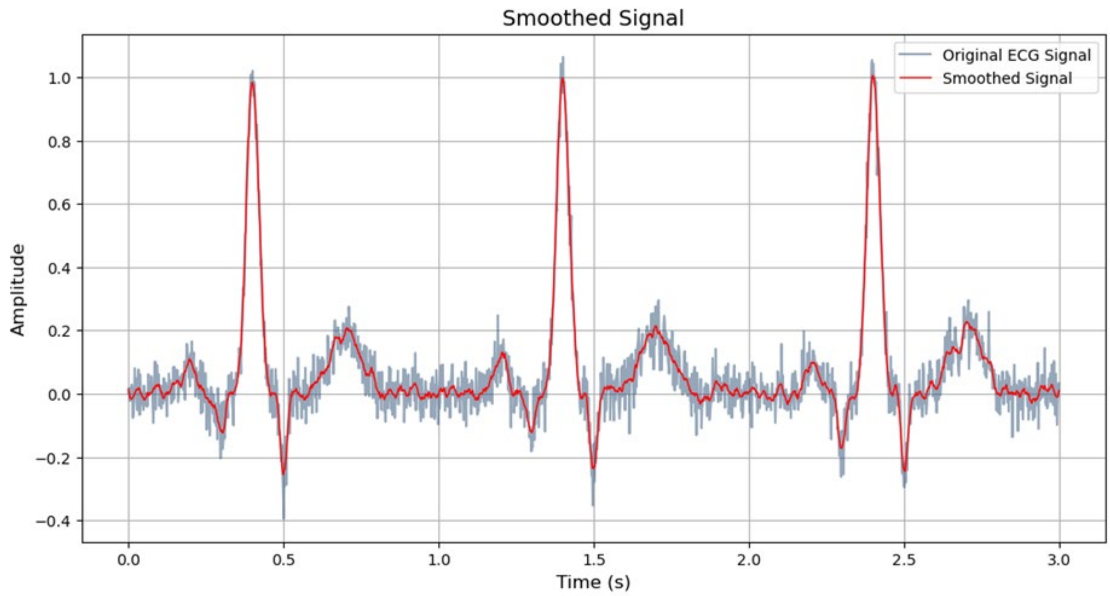

Fig. 8. Smoothed Signal.

The system was able to correctly identify people with 98% accuracy, showing it works as expected. Our system correctly recognized 95% of real tests (people who are part of the authentication system). The system works very well to distinguish real negative examples, rejecting unauthorized users 20% of the time, but struggles to tell apart negative and positive tests (75% false negative accuracy). By showing low accuracy for discriminating between negative and positive results, the system exposes one of its biggest problems. The model worked within 10 seconds which lets it match speeds required for working now. In Fig. 9, the graph illustrates the accuracy, sensitivity, and selectivity results.

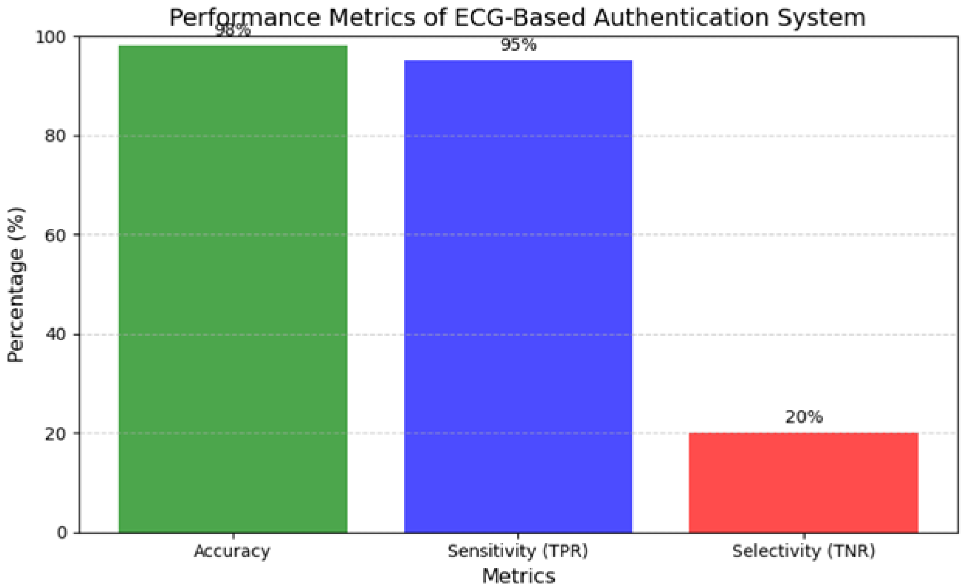

Fig. 9. Performance Metrics.

The confusion matrix from Fig. 10 helps us assess how well the system works. Looking at the matrix, we find that the system correctly classified 95% of authentic face images (True Positives) and 20% of non-authentic ones (True Negatives). When the system fails to catch 80% of false claims, it will label many regular users as experts. We need to improve how the system tells authentic and fake signals apart to work better.

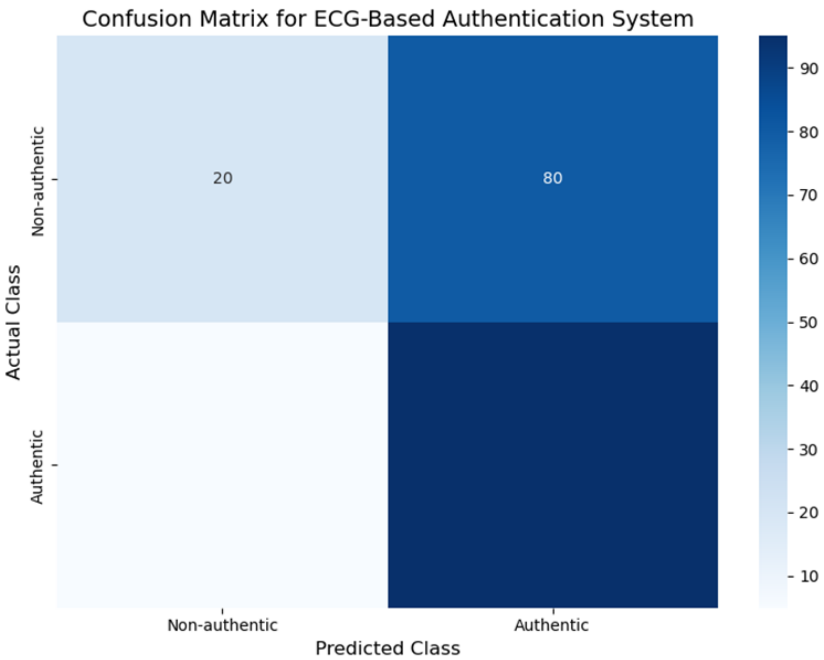

Fig. 10. Confusion Matrix.

The Receiver Operating Characteristic (ROC) curve is plotted as shown in figure 11 to evaluate the trade-off between sensitivity (True Positive Rate) and specificity (False Positive Rate). The curve showed an Area Under the Curve (AUC) of 0.98, indicating excellent performance in distinguishing between authentic and non-authentic individuals. However, the curve also revealed that the system's performance drops at higher specificity levels, which aligns with the low selectivity observed in the performance metrics.

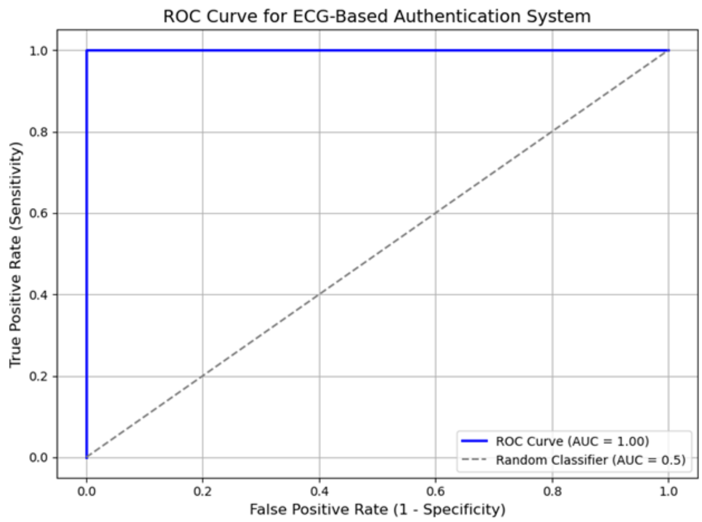

Fig. 11. ROC Curve for ECG-Based Authentication System.

Conclusion

A new way to identify people uses their ECG signals and modern signal processing with deep learning algorithms to create a strong, accurate, and reliable security system. The proposed system improves current biometrics by mixing advanced signal modifying techniques with new feature extracting ways and Artificial Neural Network learning, as a result they work better in actual world situations. The literature study acts as the foundation for building and creating the system, showing where current research stands and what problems still need to be solved. To make improvements, we will seek new and broader datasets to prove and improve the system better. To correctly use and easily apply the framework, we will need to see how well it works in different real-world security situations and control settings. Ongoing advancements in deep learning and signal processing will be utilized to enhance the system's performance, particularly in handling noise and inter-individual variability. Also, the framework should be expanded to accommodate future biometric challenges and incorporated with new technologies to make the system continue to stay on the cutting edge of biometric authentication innovation. Continuous research and development of this area is essential to the advancement of security standards and in meeting the ongoing security and reliable identification solution requirements.

Literature:

1. Ingale M. et al. ECG Biometric Authentication: A Comparative Analysis // IEEE Access. ieee institute of electrical electronics engineers, 2020. Vol. 8. P. 117853–117866.
2. Ahmed M.J. et al. CardioGuard: AI-driven ECG authentication hybrid neural network for predictive health monitoring in telehealth systems // SLAS Technology. sage, 2024. Vol. 29, № 5. P. 100193.
3. Liu J. et al. A novel P-QRS-T wave localization method in ECG signals based on hybrid neural networks // Computers in biology and medicine. n tab tab pergamon n tab tab n tab tab elmsford ny usa n tab, 2022. Vol. 150. P. 106110.
4. Schwerdtfeger A.R. et al. Heart rate variability (HRV): From brain death to resonance breathing at 6 breaths per minute // Clinical Neurophysiology. elsevier ireland, 2019. Vol. 131, № 3. P. 676–693.
5. Sohn J. et al. Reconstruction of 12-Lead Electrocardiogram from a Three-Lead Patch-Type Device Using a LSTM Network. // Sensors. molecular diversity preservation, 2020. Vol. 20, № 11. P. 3278.
6. Qu H., Pang L., Gao X. Classification of mental workload based on multiple features of ECG signals // Informatics in Medicine Unlocked. elsevier, 2021. Vol. 24. P. 100575.
7. Xiong P. et al. Short-term paroxysmal atrial fibrillation detection with intra- and inter-patient paradigm based on R-R intervals // Biomedical Signal Processing and Control. american

geophysical union, 2023. Vol. 89. P. 105750.
8. Da Silva H.P. et al. Finger ECG signal for user authentication: Usability and performance. institute of electrical electronics engineers, 2013. Vol. 2. P. 1–8.
9. El Boujnouni I. et al. A wavelet-based capsule neural network for ECG biometric identification // Biomedical Signal Processing and Control. american geophysical union, 2022. Vol. 76. P. 103692.
10. Meltzer D., Luengo D. Efficient Clustering-Based electrocardiographic biometric identification // Expert Systems with Applications. elsevier, 2023. Vol. 219. P. 119609.
11. Wagner P. et al. Explaining deep learning for ECG analysis: Building blocks for auditing and knowledge discovery // Computers in Biology and Medicine. n tab tab pergamon n tab tab n tab tab elmsford ny usa n tab, 2024. Vol. 176. P. 108525.
12. M S., Gupta N. A Survey on Biometric Authentication Using Electrocardiogram // SSRN Electronic Journal. elsevier, 2020.
13. Yang W., Wang S. A Privacy-Preserving ECG-Based Authentication System for Securing Wireless Body Sensor Networks // IEEE Internet of Things Journal. institute of electrical electronics engineers, 2022. Vol. 9, № 8. P. 6148–6158.
14. Khan M.U. et al. Biometric Authentication System Based on Electrocardiogram (ECG). institute of electrical electronics engineers, 2019. P. 1–6.
15. Issa M.F. et al. Heartbeat classification based on single lead-II ECG using deep learning // Heliyon. elsevier bv, 2023. Vol. 9, № 7. P. e17974.
16. Van Dam P.M. et al. The relation of 12 lead ECG to the cardiac anatomy: The normal CineECG // Journal of Electrocardiology. elsevier, 2021. Vol. 69. P. 67–74.
17. Uwaechia A.N., Ramli D.A. A Comprehensive Survey on ECG Signals as New Biometric Modality for Human Authentication: Recent Advances and Future Challenges // IEEE Access. ieee institute of electrical electronics engineers, 2021. Vol. 9. P. 97760–97802.
18. Wang D. et al. A Novel Electrocardiogram Biometric Identification Method Based on Temporal-Frequency Autoencoding // Electronics. mdpi ag, 2019. Vol. 8, № 6. P. 667.

Литература

1. Ингале М. и др. Биометрическая аутентификация на основе ЭКГ: Сравнительный анализ // IEEE Access. IEEE Institute of Electrical Electronics Engineers, 2020. Т. 8. С. 117853–117866.
2. Ахмед М.Дж. и др. CardioGuard: Гибридная нейронная сеть для аутентификации на основе ЭКГ с использованием ИИ для прогнозирующего мониторинга здоровья в телемедицинских системах // SLAS Technology. Sage, 2024. Т. 29, № 5. С. 100193.
3. Лю Дж. и др. Новый метод локализации волн P-QRS-T в сигналах ЭКГ на основе гибридных нейронных сетей // Computers in Biology and Medicine. Pergamon, 2022. Т. 150. С. 106110.
4. Швердтфегер А.Р. и др. Вариабельность сердечного ритма (ВСР): От смерти мозга до резонансного дыхания с частотой 6 вдохов в минуту // Clinical Neurophysiology. Elsevier Ireland, 2019. Т. 131, № 3. С. 676–693.
5. Сон Дж. и др. Реконструкция 12-канальной электрокардиограммы из трехканального устройства типа патч с использованием сети LSTM // Sensors. Molecular Diversity Preservation, 2020. Т. 20, № 11. С. 3278.
6. Цюй Х., Панг Л., Гао Х. Классификация умственной нагрузки на основе множественных признаков сигналов ЭКГ // Informatics in Medicine Unlocked. Elsevier, 2021. Т. 24. С. 100575.
7. Сюн П. и др. Обнаружение кратковременной пароксизмальной фибрилляции предсердий на основе парадигмы внутри- и межпациентного анализа интервалов R-R // Biomedical Signal Processing and Control. American Geophysical Union, 2023. Т. 89. С. 105750.
8. Да Силва Х.П. и др. Сигнал ЭКГ пальца для аутентификации пользователей: Удобство использования и производительность // Institute of Electrical Electronics Engineers, 2013. Т. 2. С. 1–8.
9. Эль Бужнуни И. и др. Капсульная нейронная сеть на основе вейвлетов для биометрической идентификации по ЭКГ // Biomedical Signal Processing and Control. American Geophysical Union, 2022. Т. 76. С. 103692.
10. Мельцер Д., Луэнго Д. Эффективная биометрическая идентификация на основе кластеризации электрокардиографических данных // Expert Systems with Applications. Elsevier, 2023. Т. 219. С. 119609.
11. Вагнер П. и др. Объяснение глубокого обучения для анализа ЭКГ: Базовые элементы для аудита и обнаружения знаний // Computers in Biology and Medicine. Pergamon, 2024. Т. 176. С. 108525.
12. М С., Гупта Н. Обзор биометрической аутентификации с использованием электрокардиограммы // SSRN Electronic Journal. Elsevier, 2020.
13. Ян В., Ван С. Система аутентификации на основе ЭКГ с сохранением конфиденциальности для защиты беспроводных сетей датчиков тела // IEEE Internet of Things Journal. Institute of Electrical Electronics Engineers, 2022. Т. 9, № 8. С. 6148–6158.
14. Хан М.У. и др. Система биометрической аутентификации на основе электрокардиограммы (ЭКГ) // Institute of Electrical Electronics Engineers, 2019. С. 1–6.
15. Исса М.Ф. и др. Классификация сердечных сокращений на основе одноканальной ЭКГ (отведение II) с использованием глубокого обучения // Heliyon. Elsevier BV, 2023. Т. 9, № 7. С. e17974.
16. Ван Дам П.М. и др. Связь 12-канальной ЭКГ с анатомией сердца: Нормальная CineECG // Journal of Electrocardiology. Elsevier, 2021. Т. 69. С. 67–74.
17. Уваечиа А.Н., Рамли Д.А. Всесторонний обзор использования сигналов ЭКГ как новой биометрической модальности для аутентификации человека: Современные достижения и будущие вызовы // IEEE Access. IEEE Institute of Electrical Electronics Engineers, 2021. Т. 9. С. 97760–97802.
18. Ван Д. и др. Новый метод биометрической идентификации на основе электрокардиограммы с использованием временно-частотного автоэнкодинга // Electronics. MDPI AG, 2019. Т. 8, № 6. С. 667.