PriMera Scientific Engineering
Volume 4 Issue 3 March 2024
DOI: 10.56831/PSEN-04-112
ISSN: 2834-2550

PriMera Scientific Publications

ML Based Enhanced Authentication Using ECG and PPG Signals for Remote Monitoring of Patients

Type: Research Article
Received: January 18, 2024
Published: February 22, 2024

Citation:
S Vallisree., et al. "ML Based Enhanced Authentication Using ECG and PPG Signals for Remote Monitoring of Patients". PriMera Scientific Engineering 4.3 (2024): 25-30.

SJ Dhyanesh, Partha Sarathy S, Harrish Kesavan and S Vallisree*

Department of Electronics Engineering, Madras Institute of Technology Campus, Anna University, Chennai, India

***Corresponding Author:** S Vallisree, Department of Electronics Engineering, Madras Institute of Technology Campus, Anna University, Chennai, India.

Abstract

There is an increased demand for individual authentication and advanced security methods with the technology advancement in all fields. The traditional methods using passwords etc. are prone to proxies. The Electrocardiogram (ECG) and Photoplethysmogram (PPG) can be used as a signature for biometric authentication systems because of their specificity, uniqueness, and unidimensional nature. In this work, ECG and PPG Based Biometric Identification Systems using Machine learning is proposed. This work provides an end-to-end architecture to offer biometric authentication using ECG and PPG biosensors through Support Vector Machine.

Keywords: ECG; PPG; Biometric Authentication; SVM and Arduino

Introduction

In contemporary security landscapes, conventional authentication methods, encompassing face recognition, fingerprint scans, and eye detection, confront inherent challenges that compromise their reliability. Factors such as changes in facial appearance, sensor contaminants, and sub-optimal lighting conditions contribute to the frequent failures of these methods. As technology evolves and computer networks expand, the need for transcendent authentication systems becomes imperative. The proliferation of large-scale networks brings forth an array of possibilities and concerns regarding identity theft, necessitating the design of authentication systems that not only ensure security but also prioritize accuracy, speed, reliability, cost-effectiveness, user-friendliness, and privacy preservation.

In this context, traditional authentication systems relying on secret keys or physical tokens exhibit limitations, primarily the assumption that only legitimate users will access them. Biometric-based personal authentication systems, on the other hand, leverage physiological or behavioural traits (such as fingerprint, iris, voice, face, palm-print, keystroke, and mouse dynamics) to ascertain the identity of the authenticating individual. While traditional systems face challenges of lost or forgotten credentials, biometric traits offer enhanced reliability as they are difficult to lose, forget, or guess. The in-

herent security of biometric traits, surpassing that of traditional passwords, enhances authentication accuracy and user convenience.

However, the exposure of anatomical traits, such as fingerprints, to potential theft and replication necessitates the exploration of novel, non-forgeable biometric traits. Recent studies have demonstrated the potential of the heart pulse as a biometric trait, offering the advantages of classic biometric traits while remaining less exposed to unauthorized access.

This thesis aims to contribute to the field of biometric authentication by developing an end-to-end system that utilizes Support Vector Machine (SVM) to authenticate individuals based on their raw Electrocardiogram (ECG) and Photoplethysmograph (PPG) signals. This innovative approach represents a significant step towards establishing a robust authentication system that verifies subject identity directly from ECG and PPG data. Our project introduces an advanced strategy that involves the simultaneous use of ECG and PPG signals for a dual authentication process, further fortifying the identification and authentication mechanisms. In critical sectors such as military applications, scientific research centers, and forensic departments, this dual authentication method holds substantial promise for enhancing security, ensuring access only to authorized personnel, and preserving the integrity of sensitive information and resources.

Methodology and Background

Convolutional Neural Network

A Convolutional Neural Network (CNN) is a special kind of deep learning algorithm that is really good at understanding pictures and signals. When it comes to checking if a person is who they say they are using signals from their heart (ECG) and pulse (PPG), a CNN can be super useful. Imagine your heart and pulse signals are like a puzzle. The CNN is like a smart friend that looks at the puzzle pieces and figures out how to put them together. It does this by using special filters to find important parts in the signals. Then, it simplifies the information but keeps the important stuff.

By showing the CNN lots of examples of heart and pulse signals, it learns what is normal for each person. It is like teaching it the unique patterns of your heart and pulse. Once it learns enough, it can recognize these patterns and tell if it's really you or not. A CNN helps in making sure you are who you say you are by understanding the special signals from your heart and pulse.

Siamese Neural Network

A Siamese Neural Network is a type of deep learning setup that involves using two or more identical sub-networks to analyze and categorize input pairs as either similar or dissimilar. Each sub-network shares a common set of weights and biases. These networks are fed pairs of inputs, like ECG or PPG signals, and then a comparison is made using a distance measure. The goal is to train the network to minimize the distance for similar input pairs (from the same person) and maximize it for dissimilar pairs (from different people). This way, the Siamese Network learns to distinguish between signals, making it useful for authenticating individuals based on their ECG or PPG patterns.

Support Vector Machine

The authentication of biometric signals such as ECG and PPG using machine learning algorithms has gained significant attention in recent years due to its reliability and security. One such algorithm is the Support Vector Machine (SVM), which has been shown to be effective for ECG and PPG signal authentication. In this approach, relevant features are extracted from the biometric signals, including heart rate, heart rate variability, and signal amplitudes. These features are then input to the SVM algorithm, which constructs a hyperplane in the feature space that maximally separates the different users. The trained SVM model can then be used for authentication, where new signals from a user are preprocessed and the extracted features are input to the model. If the model classifies the new signals as belonging to the same user as the training data, then authentication is successful.

By extracting relevant features from the biometric signals and training the SVM model to distinguish between different users, this approach has the potential to revolutionize user authentication in various applications, including healthcare, finance, and security.

The SVM algorithm offers several advantages for ECG and PPG signal authentication. Firstly, it can handle high-dimensional feature spaces, making it suitable for dealing with the complex patterns present in biometric signals. Secondly, it is robust to noise and outliers, which can be prevalent in biometric signals due to movement and other external factors. Finally, the SVM algorithm can learn complex decision boundaries, allowing it to distinguish between similar users and improve authentication accuracy.

In summary, the authentication of ECG and PPG signals using the SVM algorithm is a reliable and secure method for user authentication, offering several advantages over traditional authentication methods.

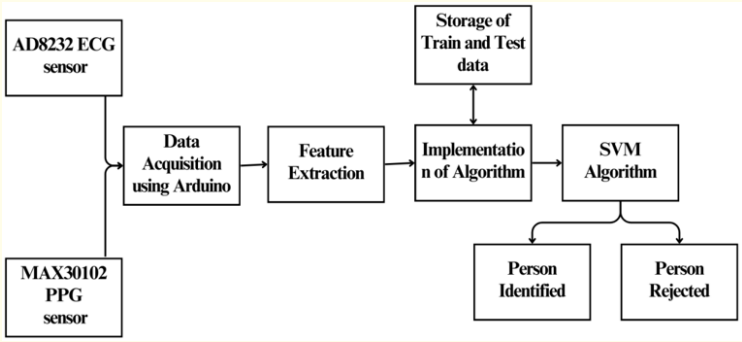

Figure 1: Block diagram of Embedded ECG and PPG Biometric Authentication.

In implementing the described machine learning approach Figure 1 for ECG and PPG signal authentication, embedded Arduino Boards are employed to gather real-time sensor data. Subsequently, feature extraction is conducted, and authentication is performed through a trial-and-error process involving CNN, SNN, and SVM machine learning algorithms. The objective is to ascertain whether the identified person aligns precisely with the expected individual. The process involves training the system to discern similarities and differences in the signals, aiding in the accurate authentication of individuals based on their unique ECG or PPG patterns. The utilization of Arduino Boards facilitates the seamless integration of sensor data, enhancing the efficiency of the overall authentication system. The ultimate outcome of this process is a reliable determination of whether the presented signals match the expected patterns, ensuring the robustness of the authentication mechanism.

Results and Discussion

Data Acquisition

For biometric authentication using Electrocardiogram (ECG) and Photoplethysmogram (PPG) data, specialized hardware (ad8232-heart sensor, MAX30102) and software (Roger meris freeware) are necessary to acquire, process, and authenticate the signals. Begin by setting up the hardware, which includes attaching ECG electrodes to the subject's body and using a PPG sensor, often integrated into a wearable device or a finger clip. Clean ECG signals were acquired by connecting the electrodes to a data acquisition device or ECG machine, while collecting PPG data using the sensor setup. 22 real-time data have been taken during both rest and at motion for ECG and PPG signals. After data acquisition, the signals were pre-processed by removing noise through filtering, normalization, and detrending.

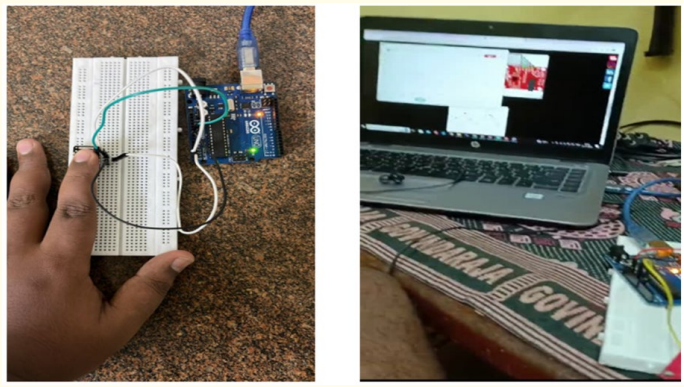

Figure 2: Real-time data acquisition of ECG and PPG Signal.

Relevant features from Figure 2 both signals were extracted that represent the individual's unique cardiovascular system, such as ECG wave morphology, intervals, and durations, as well as PPG heart rate, heart rate variability, and blood volume pulse morphology. These features were post-processed as needed for the authentication algorithm, and further implemented a biometric authentication algorithm that combines ECG and PPG features.

Feature Extraction

Feature extraction in biometric authentication using Electrocardiogram (ECG) and Photoplethysmogram (PPG) data involves processing techniques to derive relevant information from the acquired signals. Begin by pre-processing the signals to remove noise through filtering, normalization, and detrending. Features from ECG signals such as P-wave, QRS complex, and T-wave morphology, intervals, and durations, which represent the electrical activity of the heart were extracted. Parameters such as PR interval, QT interval, and RR interval, which are time intervals between different phases of the cardiac cycle were measured. From PPG signals, heart rate, heart rate variability, and blood volume pulse morphology were extracted, which provide insights into the individual's cardiovascular system.

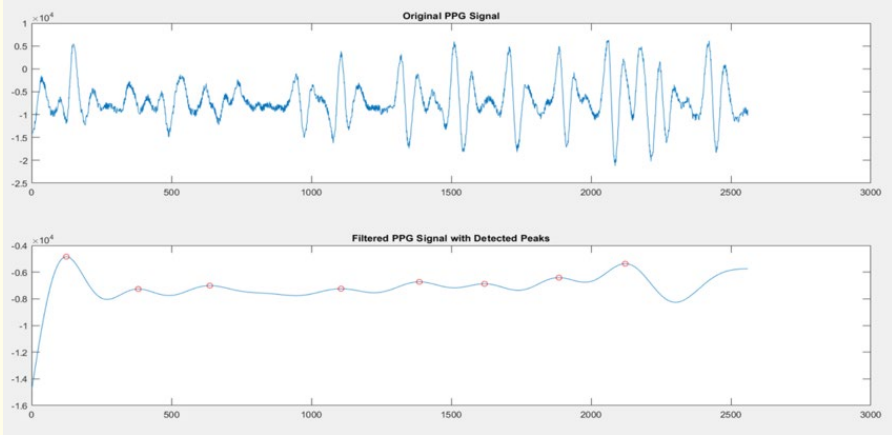

Figure 3: Feature extraction of PPG signal.

Necessary post-processing steps are performed like normalization or dimensionality reduction and these features are combined in a biometric authentication algorithm that creates a unique template for each individual. During authentication, the real-time ECG and PPG data were acquired from the user, compared it to the stored template, and grant access if the similarity measure exceeds a predefined threshold; otherwise, access is denied. Data security is ensured along with the user privacy throughout the process.

Authentication

The authentication of biometric signals such as ECG and PPG using machine learning algorithms has gained significant attention in recent years due to its reliability and security. One such algorithm is the Support Vector Machine (SVM), which is effective for ECG and PPG signal authentication. In this approach, relevant features are extracted from the biometric signals, including heart rate, heart rate variability, and signal amplitudes. These features are then input to the SVM algorithm, which constructs a hyperplane in the feature space that maximally separates the different users. The trained SVM model can then be used for authentication, where new signals from a user are preprocessed and the extracted features are input to the model. If the model classifies the new signals as belonging to the same user as the training data, then authentication is successful.

The SVM algorithm offers several advantages for ECG and PPG signal authentication. Firstly, it can handle high-dimensional feature spaces, making it suitable for dealing with the complex patterns present in biometric signals. Secondly, it is robust to noise and outliers, which can be prevalent in biometric signals due to movement and other external factors. Finally, the SVM algorithm can learn complex decision boundaries, allowing it to distinguish between similar users and improve authentication accuracy.

Classification/ Parameters	Support Vector Machine (SVM)	Convolution Neural Network (CNN)	Simple Neural Network (SNN)
Precision	0.921	0.879	0.8861
Recall	0.938	0.862	0.8862
F1 score	0.94	0.87	0.88
Accuracy	93.86%	86.51%	87.79%

Table 1: Results of various Machine Learning Algorithm.

In summary, Table 1 reveals that the authentication of ECG and PPG signals using the SVM algorithm is a reliable and secure method for user authentication, offering several advantages over traditional authentication methods. By extracting relevant features from the biometric signals and training the SVM model to distinguish between different users, this approach has the potential to revolutionize user authentication in various applications, including healthcare, finance, and security.

Conclusion

In conclusion, our study involved the collection of time-domain data from Electrocardiogram (ECG) and Photoplethysmogram (PPG) signals for double authentication from 22 individuals in both resting and motion states. The data were obtained simultaneously using ARDUINO-based sensors and converted into Excel format. This dataset serves as a valuable resource for comparing and filtering data using machine learning algorithms, including Support Vector Machine (SVM), Siamese Neural Network (SNN), and Convolutional Neural Networks (CNN). After subjecting the data to these ML algorithms, we found that the Support Vector Machine (SVM) demonstrated

a particularly noteworthy performance, achieving a high accuracy of 94% when combining both ECG and PPG signals. This accuracy is a compelling result, indicating the efficacy of SVM in correctly identifying individuals during double authentication scenarios. The utilization of SVM showcases its capability to handle complex datasets and discern patterns in time-domain data, making it a reliable choice for secure authentication applications. Moreover, the study highlights the potential of combining ECG and PPG signals for enhanced accuracy in person identification. The simultaneous capture of data in resting and motion states adds a layer of robustness to the authentication process, making it applicable in real-world scenarios where individuals may be in various physiological states.

References

1. G Wang, D John and A Nag. "Low Complexity ECG Biometric Authentication for IoT Edge Devices". 2020 IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA), Nanjing, China (2020): 145-146.
2. Sarkar Abhijit., et al. "Biometric authentication using photoplethysmography signals". 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) (2016): 1-7.
3. A Panda, S Pinisetty and P Roop. "A Novel Mapping of ECG and PPG to Ensure the Safety of Health Monitoring Applications". in IEEE Embedded Systems Letters 15.1 (2023): 49-52.
4. JD Peshave and R Shastri. "Feature extraction of ECG signal". 2014 International Conference on Communication and Signal Processing, Melmaruvathur, India (2014): 1864-1868.
5. Isakadze N and Martin SS. "How useful is the smartwatch ECG?". Trends Cardiovasc Med 30.7 (2020): 442-448.
6. Bastos Lucas., et al. "Smart Human Identification System Based on PPG and ECG Signals in Wearable Devices". 2021 International Wireless Communications and Mobile Computing (IWCMC) (2021): 347-352.
7. Aziz Saira, Ahmed Sajid and Alouini Mohamed-Slim. "ECG-based machine-learning algorithms for heartbeat classification". Scientific Reports 11 (2021) 18738.
8. DE Mancilla-Palestina., et al. "Embedded System for Bimodal Biometrics with Fiducial Feature Extraction on ECG and PPG Signals". 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Dubrovnik, Croatia (2020): 1-6.
9. Chowdhury Meghna., et al. "Deep learning via ECG and PPG signals for prediction of depth of anesthesia". Biomedical Signal Processing and Control 68 (2021): 102663.
10. Lee Hyeonjeong, Lee Jaewon and Shin Miyoung. "Using Wearable ECG/PPG Sensors for Driver Drowsiness Detection Based on Distinguishable Pattern of Recurrence Plots". Electronics 8 (2019): 192.
11. Belo D., et al. "ECG Biometrics Using Deep Learning and Relative Score Threshold Classification". Sensors (Basel) 20.15 (2020): 4078.
12. H Shahid., et al. "A Survey on AI-based ECG, PPG, and PCG Signals Based Biometric Authentication System". 2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), Quetta, Pakistan (2021): 1-6.
13. W Louis, M Komeili and D Hatzinakos. "Continuous Authentication Using One-Dimensional Multi-Resolution Local Binary Patterns (1DMRLBP) in ECG Biometrics". in IEEE Transactions on Information Forensics and Security 11.12 (2016): 2818-2832.
14. A Benabdallah and A Djebbari. "Biometric Individual Authentication System using High Performance ECG Fiducial Features". 2022 5th International Symposium on Informatics and its Applications (ISIA), M'sila, Algeria (2022): 1-6.
15. AN Uwaechia and DA Ramli. "A Comprehensive Survey on ECG Signals as New Biometric Modality for Human Authentication: Recent Advances and Future Challenges". in IEEE Access 9 (2021): 97760-97802.