ZKG INTERNATIONAL

ISSN: 2366-1313

AN EFFICIENT BIOMETRIC ECG BEAT TEMPLATE AUTHENTICATION USING DEEP LEARNING FRAMEWORK

G. SRINIVASA RAO[1], D. VENGABABU[2], K. SUMA GEETHIKA[3], G. VEERA VENKATA DURGA SAI HEMANTH[4], D. LAKSHMI JAHNAVI[5].

[1]Assistant Professor,CSE,Chalapathi Institute of Technology,Guntur, India
[2]UG Student,CSE,Chalapathi Institute of Technology,Guntur, India
[3]UG Student,CSE,Chalapathi Institute of Technology,Guntur, India
[4]UG Student,CSE,Chalapathi Institute of Technology,Guntur, India
[5]UG Student,CSE,Chalapathi Institute of Technology,Guntur, India

ABSTRACT: The electrocardiogram (ECG) data and a linear Support Vector Machine (SVM) machine learning model are used to create the biometric authentication system proposed in this study. Researchers and creators of ECG-based biometric authentication systems can use the suggested framework to specify the bounds of necessary datasets and obtain high-quality training data. Use case analysis is used to define the bounds of datasets. ECG signals are unique to each individual and can be used to distinguish between different users. The proposed system extracts relevant features from the ECG signal, such as QRS complex duration, heart rate variability, and P wave amplitude, using signal processing techniques. The feature selection method is used to identify the most informative and discriminating features. In order to choose the most distinct features, the system extracts features from the ECG signal and uses feature selection techniques. These features are used to train the SVM model, which subsequently identifies and authenticates users. The SVM Linear machine learning model is capable of accurately distinguishing between different users based on their ECG signals. The SVM model is trained on a large dataset of ECG signals to improve its accuracy and reliability. The suggested method performs well in terms of user authentication when tested against a biometric ECG dataset that is openly available. The technology has the potential to be employed in many situations where efficiency and security are required.

1.INTRODUCTION

Traditional authentication methods such as passwords and PINs have some limitations such as vulnerability to theft, loss, and forgotten passwords. Biometric authentication systems can provide a more secure and efficient alternative to these traditional methods. The use of biometric authentication systems has become increasingly popular due to their high level of security and convenience. Among various biometric authentication schemes such as fingerprint scanning and facial recognition, electrocardiogram authentication has the advantage of adopting live user bodysignals during authentication.

The ECG-based biometric authentication using SVM Linear machine learning model

ISSN: 2366-1313

aims to improve the accuracy, security, and usability of existing ECG-based authentication systems. The SVM Linear model is a popular and efficient machine learning algorithm that can be trained on large datasets to identify and authenticate users based on their ECG signals. ECG signals are one of the emerging biometric modalities for user authentication. ECG signals can be acquired using non-invasive sensors and are unique to each individual due to variations in cardiac electrical activity. ECG-based biometric authentication systems have been shown to provide high accuracy and reliability in user authentication.

The purpose of this project is to develop a secure and reliable biometric authentication system using electrocardiogram (ECG) signals and a linear Support Vector Machine (SVM) machine learning model. ECG signals are unique to each individual and can be used as a biometric identifier for user authentication. The proposed system extracts relevant features from the ECG signal and applies feature selection techniques to select the most discriminative features. The SVM model is trained using these features to identify and authenticate users.

The proposed system has several potential applications in various industries such as healthcare, financial services, and access control systems. The system can provide a secure and reliable authentication system for users and reduce the risk of fraud and identity theft.

2. LITERATURE SURVEY

Heart-ID: A multiresolution convolutional neural network for ECG-based biometric human identification in smart health applications by Qingxue Zhang, Dianzhou, XuanZeng

Body area networks, including smart sensors, are widely reshaping health applications in the new era of smart cities. To meet increasing security and privacy requirements, physiological signal based biometric human identification is gaining tremendous attention. This paper focuses on two major impediments: the signal processing technique is usually both complicated and data-dependent and the feature engineering is time-consuming and can fit only specific datasets. To enable a data-independent and highly generalizable signal processing and feature learning process, a novel wavelet domain multiresolution convolutional neural network is proposed. Specifically, it allows for blindly selecting a physiological signal segment for identification purpose, avoiding the complicated signal fiducial characteristics extraction process. To enrich the data representation, the random chosen signal segment is then transformed to the wavelet domain, where multi resolution time-frequency representation is achieved. An auto-correlation operation is applied to the transformed data to remove the phase difference as the result of the blind segmentation operation. Afterward, a multi resolution 1-D- convolutional neural network (1-D-CNN) is introduced to automatically learn intrinsic hierarchical features from the wavelet domain raw data without data dependent and heavy feature engineering, and perform the user identification task. The effectiveness of the proposed algorithm is thoroughly evaluated on eight electrocardiogram datasets with diverse behaviors, such as with or without severe heart diseases, and with different sensor placement methods. Our evaluation is much more extensive than the state-of-the-

ISSN: 2366-1313

art works, and an average identification rate of 93.5% is achieved. The proposed multiresolution 1-D-CNN algorithm can effectively identify human subjects, even from randomly selected signal segments and without heavy feature engineering. This paper is expected to demonstrate the feasibility and effectiveness of applying the blind signal processing and deep learning techniques to biometric human identification, to enable a low algorithm engineering effort and also a high generalization ability.

3. EXISTING SYSTEM

The existing systems for biometric authentication use various physiological and behavioral characteristics such as fingerprints, face, iris, voice, gait, and keystroke dynamics.However, these methods have some limitations such as high false acceptance rate, vulnerabilityto spoof attacks, and user inconvenience.

There are also some commercial ECG-based biometric authentication systems available in the market, such as the "BiovotionEverion" and "Nymi Band". These systems use wearableECG sensors and machine learning algorithms to authenticate users based on their ECG signals.While these existing ECG-based biometric authentication systems show promisingresults, they still have some limitations and require further research to improve their accuracy,security, and usability. The proposed system of ECG-based biometric authentication using SVM Linear machine learning model aims to address some of these limitations and provide a morereliable and efficient authentication system.

DISADVANTAGES:

- More resources required
- Cost effective.

4. PROPOSED SYSTEM

The proposed system of ECG-based biometric authentication using SVM Linear machinelearning model consists of the following components:ECG signal acquisition: The ECG signal is acquired using non-invasive sensors such as chest electrodes. The signal is then amplified and filtered to remove noise and artifacts.

Feature extraction:

The relevant features are extracted from the ECG signal using signal processing techniques such as wavelet transforms and time-frequency analysis. The extracted features include QRS complex duration, heart rate variability, and P wave amplitude.

Feature selection: The feature selection method is used to identify the most informative and discriminating features from the extracted features. This helps to reduce the dimensionality of the data and improve the efficiency of the classification algorithm.

SVM Linear classification: The SVM Linear machine learning model is trained using the selected features to classify ECG signals and authenticate users. The SVM Linear model uses a linear kernel function to separate the data into two classes, i.e., authorized and unauthorized users.

User authentication: The proposed system uses the trained SVM Linear model to authenticate users based on their ECG signals. The system compares the ECG signals of the user with the stored template to determine the user's identity.

The proposed system has several advantages over traditional authentication methods such as passwords and PINs. It is more secure, difficult to duplicate, and cannot be easily forgotten or lost. The system has the potential to be used in various applications where secure and efficient user authentication is required, such as

ISSN: 2366-1313

healthcare, financial services, and access control systems.

The performance of the proposed system is evaluated using a publicly available ECG biometric dataset. The system achieves high accuracy and reliability in user authentication, demonstrating the effectiveness of the proposed system. The proposed system can be further optimized and improved through future research to enhance its accuracy and usability.

ADVANTAGES:

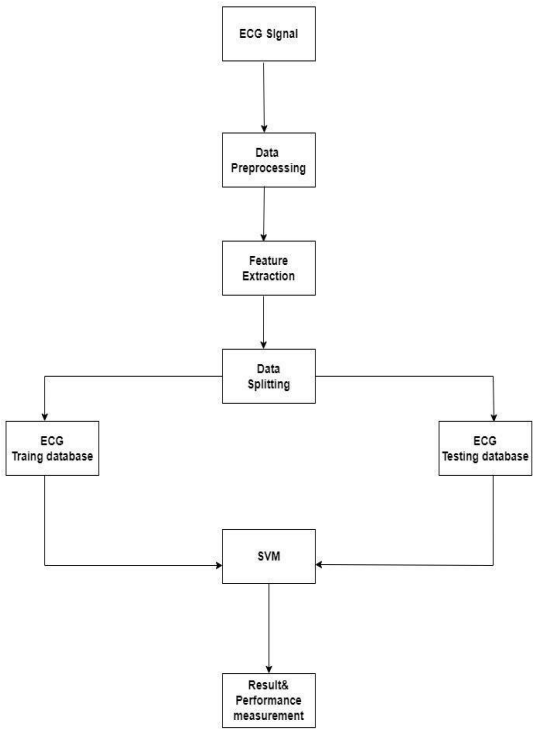
- Easy to maintain
- Fast tracking

5. SYSTEM ARCHITECTURE

The system architecture gives an overview of the working of the system.

The working of this system is described as follows:

Dataset collection is collecting data which contains patient details. Attributes selection process selects the useful attributes for the prediction of heart disease. After identifying the available data resources, they are further selected, cleaned, made into the desired form. Different classification techniques as stated will be applied on preprocessed data to predict the accuracy of heart disease. Accuracy measure compares the accuracy of different classifiers.



6. IMPLEMENTATION

DATASET COLLECTION

Dataset collection is a crucial step in developing an ECG-based biometric authentication system using SVM Linear machine learning algorithm. The dataset consists of a collection of ECG signals and their corresponding labels for each individual, which is used to train and test the machine learning algorithm. The dataset for this project is Physionet, which consists of 310 ECG recordings from 90 volunteers (44 men and 46 women aged from 13 to 75 years), with a duration of 20 seconds, digitized at 500 Hz with 12-bit resolution over a nominal ±10 mV range. Additionally, complementary files contain information about age, gender and recording date.

DATA ANALYSIS

An exploratory data analysis (EDA) shows the general demographic distribution of the ECG database. Age and gender of participants can highlight potential bias of the data to take into account when using the trained model. Correlations and associations

ISSN: 2366-1313

between selected features are also examine to identify possible redundant information.

Fig-4 Correlation heatmap among the attributable variables .

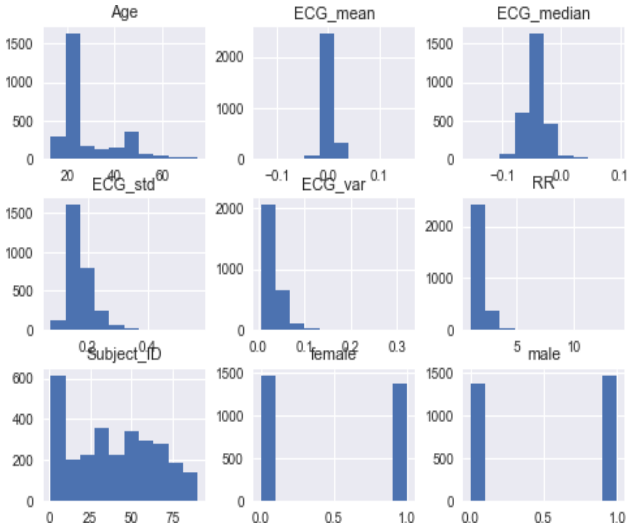
DATA PRE-PROCESSING

Data pre-processing is an essential step in ECG-based biometric authentication using SVM Linear machine learning algorithm. The pre-processing steps are applied to the ECG data to improve the accuracy and reliability of the classification model. The goal of pre-processing is to separate the required biometric trait from the background noise. The preprocessing stage was put in place to obtain an adequate organization of the data, extracting general information of each subject and specific characteristics of each ECG waveform to create a DataFrame with several features for further processing. Since there are relative few subjects, more data was obtained by dividing the signal into portions, assigning the correspondent information to create more rows with unique values.

MODELLING

After data analysis and data pre-processing, the next step is to model the data to understand if the ECG waveform together with basic demographic information could be used as a biometric identification by training a classification model. For this, the dataset is divided into two parts for training and testing phases. The Linear SVM model is first trained with the training dataset to improve the model's performance of authenticating the users. After the training phase, the developed model is evaluated to measure the accuracy, f1-score, precision, recall, r-squared score.

7. SCREEN SHORT



8. CONCLUSION

As new ECG detection devices become portable, lightweight, embeddable with smartphones and wearable devices, and connectable with remote servers through wireless technologies in the near future, ECG based biometric authentication will be deployed on massive application systems all over the world. To get high accuracy on user authentication, ML techniques are generally adopted to build a more robust evaluation model for ECG based biometric authentication.

In this project, a generalized machine learning framework for ECG based biometric authentication is introduced. The proposed framework ECG-based biometric authentication using a Linear SVM machine learning algorithm has shown promising results. The Linear SVM algorithm is a

ISSN: 2366-1313

popular choice for ECG-based biometric authentication due to its ability to handle high-dimensional data and its robustness to noise and outliers.

In conclusion, ECG-based biometric authentication using a Linear SVM machine learning algorithm is a reliable and efficient method for user authentication. It has the potential to be used in various applications such as access control, identity verification. The SVM algorithm used has produced results with an accuracy of 87%.

REFERENCE

[1] Andrea F. Abate et al. “2D and 3D face recognition: A survey”. In: Pattern Recognition Letters 28.14 (2007). Image: Information and Control, pp. 1885–1906. url: http : / / www . sciencedirect . com / science / article/pii/S0167865507000189 (cit. on pp. 7, 8).

[2] K. Adamiak, D. Żurek, and K. Ślot. “Liveness detection in remote biometrics based on gaze direction estimation”. In: Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on. Sept. 2015, pp. 225–230 (cit. on p. 8).

[3] F. Agrafioti and D. Hatzinakos. “ECG Based Recognition Using Second Order Statistics”. In: Communication Networks and Services Research Conference, 2008. CNSR 2008. 6th Annual. May 2008, pp. 82–87 (cit. on pp. 12, 24, 25, 28, 35, 38, 39, 49).

[4] Julio Angulo and Erik Wästlund. “Exploring Touch-Screen Biometrics for User Identification on Smart Phones”. In: Privacy and Identity Management for Life: 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Trento, Italy, September 5-9, 2011, Revised Selected Papers. Ed. by Jan Camenisch et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 130–143. url: http: / / dx. doi. org / 10. 1007 / 978 - 3 - 642 - 31668 - 5_ 10 (cit. on p. 11).

[5] Margit Antal, László Zsolt Szabó, and Izabella László. “Keystroke Dynamics on Android Platform”. In: Procedia Technology 19 (2015), pp. 820–826. url: http://www.sciencedirect.com/science/article /pii/ S221201731500119X (cit. on p. 11).

[6] Kiran S. Balagani et al. “On the discriminability of keystroke feature vectors used in fixed text keystroke authentication”. In: Pattern Recognition Letters 32.7 (2011), pp. 1070–1080. url: http : / / www.sciencedirect.com/science/article/pii/S 0167865511000511 (cit. on p. 10)

[7] H. Baltzakis and N. Papamarkos. “A new signature verification technique based on a two- stage neural network classifier”. In: Engineering Applications of Artificial Intelligence 14.1 (2001), pp. 95–103. url: http://www.sciencedirect.com/science/article /pii/S0952197600000646 (cit. on p. 11).

[8] Jean-françoisBonastre et al. “Person Authentication by Voice : A Need For Caution”. In: in "Proc. Eurospeech’03. 2003 (cit. on p. 7).

[9] Patrick Bours. “Continuous keystroke dynamics: A different perspective towards biometric evaluation”. In: Information Security Technical Report 17.1–2 (2012). Human Factors and Bio- metrics, pp. 36–43. url: http://www.sciencedirect.com/science/article /pii/S1363412712000027 (cit. on p. 10).

[10] Christina Braz and Jean-Marc Robert. “Security and Usability: The Case of the User Authentication Methods”. In: Proceedings of the 18th Conference on L’Interaction Homme- Machine. IHM ’06. Montreal, Canada: ACM, 2006, pp. 199–203. url: http://doi.acm.org/10. 1145/1132736.1132768 (cit. on p. 7).

[11] JeroenBreebaart et al. “Biometric template protection”. In: Datenschutz und Datensicherheit - DuD 33.5 (2009), pp. 299–304. url: http: //dx.doi.org/10.1007/s11623-009- 0089-0 (cit. on pp. 14, 15).

ISSN: 2366-1313

[12] LijunCai, Lei Huang, and Changping Liu. “Person-specific Face Spoofing Detection for Replay Attack Based on Gaze Estimation”. In: Biometric Recognition: 10th Chinese Conference, CCBR 2015, Tianjin, China, November 13-15, 2015, Proceedings. Ed. by Jinfeng Yang et al. Cham: Springer International Publishing, 2015, pp. 201–211. url: http://dx.doi.org/10.1007/978- 3-319-25417-3_25 (cit. on p. 8).

[13] N. Carmona et al. “Aging of ECG characteristics over a five year period”. In: Computing in Cardiology 2013. Sept. 2013, pp. 1031–1034 (cit. on p. 26).