Electrocardiogram biometric system: Analytical Review

Tiba Najah Khazaal Thekra Abbas
Computer Science Department - Mustansiriyah University
tiba.najah98@uomustansiriyah.edu.iq thekra.abbas@uomustansiriyah.edu.iq

Abstract:
Biometric features have recently been used for security, which has led to their widespread use. However, they can be threatened, faked, lost, or hacked. Recently, the ECG has been employed as a biometric tool, and it may be better suited because it contains precise, private, and secret information about the patient. The person's identity was safeguarded and protected, and the ECG was utilized to identify him and prevent information violations. ECG identification has a lot of benefits and high accuracy, but it can also be affected by interference and noise in the ECG signals. This paper presents a few typical electrocardiogram measurement techniques and provides a comprehensive overview of electrocardiograms.
Keywords: biometric features, threats, counterfeiting, loss, hacking, ECG, verify identity, enhance protection.

النظام البيومتري لتخطيط القلب الكهربائي: مراجعة تحليلية

طيبة نجاح خزعل ذكرى عباس
قسم علوم الحاسوب – الجامعة المستنصرية

الخلاصة:
تم مؤخراً استخدام السمات البيومترية لأغراض أمنية، مما أدى إلى انتشار استخدامها على نطاق واسع. ومع ذلك، يمكن أن يتم تهديدهم أو تزييفهم أو فقدهم أو اختراقهم. في الآونة الأخيرة، تم استخدام تخطيط القلب كأداة للقياسات الحيوية، وقد يكون أكثر ملاءمة لأنه يحتوي على معلومات محددة وخاصة وسرية عن المريض. تم الحفاظ على هوية الشخص وحمايتها، وتم استخدام مخطط كهربية القلب للتعرف عليه ومنع انتهاك المعلومات. يتمتع التعرف على تخطيط كهربية القلب بالكثير من الفوائد والدقة العالية، ولكنه قد يتأثر أيضًا بالتداخل والضوضاء في إشارات تخطيط كهربية القلب. تعرض هذه الورقة بعض تقنيات قياس مخطط كهربية القلب النموذجية وتقدم نظرة شاملة عن مخططات كهربية القلب.
الكلمات المفتاحية: السمات البيومترية، التهديدات، التزييف، الخسارة، القرصنة، تخطيط القلب، التحقق من الهوية، تعزيز الحماية.

1.Introduction

A biometric system can identify a person based on a feature vector that person has. Biometric systems stand as technological marvels, discerning and identifying individuals through unique feature vectors derived from their physical or mental attributes. Take the ubiquitous fingerprint device, a marvel of modern security—its functionality branches into two core operations: identification and verification, adapting to diverse application settings as needed [1].

Information authentication is a commonly employed technique utilized by security professionals to confirm the identities of users prior to system access. In the realm of security protocols, information authentication emerges as the bedrock, a tried-and-tested method wielded by security professionals. This approach rigorously validates user identities before granting access to sensitive systems, reinforcing the fortress of digital security [2].

The major advantage of biometric security systems is that they don't rely on what you have or can remember; instead, they identify you based on your physical attributes or behavioral traits. What makes biometric security systems shine is their emancipation from reliance on physical possessions or memorized data. One of the pioneering elements in the realm of biometric recognition, electrocardiograms (ECGs), harness the heart's electrical activity to provide a distinct identifier for individuals. Electrocardiograms (ECGs), which can be used to monitor the heart's electrical activity Because of its fundamental advantage of boosting security while lowering the need to keep or remember passwords or other credentials, biometric recognition based on ECGs or other modalities has already been suggested for several Internet of Things (IoT) applications. The exploration of ECG-based biometric recognition in various Internet of Things (IoT) applications, especially in healthcare-centric systems like IoT-based medical monitoring, has gained traction. This shows that biometric systems, as opposed to password- or ID-card-based systems, which can be stolen, can be made more user-friendly and tougher to imitate. The inherent inability to pilfer or replicate an individual's ECG stands as a pivotal advantage, bolstering resistance against fraudulent credential usage [3].

However, within the realm of ECG identification, challenges rear their heads—interference factors and pesky noise disrupt the pristine signals. Issues like power line interference, stemming from electrical supply systems and manifesting as periodic noise at 50 or 60 Hz (depending on locale), pose hurdles. The skin's inadequate contact with electrodes spawns electrode contact noise, while muscle contractions inject unwanted artifacts, creating further disruptions [4].

To mitigate these challenges, numerous strategies have been developed, including precise electrode placement, sophisticated signal filtering techniques, signal averaging methodologies, and shielding mechanisms against external electromagnetic sources. Moreover, the real-time nature of the ECG provides avenues for advancing security by verifying the liveness of the individual providing the biometric. This capability distinguishes ECG-based authentication from traditional biometrics like fingerprints, iris scans, or facial recognition, which often necessitate supplementary procedures to confirm liveness. The continuous evolution of ECG authentication heralds promising prospects for heightened security and refined authentication protocols in the future [5].

Herein lies a unique trait of the ECG—it serves as a liveness signal. The prospect of future applications verifying the biometric provider's live presence becomes tantalizingly possible. Unlike conventional biometrics necessitating additional procedures to ensure liveness, the ECG, with its intrinsic nature, paves the way for more seamless authentication processes. This potential heralds a new era where the biometric provider and carrier merge seamlessly, transcending the limitations of typical biometric authentication methodologies [6].

The subsequent sections of the paper are structured in the following manner: Section 2 provides an overview of the relevant literature. Section 3 provides an overview of the primary methods used in the pre-processing of trajectory data. Section 4 focuses on the primary methodologies for measuring trajectory similarities and identifying the shortest path. The article conclusions are stated in Section 5..

2.Related Work

The safeguarding of computer systems against unauthorized access and the accurate identification of individuals are paramount concerns in the realm of digital security. Ensuring the integrity of electronic systems is crucial to prevent breaches, data leaks, and potential cyber threats. The constant evolution of technology has led to innovative methods for enhancing security, such as biometric authentication and multifactor identification. Unauthorized access to computers can result in significant data breaches, financial losses, and compromised privacy. As a result, the development of robust techniques to detect and thwart fraudulent activities in the digital domain is of utmost importance. Electrocardiogram (ECG) technology has emerged as a promising avenue for bolstering security and personal identification. The ECG, which records the electrical activity of the heart, is a unique physiological trait that can be used to distinguish individuals with a high degree of accuracy.

There is Several authors have supported the field of ECGs Techniques, including

Gang Z.et.al (2017): This paper presents strategies for Electrocardiogram (ECG) based identification. The proposed approach involves a selecting mechanism based on information entropy to extract the entire heart beat signal, followed by a Depth Neural Network (DNN) based on Denoising AutoEncoder (DAE) for unsupervised feature selection. This process improves the robustness of the recognition system for accurate identification. The proposed selecting strategy based on information entropy effectively filters incomplete single periodic ECG signals, reducing their impact on identification accuracy. The DAE-based DNN automatically learns the features of ECG signals, facilitating the identification process. Experimental results demonstrate the effectiveness of the proposed approach. Recognition rates of 98.10% and 95.67% were achieved on self-collected calm and high-pressure datasets, respectively. The combined dataset, which includes the MIT arrhythmia database (mitdb) and self-collected data, achieved an average recognition rate of 94.39%. The paper nevertheless has a number of flaws. The robustness of the technique to various dataset types and outlier distributions was not thoroughly examined by the authors. Furthermore, the suggested algorithm's assessment was restricted to a small number of benchmark datasets, which may not accurately reflect datasets from the actual world [7].

Z. Zhao.et.al (2018): This work describes a revolutionary electrocardiogram (ECG) signal-based biometric authentication method for human identity. To overcome the drawbacks of current ECG biometric techniques, the suggested system combines a convolutional neural network (CNN) and a generalized S transformation (GST). To tackle the intricacies of ECG waveform detection and segmentation approaches, the system first use a blind segmentation strategy. This strategy avoids the need for specific identification of R-peaks and QRS waves. Next, a generalized S transformation is performed on the segmented ECG signal, capturing the ECG trajectory in the frequency domain. The getframe technology is then utilized to convert the one-dimensional signal into a two-dimensional image. Each image represents the ECG trajectory at a particular time point, providing a comprehensive representation of the changing trend in the ECG signal spectrum characteristics over time. The CNN is employed for automatic discriminative feature learning and representations, eliminating the need for laborious feature extraction algorithms. The CNN significantly reduces the workload associated with feature engineering and captures intrinsic feature patterns effectively. To evaluate the effectiveness of the proposed algorithm, experiments are conducted on three ECG databases with diverse features: normal individuals, atrial fibrillation patients, and a noisy database. Promising identification rates of 99%, 98%, and 99% are achieved, respectively, However, one weakness of the proposed system is that it may not perform well in cases where there is a high density of dataset [8].

Ruggero D.et.al (2019): This paper introduces Deep-ECG, a novel approach for electrocardiographic (ECG) biometric recognition using Convolutional Neural Networks (CNNs). The goal is to enhance the accuracy and performance of ECG-based biometric systems, which are typically less accurate compared to other physiological traits. Deep-ECG leverages the capability of CNNs to automatically extract distinctive features from one or more ECG leads. The proposed Deep-ECG approach is the first of its kind in the literature to utilize CNNs for ECG biometrics. The strengths of this paper lie in its comprehensive review of real-time big data processing techniques for ECGs detection, which is a significant challenge in many application domains. It extracts significant features from ECG signals through a deep CNN and compares biometric templates using simple and fast distance functions. Deep-ECG achieves remarkable accuracy in tasks such as identification, verification, and periodic re-authentication. Additionally, a quantization procedure enables Deep-ECG to generate binary templates, facilitating the use of ECG-based biometric systems for cryptographic applications. To address the challenge of limited training data, the paper introduces a simple method to enlarge the training dataset of ECG samples, which enhances the performance of deep neural networks. Extensive experiments were conducted on large sets of samples acquired in uncontrolled conditions, demonstrating the accuracy and robustness of Deep-ECG in non-ideal scenarios. The performance of Deep-ECG was also evaluated using the PTB Diagnostic ECG Database, achieving identification accuracy that is better or comparable to the best methods in the literature, even for signals with different characteristics than those used for training the CNN. However, this paper has some limitations. Firstly, the author did not provide a comparative analysis of different techniques, which could have helped readers to understand the relative performance of different approaches. Secondly, the paper focuses on real-time processing, and some techniques might not be suitable for real-time applications [9].

A. Goshvarpour and Atefeh G., (2019): This paper aims to develop a reliable identification system using electrocardiogram (ECG) biometrics based on a non-fiducial approach. The ECG signals of 90 participants were decomposed using matching pursuit (MP) analysis, and various statistical and nonlinear measures were extracted from the MP coefficients. The performance of the ECG features extracted by MP analysis in human identification was evaluated using the probabilistic neural network (PNN) and k-nearest neighbor (kNN) classifiers with a one vs. all strategy. The study compared different modes of feature sets, including linear attributes, nonlinear indices, all features, features selected by principal component analysis (PCA), and features selected by linear discriminant analysis (LDA), to assess their impact on classification rates. Experimental results demonstrated that the proposed identification system achieved a recognition rate of up to 99.68%. The performance of the PNN classifier was found to be superior to that of the kNN classifier. Additionally, selecting features with LDA led to higher identification rates. The paper concludes that the proposed identification system exhibits excellent performance, surpassing other methods in recognizing a group of 90 participants. The high accuracy rates achieved by the algorithm suggest its suitability for deployment in various smart systems. However, a potential weakness of the system is its dependence on the quality of input data [10].

Shenda H.et.al (2020): The CardioID method tackles these issues by learning binary codes directly from continuous ECG data, enabling faster identification compared to existing methods. It also allows for the identification of new individuals without the need for model reconstruction or retraining. A key feature of CardioID is the introduction of statistical hypothesis testing for making identification decisions, ensuring theoretical guarantees of recognition accuracy. Experiments conducted on real-world ECG data demonstrate the effectiveness of Cardio ID. It achieves a significantly higher identification accuracy, surpassing the second-best baseline by 9.84%. Furthermore, Cardio ID reduces the running time by 30.90% compared to individual baseline methods. In summary, Cardio ID is proposed as a method for human identification using ECG data. It offers faster identification by learning binary codes directly from raw ECG data and eliminates the need for reconstructing or retraining the model for new individuals. The introduction of statistical hypothesis testing ensures realistic and reliable identification decision-making. Experimental results validate the effectiveness of Cardio ID on real-world ECG data. However, the system's performance may be affected by the quality of the real-world ECG data, and the accuracy of the results depends on the choice of parameters used in the statistical algorithm [11].

Majid S. and F.Abdali-Mohammadi., (2021) propose This study focuses on designing a biometric recognition system based on electrocardiogram (ECG) signals by estimating the latent medical variables, namely functional and structural dependencies among ECG leads. Physiological signals, such as ECG, have the potential to be used in biometric recognition systems for applications like security technologies and remote access. The proposed system utilizes within-correlation and cross-correlation calculations in the time-frequency domain to estimate the functional dependencies between ECG leads. These dependencies are represented using extended adjacency matrices. To estimate the structural dependencies, a hybrid learning model is introduced, combining genetic programming and CNN trees. CNN trees perform deep feature learning using structural morphology operators. The designed system is intended for both closed-set identification and verification tasks. It is evaluated using two datasets: PTB (PTB Diagnostic ECG Database) and CYBHi (Check Your Biosignals Here Initiative). The performance of the proposed method is compared to existing state-of-the-art approaches, and it outperforms all of them. Nevertheless, a notable limitation of the suggested system is in its need on precise data input, which may be susceptible to many variables including ECG signal loss and malfunctioning sensors. Moreover, the performance of the system may be influenced by the calibre and volume of data accessible for both training and testing purposes. [12].

E. Al Alkeem .et.al (2021): This work proposes a novel identification technique for the Industrial Internet of Things (IIoT) that combines multiple biometric sources, including electrocardiogram (ECG), fingerprint, and facial image data. The use of multimodal biometrics, coupled with deep learning, allows the model to handle various input domains without requiring separate training for each modality. Additionally, the model leverages multitask learning, where losses from one task help regularize others, leading to improved overall performance. The proposed technique merges the multimodal data at both the feature level and the score level, achieving better generalization and outperforming other fusion methods. The model has demonstrated resilience against spoof attacks and has been tested on noisy and partial data, including missing modalities. The suggested approach does, however, have several drawbacks. One drawback is that identifying the characteristics that are suggestive of an ECG's behaviour necessitates a high level of topic knowledge. Using an end-to-end learning technique across the entire network with a larger biometric database is one of the suggested future research paths. This could result in identification and classification that is more accurate. Moreover, investigating the application of an attention model to determine the best modality or feature in a sample could enhance the multimodal data fusion procedure. Overall, this work presents a pioneering approach that combines multimodality, multitasking, and different fusion methods for enhanced identification and classification in the IIoT context [13].

Yefei Z.et.al (2021): The main contribution of this research is a novel fingertip ECG identification system that integrates transfer learning and a deep CNN. The proposed system eliminates the need for manual feature extraction and reduces the computational complexity, resulting in improved speed. It is also effective even with a small set of training data. The system is evaluated using 1200 ECG recordings from 600 individuals, considering five simulated scenarios. The overall training accuracy of the model exceeds 97.60% for chest-collected ECG and reaches 98.77% for fingertip-collected ECG. In real-world simulations using five public datasets, the proposed model achieves nearly 100% recognition accuracy, outperforming the original GoogLeNet network by up to 3.33%. This architecture provides a reference for practical applications of fingertip-collected ECG-based biometric systems, enhancing information network security. The study highlights the importance of resolving computational complexity, data sample requirements during training, and the impact of fingertip ECG acquisition in different activity states. The proposed deep transfer learning fusion CNN addresses these challenges and offers an individual identification method suitable for multiple scenarios. The performance of the proposed approach surpasses other methods, including locally trained CNN models, achieving an overall accuracy of 98.77% on the CYBHi dataset. In summary, this study introduces a robust fingertip ECG identification system that integrates transfer learning and a deep CNN. The system demonstrates superior recognition accuracy and contributes to the field of ECG-based biometrics and information network security. However, the paper also acknowledges some of the limitations of the proposed system, such as its reliance on a fixed set of features and the potential for false positives [14].

Carmen C.et.al (2022): This paper discusses the development of a novel identification technique based on electrocardiograms (ECGs) and musical features. The aim is to create a biometric system that can serve as an alternative or complement to traditional identification systems like passwords or tokens. The model has been tested on noisy and incomplete data, including missing modalities, and has proven resilient against spoof assaults. That said, there are a number of shortcomings with the recommended method. One disadvantage is that a deep level of subject expertise is required to recognise the features that are predictive of an ECG's behaviour. One of the recommended future study directions is the use of an end-to-end learning technique over the complete network with a larger biometric database. More accurate identification and classification may arise from this. Furthermore, exploring the use of an attention model to identify the optimal modality or feature within a sample may improve the multimodal data fusion process. Experimental evaluation using the MIT-BIH Normal Sinus Rhythm Database, which includes recordings from 18 subjects, demonstrates the effectiveness of the proposed technique. The system achieves an accuracy of 96.6% with a low error rate, as indicated by the False Acceptance Rate (FAR) and False Rejection Rate (FRR) of 0.002 and 0.004, respectively. The system shows resistance to circumvention, an important property for a biometric system, and performs well in terms of accuracy, FAR, and FRR. The proposed solution leverages the universality of cardiac signals since everyone alive has a beating heart, making it applicable to a wide population. The uniqueness of ECG records is established by previous research that demonstrates the feasibility of using fiducial and non-fiducial features for biometric purposes. The paper claims to be the first to identify users unequivocally using musical features extracted from ECG records, with high accuracy and a minimal misclassification rate [15].

Gokhan G.et.al (2022): This study provides a biometric identification system that uses a one-dimensional convolutional neural network (CNN) to merge speech and electrocardiogram (ECG) modalities. This approach's capacity to efficiently and precisely evaluate vast volumes of data is one of its advantages. Creating an identification technique that works and boosts confidence and performance is the aim. Two methods are suggested by the study: a resilient rejection algorithm and a fusion system that operates on voting. In the first method, speech and ECG modalities are combined to create a fusion system. The system achieves a 100% accuracy rate for 90 individuals in a 3-fold cross-validation setup. The proposed algorithm addresses issues caused by portable fingertip ECG devices and patient movements by introducing an ECG spike and inconsistent beats removal algorithm. The fusion method employs a voting mechanism based on the outcomes of independent systems. To stop unwanted access to the fusion system, a rejection mechanism is added in the second method. Using 90 individuals as genuine classes and 26 as imposter classes, the system achieves 92% accuracy in detecting genuine classes and 96% accuracy in rejecting imposter classes. But one possible drawback of this strategy is that it requires high-quality data inputs in order to effectively train the models [16].

Table (1): Summery Dataset, Technologies used, Result, Advantage and Dis Advantage of ECG biometrics.

Authors	Dataset	Technologies used	Result	Advantage	Dis Advantage
[7]	The MIT arrhythmia database (mitdb) with self-collected calm and high-pressure data	A selecting mechanism based on information entropy to extract complete heart beat signals, followed by a Depth Neural Network (DNN) utilizing a Denoising AutoEncoder (DAE) for unsupervised feature selection.	Specifically, the recognition rates stand at 98.10% for calm datasets and 95.67% for high-pressure datasets gathered by the researchers themselves.	• Improved Robustness • Automatic Feature Learning •High Recognition Rates	• Limited Robustness Analysis • Evaluation Restricted to Few Datasets
[8]	PTB Diagnostic ECG Database	•Deep-ECG Approach •Real-Time Big Data Processing Techniques •Quantization Procedure •Training Dataset Expansion •Evaluation on Uncontrolled Conditions	Deep-ECG demonstrated remarkable accuracy in identification, verification, and periodic re-authentication tasks.	• Novelty • Performance and Accuracy • Robustness • Quantization for Cryptographic Use	• Lack of Comparative Analysis • Focus on Real-Time Processing
[9]	Three ECG databases are utilized: • Normal Individuals • Atrial Fibrillation Patients • Noisy Database	•Generalized S Transformation (GST) •Convolutional Neural Network (CNN) •getframe Technology	Achieved high identification rates of 99% for normal individuals, 98% for atrial fibrillation patients, and 99% for a noisy database, showcasing the algorithm's promising effectiveness across diverse datasets.	• Handling Complexity • Comprehensive ECG Representation • Reduced Feature Engineering Workload • High Identification Rates	Performance in Dense Datasets
[10]	The study involved ECG signals from: 90 participants	•Matching Pursuit (MP) Analysis •Probabilistic Neural Network (PNN) and k-Nearest Neighbor (kNN) Classifiers •Feature Set Modes: Explored various feature sets, including linear attributes, nonlinear indices, all features, features selected by Principal Component Analysis (PCA), and features selected by Linear Discriminant Analysis (LDA).	The proposed identification system achieved an impressive recognition rate of up to 99.68%.The performance of the PNN classifier surpassed that of the kNN classifier in this context.	• High Recognition Rate • Classifier Performance Comparison • Impact of Feature Selection • Deployment Suitability	Data Quality Dependency: The system's performance is potentially dependent on the quality of input data

[11]	Real-world ECG data used for experimentation and validation of the CardioID method.	•Learning Binary Codes from Continuous ECG Data •Statistical Hypothesis Testing •Comparison and Evaluation	CardioID achieved significantly higher identification accuracy compared to existing methods, surpassing the second-best baseline by 9.84%.	• Faster Identification • Statistical Decision Making • Performance Improvement.	• Impact of Data Quality • Parameter Dependency: The accuracy of CardioID's results might depend on the choice of parameters used in the statistical algorithm.
[12]	PTB (PTB Diagnostic ECG Database) and CYBHi (Check Your Biosignals Here Initiative)	•Functional and Structural Dependency Estimation •Extended Adjacency Matrices •Hybrid Learning Model	When compared to existing state-of-the-art approaches, the proposed method outperformed all of them in both closed-set identification and verification tasks using the PTB and CYBHi datasets.	• Innovative Approach • Versatility • Performance Superiority	• Reliance on Accurate Data Input • Data Quality and Quantity Impact
[13]	Multiple biometric sources: Electrocardiogram (ECG), fingerprint, and facial image data are utilized for multimodal biometric identification in the Industrial Internet of Things (IIoT) context.	•Multimodal Biometrics: Combining multiple biometric sources (ECG, fingerprint, facial image) for identification. •Deep Learning •Multitask Learning •Multimodal Data Fusion	The proposed technique showcased better generalization and outperformed other fusion methods when tested on IIoT data, even in scenarios with missing or incomplete data and against spoof attacks.	• Modality Independence • Performance Enhancement • Robustness	• Domain Expertise Requirement • Future Research Directions
[14]	• 1200 ECG recordings from 600 individuals • Five simulated scenarios • Five public datasets used for real-world simulations	•Transfer Learning •Deep CNN •Deep Transfer Learning Fusion CNN	Training Accuracy exceeds 97.60% for chest-collected ECG and reaches 98.77% for fingertip-collected ECG.	• Improved Speed and Complexity Reduction • Effectiveness with Limited Training Data • High Recognition Accuracy	• Reliance on Fixed Features • Potential for False Positives
[15]	MIT-BIH Normal Sinus Rhythm Database: Contains recordings from 18 subjects.	•ECG Preprocessing and Conversion •Musical Feature Extraction •Classifier Utilization	The system achieved an accuracy of 96.6% with a low False Acceptance	• Fraud Detection Capabilities • Effectiveness and Resistance to Circumvention • Universality	• Dependency on Data Quality • Limited Dataset Size

			Rate (FAR) of 0.002 and False Rejection Rate (FRR) of 0.004, indicating a low misclassification rate.	and Uniqueness of ECG Signals	
[16]	• 90 individuals used for genuine classes • 26 individuals used for imposter classes	•One-Dimensional Convolutional Neural Network (CNN) •Voting-Based Fusion System •ECG Spike and Inconsistent Beats Removal Algorithm •Robust Rejection Algorithm	The fusion system achieved accuracy rate in identifying individuals using a voting-based mechanism in a 3-fold cross-validation setup. The rejection algorithm achieved 92% accuracy in identifying genuine classes and 96% accuracy in rejecting imposter classes, highlighting its efficacy in preventing unauthorized access.	• Efficiency in Data Analysis • High Accuracy • Addressing Device and Movement Issues	• Dependency on Data Quality • Limited Evaluation Scope

3.Fundamental strategies for electrocardiogram (ECG) data enhancement

Processing electrocardiogram (ECG) data plays a pivotal role in bolstering computer security and individual recognition. A multitude of methodologies exists for refining ECG data, each serving a specific purpose. Enhancing the quality of electrocardiogram (ECG) data is a pivotal undertaking in the realm of computer safety and individual identification. A variety of strategies can be employed for ECG data refinement, each serving a distinct purpose. Signal denoising emerges as a critical technique, aiming to eliminate artifacts or irregularities present in ECG recordings due to factors like electromagnetic interference or signal acquisition errors. Signal normalization endeavors to standardize ECG data across different individuals and recording conditions, enabling consistent analysis and comparison [17].

Feature extraction techniques are utilized to distill relevant information from the ECG waveform, thereby capturing distinctive patterns that aid in person identification. Furthermore, anomaly detection methods pinpoint irregularities or outliers in the ECG signal, which could be indicative of potential security breaches or health issues. By synergistically employing these approaches, the foundation is laid for robust ECG analysis in the pursuit of enhanced computer safety and accurate person identification [18]. These strategies aim to improve the quality, accuracy, and interpretability of ECG data, enhancing its usability in clinical diagnosis, research, and biometric applications as show below:

- Noise Reduction Techniques [19]:

Filtering Methods: Employing high-pass, low-pass, or band-stop filters to eliminate noise frequencies.

Wavelet Transform: Using wavelet-based denoising methods to separate noise from ECG signals.

Adaptive Filtering: Techniques like adaptive noise cancellation to remove various types of noise interference.

- Baseline Wander Removal [20]:
  Techniques to correct or remove baseline wander, the low-frequency noise caused by body movements or electrode contact issues. Signal normalization or subtraction methods to isolate the ECG signal from the baseline drift.
- Artifact Rejection and Correction [21]:
  Identifying and eliminating artifacts caused by muscle movements, electrode malfunction, or external interference. Techniques like blind source separation or independent component analysis to separate and discard artifactual components.
- QRS Complex Detection and Enhancement [22]:
  Accurate detection and enhancement of QRS complexes, which are vital in diagnosing heart conditions. Algorithms and techniques for precise QRS complex delineation, feature extraction, and amplitude normalization.

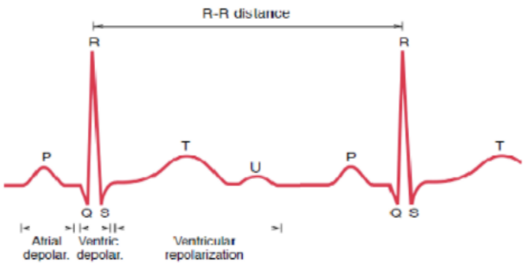

Figure (1): ECG heartbeat signal's basic shape [33].

- Signal Enhancement for Feature Extraction [23]:
  Preprocessing methods to enhance specific ECG features like P-waves, T-waves, and ST segments. Signal enhancement to improve the visibility and distinction of different ECG components for accurate analysis.
- Data Augmentation [24]:
  Synthetic generation of additional training data through techniques like resampling, adding noise, or altering signal parameters. Augmentation methods to increase the diversity and robustness of the dataset for better model training.
- Quality Assessment and Validation [25]:
  Developing metrics and procedures for assessing the quality of enhanced ECG data. Validation techniques to ensure that enhanced signals retain clinically relevant information without introducing artifacts.
- Adaptive and Machine Learning Approaches [26]:
  Using adaptive or machine learning-based algorithms to adaptively enhance ECG signals based on varying conditions or noise sources. Training models to learn and enhance ECG data, leveraging deep learning or adaptive filtering techniques.

4.Main approaches of ECG similarities measure and better measure finding by CNN

Primary Approaches for Electrocardiogram (ECG) Similarity Measurement and Enhanced Metric Discovery via Convolutional Neural Networks (CNNs)

In the realm of Electrocardiogram (ECG) similarity measurement, fundamental strategies emerge as essential tools to assess cardiac waveform resemblances. Convolutional Neural Networks (CNNs) have revolutionized this field by offering advanced techniques for accurate ECG analysis. The primary approaches to ECG similarity measurement involve leveraging the capabilities of CNNs for improved metric discovery. Traditional ECG similarity assessment methods involve waveform alignment and feature extraction, similar to trajectory data pre-processing techniques. CNNs take these techniques a step further by automatically learning relevant features directly from raw ECG data. The utilization of CNNs for ECG similarity assessment starts with data preprocessing, where ECG signals are transformed into input formats suitable for CNN architectures [27].

CNNs excel at feature extraction by employing layers that recognize distinct patterns within ECG signals. These patterns could correspond to specific morphological features, such as R-peaks or ST-segments, similar to identifying landmarks in trajectory data. CNNs' ability to capture intricate relationships within ECG waveforms mirrors the functionality of clustering methods in trajectory analysis, aiding in grouping similar segments together for effective comparison. In the context of ECG similarity measurement, CNNs serve as dynamic time warping counterparts, capable of automatically learning and accounting for variations in heart rates and morphologies. These networks can adapt to varying temporal patterns, analogous to how dynamic time warping adjusts for trajectory alignment [28].

Furthermore, CNNs contribute to improved ECG similarity assessment by addressing noise and baseline drift. The network's layers act as filters that extract meaningful features while disregarding noise, thereby enhancing the accuracy of similarity metrics. Just as noise filtering in trajectory data preprocessing eliminates irregularities, CNNs effectively denoise ECG signals. To attain enhanced metric discovery through CNNs, advanced architectures and techniques can be explored. Multi-scale CNNs, similar to wavelet transforms in trajectory analysis, can capture temporal variations in ECG signals across multiple scales, enriching the similarity measurement. Additionally, attention mechanisms within CNNs focus on critical regions of ECG waveforms, analogous to how stay point detection identifies stationary areas in trajectory data [29].

The main approaches of ECG similarities measure involve various techniques to quantify and compare ECG signals for similarity assessment. CNN (Convolutional Neural Networks) plays a role in enhancing the measurement process by offering improved feature extraction and pattern recognition capabilities. Here's an elaboration in Table 2 [30,31]:

Table(2): Measurement Approaches of ECG

ECG Similarity Measurement Approaches	Enhanced ECG Similarity Measure Using CNN
Dynamic Time Warping (DTW): DTW aligns two ECG signals, accounting for differences in signal speed and length, providing a measure of similarity.	Feature Extraction: CNNs excel at automatic feature extraction from raw data. In ECG similarity measures, CNNs can automatically identify relevant features or patterns in ECG signals without manual feature engineering.
Correlation Techniques: Pearson or Spearman correlation coefficients quantify the linear or monotonic relationship between two ECG signals, indicating similarity.	Hierarchical Representation: CNNs generate hierarchical representations of ECG signals, capturing complex patterns at different levels, enhancing the model's ability to identify similarities between signals.
Euclidean Distance: Measures the straight-line distance between points in ECG signal spaces, providing a straightforward similarity metric.	Pattern Recognition: By learning features hierarchically, CNNs excel in recognizing intricate patterns, aiding in distinguishing subtle differences or similarities in ECG signals.
Cosine Similarity: Quantifies the cosine of the angle between two ECG signal vectors, assessing similarity in direction rather than magnitude.	Adaptability and Robustness: CNNs can adapt to different ECG signal variations, noise, and anomalies, improving the accuracy and robustness of similarity measures.
	Efficient Learning: Through convolutional layers and pooling operations, CNNs efficiently learn and abstract essential features, reducing the computational complexity in measuring ECG similarities.
	Transfer Learning: Pre-trained CNN models on large datasets can be fine-tuned for specific ECG

	similarity measures, leveraging knowledge from broader domains to enhance performance.

CNNs leverage these capabilities to enhance ECG similarity measures by providing automated, more accurate, and adaptive ways to capture and compare patterns within ECG signals. Their hierarchical learning and robust feature extraction abilities make them well-suited for improving the accuracy and efficiency of similarity measurements in ECG data analysis [32].

In conclusion, the primary approaches for ECG similarity assessment find a powerful ally in Convolutional Neural Networks (CNNs). These networks revolutionize traditional methodologies by automatically learning features, adapting to variations, and effectively denoising signals. CNNs can be considered as a refined, automated version of the techniques used in trajectory data preprocessing. The exploration of advanced CNN architectures and techniques further enriches the field of ECG similarity assessment, propelling diagnostics, individual identification, and computer security to new heights [33].

5.Conclusion

This study delves into the assessment of an ECG-based biometric authentication system, highlighting the inherent value of utilizing an individual's ECG for identity verification. Unlike conventional biometrics, such as fingerprints or facial recognition, an individual's ECG pattern is deeply secure and incredibly challenging to replicate or falsify. This uniqueness stems from the fact that an individual's ECG signature is not only hereditary but also inherently tied to their physiological functioning, making it almost impossible to fabricate. The real-time vitality function of ECG stands as its most pivotal feature in the realm of biometric authentication. This functionality ensures that an ECG cannot be extracted or replicated from a deceased individual, as it necessitates the person's live presence for authentication. Furthermore, the study underscores ECG's attributes of originality, widespread acceptance, and universality as factors that render it a highly promising biometric trait. Its prevalence in medical diagnostics and familiarity within the healthcare sector also bolsters its potential as a robust biometric authentication method. Overall, the study emphasizes the unparalleled security and real-time authentication capabilities of ECG-based biometrics while also highlighting the need for ECG patterns to maintain consistency and permanence for continued success in the biometric authentication domain.

References

[1] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. IEEE security & privacy, 1(2), 33-42.

[2] Abdullah, R. M., Alazawi, S. A. H., & Ehkan, P. (2023). SAS-HRM: Secure Authentication System for Human Resource Management. Al-Mustansiriyah Journal of Science, 34(3), 64-71.

[3] Zhao, C. X., Wysocki, T., Agrafioti, F., & Hatzinakos, D. (2012, September). Securing handheld devices and fingerprint readers with ECG biometrics. In 2012 IEEE fifth international conference on biometrics: theory, applications and systems (BTAS) (pp. 150-155). IEEE.

[4] Wu, S. C., Hung, P. L., & Swindlehurst, A. L. (2020). ECG biometric recognition: unlinkability, irreversibility, and security. IEEE Internet of Things Journal, 8(1), 487-500.

[5] Agrafioti, F., & Hatzinakos, D. (2009). ECG biometric analysis in cardiac irregularity conditions. Signal, Image and Video Processing, 3(4), 329-343.

[6] Berkaya, S. K., Uysal, A. K., Gunal, E. S., Ergin, S., Gunal, S., & Gulmezoglu, M. B. (2018). A survey on ECG analysis. Biomedical Signal Processing and Control, 43, 216-235.

[7] Zheng, G., Ji, S., Dai, M., & Sun, Y. (2017). ECG based identification by deep learning. In Biometric Recognition: 12th

Chinese Conference, CCBR 2017, Shenzhen, China, October 28-29, 2017, Proceedings 12 (pp. 503-510). Springer International Publishing.
[8] Zhao, Z., Zhang, Y., Deng, Y., & Zhang, X. (2018). ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation. Computers in biology and medicine, 102, 168-179.
[9] Labati, R. D., Muñoz, E., Piuri, V., Sassi, R., & Scotti, F. (2019). Deep-ECG: Convolutional neural networks for ECG biometric recognition. Pattern Recognition Letters, 126, 78-85.
[10] Goshvarpour, A., & Goshvarpour, A. (2019). Human identification using a new matching pursuit-based feature set of ECG. Computer methods and programs in biomedicine, 172, 87-94.
[11] Hong, S., Wang, C., & Fu, Z. (2020). Cardioid: learning to identification from electrocardiogram data. Neurocomputing, 412, 11-18.
[12] Sepahvand, M., & Abdali-Mohammadi, F. (2021). A novel multi-lead ECG personal recognition based on signals functional and structural dependencies using time-frequency representation and evolutionary morphological CNN. Biomedical Signal Processing and Control, 68, 102766.
[13] Al Alkeem, E., Yeun, C. Y., Yun, J., Yoo, P. D., Chae, M., Rahman, A., & Asyhari, A. T. (2021). Robust deep identification using ECG and multimodal biometrics for industrial internet of things. Ad Hoc Networks, 121, 102581.
[14] Zhang, Y., Zhao, Z., Deng, Y., Zhang, X., & Zhang, Y. (2021). Human identification driven by deep CNN and transfer learning based on multiview feature representations of ECG. Biomedical Signal Processing and Control, 68, 102689.
[15] Camara, C., Peris-Lopez, P., Safkhani, M., & Bagheri, N. (2022). ECGsound for human identification. Biomedical Signal Processing and Control, 72, 103335.
[16] Guven, G., Guz, U., & Gürkan, H. (2022). A novel biometric identification system based on fingertip electrocardiogram and speech signals. Digital Signal Processing, 121, 103306.
[17] Schläpfer, J., & Wellens, H. J. (2017). Computer-interpreted electrocardiograms: benefits and limitations. Journal of the American College of Cardiology, 70(9), 1183-1192.
[18] Srivastva, R., Singh, A., & Singh, Y. N. (2021). PlexNet: A fast and robust ECG biometric system for human recognition. Information Sciences, 558, 208-228.
[19] Kumar, A., Ranganatham, R., Kumar, M., & Komaragiri, R. (2020). Hardware emulation of a biorthogonal wavelet transform-based heart rate monitoring device. IEEE Sensors Journal, 21(4), 5271-5281.
[20] Li, G., Ullah, S. W., Li, B., Lin, J., & Wang, H. (2020, December). Baseline wander removal for ECG signals based on improved EMD. In 2020 15th IEEE International Conference on Signal Processing (ICSP) (Vol. 1, pp. 484-487). IEEE.
[21] Al Osman, H., Eid, M., & El Saddik, A. (2014). A pattern-based windowed impulse rejection filter for nonpathological HRV artifacts correction. IEEE Transactions on Instrumentation and Measurement, 64(7), 1944-1957.
[22] Karpagachelvi, S., Arthanari, M., & Sivakumar, M. (2010). ECG feature extraction techniques-a survey approach. arXiv preprint arXiv:1005.0957.
[23] Goldberger, A. L., Amaral, L. A., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., ... & Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. circulation, 101(23), e215-e220.
[24] Ganapathy, N., Swaminathan, R., & Deserno, T. M. (2021). Adaptive learning and cross training improves R-wave detection in ECG. Computer

Methods and Programs in Biomedicine, 200, 105931.

[25] Pan, J., & Tompkins, W. J. (1985). A real-time QRS detection algorithm. IEEE transactions on biomedical engineering, (3), 230-236.

[26] Zokaee, S., & Faez, K. (2012). Human identification based on ECG and palmprint. International Journal of Electrical and Computer Engineering, 2(2), 261.

[27] Serhani, M. A., T. El Kassabi, H., Ismail, H., & Nujum Navaz, A. (2020). ECG monitoring systems: Review, architecture, processes, and key challenges. *Sensors*, *20*(6), 1796. .

[28] Regouid, M., Touahria, M., Benouis, M., & Costen, N. (2019). Multimodal biometric system for ECG, ear and iris recognition based on local descriptors. Multimedia Tools and Applications, 78(16), 22509-22535.

[29] Houssein, E. H., Kilany, M., & Hassanien, A. E. (2017). ECG signals classification: a review. International Journal of Intelligent Engineering Informatics, 5(4), 376-396.

[30] Bassiouni, M., Khalefa, W., El-Dahshan, E. S. A., & Salem, A. B. M. (2015). A study on the Intelligent Techniques of the ECG-based Biometric Systems. Recent Advances in Electrical Engineering, 26-31.

[31] Prakash, A. J., Patro, K. K., Hammad, M., Tadeusiewicz, R., & Pławiak, P. (2022). BAED: A secured biometric authentication system using ECG signal based on deep learning techniques. Biocybernetics and Biomedical Engineering, 42(4), 1081-1093.

[32] Al Alkeem, E., Yeun, C. Y., Yun, J., Yoo, P. D., Chae, M., Rahman, A., & Asyhari, A. T. (2021). Robust deep identification using ECG and multimodal biometrics for industrial internet of things. Ad Hoc Networks, 121, 102581.

[33] Serhani, M. A., T. El Kassabi, H., Ismail, H., & Nujum Navaz, A. (2020). ECG monitoring systems: Review, architecture, processes, and key challenges. Sensors, 20(6), 1796.