Enhanced Information Security with ECG Biometric Authentication

Kriti Verma*, Amit Kaul

Department of Electrical Engineering, National Institute of Technology Hamirpur, Himachal Pradesh, India

* Corresponding author

doi: https://doi.org/10.21467/proceedings.178.29

ABSTRACT

The emergence of electronic health technologies has revolutionized the healthcare industry, leading to significant improvements in medical services at reduced and affordable costs. However, management of health information suffers from a lot of security and privacy challenges, which include user authentication, data integrity, data confidentiality, and safeguarding patient privacy. Biometric technologies address these issues by providing security model to ensure that only authorized personnel have access to their respective health data. This paper proposes an authentication approach utilizing Electrocardiogram (ECG) signals to enhance privacy and information security through the application of AC/DCT for feature extraction and using k-NN and SVM models as the classifiers. The study has been conducted on the NITH Multimodal Biometric Database, which comprises recordings of 15 healthy individuals and is divided into two sessions of data. The best performance on the basis of ACC and EER recorded on the dataset are 99% and 0.3% for same session data, and an ACC and EER of 96.4% and 1.19% are achieved for across session data.

Keywords: Information security, ECG, Authentication, k-NN, SVM, AC-DCT

1 Introduction

Biomedical signals such as ECG, EEG, PPG, etc. are stochastic in nature and reflect the aggregated action potentials within the subdermal tissues of living organisms [1]. They represent the synchronized ionic and electrical activities of muscular and neural cells, exhibiting both temporal and spatial characteristics. These signals not only provide real-time insight about the body's biomedical status but also serve as vital early warning indicators for impending health issues. Another important fact that comes up while dealing with bio-signals is confidentiality, data integrity, data availability, user authentication, and patient privacy protection [2]. Therefore, it is vital to safeguard sensitive user information from unauthorized access. Not only safeguarding the medical data of the user but also protecting other sensitive information about the individual can be done using biometrics. In this context, the use of electrocardiogram (ECG) signals as biometric markers was explored. While traditional biometric methods like fingerprint recognition, gait analysis, and iris scanning have been widely adopted, they come with limitations, such as the risk of forgery through imitation. ECG, on the other hand, is non-invasive, continuously available, and closely tied to an individual's physiological responses. ECG measures the heart's electrical activity, offering unique temporal patterns that are difficult to forge and also ensuring the liveliness of the user. For such usage, some important steps are to be kept in mind. Such as, while signal measurement noise gets inevitably introduced, noise elimination as a pre-processing step becomes crucial. Only through signal processing meaningful information can be deciphered from them for specialized applications, including wireless transmission to medical or emergency centres for immediate response and care and even authentication [3]. To address this, appropriate pre-processing steps for signal data are implemented before utilizing it for authentication.

Proceedings DOI: 10.21467/proceedings.178; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-984081-8-1

The application of machine learning techniques has not remained restricted to traditional computational fields but has also found application in the medical field, revolutionizing processes such as disease diagnosis, drug discovery, personalized treatment plans, and patient monitoring. These techniques improve the ability of the system to be utilized for increasing the accuracy and efficiency of the system. This necessitates the utilization of robust machine learning models that are trained with large datasets to ensure accurate learning of features. A pre-trained network can be designed using a straightforward process, which can then be utilized to tackle specific problems. In this a model has been suggested that involves feature extraction using the AC/DCT method and utilizes SVM and k-NN classifiers for authentication.

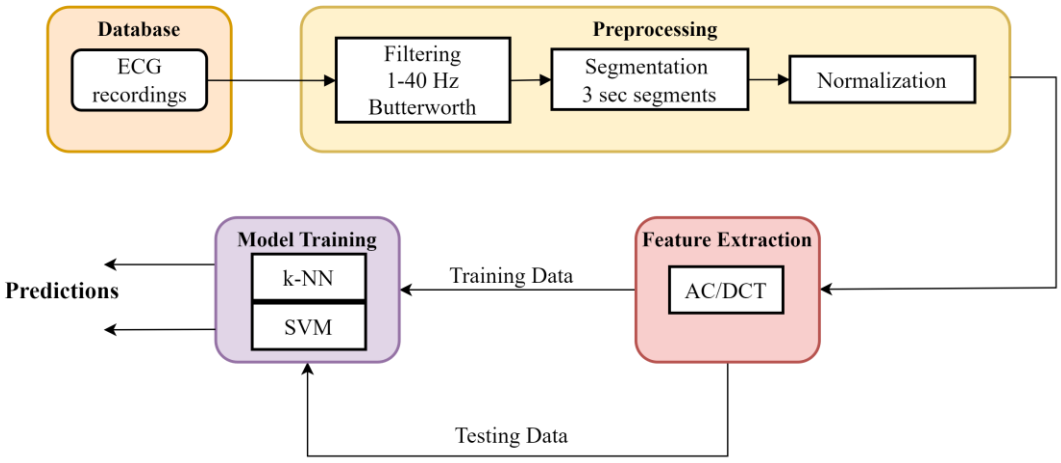

Figure1: User Authentication

2 Topic of Study

The utility of ECG for user identification is not a recent development; as early as 1977, George Forsen et al. recognized the potential of ECG for personal authentication [4], [5]. Biometric approaches have mainly focused on fiducial techniques [6] (onset and offset of P-QRS-T) and non-fiducial techniques (DCT, DWT, etc.) [7][8]. Recent focus in academic literature has shifted towards harnessing learned features extracted from deep learning models [9], [10] for intelligent feature selection [11]. Similar studies in [12], [13] employed biosignals for classification purposes using classifiers such as Support Vector Machine, Artificial Neural Network, Convolutional Neural Network etc. After analyzing the studies, it became evident that relying on traditional biometric approaches for authentication is susceptible to spoofing and may result in reduced accuracy. Utilizing ECG signals with engineered features enhances accuracy while reducing time. In this study, a variety of pre-processing techniques have been employed to enhance the quality of signals. This step is crucial, as any noise present in the signals could lead the models to learn incorrect features. After applying the pre-processing techniques, the AC/DCT features were extracted from the ECG signal. The model was then trained using k-Nearest Neighbor and Support Vector Machine algorithms for both within-session and across-session scenarios.

3 Methodology

The process of biometric authentication is broken down into pre-processing, feature extraction, model training, and then authentication. Firstly, user data is collected and saved into a database [14], this study utilized the NITH MBD introduced in 3.1. This data is used to train the model, but before training, it is very important to clean the data before feeding it into the models, pre-processing details are described in 3.2, including data filtering, segmentation, and normalization of the signal. Figure 1 describes the proposed approach for the user authentication task. The data is split into training data to obtain a user template first, and then machine learning models are tested on the testing data. The model produces different weights,

Proceedings DOI: 10.21467/proceedings.178
ISBN: 978-81-984081-8-1

Series: AIJR Proceedings
ISSN: 2582-3922

and the one that yields the least error and increased accuracy is saved to a folder, which is further used for the validation and testing.

3.1 Databases

The proposed work is trained and validated on NITH MBD [15][16], which is a private database containing 15 healthy individuals' data collected using the BIOPAC MP-150 system with a gap of 2 months between training and testing samples with a sampling frequency of 1 kHz.

3.2 Preprocessing

Pre-processing is vital because it ensures that raw data is in a suitable form for analysis. By cleaning out noise and inconsistencies, filtering irrelevant information, normalizing data ranges, and transforming

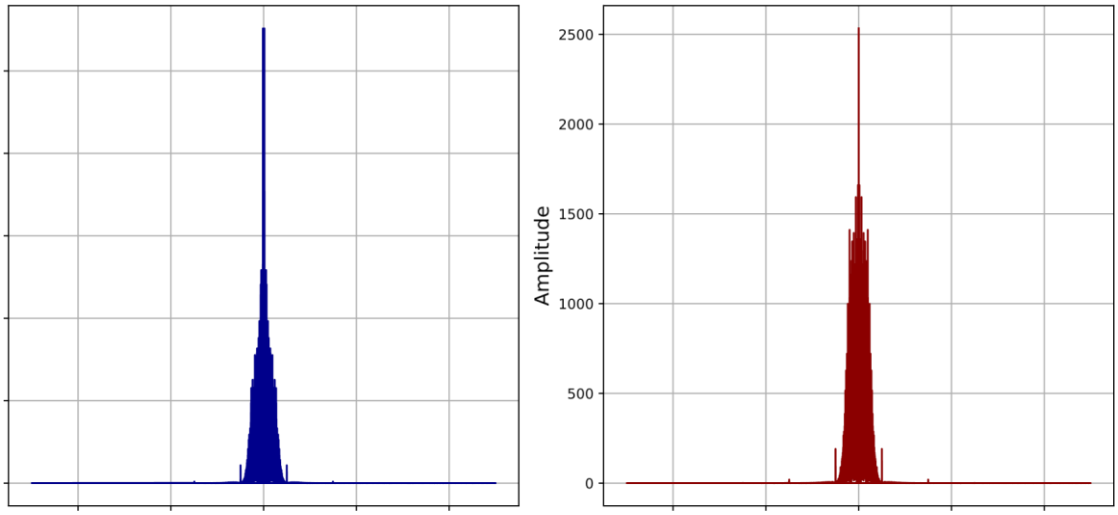

Figure 2: FFT of ECG signal

variables into more meaningful representations, pre-processing enhances the quality and reliability of the data. This step significantly improves the effectiveness of subsequent analysis techniques, allowing for more accurate insights and informed decision-making.

Filtering During the acquisition process from devices, raw signals are susceptible to contamination by various forms of noise. Consequently, it becomes essential to engage in data cleaning procedures to mitigate these effects. The presence of noise not only compromises the quality of the signal but also hampers the understanding of the data, increasing the likelihood of erroneous diagnoses. An FFT of ECG is shown in Figure 2, which shows the frequency range of the signals, which does not exceed 50 Hz for the ECG signal, thus appropriate filters are to be designed. ECG signals are mainly affected by:

a. Baseline wander in the range 0.1–0.5 Hz is caused by respiration, body movements, etc.
b. Power line interference in the range 50/60 Hz due to the interference caused by the electric devices.

In order to improve the quality of the data, the signal was first smoothed with a moving average filter. The NITH-MBD was pre-processed using a 4^{th} order Butterworth band pass filter with a cut-off frequency of 1 and 40 Hz for the ECG signal [17], [18].

Segmentation Segmentation, a fundamental procedure in signal processing, involves partitioning a signal into smaller segments. This decomposition serves various objectives, such as isolating distinct features within the signal, refining the accuracy of classification algorithms, and easing the computational load of subsequent analyses.

In this study, the signal underwent segmentation, dividing it into segments lasting 3 seconds each. Following this segmentation, the next step involved normalization, a technique aimed at standardizing the data to a consistent scale or range.

Normalization In the process of obtaining electrocardiogram (ECG) signals, variations in the amplitude range often occur across different recording sessions. To address this issue and ensure consistency in analysis, it becomes necessary to implement appropriate scaling techniques across the entire database.

Normalization is a step undertaken to standardize the amplitude ranges of ECG signals. In this particular case, the Standard scaling technique is employed to normalize the signals. This normalization process helps align the amplitude ranges of all ECG signals within the database, facilitating more consistent and reliable analysis across different recording sessions.

$$x_{scaled} = \frac{x - \mu}{\sigma} \tag{1}$$

where μ and σ is the mean and standard deviation of the signal and x_{scaled} is the scaled value.

3.3 Feature Extraction with AC/DCT

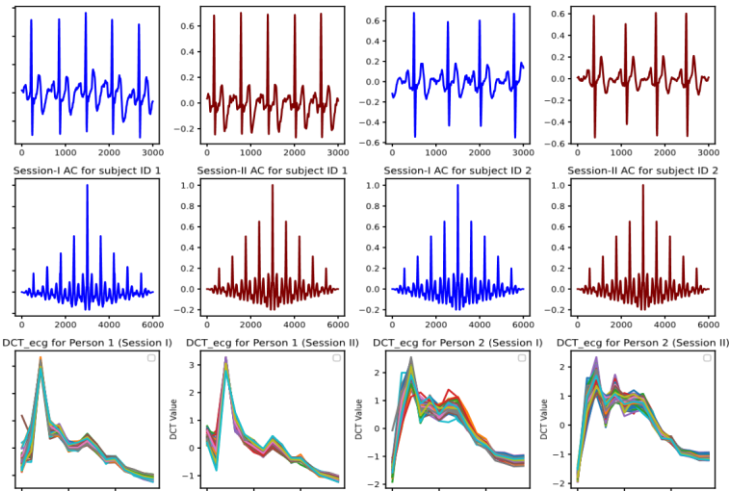

Figure 3: AC/DCT of Session-I and Session-II for subject ID 1 and ID 2

Feature extraction is crucial to transform data into a distinctive, informative, and compact form, ensuring optimal efficiency in both data storage and processing. If the extracted features fail to precisely represent the utilized signals and lack relevance, classification algorithms employing such features may encounter challenges in identifying the feature classes accurately.

In a biometric authentication system, extracting features that accurately capture the unique characteristics of an individual is crucial. However, relying solely on fiducial points may lead to insufficient representation of discriminative features, as these methods heavily rely on the precise localization of ECG wave boundaries. Thus, AC/DCT method has been used, which was first proposed by Plataniotis et al. [19] for 5-second data, was used. Auto-correlation is a statistical measure of the similarity between a signal and itself at different time lags. The pre-processed signal is used to calculate the normalized autocorrelation R_{xx} using the expression:

$$R_{xx}(m) = \frac{R_{xx}(m)}{R_{xx}(0)} = \frac{\sum_{\sigma=0}^{N-m} x(\sigma)x(\sigma+m)}{R_{xx}(0)} \tag{2}$$

where m is the time lag that takes the values from 0 to M-1, where M is empirically chosen to be 200 and is very small in comparison to N, which is the length of the windowed signal.

Proceedings DOI: 10.21467/proceedings.178
ISBN: 978-81-984081-8-1

Series: AIJR Proceedings
ISSN: 2582-3922

The Discrete Cosine Transform (DCT) is a mathematical technique utilized in signal processing to represent a finite sequence of data points as a sum of cosine functions oscillating at different frequencies. Similar to the Discrete Fourier Transform (DFT), the DCT operates on a discrete set of data points. However, unlike the DFT, the DCT exclusively utilizes real numbers, making it particularly suitable for processing real-valued signals. The DCT is commonly employed for dimension reduction, a process aimed at reducing the number of data points required to represent a signal while retaining essential information. This reduction in dimensionality is achieved by expressing the signal using fewer coefficients obtained from the DCT transformation. These coefficients capture the essential frequency components of the signal while discarding redundant or less significant information. By representing the signal using a smaller set of coefficients derived from the DCT, dimension reduction helps streamline data storage, transmission, and processing. After finding the autocorrelation of the signal, DCT is applied in order to reduce the dimensions. Again, the first 15 DCT coefficients were empirically chosen.

3.4 Classification

Following feature extraction, the authentication process proceeds with the application of classifiers. Classification techniques play a pivotal role in this stage, involving the training of a classifier using labeled data. This labeled dataset serves as a reference, with each sample assigned to a specific category or class.

The trained classifier utilizes the patterns learned from the labeled data to categorize new, unlabeled samples based on their similarity to the labeled categories. By generalizing from the labeled dataset, the classifier can accurately classify unseen instances, thereby facilitating the authentication process. Classification techniques offer a systematic approach to organizing and categorizing data, enabling the identification and verification of samples based on their characteristics. This ensures robust authentication by effectively distinguishing between different classes or categories. These classifiers utilized include kNearest Neighbors (k-NN) and Support Vector Machines (SVM). During the authentication process, the dataset is divided into different subsets for training and evaluation. For intra-session authentication, the data is split into a ratio of 50-20-30 for training, validation, and testing, respectively. This allows for a comprehensive assessment of the classifier's performance within the same session. Conversely, for inter-session authentication, training and validation are conducted using session-I data, while testing is performed using session-II data. This ensures that the classifier's ability to generalize across sessions and different leads is evaluated effectively, providing valuable insights into its robustness and reliability in real-world scenarios.

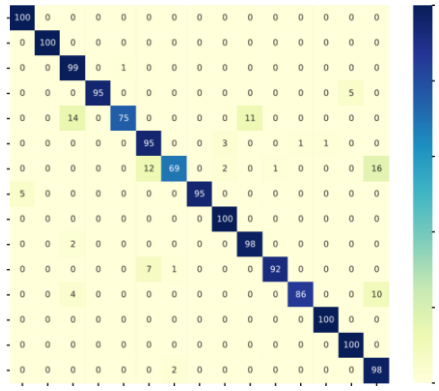

Figure 4: Confusion Matrix of k-NN

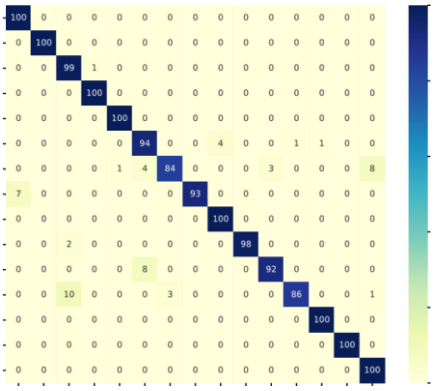

Figure 5: Confusion Matrix of SVM

k-nearest neighbors algorithm (k-NN) The first classification method employed is the k-nearest neighbors algorithm. This algorithm classifies data points based on the majority label of their k nearest neighbors in the feature space, utilizing a distance metric to measure similarity between data points. The value of hyper-parameters influencing the algorithm's performance, such as the weight function, neighbors, and distance

measure, is selected using a grid search method to get the best result. The Figure 4 shows the confusion matrix summarizing the model's predictions for k-NN.

Support Vector Machine (SVM) The Support Vector Machine algorithm, utilized for multi-class classification, is a powerful and versatile supervised learning method. It operates by finding the optimal hyperplane to separate classes in the feature space. SVM maximizes the margin between the hyperplane and the support vectors nearest data points from each class. Different types of kernels—linear, rbf, and poly—were employed with linear kernel giving the best result, each subjected to a grid search on other parameters such as the regularization parameter and the gamma parameter to obtain the best results. This approach ensured the fine-tuning of SVM's performance for the classification tasks. The Figure 5 shows the confusion matrix summarizing the model's predictions for SVM.

4 Result and Discussions

Table 1 shows the detailed classification reports of both the models used. The classification report consists of P, R, f1-s and S which represents precision, re-call, f1-score and support respectively. To understand how accurately the model predicts the target, its performance was evaluated using classification model assessment. Different measures can be applied based on the specific usage. The performance metrics

Table 1: Across Session k-NN and SVM classification report

ID	k-NN				SVM			
	P	R	f1-s	S	P	R	f1-s	S
0	0.95	1.00	0.98	100	0.93	1.00	0.97	100
1	1.00	1.00	1.00	100	1.00	1.00	1.00	100
2	0.89	0.99	0.94	100	0.83	0.99	0.90	100
3	0.99	1.00	1.00	100	1.00	0.95	0.97	100
4	0.99	1.00	1.00	100	0.99	0.75	0.85	100
5	0.89	0.94	0.91	100	0.83	0.95	0.89	100
6	0.97	0.84	0.90	100	0.96	0.69	0.80	100
7	1.00	0.93	0.96	100	1.00	0.95	0.97	100
8	0.96	1.00	0.98	100	0.95	1.00	0.98	100
9	1.00	0.98	0.99	100	0.90	0.98	0.94	100
10	0.97	0.92	0.94	100	0.99	0.92	0.95	100
11	0.99	0.86	0.92	100	0.99	0.86	0.92	100
12	0.99	1.00	1.00	100	0.99	1.00	1.00	100
13	1.00	1.00	1.00	100	0.95	1.00	0.98	100
14	0.92	1.00	0.96	100	0.79	0.98	0.87	100
Accuracy	0.93			1500	0.96			1500

Proceedings DOI: 10.21467/proceedings.178
ISBN: 978-81-984081-8-1

Series: AIJR Proceedings
ISSN: 2582-3922

used for the evaluation of the model are Average Accuracy (ACC) and Equal Error Rate (EER), where Average Accuracy is given as follows:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

where TP, TN, FP and FN are true positive, true negative, false positive and false negative respectively. (EER) is given as follows:

$$EER = \frac{FPR + (1 - TPR)}{2} \tag{4}$$

where TPR is the true positive rate and FPR is the false positive rate given by the following formula:

$$TPR = \frac{TP}{TP + FN} \tag{5}$$

$$FPR = \frac{FN}{FP + TN} \tag{6}$$

For the same session data, the ACC scores for k-NN and SVM are recorded to be 98.9% and 99.3% and the ERR of 1.7% and 0.3% respectively. For across-session data, an ACC of 93.4% and 96.4% and an ERR of 3.49% and 1.19%, respectively, were achieved.

Table 2: Result in terms of ACC and EER

Session	k-NN		SVM	
	ACC (%)	EER (%)	ACC (%)	EER (%)
Session -1	98.8	1.7	99.8	0.3
Session -2	98.4	1.9	99.5	0.5
Across	93.4	3.5	96.4	1.2

5 Conclusions

Biometric authentication utilizing the AC/DCT method for ECG signals offers a robust and secure means of verifying individual identity, thereby enhancing information security in various applications, such as access control systems, financial transactions, and healthcare environments. In this study, AC/DCT method was utilized as the feature extractor in conjunction with machine learning algorithms for authentication purposes. Unlike fiducial methods, which necessitate knowledge of the ECG waveform, this approach can be applied directly to raw data with minimal filtering processes and a small amount of data, specifically 3 seconds in this case. This makes it convenient to use ECG as a biometric measure. Furthermore, it does not require ECG waveform segmentation into P-QRST, which requires additional processing techniques. Using machine learning methods for ECG signal authentication has shown high accuracies consistently, even across different sessions. Notably, the best results were attained using the SVM algorithm.

6 Declarations

6.1 Competing Interests

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

6.2 Publisher's Note

AIJR remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

How to Cite

Kriti Verma, Amit Kaul (2025). Enhanced Information Security with ECG Biometric Authentication. *AIJR Proceedings*, 275-282. https://doi.org/10.21467/proceedings.178.29

References

1. Radek Martinek, Martina Ladrova, Michaela Sidikova, Rene Jaros, Khosrow Behbehani, Radana Kahankova,and Aleksandra Kawala-Sterniuk. Advanced bioelectrical signal processing methods: past, present and future approach—partI: cardiac signals. *Sensors*, 21(15):5186, 2021.
2. Sergio Martínez, David Sánchez, and Aida Valls. A semantic framework to protect the privacy of electronichealth records with non-numerical attributes. *Journal of biomedical informatics*, 46(2):294–303, 2013.
3. Mehdi Hazratifard, Vibhav Agrawal, Fayez Gebali, Haytham Elmiligi, and Mohammad Mamun. EnsembleSiamese Network (ESN) using ECG signals for human authentication in smart healthcare system. *Sensors*, 23(10):4727, 2023.
4. Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1):4–20, 2004.
5. Ruggero Donida Labati, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. Deep-ECG: Convolutional neural networks for ECG biometric recognition. *Pattern Recognition Letters*, 126:78–85, 2019.
6. Lena Biel, Ola Pettersson, Lennart Philipson, and Peter Wide. ECG analysis: a new approach in humanidentification. *IEEE transactions on instrumentation and measurement*, 50(3):808–812, 2001.
7. Konstantinos N Plataniotis, Dimitrios Hatzinakos, and Jimmy KM Lee. ECG biometric recognition withoutfiducial detection. In *2006 Biometrics symposium: Special session on research at the biometric consortium conference*, pages 1–6. IEEE, 2006.
8. Yongjin Wang, Foteini Agrafioti, Dimitrios Hatzinakos, and Konstantinos N Plataniotis. Analysis of humanelectrocardiogram for biometric recognition. *EURASIP journal on Advances in Signal Processing*, 2008:1–11, 2007.
9. Nisha Gautam, Amit Kaul, Ravinder Nath, AS Arora, and Sushil Chauhan. Multialgorithmic approach forECG based human recognition. *Journal of Applied Security Research*, 7(4):399–408, 2012.
10. Anfal Ahmed Aleidan, Qaisar Abbas, Yassine Daadaa, Imran Qureshi, Ganeshkumar Perumal, Mostafa EAIbrahim, and Alaa ES Ahmed. Biometric-Based Human Identification Using Ensemble-Based Technique and ECG Signals. *Applied Sciences*, 13(16):9454, 2023.
11. Suwhan Baek, Juhyeong Kim, Hyunsoo Yu, Geunbo Yang, Illsoo Sohn, Youngho Cho, and Cheolsoo Park.Intelligent Feature Selection for ECG-Based Personal Authentication Using Deep Reinforcement Learning. *Sensors*, 23(3):1230, 2023.
12. Ali I Siam, Ahmed Sedik, Walid El-Shafai, Atef Abou Elazm, Nirmeen A El-Bahnasawy, Ghada M El Banby,Ashraf AM Khalaf, and Fathi E Abd El-Samie. Biosignal classification for human identification based on convolutional neural networks. *International journal of communication systems*, 34(7):e4685, 2021.
13. Md Shamimul Islam and Ibrahim Elwarfalli. Deep Learning-Powered ECG-Based Biometric Authentication.In *2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM)*, pages 1–6. IEEE, 2023.
14. Teresa MC Pereira, Raquel C Conceição, Vitor Sencadas, and Raquel Sebastião. Biometric recognition: Asystematic review on electrocardiogram data acquisition methods. *Sensors*, 23(3):1507, 2023.
15. A Kaul, N Gautam, R Jain, D Choudhary, R Nath, AS Arora, and S Chauhan. NITH MBD-multimodalbiometric database. In *Proceedings of 2nd International Conference on Biomedical Engineering and Assistive Technologies (BEATs)*, 2012.
16. Amit Kaul, AS Arora, and Sushil Chauhan. ECG based human authentication using synthetic ECG template.In *2012 IEEE International Conference on Signal Processing, Computing and Control*, pages 1–4. 2012.
17. Amit Kaul, AS Arora, and Sushil Chauhan. AI-Based Approach for Person Identification Using ECG Biometric. In *AI and Deep Learning in Biometric Security*, pages 133–153. CRC Press, 2021.
18. AA Fedotov. Selection of parameters of bandpass filtering of the ECG signal for heart rhythm monitoringsystems. *Biomedical Engineering*, 50:114–118, 2016.
19. Hugo Plácido Da Silva, Ana Fred, André Lourenço, and Anil K Jain. Finger ECG signal for user authentication: Usability and performance. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–8. IEEE, 2013.