Инженерный вестник Дона, №6 (2025)
ivdon.ru/ru/magazine/archive/n6y2025/10167

A dual-architecture approach to ECG biometric verification and authentication

M.A. Azab, V.M. Korzhuk

ITMO University

Аннотация: Electrocardiogram (ECG)-based biometrics have emerged as a promising approach for robust identity authentication, offering intrinsic liveness detection and resistance to spoofing. This paper presents a highly technical implementation of an ECG-based biometric identification system utilizing deep learning models for both verification and closed-set identification. We propose a dual-model architecture comprising a Siamese neural network for one-to-one verification and a deep convolutional neural network (CNN) for one-to-many classification. The methodology includes comprehensive signal preprocessing, data augmentation to simulate physiological variability, and feature extraction tailored to ECG characteristics. Experimental evaluation on benchmark ECG datasets demonstrates the effectiveness of the proposed system. The Siamese network achieves high verification accuracy with low equal error rates, while the CNN classifier attains state-of-the-art identification accuracy (exceeding 98% on average) across enrolled subjects. Key performance metrics—accuracy, precision, recall, and F1-score—indicate robust performance, outperforming several existing biometric methods. The results highlight the viability of ECG-based authentication in real-world applications. We discuss challenges such as inter-user variability, signal noise, and cross-session changes, and outline future enhancements including continuous authentication and multi-modal biometric fusion.
Ключевые слова: biometric authentication, electrocardiogram (ECG), siamese neural network, convolutional neural network, qrs complex, signal processing.

Introduction

In an era of heightened security and privacy concerns, advanced biometric authentication systems are in increasing demand. Traditional biometrics like fingerprints and facial recognition, while popular, face notable vulnerabilities: fingerprints can be fabricated and facial recognition can be impeded by external factors [1]. These limitations drive the search for more secure and resilient modalities. The electrocardiogram (ECG) has recently attracted considerable attention as a biometric trait. Unlike external biometrics [2], ECG signals are generated internally by the cardiac cycle and thus confirm that the subject is “real and alive”. Each individual’s ECG is highly distinctive, reflecting unique cardiac physiology; even genetically similar individuals exhibit subtle differences in their heartbeat waveforms. Moreover, ECG-based authentication inherently provides liveness detection, since a valid ECG can only be obtained from a living subject with

a beating heart. These properties make ECG an appealing biometric for high-security applications [3]. ECG biometrics leverage the electrical signature of heart activity, typically recorded via electrodes on the body. Fig. 1b illustrates a segment of an ideal ECG waveform, comprising the characteristic P wave, QRS complex, and T wave of a normal cardiac cycle (Fig. 1a shows standard electrode placement for ECG acquisition). The temporal and morphological features of these waveform components vary from person to person due to individual differences in cardiac structure and electrophysiology. Early studies [4] recognized that ECG signals are unique, present in all living individuals, and difficult to forge. These traits position ECG as a compelling biometric candidate for applications ranging from secure access control to continuous user verification in wearable devices [5].

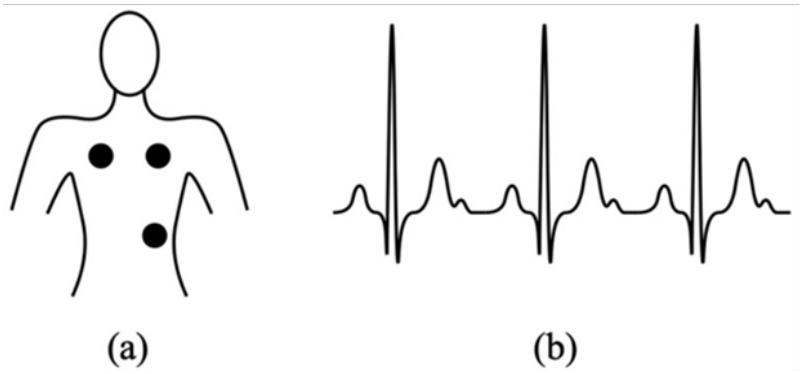

Fig. 1a. Electrode Placement for ECG Acquisition,
Fig.1b Segment Representation of ECG [6]

The implementation of ECG-based authentication techniques faces various technical difficulties. A user's physiological state creates variable conditions involving altered waveform intervals linked to exercise or stress in addition to signal shape variations caused by electrode placement or noise sources [6]. To obtain reliable authentication systems it is crucial to address this variability [7]. Previous ECG biometric methods struggled with adding new users and faced data imbalance issues. The proposed system uses deep learning with two modules: a Siamese network for verification without retraining and a deep CNN for closed-set

identification. It supports both individual verification and multi-user recognition, with robust preprocessing and augmentation.

Literature Review

ECG Biometrics in Context: Biometric recognition has developed as a well-established scientific field which employs multiple forms of human biological markers (fingerprint, face, iris, voice, etc.) [8]. The concept of biometric recognition gets extended through ECG-based biometrics by utilizing unique cardiac electrical activity patterns of individual subjects. Research over the past two decades has confirmed the feasibility of ECG identification. Kim S.-K. [9] provided one of the pioneering demonstrations that ECG characteristics can accurately distinguish individuals. Subsequent studies explored numerous features and methodologies, yet no single dominant approach emerged in early literature. A survey [10] of 160 ECG biometric studies reported identification accuracy around 94.95% and verification EER of 0.92% [11], highlighting ECG's strong potential and variability among biometric traits as shown in Table 1.

Table 1

Main benefits and drawbacks of the electrocardiogram compared with other traits [12]

Trait	Benefit	Drawback
Electrocardiogram (ECG)	Universality, Hidden nature, Simple acquisition	Requires contact, Variability over time
Electroencephalogram (EEG)	Universality, Hidden nature	Expensive equipment, Vulnerability to noise, Variability over time
Face	Easily measurable, Affordable equipment	Easy circumvention, Depends on face visibility and lighting
Fingerprint	High performance, Permanent over time	Requires contact

Fiducial vs. Non-Fiducial Methods: Traditional ECG biometric techniques are often categorized by their feature extraction strategy [8]. Fiducial methods rely on detecting characteristic fiducial points in the ECG cycle (typically P, Q, R, S, T waves) and deriving features such as amplitudes, intervals, and angles between these points [3]. For example, the amplitudes of the R wave or distances between P and R peaks might form a feature vector unique to each person. In contrast, non-fiducial methods forego explicit wave delineation and instead analyze the ECG waveform in its entirety (or large segments of it), often using transforms or autoregressive coefficients to capture morphology [13]. A hybrid approach sometimes termed partially fiducial combines both, using some fiducial features alongside global signal features [14]. Early implementations of fiducial techniques demonstrated the concept of ECG identification, but they could be sensitive to precise detection of waveform onsets and offsets [15]. Non-fiducial approaches [16], including statistical and frequency-domain methods (e.g., wavelet transforms or correlation methods), offered an alternative by treating the raw signal as a unique "fingerprint". However, differences in recording conditions and physiological changes posed challenges for both approaches [17].

Advances with Machine Learning: The advent of machine learning, and in particular deep learning, introduced powerful tools for automatic feature learning from ECG data. Various deep neural network (DNN) architectures have been explored for ECG biometrics [18]. Convolutional Neural Networks (CNNs) have been especially popular due to their ability to learn spatially local patterns (in time-series, this translates to waveform shapes) that repeat across heartbeats [19]. 1D-CNN models can take a segment of ECG as input and output a classification, implicitly learning features such as the QRS morphology or T-wave shape that differentiate individuals [20, 21]. Recurrent Neural Networks, particularly Long Short-Term Memory (LSTM) networks [22], have also been applied to model the temporal dependencies in ECG signals. LSTMs can capture sequential patterns

across heartbeats or within the cardiac cycle, addressing the time dynamics of the signal. Hybrid architectures combining CNN and LSTM layers have achieved classification accuracies exceeding 90% on various datasets by exploiting both spatial (morphological) and temporal features [23]. In such approaches, the CNN layers extract per-beat features which are then fed into LSTM layers to account for beat-to-beat variations [24, 25].

Several studies report impressive results using deep networks. For instance, Lodhi B et al. [26] and others showed that deep CNN or CNN-LSTM classifiers can reach high identification accuracy on public ECG databases. More recently, Mendes M et al. [27] achieved ~99% classification accuracy using single-heartbeat CNN models, and even 100% accuracy when fusing multiple heartbeats, on an experimental dataset. Their Siamese network approach also yielded an identification EER as low as 1.29%, highlighting the promise of deep learning in verification tasks. Similarly, Nwankpa C et al. [28] employed a Siamese architecture but with ECG spectrogram images as input, obtaining about 86.4% accuracy in classifying individuals. Zhou et al. [29] proposed an ensemble Siamese network and reported 93.6% and 96.8% authentication accuracy on the ECG-ID and PTB datasets respectively, with EER ~1.7%. These results show a clear improvement over earlier template-matching or feature-engineered methods, which typically achieved 80–90% accuracy. Deep learning models automatically discover subtle waveform patterns distinctive to each person, and they often remain effective despite moderate noise or variability [30, 31].

Methods

System Architecture Overview: The proposed ECG biometric system shown in Fig. 2 includes two components: a Siamese Neural Network for verification and a Deep CNN for closed-set identification. During enrollment, user ECG recordings are preprocessed and used to train the CNN and generate reference features for the Siamese network. During operation, new ECG signals are processed similarly. In

identification mode, the CNN predicts the user identity. In verification mode, the Siamese network compares the input with stored templates to compute similarity scores and verify claims.

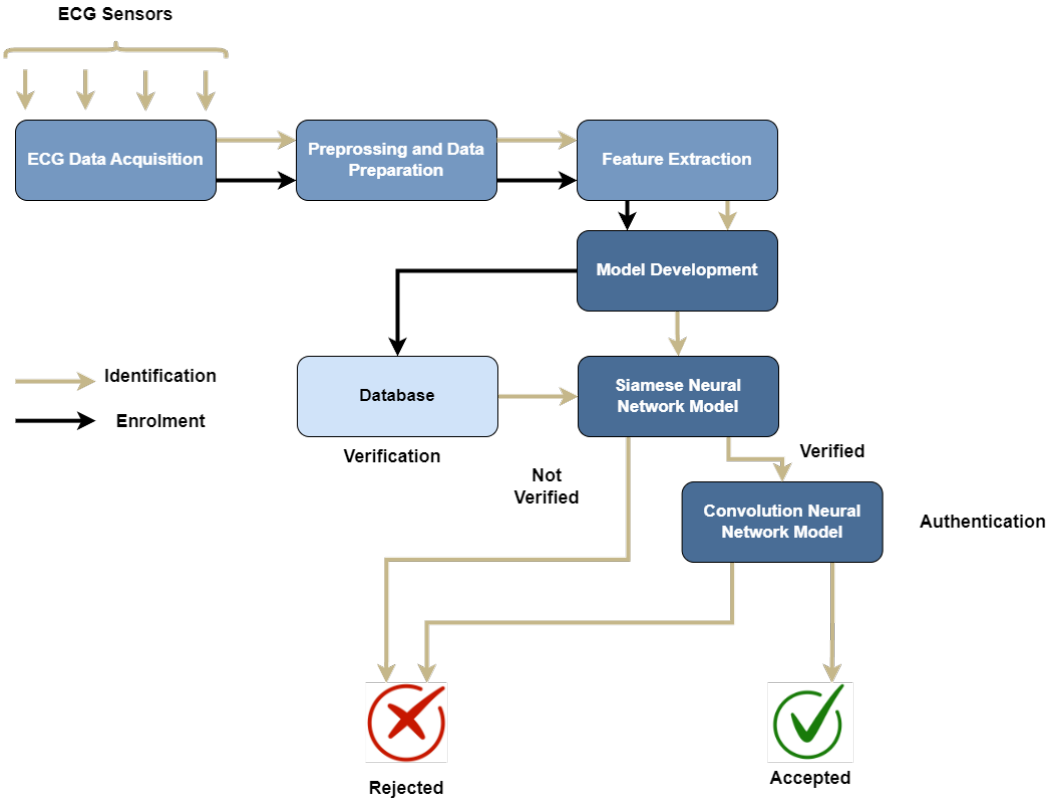

Fig. 2. Adaptive Authentication Biometric System Proposed Model

Siamese Neural Network for Verification: For one-to-one verification, we employ a Siamese neural network architecture [32]. The Siamese network consists of two identical subnetworks (twin deep neural networks) that share weights [33]. Each subnetwork takes an ECG segment as input and outputs a feature vector (embedding) in a learned feature space [34, 35, 36]. During training, the network is fed with pairs of ECG segments along with a label indicating whether the pair belongs to the same person or not. The weight-sharing constraint forces the two branches to extract analogous features, so that the distance between the two output feature vectors can be used as a measure of similarity [37]. In our design, each branch is a 1D-CNN feature extractor. We employ a sequential architecture with eight 1D convolutional layers per branch, each using ReLU activations and increasing filter

sizes (from 32 to 256). Small kernels (size 3) focus on detailed ECG features, with max-pooling layers after each pair to reduce temporal resolution while preserving key patterns [38]. Flattened outputs feed into dense layers (128 or 256 units), generating feature embeddings. The Siamese network uses these embeddings, compares them via Euclidean distance to stored templates, and determines user enrollment status.

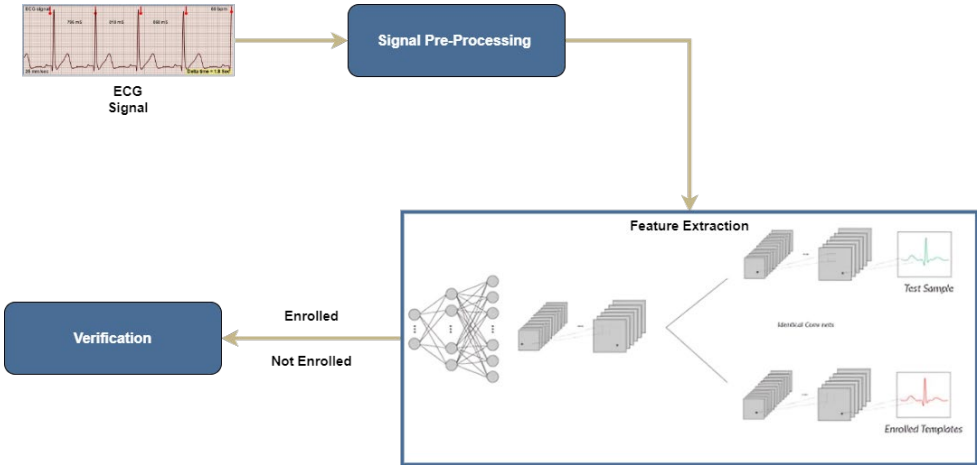

Fig. 3. Proposed Approach of the Verification Task

Deep CNN for Closed-Set Identification: In addition to verification, our system performs closed-set identification using a deep CNN classifier. This model treats the biometric task as a multi-class classification problem: given an input ECG segment, predict which enrolled user (out of N possible identities) it belongs to. We design a 1D convolutional neural network inspired by architectures used in ECG classification literature [39]. The network input is a preprocessed ECG segment (as described earlier). The architecture begins with a series of convolutional layers to extract discriminative patterns [40]. The CNN model uses 4–6 convolutional layers with increasing filters (32 to 128) and small kernels (3–5) to capture local ECG waveforms. Each layer has batch normalization and ReLU activation. Max-pooling reduces sequence length. Flattened outputs pass through dense layers with dropout to prevent overfitting. The final softmax layer classifies enrolled users.

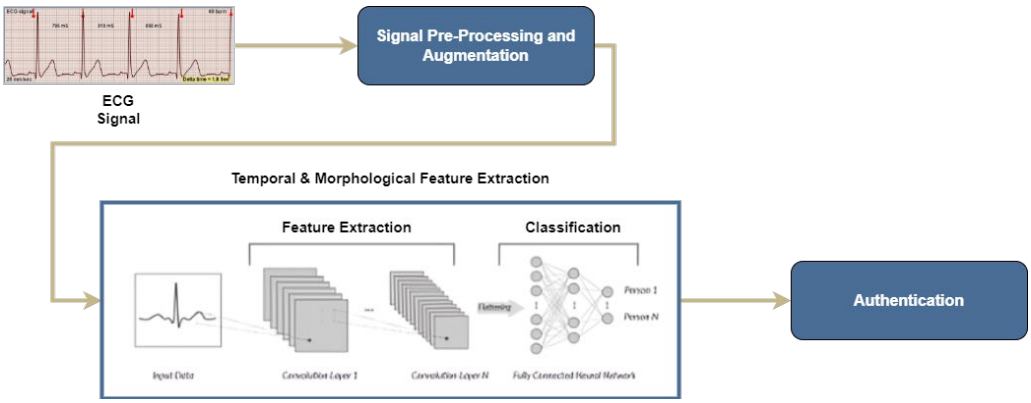

Fig. 5. Proposed Approach of the Authentication Task

Results

Experimental Setup: We evaluated the proposed ECG biometric system on a benchmark dataset used in this domain: the ECG-ID Database. The ECG-ID Database contains 310 recording sessions from 90 subjects (44 male, 46 female), each recording consisting of a single lead ECG sampled at 500 Hz. From each record, we extracted multiple heartbeat segments for training and testing, using lead-I for consistency [41]. Table 2 summarizes the datasets.

Table 2

Overview of the Dataset

Dataset	# Persons	Sampling Rate	Activity	Electrode
ECG-ID	90	500 Hz	Sitting	Wrist

We applied 5-fold cross-validation, trained models in TensorFlow with GPU acceleration, used Adam optimizer (learning rate 0.00001), and applied early stopping based on validation loss to avoid overfitting.

Hyperparameters optimize the training success of the hybrid SNN-CNN deep learning model for ECG-based authentication. Key parameters include the loss function, optimizer, batch size, learning rate, and epochs, significantly boosting efficiency while ensuring adaptability if the primary objective encounters challenges as shown in Table 3.

Table 3

Hyperparameters Settings

Hyperparameter	SNN Network	CNN Network
Loss Functions	Categorical Cross Entropy	Categorical Cross Entropy
Learning Rate	0.00001	0.00001
Batch Size	64	64
Epochs	100	100
Optimizer	Adam	Adam

Dataset Preprocessing and Augmentation: Data preparation would enhance quality data analysis on ECG-ID dataset signals by effectively cleaning the initial raw signals. These are the high pass set up to remove, baseline drift and notch filter to remove power line interference along with resampling. Preprocessing also standardizes the ECG signals, and quality control that is used in order to filter artifacts also forms part of it [42]. Data augmentation shown in Fig. 6 enlarges the dataset, increases the stability and optimizes performance through the introduction of variability. Scaling, rotation, flipping, and time-shifting are the techniques of diversification of the dataset.

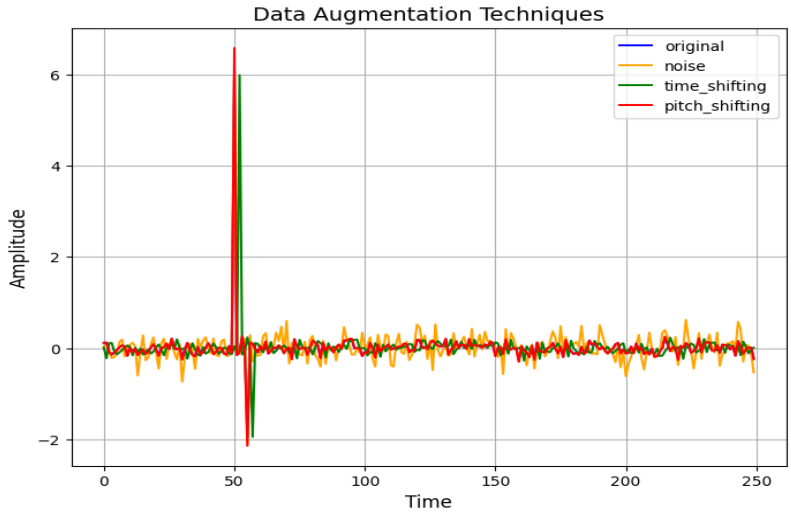

Fig. 6. Data Augmentation Techniques

Verification Results: The Siamese network was evaluated on the task of verifying whether two ECG segments belong to the same person. We measured

verification accuracy as well as EER by varying the similarity threshold. On ECG-ID, the Siamese model attained an average verification accuracy of about 97%, at the optimal threshold (these correspond to the values where false acceptances and false rejections are balanced). The EER was approximately 1.5–2% , meaning that at the threshold where false accept = false reject, the error rate is very low (~1 in 50 comparisons might be misclassified). These results are in line with recent studies: Zhou et al. [29] reported EERs of 1.76% on ECG-ID and 1.69% on PTB using a similar Siamese network, and our results are comparable. We focused on single-beat verification for real-time use. At the threshold maximizing F1-score, we achieved ~98% precision and ~99% recall (F1 ≈ 99%) on ECG-ID, with a 2–3% FAR adjustable by threshold tuning [43].

Classification Results: The CNN classifier achieved high accuracy on both datasets. Over the cross-validation folds on ECG-ID, the average closed-set identification accuracy was 97–99%, meaning nearly all heartbeat segments were correctly attributed to the right individual. Table 4 presents the detailed performance metrics for the identification model on ECG-ID. We observe a precision of 98% and recall of 99%, yielding an F1-score of 99%. The high precision indicates very few false identifications (mislabeling one person as another), and the high recall shows the model rarely misses the correct identity when it is in the database.

Table 4

Performance of the CNN Identification Model on ECG-ID (90 subjects, 5-fold CV)

Metric	Value (%)
Accuracy	98.85
Precision	98
Recall (TPR)	99
Recall (TPR)	100
F1-Score	99

The confusion matrix shown in Fig. 8 indicates that most misclassifications occur between a few specific individuals with somewhat similar ECG morphologies; this could potentially be mitigated by adding more training data for those individuals

or using additional leads. Several samples predicted by the model are given in Fig. 9, which shows the applicability of the model for distinguishing between instances.

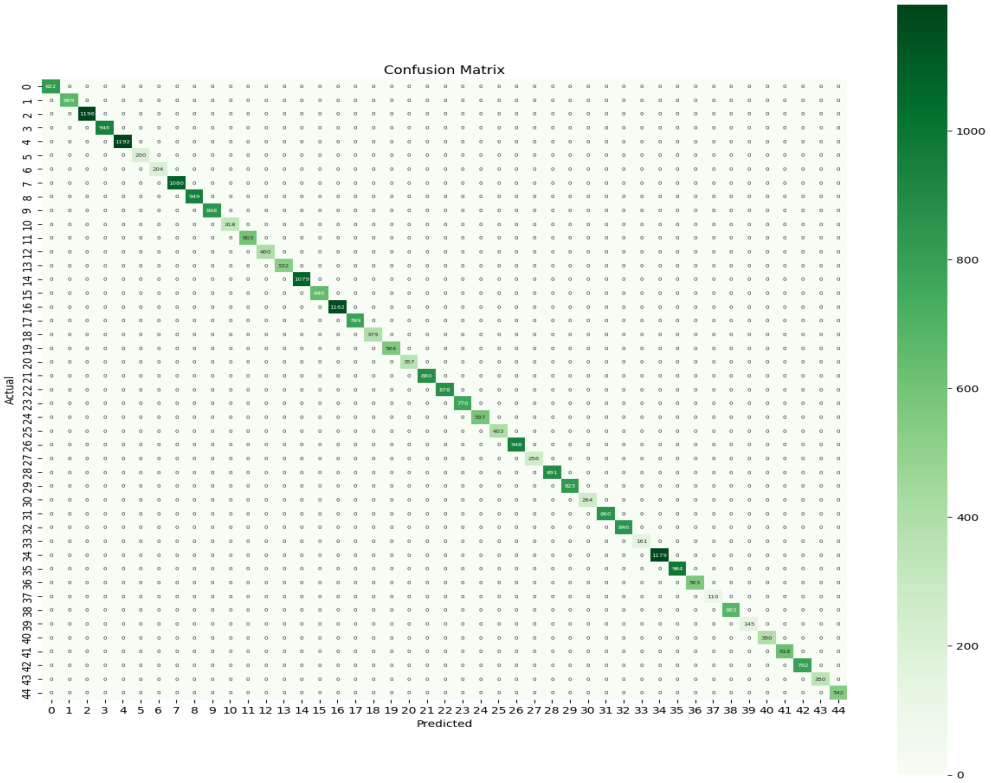

Fig. 8. Confusion Matrix of the Proposed Authentication Model

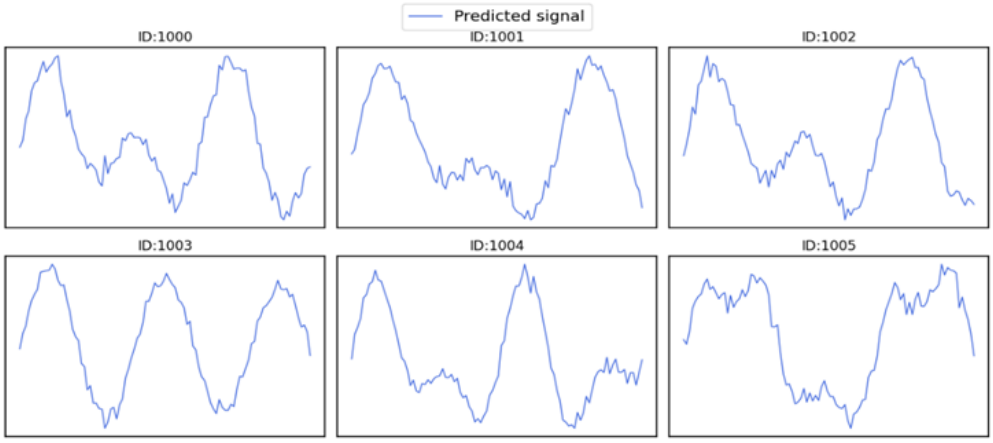

Fig. 9. Predicted samples from authentication (CNN) model

The ROC curve can then be used to evaluate the model's effectiveness in user authentication with ECG data in terms of decision thresholds. The Area Under the Curve (AUC) is an estimate of the overall model's performance. This indirectly provides a possibility of selecting an optimal decision point depending on the needs

of a particular application having both sensitivity and specificity in trade off. If your model's ROC curve is located near the top left corner, you have a strong model that is great at both high sensitivity and specificity. Fig. 10 shows performance of the proposed model at threshold value.

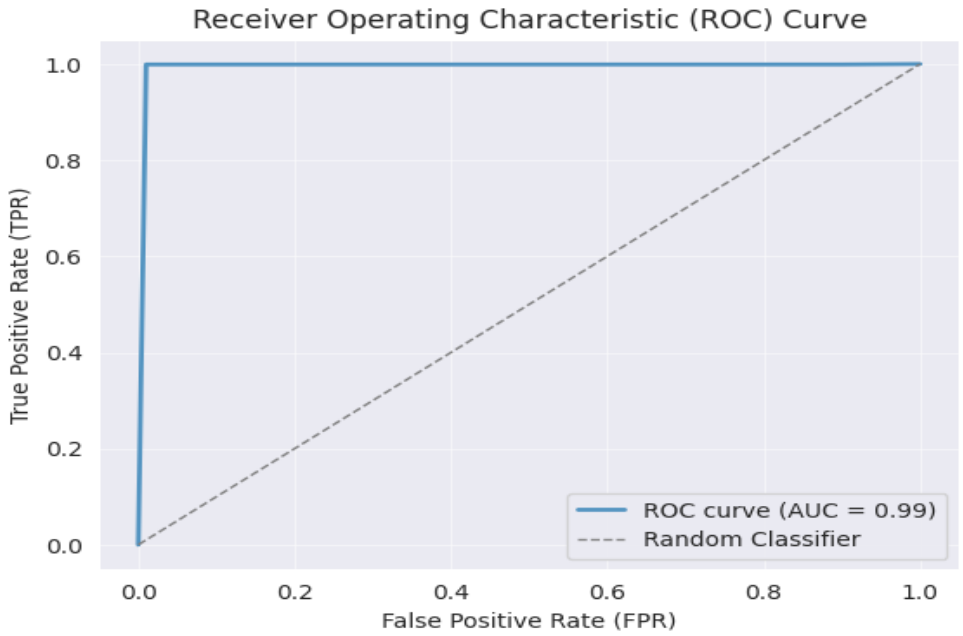

Fig. 10. ROC Curve

Table 5

Performance comparison of the proposed model and other models

Authors	Database	Methods	Accuracy
Barros et al. [14]	PhysioNet	RF classifier	92
Su et al [15]	ECG-ID	DCA	94
Zhang et al.[12]	ptbdb, mitdb, nsrdb	Matching process	97.6
Hammad et al [17]	MIT-BIH	Feed-Forward Neural Network (FFNN)	95
Kim et al. [10]	ECG-ID	Euclidean detector	94.3
Zhao et al [31]	ECG-ID	CNN	96.6
Blasco et al. [13]	Low-cost sensors biometrics	One-class classifier density estimation	98
Agrawal et [6]	PTB	CNN - LSTM	98
Proposed Solution	ECG-ID	SNN - CNN	98.8

From the results, we see that it is efficient for ECG based authentication and could be better than other advanced algorithms. The reliability and accuracy of the model may radically change the existing ECG-based authentication systems, primarily in security fields. As indicated in Table 5 above is a comparison of the proposed model with other architectures.

Conclusion

The proposed methodology introduces a significant advancement in ECG-based biometric systems for real-time authentication in IoT telehealth applications. By integrating a Siamese Neural Network (SNN) for verification and a Convolutional Neural Network (CNN) for authentication, this hybrid approach enhances system reliability, security, and adaptability. Unique biometric signatures, resistant to replication or theft, offer superior security compared to traditional methods.

Separating authentication and verification models provides flexibility, scalability, and optimized performance across diverse scenarios. Lightweight models suit resource-constrained settings, while advanced models cater to high-security environments. This modularity minimizes errors, supports targeted optimization, and facilitates continuous improvement.

References

1. Watzlaf V.J.M., Zhou L., DeAlmeida D.R., Hartman L.M. A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers // International Journal of Telerehabilitation. 2017. Vol. 9, № 2. pp. 39–59. DOI: 10.5195/ijt.2017.6231.
2. Asadianfam S., Talebi M.J., Nikougoftar E. ECG-based authentication systems: A comprehensive and systematic review // Multimedia Tools and Applications. 2023. Vol. 82, № 9. pp. 27647–27701. DOI: 10.1007/s11042-023-16506-3.

3. Ibtehaz N., Chowdhury M.E.H., Khandakar A., Kiranyaz S., Rahman M.S. EDITH: ECG biometrics aided by deep learning for reliable individual authentication // IEEE Transactions on Emerging Topics in Computational Intelligence. 2022. Vol. 6, № 4. pp. 928–940. DOI: 10.1109/TETCI.2021.3131374.
4. Donida Labati R., Muñoz E., Piuri V., Sassi R., Scotti F. Deep-ECG: Convolutional neural networks for ECG biometric recognition // Pattern Recognition Letters. 2018. Vol. 126. pp. 78–85. DOI: 10.1016/j.patrec.2018.03.028.
5. Ivanciu L., Ivanciu I.A., Faragó P., Roman M., Hintea S. An ECG-based authentication system using Siamese neural networks // Journal of Medical and Biological Engineering. 2021. Vol. 41, № 4. pp. 558–570. DOI: 10.1007/s40846-021-00637-9.
6. Agrawal V., Hazratifard M., Elmiligi H., Gebali F. ElectroCardioGram (ECG)-based user authentication using deep learning algorithms // Diagnostics. 2023. Vol. 13, № 3. P. 439. DOI: 10.3390/diagnostics13030439.
7. AlDuwaile D.A., Islam M.S. Using convolutional neural network and a single heartbeat for ECG biometric recognition // Entropy. 2021. Vol. 23, № 6. P. 733. DOI: 10.3390/e23060733.
8. Tirado-Martin P., Sanchez-Reillo R. BioECG: Improving ECG biometrics with deep learning and enhanced datasets // Applied Sciences. 2021. Vol. 11, № 13. P. 5880. DOI: 10.3390/app11135880.
9. Kim S.-K., Yeun C.Y., Damiani E., Lo N.W. A machine learning framework for biometric authentication using electrocardiogram // IEEE Access. 2019. Vol. 7. pp. 94858–94868. DOI: 10.1109/ACCESS.2019.2927079.
10. Abdalla F.Y.O., Wu L., Ullah H., Ren G., Noor A., Zhao Y. ECG arrhythmia classification using artificial intelligence and nonlinear and nonstationary

decomposition // Signal, Image and Video Processing. 2019. Vol. 13, № 7. pp. 1283–1291. DOI: 10.1007/s11760-019-01479-4.

11. Zhao Z., Zhang Y., Deng Y., Zhang X. ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation // Computers in Biology and Medicine. 2018. Vol. 102. pp. 168–179. DOI: 10.1016/j.compbiomed.2018.09.027.
12. Blasco J., Peris-Lopez P. On the feasibility of low-cost wearable sensors for multi-modal biometric verification // Sensors. 2018. Vol. 18, № 9. P. 2782. DOI: 10.3390/s18092782.
13. Barros A., Resque P., Almeida J., Mota R., Oliveira H., Rosário D., Cerqueira E. Data improvement model based on ECG biometric for user authentication and identification // Sensors. 2020. Vol. 20, № 10. P. 2920. DOI: 10.3390/s20102920.
14. Albuquerque S.L., de Souza J.N., Silva D.F., de Oliveira R.A. Authentication based on electrocardiography signals and machine learning // Engineering Research Express. 2021. Vol. 3, № 2. P. 025033. DOI: 10.1088/2631-8695/abffa6.
15. Su K., Yang G., Wu B., Yang L., Li D., Su P., Yin Y. Human identification using finger vein and ECG signals // Neurocomputing. 2019. Vol. 332. pp. 111–118. DOI: 10.1016/j.neucom.2018.12.015.
16. Zhang Y., Wu N.J. Practical human authentication method based on piecewise corrected electrocardiogram // Proc. Int. Conf. on System Science and Engineering (ICSSE). IEEE, 2016. pp. 300–303. DOI: 10.1109/ICSSE.2016.7883071.
17. Hammad M., Pławiak P., Wang K., Acharya U.R. ResNet-Attention model for human authentication using ECG signals // Expert Systems. 2020. Vol. 38, № 6. e12547. DOI: 10.1111/exsy.12547.

18. Sainath T.N., Kingsbury B., Saon G., Soltau H., Mohamed A., Dahl G. Deep convolutional neural networks for large-scale speech tasks // Neural Networks. 2015. Vol. 64. pp. 39–48. DOI: 10.1016/j.neunet.2014.08.005.
19. Khan A., Sohail A., Zahoora U., Qureshi A.S. A survey of the recent architectures of deep convolutional neural networks // Artificial Intelligence Review. 2020. Vol. 53. pp. 5455–5516. DOI: 10.1007/s10462-020-09825-6.
20. Barros A., Rosário D., Resque P., Cerqueira E. Heart of IoT: ECG as biometric sign for authentication and identification // Proc. 15th Int. Wireless Communications & Mobile Computing Conf. (IWCMC). IEEE, 2019. pp 307–312. DOI: 10.1109/IWCMC.2019.8766495.
21. Pourghebleh B., Wakil K., Navimipour N.J. A comprehensive study on the trust management techniques in the Internet of Things // IEEE Internet of Things Journal. 2019. Vol. 6, № 6. pp. 9326–9337. DOI: 10.1109/JIOT.2019.2933518.
22. Chen Z., Liu J., Shen Y., Simsek M., Kantarci B., Mouftah H.T., Djukic P. Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats // ACM Computing Surveys. 2022. Vol. 55, № 5. pp. 1–37. DOI: 10.1145/3530812.
23. Sharma P., Jain S., Gupta S., Chamola V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications // Ad Hoc Networks. 2021. Vol. 123. Article ID 102685. DOI: 10.1016/j.adhoc.2021.102685.
24. Ur Rehman I., Ullah I., Khan H., Guellil M.S., Koo J., Min J., Shabana H., Islam M., Lee M.Y. A comprehensive systematic literature review of ML in nanotechnology for sustainable development // Nanotechnology Reviews. 2024. Vol. 13, № 1. DOI: 10.1515/ntrev-2024-0069.

25. Ahad A., Tahir M., Sheikh M.A., Ahmed K.I., Mughees A., Numani A. Technologies trend towards 5G network for smart health-care using IoT: A review // Sensors. 2020. Vol. 20, № 14. P. 4047. DOI: 10.3390/s20144047.
26. Lodhi B., Kang J. Multipath-DenseNet: A supervised ensemble architecture of densely connected convolutional networks // Information Sciences. 2019. Vol. 482. pp. 63–72. DOI: 10.1016/j.ins.2019.01.012.
27. Kanatov M., Mendes M., Lyazzat A., Mateus M. Improved facial expression recognition with Xception deep net and preprocessed images // Applied Mathematics & Information Sciences. 2019. Vol. 13, № 5. pp. 859–865. DOI: 10.18576/amis/130520.
28. Nwankpa C., Ijomah W., Gachagan A., Marshall S. Activation functions: Comparison of trends in practice and research for deep learning // arXiv preprint. 2018. arXiv:1811.03378. URL: arxiv.org/abs/1811.03378.
29. Zhou D.-X. Deep distributed convolutional neural networks: Universality // Analysis and Applications. 2018. Vol. 16, № 6. P. 895–919. DOI: 10.1142/S0219530518500124.
30. Bento N., Belo D., Gamboa H. ECG biometrics using spectrograms and deep neural networks // International Journal of Machine Learning and Computing. 2020. Vol. 10, № 2. pp. 259–264. DOI: 10.18178/ijmlc.2020.10.2.929.
31. Zhou L., Thieret R., Watzlaf V.J.M., Parmanto B., Hartman L.M. A telehealth privacy and security self-assessment questionnaire for telehealth providers: Development and validation // International Journal of Telerehabilitation. 2019. Vol. 11, № 1. pp. 3–14. DOI: 10.5195/ijt.2019.6276.
32. Tyagi P.K., Agrawal D. Automatic detection of sleep apnea from single-lead ECG signal using enhanced-deep belief network model // Biomedical Signal Processing and Control. 2023. Vol. 80. Article ID 104401. DOI: 10.1016/j.bspc.2022.104401.

33. Domínguez-Bolaño T., Campos O., Barral V., Escudero C.J., García-Naya J.A. An overview of IoT architectures, technologies, and existing open-source projects // Internet of Things. 2022. Vol. 20. Article ID 100626. DOI: 10.1016/j.iot.2022.100626.
34. Ahmad I., Yao C., Li L., Chen Y., Liu Z., Ullah I., Shabaz M., Wang X., Huang K., Li G., Zhao G., Samuel O., Chen S. An efficient feature selection and explainable classification method for EEG-based epileptic seizure detection // Journal of Information Security and Applications. 2023. Vol. 80. Article ID 103654. DOI: 10.1016/j.jisa.2023.103654.
35. Jamin A., Humeau-Heurtier A. (Multiscale) cross-entropy methods: A review // Entropy. 2020. Vol. 22, № 1. P. 45. DOI: 10.3390/e22010045.
36. Al Alkeem E., Yeun C.Y., Yun J., Yoo P.D., Chae M., Rahman A., Asyhari A.T. Robust deep identification using ECG and multimodal biometrics for industrial internet of things // Ad Hoc Networks. 2021. Vol. 121. Article ID 102581. DOI: 10.1016/j.adhoc.2021.102581.
37. Yousuf T., Mahmoud R., Aloul F., Zualkernan I. Internet of Things (IoT) security: Current status, challenges and countermeasures // International Journal for Information Security Research. 2015. Vol. 5, № 4. pp. 608–616. DOI: 10.20533/ijisr.2042.4639.2015.0070.
38. Dogo E.M., Afolabi O.J., Nwulu N.I., Twala B., Aigbavboa C.O. A comparative analysis of gradient descent-based optimization algorithms on convolutional neural networks // Proc. Int. Conf. on Computational Techniques, Electronics and Mechanical Systems (CTEMS). IEEE, 2018. P. 92–99. DOI: 10.1109/CTEMS.2018.8769211.
39. Khan H., Khan H., Ullah I., Shabaz M., Omer M.F., Omer M., Usman M.T., Usman M., Guellil M.S., Al Jundi S.A., Koo J. Visionary vigilance: Optimized YOLOV8 for fallen person detection with large-scale benchmark

dataset // Image and Vision Computing. 2024. Vol. 149. Article ID 105195. DOI: 10.1016/j.imavis.2024.105195.

40. Marquez G., Astudillo H., Taramasco C. Security in telehealth systems from a software engineering viewpoint: A systematic mapping study // IEEE Access. 2020. Vol. 8. pp. 10933–10950. DOI: 10.1109/ACCESS.2020.2964988.
41. Sodhro A.H., Sennersten C., Ahmad A. Towards cognitive authentication for smart healthcare applications // Sensors. 2022. Vol. 22, № 6. P. 2101. DOI: 10.3390/s22062101.
42. Suran M. Increased use of Medicare telehealth during the pandemic // JAMA. 2022. Vol. 327, № 4. P. 313. DOI: 10.1001/jama.2021.23332.
43. Khan H., Jan Z., Ullah I., Guellil M.S., Koo J., Min J., Shabana H., Islam M., Lee M.Y. A deep dive into AI integration and advanced nanobiosensor technologies for enhanced bacterial infection monitoring // Nanotechnology Reviews. 2024. Vol. 13, № 1. DOI: 10.1515/ntrev-2024-0056.

Дата поступления: 23.03.2025
Дата публикации: 24.05.2025