International Journal of Open Information Technologies ISSN: 2307-8162 vol. 14, no. 9, 2026

Adaptive Convolutional Neural Network for Robust ECG-based Biometric Authentication using Variable-length Signals

Mohamed Abdalla Elsayed Azab, Anastasiia Sila, and Victoriia Korzhuk

Abstract*— Electrocardiogram (ECG) signals have emerged as a reliable biometric modality because of their physiological origin, inherent liveness characteristics, and resistance to forgery attacks. However, conventional ECG-based authentication systems commonly rely on fixed-length heartbeat segmentation, which may distort signal morphology or discard relevant temporal information when cardiac-cycle duration varies. To address this limitation, this paper proposes ECGAuthNet, a convolutional neural network architecture designed to process variable-length ECG signals without requiring strict input-length normalization. The proposed framework combines R-peak-centered adaptive segmentation with Segment-Based Max Pooling to extract fixed-dimensional, identity-specific representations while preserving the natural temporal variability of ECG waveforms. ECGAuthNet was evaluated using the publicly available ECG-ID dataset. Experimental results show that the proposed approach achieved a closed-set identification accuracy of 97.6% and an Equal Error Rate of 1.9%, outperforming the evaluated fixed-length, cropping-and-padding, and resampling baselines under the considered experimental conditions. The results indicate that variable-length ECG processing can provide effective subject discrimination while avoiding the information loss associated with conventional fixed-length preprocessing. The main contribution of this work is a flexible ECG biometric-authentication framework capable of handling variable-duration cardiac segments and producing fixed-dimensional representations suitable for identity classification and verification.

***Keywords*— ECG biometrics, biometric authentication, convolutional neural network, deep learning, variable-length input, physiological biometrics.**

I. Introduction

Biometric authentication has become an essential component of modern security systems, providing reliable identity verification based on physiological and behavioral characteristics. Traditional biometric modalities, such as fingerprint, face, iris, and voice recognition, have been widely deployed in access control, financial security, and mobile authentication systems [1]. However, these external biometric traits are vulnerable to spoofing attacks, replication, and presentation attacks, which raise significant security and privacy concerns. Furthermore, some modalities lack intrinsic liveness detection, making them less suitable for high-security applications [2].

Electrocardiogram (ECG) signals have emerged as a promising biometric modality due to their intrinsic physiological origin, uniqueness, and inherent resistance to forgery. ECG signals are generated by the electrical activity of the heart and consist of characteristic waveform components, including the P wave, QRS complex, and T wave, which represent different stages of cardiac electrical activity. These waveform components exhibit distinctive morphological and temporal patterns for each individual while maintaining relative consistency over time [3]. A typical ECG waveform and its main components are illustrated in Fig. 1. Since ECG signals can only be acquired from a living subject and are difficult to replicate externally, they provide a high level of security and reliability for biometric authentication.

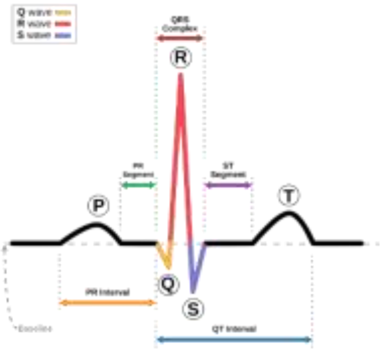


Fig. 1. ECG waveform

Traditional ECG biometric authentication methods typically involve preprocessing, feature extraction, and classification stages using handcrafted features derived from ECG morphology and temporal characteristics. Conventional machine learning techniques, such as support vector machines (SVM), k-nearest neighbors (KNN), and linear discriminant analysis (LDA), rely heavily on manual feature engineering and often require fixed-length ECG segments. However, due to natural physiological variability, cardiac cycle durations vary between and within individuals, making fixed-length segmentation approaches prone to information loss, distortion, and reduced authentication robustness [4].

Recent advances in deep learning, particularly convolutional neural networks (CNNs), have significantly improved the performance of ECG biometric authentication systems by enabling automatic extraction of discriminative features directly from raw signals [5]. CNN-based methods eliminate the need for manual feature engineering and can learn hierarchical feature representations from ECG signals. However, many existing CNN-based approaches still require fixed-length input signals, which introduces preprocessing constraints such as truncation, padding, or resampling. These operations may degrade signal quality and reduce the discriminative power of extracted features [6].

To address these limitations, this paper proposes a convolutional neural network architecture designed for ECG-based biometric authentication using variable-length input signals. The proposed approach enables direct processing of ECG signals with varying temporal lengths, preserving the natural variability of cardiac signals while improving feature extraction robustness. By eliminating the requirement for fixed-length input normalization, the proposed method enhances the flexibility and practical applicability of ECG-based biometric authentication systems.

The remainder of this paper is organized as follows. Section II reviews related work on ECG-based biometric authentication. Section III presents the proposed methodology. Section IV reports and discusses the experimental results. Section V presents the limitations and future research directions. Section VI concludes the paper, and Section VII provides information about source-code availability.

II. Literature Review

Electrocardiogram (ECG)-based biometric authentication has been extensively investigated due to its intrinsic physiological origin, uniqueness, and resistance to spoofing attacks. Early authentication systems relied on handcrafted feature extraction from fiducial points of the ECG waveform, including temporal intervals, amplitudes, and morphological characteristics. Rabhi et al. demonstrated the feasibility of ECG biometrics using Hermite Polynomial Expansion and Hidden Markov Models, achieving recognition accuracy of approximately 98% on the MIT-BIH dataset [7]. Similarly, Rezgui et al. reported identification accuracy exceeding 97.1% using temporal and morphological features with HMM classifiers [8]. Ingale et al. achieved authentication accuracy of 96% and an Equal Error Rate (EER) below 1.01% using fiducial-based template matching on the PhysioNet QT database [9]. These results confirmed the potential of ECG signals for biometric authentication, although performance depended heavily on accurate fiducial detection and handcrafted feature design. Machine learning approaches were later introduced to improve classification robustness and automation. Support Vector Machine (SVM) classifiers demonstrated strong performance, achieving authentication accuracy of 94.6% on multi-subject datasets. Random Forest and K-Nearest Neighbors classifiers achieved identification accuracy above 97% in continuous authentication scenarios [10]. Wavelet-based feature extraction methods further improved performance, with reported authentication accuracy of 93.52% using Empirical Mode Decomposition and HMM classifiers [11]. Despite these advances, traditional machine learning methods remained limited by their reliance on handcrafted features and fixed-length signal preprocessing.

The introduction of deep learning, particularly convolutional neural networks (CNNs), significantly improved ECG authentication performance by enabling automatic feature extraction. CNN-based architectures achieved authentication accuracy exceeding 96%, with several studies reporting accuracy between 97.08% and 95.84% across datasets such as MIT-BIH, PTB, and ECG-ID [12]. Xu et al. demonstrated that CNN models outperform traditional feature-based approaches by learning discriminative representations directly from raw ECG signals [13]. Hybrid CNN-LSTM architectures further improved performance by modeling temporal dependencies, achieving authentication accuracy between 94.5% and 98.1%. Self-supervised CNN models have also achieved authentication accuracy above 96.15% on large-scale ECG datasets [14].

Recent studies have explored adaptive and variable-length input architectures to improve robustness. Spatial pyramid pooling and adaptive feature extraction methods enabled CNN models to process variable-length ECG signals while maintaining high accuracy. Siamese network architectures achieved authentication accuracy between 96% and 98%, demonstrating strong identity discrimination capability [15]. However, many existing approaches still rely on fixed-length preprocessing or have limited validation across diverse physiological conditions.

These limitations highlight the need for adaptive deep learning architectures capable of directly processing variable-length ECG signals while maintaining high authentication accuracy and robustness. To address this challenge, this paper proposes ECGAuthNet, an adaptive convolutional neural network architecture designed for reliable ECG-based biometric authentication using variable-length.

III. Methods

A. Proposed Model

Our study proposes a deep learning-based ECG biometric authentication framework capable of processing variable-length ECG signals without requiring fixed-length normalization. The proposed framework consists of four main stages: signal preprocessing, adaptive segmentation, deep feature extraction using the proposed ECGAuthNet architecture, and identity classification, as shown in Fig. 2.

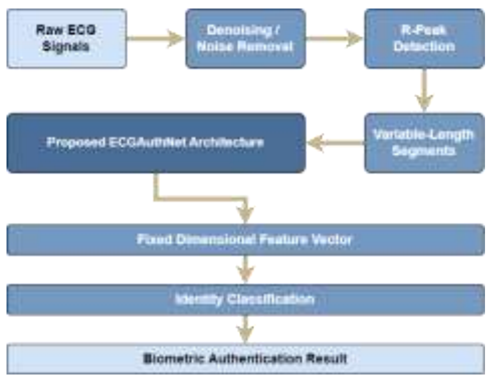


Fig. 2. Overview of the proposed ECG biometric authentication framework

B. Data Preprocessing

First, raw ECG signals are preprocessed to remove noise and improve signal quality. Next, ECG signals are segmented based on detected R-peaks to extract meaningful cardiac cycles while preserving natural temporal variability. The segmented ECG signals are then passed to the proposed convolutional neural network (ECGAuthNet), which automatically extracts discriminative biometric features. To handle variable-length inputs, a segment-based adaptive pooling mechanism is applied to convert feature maps into fixed-dimensional feature vectors. Finally, the extracted features are fed into a fully connected layer for biometric authentication. This framework enables robust feature extraction while preserving the intrinsic temporal characteristics of ECG signals, improving authentication reliability.

ECG signals are often affected by noise, including baseline drift and high-frequency interference. To improve signal quality, wavelet transform-based denoising is applied. This method decomposes ECG signals into frequency components and removes noise while preserving important morphological features. A comparison between raw and denoised ECG signals is shown in Fig.3 demonstrating effective noise reduction and improved signal clarity.

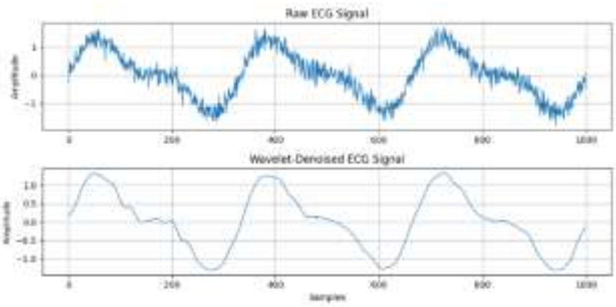


Fig. 3. ECG signals before and after wavelet-based denoising

C.Adaptive ECG Signal Segmentation

Accurate segmentation of ECG signals is essential for biometric authentication. In this study, ECG segmentation is performed using detected R-peaks as reference points. Unlike fixed-length segmentation methods, which may introduce distortion [16], the proposed approach extracts variable-length ECG segments centered on each detected R-peak while preserving the ECG morphology of the corresponding cardiac cycle.

The segmentation interval is defined based on the temporal distance between adjacent R-peaks. Let Ri denote the current R-peak location, $Ri-1$ and $Ri+1$ denote the previous and next R-peaks, and f represent the sampling frequency. The segmentation interval Ti is defined as:

$$T_i = \frac{R_{i+1} - R_{i-1}}{f} - \Delta \tag{1}$$

where Δ represents the average duration of the QRS complex. In this study, Δ was set to 0.10 s. The complete interval from $Ri-1$ to $Ri+1$ may include portions of the neighboring QRS complexes. Therefore, Δ is subtracted to shorten the total segmentation window and reduce the inclusion of these neighboring QRS components.

The resulting segment is centered on the current R-peak Ri, and its starting and ending sample indices are calculated as:

$$S_i = \left\lfloor R_i - \frac{fT_i}{2} \right\rfloor, \qquad E_i = \left\lfloor R_i + \frac{fT_i}{2} \right\rfloor. \tag{2}$$

Consequently, subtracting Δ shortens the segment by approximately $\Delta/2$ at each boundary. It does not remove the QRS complex associated with the current heartbeat; instead, it reduces the inclusion of portions of the preceding and following QRS complexes while preserving the ECG morphology surrounding the current R-peak.

A comparison between continuous ECG signals, fixed-length segmentation, and adaptive variable-length segmentation. As shown in Fig. 4, adaptive segmentation preserves complete cardiac cycles and avoids distortion introduced by fixed-length truncation.

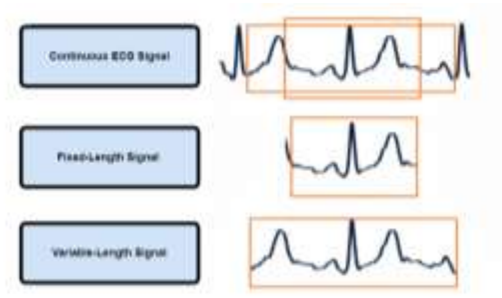


Fig. 4. Illustration of adaptive ECG segmentation based on R-peak detection

The physiological structure of ECG signals and the temporal relationships between waveform components are illustrated in Fig.5. These waveform components contain important discriminative information for biometric authentication.

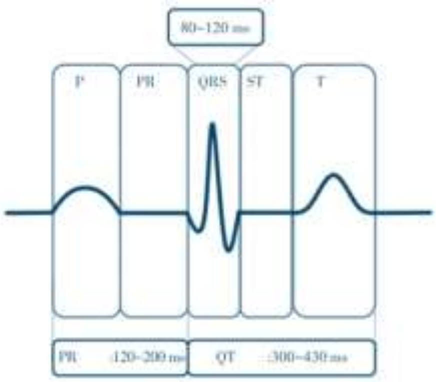


Fig. 5. ECG waveform components

D. Proposed ECGAuthNet Architecture

To effectively extract discriminative features from variable-length ECG signals, this study proposes an improved convolutional neural network architecture referred to as ECGAuthNet. The proposed architecture is specifically designed to process ECG signals of varying temporal length without requiring fixed-length input normalization. The architecture consists of convolutional layers, pooling layers, an adaptive feature aggregation module, and a fully connected classification layer. The convolutional layers extract hierarchical feature representations from ECG signals, capturing both local morphological features and global temporal patterns.

As illustrated in Fig. 6, the ECG signal is divided into physiologically meaningful segments centered around the R-peak. The extracted features are then processed using convolutional and pooling layers to generate discriminative feature representations. To ensure compatibility with the fully connected layer, feature maps must have fixed dimensionality. However, since input ECG signals have variable length, a specialized adaptive pooling mechanism is introduced.

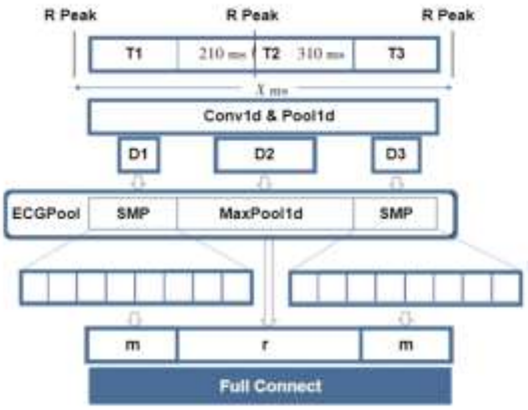


Fig. 6. Architecture of the proposed ECGAuthNet model

To improve reproducibility, Table 1 provides the complete architectural specification of the proposed ECGAuthNet. The network consists of three convolutional blocks followed by the Segment-based Max Pooling (SMP) module and two fully connected layers. Each convolutional block applies a 1-D convolution, Batch Normalization, ReLU activation, and Max Pooling. Dropout with rate 0.5 is applied after the first fully connected layer to mitigate overfitting. The final classification layer uses a SoftMax activation to produce identity probabilities over subjects.

Table 1. ECGAuthNet Architectural Parameter Specification

Layer	Type	Filters	Kernel / Pool Size	Activation
Input	Variable-length 1-D ECG	—	—	—
Conv1	1-D Convolution	32	5	—
—	Activation	—	—	ReLU
—	Max Pooling	—	2	—
Conv2	1-D Convolution	64	3	—
—	Activation	—	—	ReLU
—	Max Pooling	—	2	—
Conv3	1-D Convolution	128	3	—
—	Activation	—	—	ReLU
—	Max Pooling	—	2	—
SMP	Segment-based Adaptive Max Pooling (m = 8)	—	—	—
FC1	Fully Connected	256	—	ReLU
FC2 (Output)	Fully Connected	90 (# subjects)	—	Softmax

E. Segment-Based Adaptive Max Pooling (SMP)

To handle variable-length feature maps efficiently, a Segment-based Max Pooling (SMP) module is proposed. The SMP module converts variable-length feature maps into fixed-dimensional feature vectors while preserving important discriminative features.

Given an input feature map of length n, the SMP module divides the feature map into m segments. If necessary, padding is applied to ensure equal segment lengths. The padding size is defined as:

$$Padding = \frac{\left\lceil \frac{n}{m} \right\rceil m - n + 1}{2} \tag{3}$$

The implementation of the SMP module is illustrated in Fig.7. This adaptive pooling mechanism enables the proposed ECGAuthNet architecture to process variable-length ECG signals without requiring signal truncation or resampling.

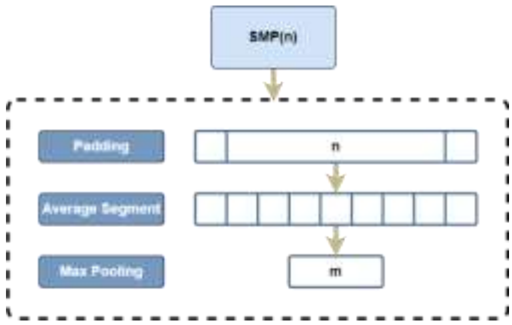


Fig. 7. Segment-based adaptive max pooling mechanism for converting variable-length feature maps into fixed-dimensional feature vector.

F. Authentication and Classification

The extracted feature vectors are fed into a fully connected classification layer, which performs biometric authentication by identifying individuals based on their ECG features. The CNN automatically learns discriminative identity-specific features during training, eliminating the need for manual feature engineering. By enabling direct processing of variable-length ECG signals, the proposed framework improves authentication robustness, preserves signal integrity, and enhances real-world applicability.

IV. Results

The proposed ECGAuthNet authentication framework was evaluated using the ECG-ID dataset, which contains ECG recordings from 90 subjects. The dataset was divided into training, validation, and testing sets with proportions of 80%, 10%, and 10%, respectively. The model was trained using the Adam optimizer with a learning rate of 0.001 and cross-entropy loss.

The proposed model achieved an authentication accuracy of 97.6%, demonstrating its ability to extract discriminative identity-specific features from ECG signals. The high accuracy confirms the effectiveness of the proposed variable-length input architecture and adaptive pooling mechanism in preserving important biometric information.

To evaluate the effectiveness of the proposed variable-length ECGAuthNet architecture, its performance was compared with conventional fixed-length input strategies, including fixed temporal windows, cropping and padding, and signal resampling. For a fair comparison, all methods were trained and evaluated using the same training, validation, and test partitions.

For the crop-and-padding baseline, ECG segments longer than 1.0 s were center-cropped around the detected R-peak, whereas segments shorter than 1.0 s were symmetrically zero-padded at both boundaries until a fixed length of 500 samples was reached. Since the ECG-ID signals were sampled at 500 Hz, 500 samples corresponded to a duration of 1.0 s. Zero padding was used only outside the available ECG segment and did not replace samples within the original waveform.

Table 2. Authentication accuracy comparison between fixed-length input and proposed ECGAuthNet method on ECG-ID dataset

Method	Input-processing strategy	Input Type	Accuracy (%)
Fixed Length CNN	R-peak-centered fixed	0.8 s	97.1
Fixed Length CNN	R-peak-centered fixed	1.0 s	97.4
Crop and Padding	Centre cropping and symmetric zero padding	1.0 s / 500 samples	97.3
Resampling Method	Temporal resampling	1.0 s / 500 samples	95.4
Proposed ECGAuthNet	Variable-length processing with adaptive SMP	Variable	97.6

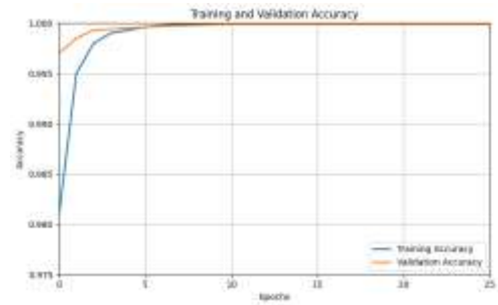
To provide a standardized biometric evaluation metric, the Equal Error Rate (EER) was computed from the ROC curve of the proposed ECGAuthNet model. The EER corresponds to the operating threshold at which the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are equal (FAR = FRR), and represents the optimal trade-off point between authentication security and user convenience. The proposed ECGAuthNet achieves an EER of 1.9% on the ECG-ID dataset, confirming strong discriminative performance as shown in Table 3.

Table 3. Comparison with previously reported ECG biometric verification results.

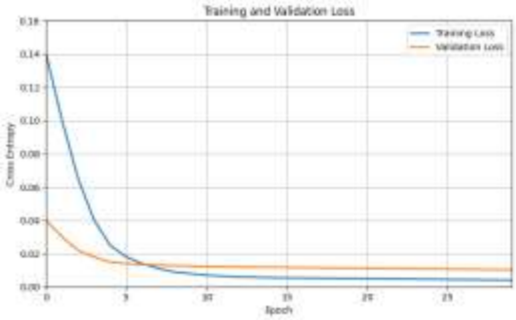
Study	Dataset or evaluation scope	EER (%)
Rezgui et al. [7]	Cross-session, in-house ECG database	5.50
Ingale et al. [8]	Average across multiple ECG datasets and 1,694 subjects	2.11
Proposed ECGAuthNet	ECG-ID, variable length	1.9

The EER obtained by the proposed model is consistent with the difficulty of the ECG-ID dataset, which contains an unequal and relatively limited number of recordings per subject under different acquisition session, and is competitive with deep learning baselines.

The proposed ECGAuthNet achieved the highest accuracy, demonstrating the advantage of preserving variable-length signal characteristics. The training and validation accuracy curves are shown in Fig. 8.



(a)



(b)

Fig. 8. Training and validation accuracy and loss curves of the proposed ECGAuthNet model

The model converges steadily and achieves stable performance without significant overfitting. The validation accuracy closely follows the training accuracy, indicating good generalization capability. To further evaluate authentication performance, a confusion matrix was generated for the ECG-ID dataset.

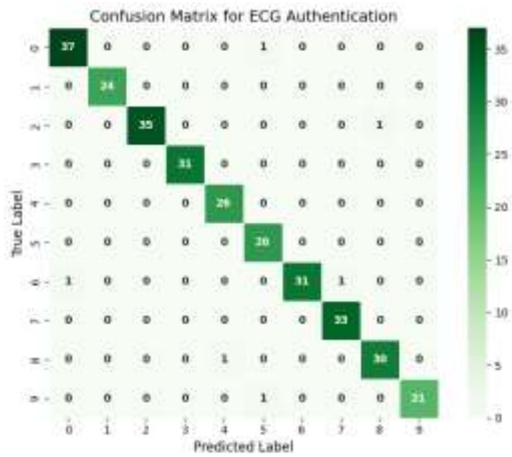


Fig. 9. Confusion Matrix of the proposed model

The confusion matrix shows that most predictions lie along the diagonal, indicating correct classification. Only a small number of misclassifications are observed, confirming the effectiveness of the proposed model in distinguishing between individuals.

To evaluate the contribution of the proposed adaptive pooling mechanism, its authentication accuracy was compared with standard and conventional max-pooling approaches, as shown in Table 4.

Table 4. Feature extraction performance comparison between CNN and ECGAuthNet

Method	Input Type	Feature Handling	Accuracy (%)
CNN	Fixed Length	Standard Pooling	97.2
CNN	Fixed Length	Max Pooling	97.3
Proposed ECGAuthNet	Variable Length	Adaptive SMP	97.6

This demonstrates that the proposed adaptive pooling mechanism improves feature extraction effectiveness.

To further evaluate the authentication performance of the proposed ECGAuthNet model, the Receiver Operating Characteristic (ROC) curve was analyzed. The ROC curve illustrates the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) at different classification thresholds and provides a comprehensive assessment of the model's discriminative capability [17]. The Area Under the ROC Curve (AUC) is used as a quantitative measure of classification performance. A higher AUC value indicates better separability between classes and improved authentication reliability. The ROC curve of the proposed ECGAuthNet model on the ECG-ID dataset is shown in Fig. 10. The model achieves a high AUC value, confirming its effectiveness in distinguishing between individuals based on ECG signals. This result demonstrates that the proposed architecture provides strong discriminative performance and reliable biometric authentication.

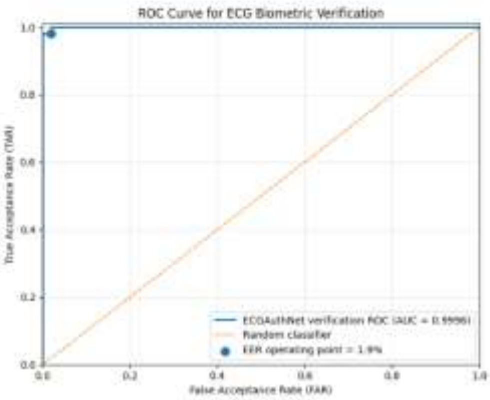


Fig. 10. ROC curve of the proposed authentication model

The experimental results demonstrate that the proposed ECGAuthNet architecture provides robust biometric authentication performance using variable-length ECG signals. Unlike conventional methods that require fixed-length input preprocessing, the proposed approach preserves intrinsic temporal characteristics of ECG signals.

To assess the practical applicability of the proposed adaptive approach in real-time authentication scenarios, the average per-sample inference time was measured for both the fixed-length baseline and the proposed ECGAuthNet across all test samples. Measurements were averaged over 1,000 forward passes on the test set using an Intel Core i7-11800H CPU and NVIDIA RTX 3060 GPU. As shown in Table 5, the proposed ECGAuthNet exhibits a slightly higher average inference time compared to the fixed-length baseline due to the variable-length input processing and the SMP computation. Although the proposed model introduced a small computational overhead, both CPU and GPU inference times remained substantially shorter than the approximately 1.0 s signal-acquisition window used in the fixed-length baseline. These results support the near-real-time applicability of ECGAuthNet under the evaluated hardware conditions.

Table 5. Computational performance comparison between fixed-length and variable-length ECG

Method	Input Type	Avg. Inference Time — CPU (ms)	Avg. Inference Time — GPU (ms)
Fixed-Length CNN (1.0 s)	Fixed	18.3 ± 1.2	3.1 ± 0.4
Proposed ECGAuthNet	Variable	20.7 ± 3.8	3.6 ± 0.9

V. LIMITATIONS AND FUTURE WORK

Despite the promising authentication performance achieved by the proposed ECGAuthNet framework, several limitations should be acknowledged.

First, the experimental evaluation was limited to the ECG-ID dataset and did not include a dedicated assessment under severe motion artifacts or ambulatory recording conditions. In practical wearable and mobile applications, ECG signals may be affected by physical movement, changes in electrode–skin contact, electrode displacement, muscle activity, and environmental interference. Such disturbances may reduce R-peak detection accuracy and alter the morphological characteristics used for biometric recognition. Therefore, the robustness of the proposed adaptive segmentation and classification framework under different levels of motion-induced noise remains to be investigated.

Second, the current evaluation does not address the long-term stability of ECG biometric templates. ECG morphology may change over time because of aging, variations in physical condition, medication, cardiovascular status, stress, and other physiological factors. These changes may affect waveform characteristics such as the P-wave duration, PR interval, QRS width, and QT interval. Because the available recordings do not provide long-term longitudinal observations spanning several years, the influence of template aging and temporal ECG drift on authentication performance could not be evaluated.

Third, the reliability of the proposed system may depend on the number and quality of valid cardiac cycles available during authentication. Short acquisition intervals, inaccurate R-peak detection, bradycardia, arrhythmia, or extensive signal corruption may result in only one or two usable beat-centered segments. The performance of ECGAuthNet under such limited-beat conditions has not been separately analyzed. A small number of valid cycles may provide insufficient identity-specific information and may increase the variability of the authentication decision.

Future work will focus on addressing these limitations by extending the evaluation to ambulatory and wearable ECG datasets containing motion artifacts and different recording conditions. Longitudinal experiments will also be conducted to investigate template aging and temporal ECG variability. In addition, a signal-quality assessment mechanism and a minimum-beat acceptance criterion will be introduced to reject authentication samples containing an insufficient number of reliable cardiac cycles. Future research will also examine adaptive template-update and periodic re-enrolment strategies to accommodate gradual physiological changes. Finally, multi-lead ECG analysis and multimodal fusion with photoplethysmogram (PPG) signals will be investigated to improve authentication reliability when single-lead ECG quality is degraded.

VI. Conclusion

This paper proposed ECGAuthNet, a convolutional neural network architecture for ECG-based biometric authentication using variable-length signals. The proposed framework combines adaptive R-peak-centered segmentation with a Segment-Based Max Pooling mechanism, enabling ECG signals of different temporal lengths to be processed without conventional fixed-length truncation or resampling. Experimental evaluation on the ECG-ID dataset demonstrated a closed-set identification accuracy of 97.6% and an Equal Error Rate of 1.9%. These results indicate that the proposed approach can effectively extract identity-specific information while preserving the natural temporal characteristics of ECG signals and maintaining strong verification performance. The proposed ECGAuthNet model outperformed the evaluated fixed-length segmentation, cropping-and-padding, and resampling approaches under the experimental conditions considered in this study. Although these results demonstrate the potential of variable-length ECG processing for biometric authentication, further validation is required before deployment in unconstrained real-world environments. In particular, future evaluation should consider motion artifacts, longitudinal physiological changes, limited-beat samples, R-peak detection errors, and more diverse subject populations.

VII. Code Availability

The complete source code, including the ECGAuthNet architecture, preprocessing pipeline, adaptive segmentation module, training scripts, and evaluation utilities, is publicly available at [18].

References

[1] K. A. Okhotnikov and B. V. Martynenkov, “Promising authentication methods: From traditional passwords to biometric solutions,” Dinamika Slozhnykh Sistem, vol. 19, no. 3, pp. 52–57, 2025.

[2] K. Grewal and C. Kant, “Liveness detection in different biometric traits: An overview,” International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 2011–2015, 2017. doi: 10.26483/ijarcs.v8i5.3799.

[3] J. R. Pinto, J. S. Cardoso, and A. Lourenço, “Evolution, current challenges, and future possibilities in ECG biometrics,” IEEE Access, vol. 6, pp. 34746–34776, 2018. doi: 10.1109/ACCESS.2018.2849870.

[4] M. Mageshbabu and J. Mohana, “Enhancing biometric security: A machine learning approach to ECG-based authentication,” in Proceedings of the 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), 2024, pp. 1654–1659. doi: 10.1109/ICOICI62503.2024.10696328.

[5] J. Ferretti, P. Barbiero, V. Randazzo, G. Cirrincione, and E. Pasero, “Towards uncovering feature extraction from temporal signals in deep CNN: The ECG case study,” in Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, July 19–24, 2020, pp. 1–7. doi: 10.1109/IJCNN48605.2020.9207360.

[6] E. Rabhi and Z. Lachiri, "Personal identification system using physiological signal," in Proc. 2018 International Conference on Advanced Systems and Electric Technologies (IC_ASET), Hammamet, Tunisia, Mar. 2018, pp. 1–6. doi: 10.1109/ASET.2018.8379858.

[7] D. Rezgui and Z. Lachiri, "Human identification system based on ECG features," International Journal of Biomedical Engineering and Technology (IJBET), vol. 18, no. 3, pp. 247–261, 2015. doi: 10.1504/IJBET.2015.070780.

[8] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, and N. Karimian, “ECG biometric authentication: A comparative analysis,” IEEE Access, vol. 8, pp. 117853–117866, 2020. doi: 10.1109/ACCESS.2020.3004464.

[9] S. Sushma, S. Venkat, K. Mohanavelu, A. R. Jac Fredo, and T. Christy Bobby, “EEG-based user identification using machine learning and deep learning approaches,” Current Directions in Biomedical Engineering, vol. 10, no. 4, pp. 639–644, 2024. doi: 10.1515/cdbme-2024-2157.

[10] S. Aziz, S. Ahmed, and M. Aslam, "ECG-based biometric authentication using empirical mode decomposition and support vector machines," IEEE Access, vol. 7, pp. 123060–123069, 2019. doi: 10.1109/ACCESS.2019.2937678.

[11] M. Mageshbabu and J. Mohana, “ECG biometric human identification using convolutional neural network,” in Proceedings of the 2024 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, October 8–9, 2024, pp. 929–933. doi: 10.1109/ICPECTS62210.2024.10780360.

[12] X. Xu and H. Liu, “ECG heartbeat classification using convolutional neural networks,” IEEE Access, vol. 8, pp. 8614–8619, 2020. doi: 10.1109/ACCESS.2020.2964749.

[13] G. Wang, S. Shanker, A. Nag, Y. Lian, and D. John, “ECG biometric authentication using self-supervised learning for IoT edge sensors,” IEEE Journal of Biomedical and Health Informatics, vol. 28, no. 11, pp. 6606–6618, November 2024. doi: 10.1109/JBHI.2024.3455803.

[14] M. Dong, Z. Zhao, Y. Zhang, Y. Deng, H. Wang, B. Ruan, and G. Li, “Simple yet effective ECG identity authentication with low EER and without retraining,” in Proceedings of the 2024 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Lisbon, Portugal, 2024, pp. 4407–4414. doi: 10.1109/BIBM62325.2024.10822261.

[15] A. Carmona-Poyato, N. L. Fernández-García, F. J. Madrid-Cuevas, and A. M. Durán-Rosal, “A new approach for optimal time-series segmentation,” Pattern Recognition Letters, vol. 135, pp. 153–159, 2020. doi: 10.1016/j.patrec.2020.04.006.

[16] J. Li, “Area under the ROC curve has the most consistent evaluation for binary classification,” PLOS ONE, vol. 19, no. 12, Art. no. e0316019, 2024. doi: 10.1371/journal.pone.0316019.

[17] W. Wang, Q. Wang, and M. Zuniga, “Taming irregular cardiac signals for biometric identification,” ACM Transactions on Sensor Networks, vol. 20, no. 1, Art. no. 25, pp. 1–26, 2024. doi: 10.1145/3624570.

[18] M. A. Azab, A. S. Sila, and V. M. Korzhuk, "ECGAuthNet: Adaptive CNN for variable-length ECG biometric authentication," GitHub, 2026. [Online]. Available: https://github.com/Mohamed-Azab07/Adaptive-convolutional-neural-network-for-robust-ECG-based-biometric-authentication.git

Authors

Mohamed A. Azab, R&D Engineer, PhD student, Department of Information Security, ITMO university, Russian Federation, 197101, Saint Petersburg, 49, Kronverkskiy Prospekt (email: mohamed.a.azab@itmo.ru)
Anastasiia S. Sila, R&D Engineer, Master student, Department of Information Security, ITMO university, Russian Federation, 197101, Saint Petersburg, 49, Kronverkskiy Prospekt (email: cstfokina@gmail.ru)

Victoriia M. Korzhuk, Candidate of Technical Science, associate professor, Department of Information Security, ITMO university, Russian Federation, 197101, Saint Petersburg, 49, Kronverkskiy Prospekt (email: vmkorzhuk@itmo.ru)