УДК 004.056.53

A SECURED MULTIMODAL ECG BIOMETRIC AUTHENTICATION SYSTEM USING DEEP LEARNING

Азаб М. А. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Коржук В.М. (ИТМО)

Abstract. The growing demand for secure and continuous authentication has highlighted the limitations of traditional biometric modalities such as passwords, fingerprints, and facial recognition. Electrocardiogram (ECG) signals have emerged as a robust biometric trait due to their physiological uniqueness, inherent liveness detection, and resistance to spoofing attacks. This work presents a secured multimodal biometric authentication system based on ECG signals and deep learning techniques. The proposed approach integrates signal preprocessing, heartbeat segmentation, and deep neural network-based feature learning within a multimodal fusion framework.

Main Part. ECG-based biometric authentication leverages the electrical activity of the heart, which reflects unique morphological and temporal characteristics for each individual. Unlike static biometrics, ECG signals provide continuous authentication and are inherently difficult to forge. However, ECG authentication systems face several challenges [1], including signal noise, temporal variability, and difficulties in extracting reliable features such as fiducial points. To address these challenges, the proposed system follows a structured authentication pipeline. Raw ECG signals are first acquired and preprocessed to remove noise and artifacts [2]. R-peaks are then detected to enable accurate heartbeat segmentation. The segmented beats are used as input to deep learning models, which automatically learn discriminative features without relying on handcrafted feature extraction. To further improve robustness, a multimodal biometric fusion strategy is employed by integrating ECG with complementary physiological signals such as photoplethysmography (PPG) [3]. Deep neural networks are used to learn joint representations from multiple modalities, reducing sensitivity to signal variability and improving resistance to spoofing. Experimental evaluation using public ECG datasets demonstrates that accurate R-peak detection and beat-level aggregation significantly enhance authentication performance, achieving high detection and classification accuracy [4].

Conclusion. This work presents a secured multimodal ECG biometric authentication system using deep learning. By combining precise ECG signal processing, deep neural network-based feature learning, and multimodal biometric fusion, the proposed framework achieves high authentication accuracy and robustness. The results confirm the suitability of ECG-based biometrics for secure and continuous authentication, particularly in telehealth and remote systems. Future research will focus on large-scale validation, real-time deployment, and privacy-preserving implementations compliant with regulatory standards.

List of References:

1. Kumar, A., Zhang, D., & Smith, J. Uniqueness and Security of ECG Biometrics // Journal of Biomedical Engineering. 2021. Vol. 45, No. 3. P. 123-135.
2. Zhang, L., Chen, X., & Liu, Y. Advancements in Wearable ECG Sensors for Telehealth Applications // IEEE Transactions on Biomedical Engineering. 2022. Vol. 69, No. 8. P. 2456-2467.
3. Sufi, F., Islam, M., & Wang, H. Preprocessing Techniques for ECG Signal Analysis // Biomedical Signal Processing and Control. 2020. Vol. 58. P. 101829.
4. Liu, J., Wang, R., & Li, T. Deep Learning for ECG-Based Biometric Authentication // Nature Machine Intelligence. 2023. Vol. 5, No. 2. P. 156-168.