Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871

Vol. 6, No. 4, August 2025, Page. 1911-1924
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.5098

Multimodal Biometric Recognition Based on Fusion of Electrocardiogram and Fingerprint Using CNN, LSTM, CNN-LSTM, and DNN Models

Winda Agustina[1], Dodon Turianto Nugrahadi[2,*] Mohammad Reza Faisal[3], Triando Hamonangan Saragih[4], Andi Farmadi[5], Irwan Budiman[6], Jumadi Mabe Parenreng[7], Muhammad Alkaff[8]

[1,2,3,4,5,6]Department of Computer Science, Lambung Mangkurat University, Banjarbaru, Indonesia
[7]Informatics and Computer Engineering Department, Universitas Negeri Makassar, Indonesia
[8]Department of Information Technology, Lambung Mangkurat University, Banjarmasin, Indonesia
[8]Computer Science Department, Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah, Saudi Arabia

Email: [2]dodonturianto@ulm.ac.id

Received : Jul 14, 2025; Revised : Aug 4, 2025; Accepted : Aug 6, 2025; Published : Aug 18, 2025

Abstract

Biometric authentication offers a promising solution for enhancing the security of digital systems by leveraging individuals' unique physiological characteristics. This study proposes a multimodal authentication system using deep learning approaches to integrate fingerprint images and electrocardiogram (ECG) signals. The datasets employed include FVC2004 for fingerprint data and ECG-ID for ECG signals. Four deep learning architectures—Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), CNN-LSTM, and Deep Neural Network (DNN)—are evaluated to compare their effectiveness in recognizing individual identity based on fused multimodal features. Feature extraction techniques include grayscale conversion, binarization, edge detection, minutiae extraction for fingerprint images, and R-peak–based segmentation for ECG signals. The extracted features are combined using a feature-level fusion strategy to form a unified representation. Experimental results indicate that the CNN model achieves the highest classification accuracy at 96.25%, followed by LSTM and DNN at 93.75%, while CNN-LSTM performs the lowest at 11.25%. Minutiae-based features consistently yield superior results across different models, highlighting the importance of local feature descriptors in fingerprint-based identification tasks. This research advances biometric authentication by demonstrating the effectiveness of feature-level fusion and CNN architecture for accurate and robust identity recognition. The proposed system shows strong potential for secure and adaptive biometric authentication in modern digital applications.

Keywords : *Biometric Recognition, CNN, ECG, Feature Fusion, Fingerprint, Multimodal*

1. INTRODUCTION

Cybersecurity is critical in protecting personal data and systems from online threats in the current digital era. The increasing adoption of technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI) has heightened the risks of cyberattacks, including ransomware, phishing, and intrusions targeting sensitive data [1] [2]. These threats exploit system vulnerabilities and user weaknesses, such as limited security awareness. Thus, a holistic approach is required, encompassing advanced security technologies, clear policy frameworks, and user education. Emerging technologies such as AI and machine learning (ML) have shown promise in enabling the automatic detection and mitigation of cyberattacks [3] [4]. Ensuring cybersecurity resilience demands coordinated efforts among governments, industry stakeholders, and the general public.

Many systems have adopted biometric technologies to address digital security challenges as a more secure and practical authentication method. Biometrics verify an individual's identity by authenticating unique biological characteristics [5] [6]. This technology utilizes distinctive physical or behavioral traits—such as fingerprints, facial features, or heartbeat patterns—to directly authenticate users. Unlike passwords, which can be stolen or forgotten, biometric data is difficult to forge, thus offering stronger protection against threats such as identity theft and social engineering attacks[7] [8]. Furthermore, biometric systems enable passwordless authentication, providing a faster and more user-friendly experience [9] [10]. As a result, biometrics are increasingly regarded as a future-oriented solution for enhancing cybersecurity across various digital applications [11] [12].

However, unimodal biometric systems still face several limitations, including sensitivity to noise, vulnerability to spoofing attacks, and inconsistent accuracy under varying environmental conditions [13]. To overcome these issues, multimodal biometric approaches have been developed, combining two or more types of biometric data simultaneously. This approach has proven superior in increasing accuracy, reliability, and resilience against data manipulation and cyber threats. By leveraging the strengths of each modality, multimodal biometric systems can provide more consistent authentication results and adaptability across diverse user and environmental conditions [14]. In addition to reinforcing security, this approach also broadens the scope of authentication and enhances its flexibility for implementation in public services, finance, and cyber-physical systems [15].

Feature-level fusion is a crucial strategy for enhancing authentication effectiveness in implementing multimodal biometric systems. This method combines information from various biometric modalities at the feature representation stage before classification. By unifying the unique characteristics of each data type—such as texture patterns, shapes, or biological signals—the system can construct a richer and more discriminative identity representation. This significantly strengthens system robustness against spoofing and data manipulation, as authentication validity no longer relies on a single biometric source [16] [17]. Furthermore, feature fusion reduces the likelihood of identification errors caused by noise or degradation in one modality. In cybersecurity, this approach improves authentication accuracy and supports the development of more resilient, adaptive identity verification systems that are difficult to breach via social engineering or unauthorized access [18].

In modern biometric systems, feature extraction is a critical initial stage for preparing data before classification [19] [20]. This study performs feature extraction using a machine learning-based approach through a series of image processing techniques, including grayscale conversion, binarization, edge detection, and minutiae extraction. These steps capture key characteristics of biometric images, particularly fingerprints, enabling the system to recognize patterns more efficiently. The extracted features are then used as input for classification using various deep learning architectures, namely Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), a hybrid CNN-LSTM model, and Deep Neural Network (DNN). This combination of feature extraction and classification has proven effective in improving the accuracy of biometric authentication systems, owing to the ability of deep learning models to recognize complex patterns and automatically accommodate variability in biometric data [21] [22].

One of the recent approaches in fingerprint recognition is the Gravitational Search Decision Forest (GSDF), which combines the exploration capabilities of the Gravitational Search Algorithm (GSA) with the classification power of Random Forest (RF). This method explicitly addresses identification challenges in latent and full fingerprint images, particularly low-quality ones commonly found in forensic scenarios. The process begins with image enhancement using a combination of ridge dictionary and Gabor filters, followed by minutiae feature extraction using the crossing number method and feature selection to eliminate spurious minutiae. GSDF then constructs a decision forest by employing GSA mass agents that randomly generate decision trees based on RF principles. Experimental results on the

NIST SD27 and FVC2004 datasets indicate that GSDF outperforms other algorithms such as RF, Decision Tree (DT), Backpropagation Neural Network (BPNN), and K-Nearest Neighbors (KNN), achieving an accuracy of 92.56% for latent fingerprints and 96.56% for full fingerprints [23].

In addition, neural network-based approaches have also been proposed as fingerprint matching algorithms that combine edge-based features with convolutional neural networks (CNN). This method eliminates the need for manual feature extraction by utilizing Prewitt and Laplacian of Gaussian filters during the image enhancement stage, followed by CNN training using data from four subsets of the FVC2004 dataset. Experimental results show a maximum validation accuracy of 98.7% and a test accuracy of up to 75.6%, although overfitting was observed after the seventh epoch. This study highlights that integrating edge enhancement techniques within CNNs can efficiently improve fingerprint matching performance in large-scale biometric systems [24].

Another study proposed a biometric verification system based on electrocardiogram (ECG) signals using a One-Dimensional Convolutional Neural Network (1D-CNN) architecture. The study utilized the ECG-ID dataset and compared classification performance based on two types of ECG signal segments: PQRS and PQRST waves. After a preprocessing stage involving IIR filtering and extracting 18 features from time-domain, cepstral, and morphological descriptors, the 1D-CNN model was evaluated for automatic individual identification. Experimental results indicated that the PQRST wave segment yielded the highest accuracy, reaching 91.57%. Although this accuracy does not yet meet the performance threshold of commercial systems, the study demonstrates the potential of 1D-CNN architectures in processing physiological signals for identification purposes. It underscores the importance of selecting representative signal segments to enhance the performance of ECG-based authentication systems [25].

In line with behavior- and signal-based approaches, a study highlighted the critical role of preprocessing in enhancing the performance of ECG-based identification systems. The study examined the impact of R-peak-based segmentation techniques on the performance of Support Vector Machine (SVM), Naive Bayes, and Random Forest classifiers. The results showed that Random Forest achieved the highest accuracy at 85%, representing an improvement of over 40% compared to previous segmentation methods. This research underscores that system effectiveness depends on the classification model and the preprocessing strategy, particularly under limited data conditions [26].

Furthermore, ensemble classification approaches have been implemented by proposing a combination of Support Vector Machine (SVM), Naive Bayes, and Random Forest for detecting five heartbeats using the MIT-BIH dataset. By employing the Residual Exemplars Local Binary Pattern feature extraction technique, the ensemble method demonstrated improved performance compared to individual classifiers, although overall accuracy remained below 94%. These findings reinforce the continued relevance of ensemble methods based on conventional models, particularly when optimized with appropriate statistical feature extraction techniques [27].

Based on the literature review and the potential offered by each approach, this study aims to compare the performance of several deep learning algorithms—namely, CNN, LSTM, CNN-LSTM, and DNN—in classifying multimodal biometric data. The primary focus is to evaluate the accuracy of each model architecture in recognizing user identities based on a combination of two biometric modalities: electrocardiogram (ECG) signals and fingerprint images. In addition to assessing model performance, this study also seeks to identify the most efficient and stable algorithm for handling multimodal characteristics, as well as to determine the most appropriate feature extraction techniques for each data type, such as grayscale conversion, binarization, edge detection, and minutiae extraction for fingerprint images, and signal normalization for ECG data. Specifically, this study aims to evaluate the performance of CNN, LSTM, CNN-LSTM, and DNN models in a multimodal biometric system that combines ECG and fingerprint features to achieve accurate and robust identity recognition.

Accordingly, this research is expected to contribute to developing biometric authentication systems that are more accurate, reliable, and adaptive to data variability, while also strengthening the foundation for selecting suitable model architectures and preprocessing techniques for implementing deep learning-based security systems.

2. METHOD

2.1. Dataset

This study utilizes two distinct types of biometric data: electrocardiogram (ECG) signals and fingerprint images. The process begins with collecting ECG data obtained from the ecg_id_raw_filtered subset of the ECG-ID dataset. This dataset has undergone a prior filtering process to remove noise that may interfere with signal quality using a bandpass filter [11] [28]. Each individual in the dataset has eight signal samples, which are divided into six samples for training and two for testing. A total of 7,491 features were extracted from the ECG data.

For fingerprint biometric data, this study employs the publicly available FVC2004 dataset, which contains a variety of fingerprint images from multiple individuals. Each image in the dataset represents a unique fingerprint pattern that serves as a visual biometric identifier. As shown in Table 2, the data is organized into four distinct databases (DB1 to DB4) as part of the data processing and validation stages. Each database includes ten individuals to ensure a balanced distribution. Furthermore, each database is divided into two subsets: DB Train, consisting of six samples per individual, and DB Test, consisting of two samples per individual. This structured division is designed to maintain an optimal balance between training and testing data while minimizing the risk of data leakage during the model validation process.

Table 1. Electrocardiogram Data

Person	ECG_TRAIN records	ECG_TEST records	Number of ECG Features
person_01	6	2	7.491
person_02	6	2	7.491
person_03	6	2	7.491
person_04	6	2	7.491
person_05	6	2	7.491
…	…	…	…
person_35	6	2	7.491
person_36	6	2	7.491
person_37	6	2	7.491
person_38	6	2	7.491
person_39	6	2	7.491
person_40	6	2	7.491

Table 2. Fingerprint Data

Database	Individual Range	Number of Individuals	Train Set (6 images/individual)	Test Set (2 images/individual)	Total Data per DB
DB1	person_01 - person_10	10	60	20	80
DB2	person_11 - person_20	10	60	20	80
DB3	person_21 - person_30	10	60	20	80
DB4	person_31 - person_40	10	60	20	80
Total	person_01 - person_40	40	240	80	320

Once both data types were collected and processed, they were integrated into a multimodal biometric system. The goal is to leverage the complementary strengths of each modality—temporal features from the ECG signals and spatial features from fingerprint images—to construct a more accurate and secure authentication system [12].

The summary of the data used in this study is presented in Table 1 for the ECG data and Table 2 for the fingerprint data. The visualizations of both ECG and fingerprint data are shown in Figure 1.

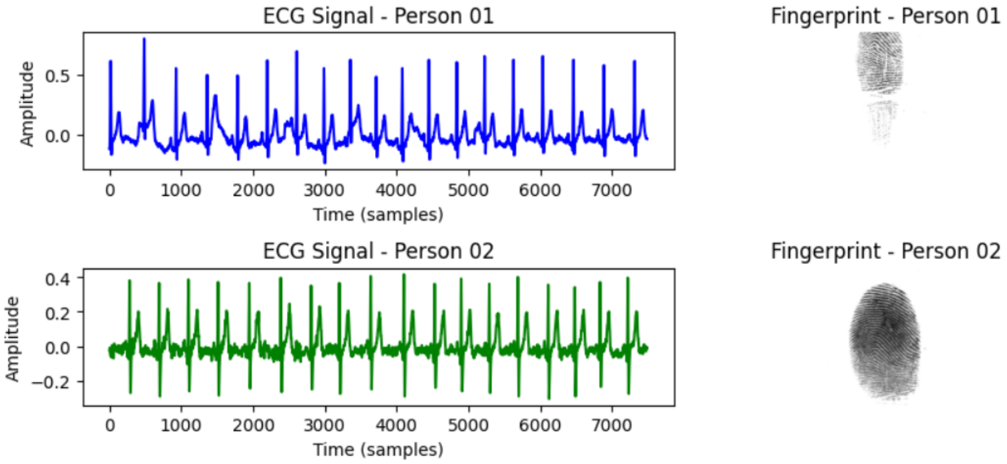

Figure 1. Example of ECG and Fingerprint Data

2.2. Method

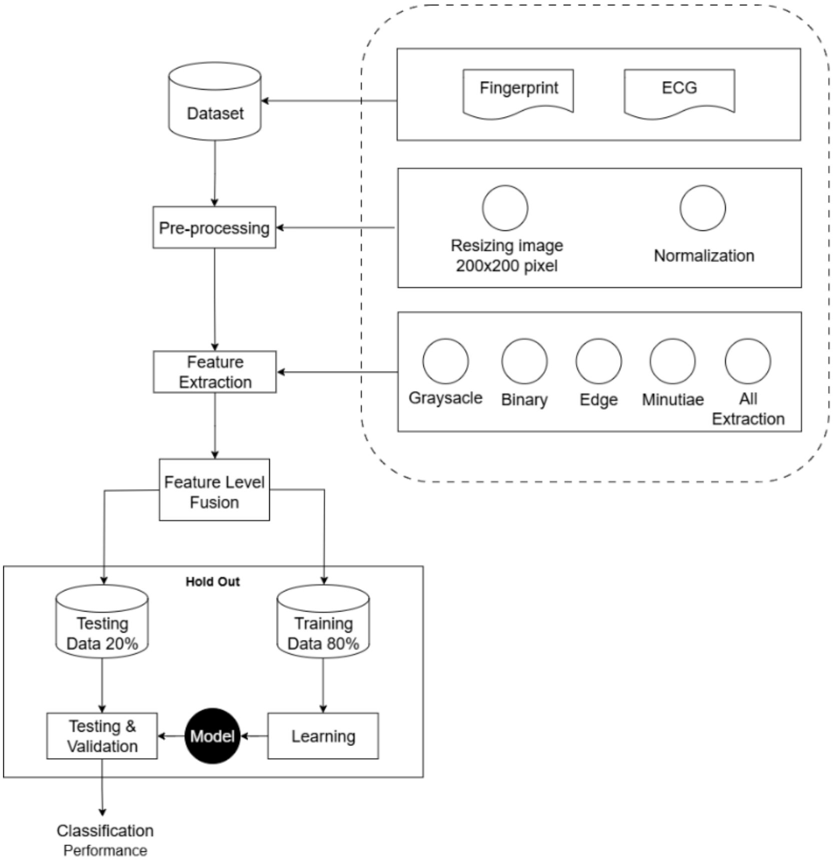

Figure 2.Research flow

The datasets and methods employed in this study were applied to extract features and perform classification within a multimodal biometric authentication system. The overall process flow is illustrated in Figure 2.

The preprocessing stage was conducted to prepare the data before feature extraction for fingerprint images and electrocardiogram (ECG) signals. Each fingerprint image was first converted to grayscale to simplify the visual information and reduce color dimensions without losing essential textural details. Then, all images were resized to 200×200 pixels to ensure dimensional consistency and proportional uniformity across samples, facilitating the model's learning process [29]. For ECG signals, normalization was performed using the StandardScaler method, which transforms values into a distribution with a mean of 0 and a standard deviation of 1 [30]:

$$z = \frac{x-\mu}{\sigma} \qquad (1)$$

Where x is the original value, μ the mean, and σ the standard deviation. This scaling harmonizes the feature ranges across both modalities and enhances the model's training stability and convergence [31].

In the next stage, fingerprint feature extraction was conducted using five primary methods: grayscale conversion, binarization, edge detection (Sobel), minutiae extraction, and feature aggregation. Minutiae points such as ridge endings and bifurcations were extracted using the Crossing Number (CN) algorithm [32]:

$$CN(p) = \frac{1}{2} + \sum_{i=1}^{8} |P(i) - P(i+1)| \qquad (2)$$

Where $P(i)$ denotes the binary value of the 8-neighborhood pixels around pixel p, with $P(9) = P(1)$. CN = 1 indicates a ridge ending; CN = 3 indicates a bifurcation [33].

For multimodal fusion, extracted features from both modalities were combined at the feature-level using concatenation:

$$F_{fused} = \left[F_{fingerprint} \parallel F_{ECG}\right] \qquad (3)$$

This fusion strategy preserves the richness of the individual modalities and enables a more discriminative representation for classification [34].

The evaluation process used classification accuracy as the primary performance metric, defined as:

$$Accuracy = \frac{TP+TN}{TP+ TN+FP+FN} \qquad (4)$$

Where:

- TP: True Positive
- TN: True Negative
- FP: False Positive
- FN: False Negative

Four deep learning models were employed for the classification task: Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), CNN-LSTM, and Deep Neural Network (DNN). Each model offers specific advantages. CNN is highly effective at extracting spatial features from biometric images such as fingerprints due to its ability to capture local patterns automatically [35].

LSTM, on the other hand, is designed for handling sequential data like ECG signals, owing to its capability to retain long-term contextual information [36]. The CNN-LSTM hybrid combines the strengths of both architectures, enabling the system to simultaneously process spatial features from images and temporal features from signals, making it particularly well-suited for multimodal data [37] [7]. DNN provides a flexible, multilayered architecture that handles complex, non-linear relationships in fused features from diverse sources [38]. Overall, CNN-based multimodal authentication systems have demonstrated superior performance compared to unimodal approaches, in terms of accuracy and robustness against data variability [39].

3. RESULT

Data preprocessing improved classification accuracy, particularly when applied with deep learning models. For fingerprint images, converting them to grayscale and resizing them to 200×200 pixels ensured uniformity and facilitated better understanding by the model. In the case of ECG signals, normalization using the StandardScaler helped balance the data values, enabling the model to recognize patterns more accurately without being affected by differences in scale.

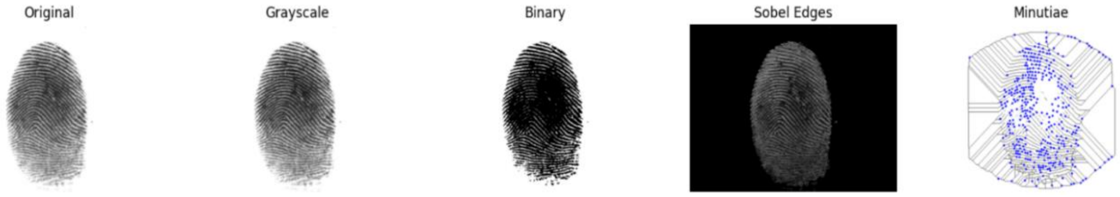

Figure 3. Figure of Feature Extraction Results

Figure 3 illustrates the results of each fingerprint image transformation step in the feature extraction process. The procedure begins with grayscale conversion, simplifying visual information by removing color dimensions while preserving essential ridge texture details. This is followed by binarization, which enhances the contrast between ridges and valleys, making the fingerprint patterns easier to segment. The application of the Sobel operator enables sharper and more accurate edge detection, clarifying the contours of ridge structures. Finally, minutiae points—such as ridge endings and bifurcations—are extracted, serving as unique and critical features for biometric identification [40]. Each stage significantly improves the quality of extracted features, thereby enhancing the classification performance of the multimodal biometric authentication system [7], [41].

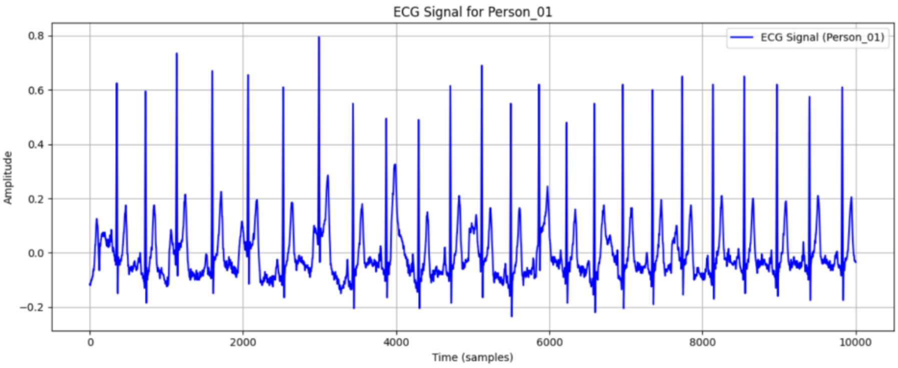

Figure 4. ECG Signal Before R-Peak Detection

Figure 4 illustrates the complete ECG signal before preprocessing, capturing the full waveform including relevant and non-relevant segments.

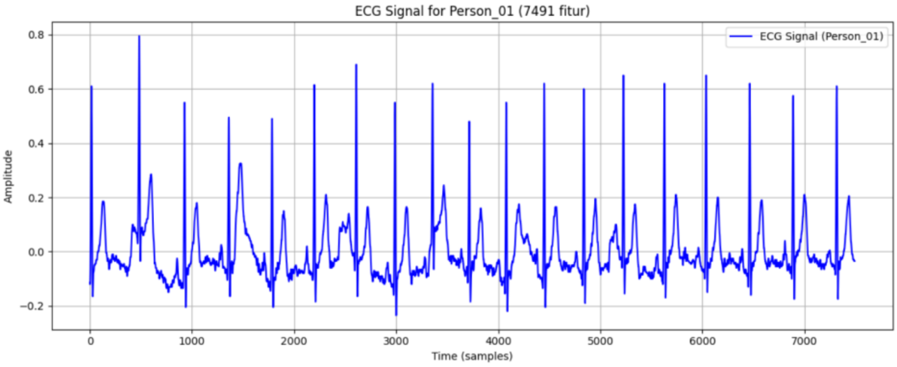

Figure 5. ECG Signal After R-Peak Detection

Figure 5 presents the trimmed ECG signal starting from the first detected R-peak point, which marks the beginning of the most informative cardiac cycle. A signal length trimming process was applied to the ECG data to ensure feature uniformity across samples. Initially, each signal contained 10,000 features; however, not all these segments were necessary for identity recognition. By cropping the signals based on R-peak detection—representing the primary peaks of the cardiac waveform—a more concise and relevant subset of 7,491 features was obtained. This reduction improved model learning efficiency and enhanced its ability to recognize user identity through ECG signals [42].

After extracting features from fingerprint images and ECG signals, the two feature sets were combined using a feature-level fusion method. This technique merges information from both data types into a single fused feature vector, which is then used as input to the deep learning models. Such fusion improves system accuracy, as features from one modality can compensate for limitations in the other. Additionally, the system becomes more stable and robust against noise or data variability disturbances.

Table 3. Classification Model Results

Extraction Feature	Number of Features	Machine Learning Algorithm	Accuracy (%)
Grayscale	40000	**CNN**	**83.75**
		LSTM	3.00
		CNN-LSTM	6.25
		DNN	2.50
Binary	40000	**CNN**	**80.00**
		LSTM	16.25
		CNN-LSTM	7.50
		DNN	2.50
Edge (Sobel Filter)	40000	**CNN**	**71.25**
		LSTM	22.50
		CNN-LSTM	11.25
		DNN	3.75
Minutiae	200	**CNN**	**96.25**
		LSTM	93.75
		CNN-LSTM	2.50
		DNN	93.75

Table 3 presents the classification accuracy results based on four fingerprint image feature types: grayscale, binary, edge (Sobel), and minutiae, using four deep learning architectures: CNN, LSTM, CNN-LSTM, and DNN. CNN consistently achieved the highest accuracy across all feature types.

The highest accuracy was obtained using minutiae features, reaching 96.25% with CNN, followed by LSTM and DNN at 93.75%. Grayscale and binary features also produced high accuracies of 83.75% and 80.00% with CNN, respectively. Meanwhile, the edge (Sobel) feature yielded lower performance, with a maximum accuracy of 71.25%. These results indicate that minutiae features are the most effective for fingerprint identification, and CNN is the most suitable architecture for visual feature classification.

4. DISCUSSIONS

After obtaining the classification results from each deep learning model, this stage aims to conduct further analysis of the performance of each model.

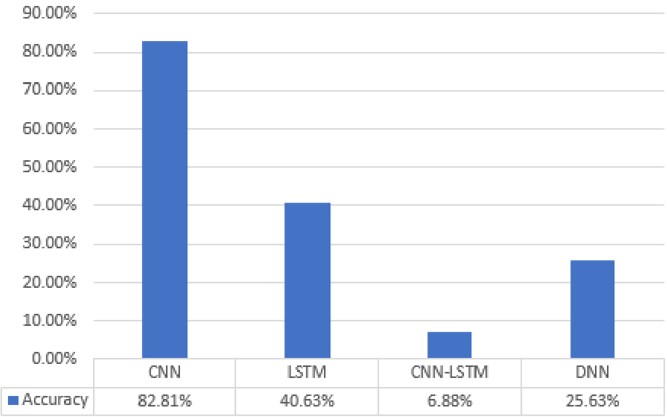

Figure 6. Average Model Results

As shown in Figure 6, the CNN model achieved the highest classification performance with an accuracy of 82.81%, demonstrating its strong capability in extracting and recognizing visual patterns from fingerprint image data. In contrast, the LSTM model recorded an accuracy of 40.63%, indicating that while it is effective for sequential data such as ECG signals, its performance declines when applied more generally to multimodal data. The DNN model yielded an accuracy of 25.63%, suggesting its limitations in optimally handling the diversity of features in multimodal data. Meanwhile, the CNN-LSTM hybrid model attained the lowest accuracy at 6.88%, indicating that this combined architecture was ineffective under the specific data configuration and feature extraction techniques used in this experiment. Overall, these results highlight the importance of selecting model architectures that are well-suited to the characteristics of the data to achieve optimal classification performance.

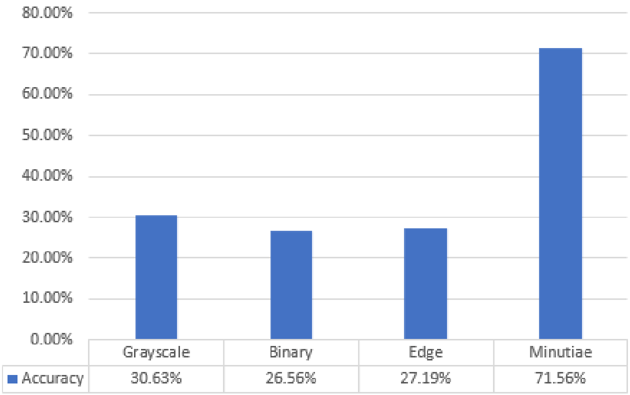

Figure 7. Average Feature Extraction Results

Figure 7 compares classification accuracies for each feature extraction method used in the biometric classification system. Among the four evaluated methods, minutiae-based features yielded the highest classification performance, achieving an accuracy of 71.56%. This result indicates that minutiae features are more effective in representing critical characteristics of fingerprint patterns. In contrast, the grayscale, binary, and edge-based methods recorded accuracies of 30.63%, 26.56%, and 27.19%, respectively. These relatively low performances suggest that the information derived from basic visual extraction techniques is not sufficiently robust to support optimal classification. These findings highlight the significant impact of feature extraction techniques on the quality of classification outcomes in fingerprint-based biometric systems.

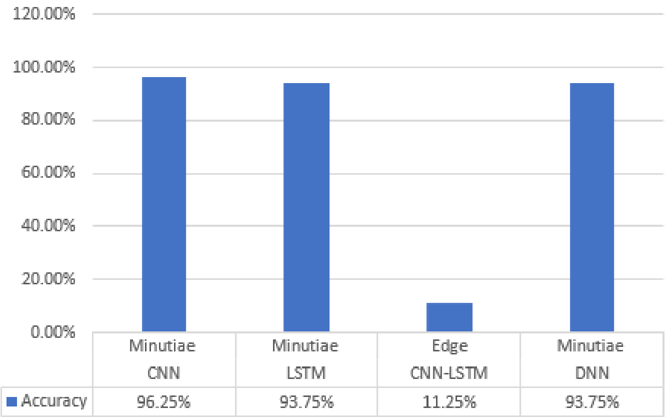

Figure 8. Best Performance of the Model

Figure 8 compares classification accuracies resulting from various combinations of deep learning models and feature extraction methods applied to biometric data. The results indicate that the combination of minutiae features and the CNN model achieved the highest accuracy at 96.25%, followed by the combinations of minutiae with LSTM and DNN models, each recording an accuracy of 93.75%. These findings suggest that minutiae features exhibit high stability and effectiveness in supporting the classification process, even when processed using different model architectures.

The CNN model proved particularly efficient in extracting spatial information from minutiae features, which reflect the unique structure of fingerprints, such as ridge endings and bifurcations. Likewise, the LSTM model demonstrated strong performance with minutiae features, indicating that this memory-based architecture can effectively capture sequential local patterns. In contrast, combining the CNN-LSTM model with edge-based features resulted in significantly lower accuracy, at only 11.25%, suggesting that edge features are less representative when used within such a hybrid architecture. Overall, these results emphasize the importance of selecting relevant and architecture-compatible features to enhance the performance of biometric classification systems.

We compared the proposed model's performance against several previous studies that utilized similar types of biometric data. As shown in Table 4, the proposed multimodal biometric system achieved an accuracy of 96.25%, demonstrating competitive performance compared to alternative approaches. While some unimodal methods, such as CNN with edge features on fingerprint data, achieved high validation accuracy (98.7%) but lower test accuracy (75.6%), and the GSDF method reached 96.56% on full fingerprint images, our proposed multimodal approach showed a more balanced performance and greater robustness to data variability. ECG-based models such as 1D-CNN (91.57%) and traditional ensemble approaches (85% to below 94%) generally performed less than our method. By integrating fingerprint and ECG data through feature-level fusion and deep learning models, our approach has proven effective in enhancing accuracy while reinforcing the reliability of the authentication system under various verification scenarios. Therefore, the multimodal approach remains relevant and promising for the development of reliable and adaptive biometric identification systems in the future.

Table 4. Comparison with Related Works

Ref	**Biometric**	**Method**	**Performance Accuracy (%)**
[23]	Fingerprint	GSDF (GSA + RF)	92.56 (Latent); 96.56 (Full)
[24]	Fingerprint	CNN + Edge Features	98.7 (Validation); 75.6 (Testing)
[25]	ECG	1D-CNN + PQRST Segment	91.57
[26]	ECG	R-Peak + Ensemble Classifier	85.00
[27]	ECG	Ensemble (SVM + NB + RF)	>94.00
Our Proposed Method	Fingerprint + ECG (Multimodal)	Feature Fusion + Ensemble Classifier	96.25

This study makes a scientific contribution to the field of informatics by designing an authentication architecture that combines feature-level fusion with ensemble classification based on deep learning, resulting in an adaptive and scalable authentication system. Unlike previous studies focused on unimodal optimization, this research bridges the integration of heterogeneous biometric signals and offers a practical approach for secure identity verification systems, particularly relevant for real-world applications such as e-government, smart healthcare, and cyber-physical systems. Furthermore, this study enriches the literature by presenting a replicable methodology emphasizing standardized preprocessing, feature harmonization, and model adaptability as foundational elements in developing AI-based biometric systems.

5. CONCLUSION

This study proposed a multimodal biometric authentication system by integrating two types of biometric data—fingerprint images and electrocardiogram (ECG) signals—using a feature-level fusion approach and multiple deep learning architectures. Evaluation results demonstrated that the CNN model, combined with minutiae features extracted from fingerprint images, achieved the highest classification accuracy of 96.25%, outperforming other models such as LSTM, DNN, and CNN-LSTM. These findings confirm that the choice of feature extraction techniques—particularly minutiae extraction—significantly impacts system accuracy.

Although several unimodal and ECG-based models in previous studies have reported competitive accuracy levels, the proposed system exhibits superior stability and robustness against data variability. Therefore, the multimodal approach is more reliable and adaptive in addressing biometric authentication challenges under diverse real-world conditions. Furthermore, this research contributes to selecting appropriate deep learning architectures and preprocessing strategies for future AI-driven digital security systems implementations.

Looking ahead, future research directions may focus on several strategic aspects. First, using more diverse datasets—considering acquisition devices, environmental conditions, and user demographics—can enhance model generalization. Second, exploring more advanced architectures such as Transformer networks or attention-based mechanisms holds promise for better handling spatial-temporal data patterns. Third, developing lightweight models optimized for resource-constrained environments like the Internet of Things (IoT) and edge computing platforms ensures deployment feasibility.

Furthermore, integrating multimodal biometric systems with two-factor authentication mechanisms can further strengthen security, with validation based on industry-standard benchmarks such as ROC curves, Equal Error Rate (EER), and compliance with FIDO2 protocols. Finally, evaluating the system in low-resource environments is essential to ensure its practical applicability in real-time and embedded systems. The proposed multimodal biometric authentication system is expected to meet the performance, efficiency, and security standards necessary for real-world deployment across public and industrial domains through these extended approaches.

REFERENCES

[1] A.-R. Despa, "Overcoming Obstacles: A Closer Look at the Most Pressing Challenges in Cybersecurity," *International Journal of Information Security and Cybercrime*, p., 2023, doi: 10.19107/ijisc.2023.02.04.

[2] Sushil Mahato, Ranjit Sah, and Sushil Sapkota, "Cybersecurity Challenges and Threats: The Risks in Digital World," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 651–655, Nov. 2024, doi: 10.48175/IJARSCT-22497.

[3] N. A. Mirjat, "AI and Machine Learning: Transforming the Landscape of Cybersecurity," *Bulletin of Engineering Science and Technology*, vol. 1, pp. 40–59, 2024, [Online]. Available: https://consensus.app/papers/ai-and-machine-learning-transforming-the-landscape-of-mirjat/449c39cd69905a149652e029a3b4e067/

[4] S. Pandey, "Cybersecurity Trends and Challenges," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 07, no. 08, Aug. 2023, doi: 10.55041/ijsrem25323.

[5] A. Dinesh, C. D. P. Reddy, G. Gopi, R. Jain, and T. Shankar, "A Durable Biometric Authentication Scheme via Blockchain," *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, pp. 1–5, 2021, doi: 10.1109/ICAECT49130.2021.9392415.

[6] A. Sindar, A. S. Sinaga, A. S. Sitio, and S. Dewi, "IDENTIFICATION OF BIOMETRIC DEEPFAKES USING FEATURE LEARNING DEEP LEARNING," vol. 3, no. 4, 2022, doi: 10.20884/1.jutif.2022.3.4.461.

[7] A. Kailas and G. N. Keshava Murthy, "Deep learning based biometric authentication using electrocardiogram and iris," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 1, pp. 1090–1103, Mar. 2024, doi: 10.11591/ijai.v13.i1.pp1090-1103.

[8] R. Kumar, "Biometrics and Password Less Authentication: The Future of Digital Security," *International Journal of Innovative Science and Research Technology (IJISRT)*, p., 2024, doi: 10.38124/ijisrt/ijisrt24jul541.

[9] M. I. M. Yusop, N. H. Kamarudin, N. H. S. Suhaimi, and M. K. Hasan, "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity," *IEEE Access*, vol. 13, pp. 13919–13943, 2025, doi: 10.1109/ACCESS.2025.3528960.

[10] T. Oduguwa and A. Arabo, "Passwordless Authentication Using a Combination of Cryptography, Steganography, and Biometrics," *Journal of Cybersecurity and Privacy*, vol. 4, no. 2, pp. 278–297, Jun. 2024, doi: 10.3390/jcp4020014.

[11] A. Jackson *et al.*, "Biometric Authentication for the Mitigation of Human Risk on a Social Network," in *Human Factors in Cybersecurity*, AHFE International, 2024. doi: 10.54941/ahfe1004763.

[12] N. D. Miranda, L. Novamizanti, and S. Rizal, “CONVOLUTIONAL NEURAL NETWORK PADA KLASIFIKASI SIDIK JARI MENGGUNAKAN RESNET-50,” *Jurnal Teknik Informatika (Jutif)*, vol. 1, no. 2, pp. 61–68, Dec. 2020, doi: 10.20884/1.jutif.2020.1.2.18.

[13] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, "A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and

Template Protection," *IEEE Access*, vol. 12, pp. 64300–64334, 2024, doi: 10.1109/ACCESS.2024.3395417.

[14] Diptadip Maiti and Madhuchhanda Basak, "Multimodal biometric integration: Trends and insights from the past quinquennial," *World Journal of Advanced Research and Reviews*, vol. 23, no. 3, pp. 1590–1605, Sep. 2024, doi: 10.30574/wjarr.2024.23.3.2741.

[15] Lakshmi Narayana Gupta Koralla, "Biometric data and behavior analysis," *World Journal of Advanced Research and Reviews*, vol. 26, no. 1, pp. 339–350, Apr. 2025, doi: 10.30574/wjarr.2025.26.1.1084.

[16] C. Yuan, S. Jiao, X. Sun, and Q. Wu, "MFFFLD: A Multimodal-Feature-Fusion-Based Fingerprint Liveness Detection," *IEEE Trans Cogn Dev Syst*, vol. 14, pp. 648–661, 2021, doi: 10.1109/TCDS.2021.3062624.

[17] M. H. Safavipour, M. A. Doostari, and H. Sadjedi, "A hybrid approach to multimodal biometric recognition based on feature-level fusion of face, two irises, and both thumbprints," *J Med Signals Sens*, vol. 12, no. 3, pp. 177–191, Jul. 2022, doi: 10.4103/jmss.jmss_103_21.

[18] Y. Wang, D. Shi, and W. Zhou, "Convolutional Neural Network Approach Based on Multimodal Biometric System with Fusion of Face and Finger Vein Features," *Sensors*, vol. 22, no. 16, Aug. 2022, doi: 10.3390/s22166039.

[19] W. Yang, S. Wang, J. Hu, X. Tao, and Y. Li, "Feature extraction and learning approaches for cancellable biometrics: A survey," Feb. 01, 2024, *John Wiley and Sons Inc*. doi: 10.1049/cit2.12283.

[20] H. Mehraj and A. Mir, "Robust Multimodal Biometric System Based on Feature Level Fusion of Optimiseddeepnet Features," *Wirel Pers Commun*, vol. 127, pp. 2461–2482, 2021, doi: 10.1007/s11277-021-09075-x.

[21] A. Hussian, F. Murshed, M. N. Al-Andoli, and G. Aljafari, "A Hybrid Deep Learning Approach for Secure Biometric Authentication Using Fingerprint Data," *Computers*, p., 2025, doi: 10.3390/computers14050178.

[22] H. Bendjenna, Y. Belhocine, A. Khemane, and A. Meraoumia, "Beyond Traditional Methods: Feature Fusion for Robust Biometric Identification," *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pp. 1–8, 2024, doi: 10.1109/PAIS62114.2024.10541249.

[23] M. Kumar and D. Kumar, "An efficient gravitational search decision forest approach for fingerprint recognition."

[24] D. L. Andreea-Monica, S. Moldovanu, and L. Moraru, "A Fingerprint Matching Algorithm Using the Combination of Edge Features and Convolution Neural Networks," *Inventions*, vol. 7, no. 2, Jun. 2022, doi: 10.3390/inventions7020039.

[25] F. Taliningsih *et al.*, "Biometric Verification Based on ECG Signal using 1 Dimensional Convolutional Neural Network," *2022 1st International Conference on Information System & Information Technology (ICISIT)*, pp. 204–209, 2022, doi: 10.1109/ICISIT54091.2022.9872891.

[26] D. Nugrahadi, M. Faisal, R. Herteno, I. Budiman, F. Abadi, and I. Sutedja, "An Effective Preprocessing Data on Performance of Machine Learning for ECG-Based Personal Authentication," *Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology*, p., 2023, doi: 10.1145/3626641.3626943.

[27] M. Ramkumar, M. Alagarsamy, A. Balakumar, and S. Pradeep, "Ensemble classifier fostered detection of arrhythmia using ECG data," *Med Biol Eng Comput*, vol. 61, pp. 2453–2466, 2023, doi: 10.1007/s11517-023-02839-6.

[28] M. Irhamsyah, M. Melinda, J. Alifa, J. Prayoga, and Y. Iskandar, "ECG Atrial Fibrillation Signal Classification Method Based on Discrete Wavelet Transform (DWT) and DenseNet-121," *2024 10th International Conference on Smart Computing and Communication (ICSCC)*, pp. 619–624, 2024, doi: 10.1109/ICSCC62041.2024.10690792.

[29] M. Hirsi Mohamed, "Fingerprint Classification Using Deep Convolutional Neural Network," *Journal of Electrical and Electronic Engineering*, vol. 9, no. 5, p. 147, 2021, doi: 10.11648/j.jeee.20210905.11.

[30] S. Khan *et al.*, "A Deep Learning Framework for the Classification of ECG Signals," in *2022 International Conference on Engineering and Emerging Technologies (ICEET)*, 2022, pp. 1–5. doi: 10.1109/ICEET56468.2022.10007143.

[31] N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal Approach for Enhancing Biometric Authentication," *J Imaging*, vol. 9, no. 9, Sep. 2023, doi: 10.3390/jimaging9090168.

[32] J. Mabe Parenreng *et al.*, "INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION journal homepage : www.joiv.org/index.php/joiv INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION Solution for Public Smart Dispenser Using Digital Payment Based on the Fingerprint Minutiae Algorithm." [Online]. Available: www.joiv.org/index.php/joiv

[33] B. H. Situmorang, “Identification of Biometrics Using Fingerprint Minutiae Extraction Based on Crossing Number Method,” *Komputasi: Jurnal Ilmiah Ilmu Komputer dan Matematika*, vol. 20, no. 1, pp. 71–80, Dec. 2022, doi: 10.33751/komputasi.v20i1.6814.

[34] U. Sumalatha, K. Prakasha, S. Prabhu, and V. C. Nayak, "Multimodal biometric authentication: a novel deep learning framework integrating ECG, fingerprint, and finger knuckle print for high-security applications," *Engineering Research Express*, vol. 7, no. 1, Mar. 2025, doi: 10.1088/2631-8695/ad9aa0.

[35] P. Nahar, N. Chaudhari, and S. Tanwani, "Fingerprint classification system using CNN," *Multimed Tools Appl*, vol. 81, pp. 24515–24527, 2022, doi: 10.1007/s11042-022-12294-4.

[36] H. Zacarias, J. A. L. Marques, V. Felizardo, M. Pourvahab, and N. M. Garcia, "ECG Forecasting System Based on Long Short-Term Memory," *Bioengineering*, vol. 11, no. 1, Jan. 2024, doi: 10.3390/bioengineering11010089.

[37] S. Mageshbabu and J. Mohana, "Enhanced ECG-Based Biometric Authentication using a Hybrid CNN-LSTM Framework," *2024 First International Conference on Software, Systems and Information Technology (SSITCON)*, pp. 1–7, 2024, doi: 10.1109/SSITCON62437.2024.10796214.

[38] S. Son and K. Oh, "Integrated framework for estimating remaining useful lifetime through a deep neural network," *Appl. Soft Comput.*, vol. 122, p. 108879, 2022, doi: 10.1016/j.asoc.2022.108879.

[39] S. A. El-Rahman and A. S. Alluhaidan, "Enhanced multimodal biometric recognition systems based on deep learning and traditional methods in smart environments," *PLoS One*, vol. 19, no. 2 February, Feb. 2024, doi: 10.1371/journal.pone.0291084.

[40] N. V Keerthana and M. Parimala Devi, "A Comprehensive Analysis of Minutiae Point Extraction in Biometric FingerPrint," in *2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2024, pp. 319–322. doi: 10.1109/SMART63812.2024.10882188.

[41] Q. Huang, "Multimodal Biometrics Fusion Algorithm Using Deep Reinforcement Learning," *Math Probl Eng*, vol. 2022, 2022, doi: 10.1155/2022/8544591.

[42] H. Zehir, T. Hafs, and S. Daas, "Healthcare Decision-Making with an ECG-Based Biometric System," *2023 International Conference on Decision Aid Sciences and Applications (DASA)*, pp. 88–92, 2023, doi: 10.1109/DASA59624.2023.10286620.