Vol.3, No.5, Page 1145- 1154, 2025 https://doi.org/10.59628/jast.v3i5.1831 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

Deep Convolutional Neural Networks for Fingerprint Classification

Ghaleb H.Aljafary * and Abdulrahman Hussian

Department of Computer Science, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen

*Corresponding author: Abdulrahmancs.is@gmail.com

Abstract

Fingerprint recognition has widespread security applications owing to its uniqueness, permanence, and simplicity in capture. However, conventional fingerprint authentication systems face high false acceptance and rejection rates and susceptibility to spoofing attacks. To address these issues, this study proposes a deep learning-based fingerprint authentication system using a Convolutional Neural Network (CNN) with five convolution layers to derive robust spatial features. The model was trained and cross-validated on the SOCOFing dataset with regularization and data augmentation to enhance generalization and spoof resistance. Experimental results show that the proposed CNN achieved a training accuracy of 99.10% with a loss of 0.0223 and a validation accuracy of 98.89% with a loss of 0.0114. Moreover, the model maintained a low false acceptance rate of 0.33% and false rejection rate of 0.25%, demonstrating its efficacy and credibility for secure and real-time biometric authentication. A rigorous comparison with conventional CNN models and DCCN architectures confirmed that the proposed model provides higher accuracy, lower computational cost, and stronger resistance to spoofing attacks. These findings indicate that the proposed system successfully addresses existing limitations and offers a practical, scalable, and reliable solution for fingerprint verification using deep CNN architectures.

Article Info

Keywords:
Deep learning, CNN, fingerprint recognition, biometric authentication, security, feature extraction.

Article History:
Received: 20-May-2025,
Revised: 23-June-2025,
Accepted: 28-July-2025,
Available online: 28 October 2025.

1. INTRODUCTION

Fingerprint recognition is a widely used biometric modality due to its uniqueness, permanence, and ease of capture, finding applications in law enforcement, banking, healthcare, and border protection because of its accuracy and low cost. However, traditional systems face challenges such as spoofing attacks, false acceptance/rejection rates, and limited scalability on large heterogeneous databases, which reduce reliability in high-security applications [1]. Recent advances in deep learning, particularly Convolutional Neural Networks (CNNs), have significantly improved biometric authentication. CNNs automatically extract complex spatial features from fingerprint images, offering superior adaptability and robustness compared to traditional methods relying on handcrafted features [2–4].Previous studies using shallow networks reported moderate success: Radzi et al. (2024) applied LeNet-5 achieving 95.8% accuracy, Fairuz et al. (2023) used AlexNet with transfer learning for 95.2%, and Das et al. (2023) developed a three-layer CNN reaching 96%. Some approaches combined CNNs with LSTMs, but this increased model complexity and inference time.

This study proposes a five-layer CNN for fingerprint verification that balances depth, accuracy, and computational efficiency [5]. Trained on large heterogeneous datasets with data augmentation and regularization, the model achieved high classification accuracy, low error rates, and strong spoof resistance. Unlike shallow or hybrid networks with high computational costs, the proposed architecture efficiently extracts discriminative hierarchical features, enhancing generalization across diverse samples.

Key contributions include:

1. a deep CNN architecture with strong feature extraction.

2. comprehensive performance evaluation using ac-

curacy, FAR, FRR, and F1-score.

3. testing under varied data and spoofing conditions.

4. comparison with state-of-the-art methods, demonstrating superior reliability and efficiency.

This approach provides a scalable and practical solution for real-time fingerprint authentication.

2. RELATE WORK

Fingerprint recognition is a widely used biometric modality due to its ease of use, low cost, and high accuracy. However, traditional matching algorithms face challenges such as spoofing, poor image quality, and limited scalability in real-world applications [1, 2]. To overcome these limitations, deep learning, particularly CNNs, has been increasingly adopted for automatic learning of robust spatial features from large-scale data, improving both accuracy and anti-spoofing performance [3, 4].

Early studies using shallow CNNs showed promising results; for instance, Radzi et al. (2024) applied LeNet-5 achieving 95.8% accuracy, Das et al. (2023) developed a five-layer CNN reaching 96%, and Fairuz et al. (2023) used AlexNet with transfer learning for 95.2% accuracy [6, 7]. Despite their effectiveness, these models were limited in scalability and robustness.

Advanced CNN architectures have been introduced to enhance security. Zhao et al. (2024) proposed a multi-scale CNN capturing both fine and coarse fingerprint features, while other studies demonstrated strong spoof detection capabilities [8, 9]. Our study bridges the gap between shallow and deep networks by proposing a five-layer CNN that improves feature extraction, spoofing resilience, and overfitting mitigation. With preprocessing, data augmentation, and regularization, the model generalizes well across diverse inputs [10, 11]. Unlike computationally intensive ensemble methods, our CNN balances efficiency and accuracy, achieving 99.10% accuracy with a 2.65-second inference time [7, 12, 13].

Deep CNNs are also being integrated with IoT applications to enable real-time biometric security in healthcare and identification systems [14]. Overall, adopting deep CNNs with advanced preprocessing and regularization is crucial for secure, scalable, and real-time fingerprint authentication, offering superior robustness, hierarchical feature representation, and applicability in practical scenarios. Table 1 summarizes key differences between shallow and deep CNNs in depth, feature representation, robustness, and real-time suitability.

3. METHODOLOGY AND MATERIALS

To enhance fingerprint authentication security, this study uses deep CNNs for feature extraction and classification. Preprocessing involves resizing images to 96 × 96 pixels, normalizing pixel values, and applying data augmentation.

Table 1. Comparison Between Traditional CNN and Proposed Deep CNN (DCNN)

Feature	Traditional (CNNs)	Deep (CNNs)
Network Depth	2–3 layers, limited feature extraction	5+ layers, up to 200, enabling deeper features
Feature Representation	Low-level features like edges and textures	Multi-level hierarchical features for better discrimination
Robustness& Security	Prone to overfitting, less robust	More robust via depth, augmentation, regularization
Recognition Accuracy	Moderate accuracy	Superior accuracy, fewer errors
Real-Time Suitability	Lower complexity but limited security	Balanced depth and efficiency for real-time use

including rotation, flipping, and contrast adjustment, improving robustness, generalization, and resistance to spoofing.

The CNN captures abstract spatial features, such as ridge patterns and texture variations, essential for distinguishing real from fake fingerprints. Training employed the Adam optimizer with categorical cross-entropy loss for effective convergence. To prevent overfitting, learning rate scheduling and early stopping were used, with an 80–20 train-validation split.

Model performance was evaluated using accuracy, precision, recall, F1-score, and ROC curves. The proposed CNN achieved 99.10% accuracy, demonstrating high reliability, strong anti-spoofing capability, and cost-effective secure fingerprint verification suitable for real-world biometric applications.

3.1. System Workflow

The fingerprint images were first preprocessed by resizing them to 96 × 96 pixels to meet the input requirements of the proposed CNN model (Figure 1). The dataset served as the foundation for training and testing.

3.2. Preprocessing

Raw fingerprint images undergo several preprocessing steps before training and testing to enhance security and stability in recognition. Initially, all images are resized to a standard 96 × 96 pixels to introduce homogeneity, enabling the deep CNN to learn discriminative features crucial for secure identification. Pixel values are normalized to the 0–1 range, stabilizing training, improving convergence, and reducing sensitivity to variations in lighting or sensor noise that could compromise spoofing resistance.

The dataset is split into training, validation, and testing sets, allowing the model to be trained on one subset while

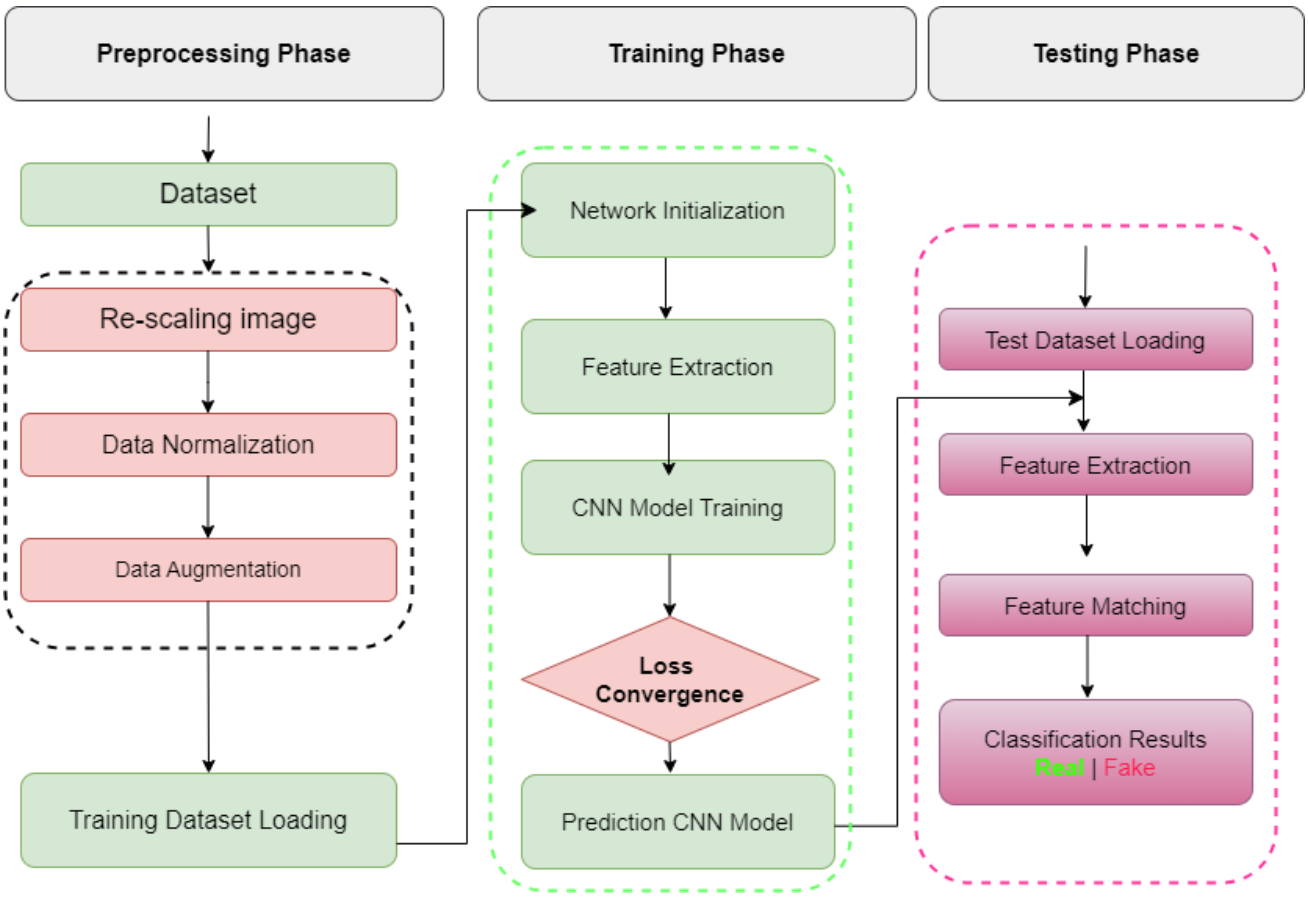

Figure 1. CNN Model Workflow

rigorously evaluating generalization on unseen samples, essential for real-world deployment. After training, performance is assessed using standard evaluation metrics to ensure reliability and robustness. The trained CNN model is then used to predict new fingerprint inputs. Optimization algorithms and hyperparameter tuning further enhance performance and prevent overfitting.

This CNN-based approach provides strong generalization, high precision, and enhanced security, making it suitable for practical fingerprint verification applications.

3.3. Architecture of the Proposed Network

The proposed deep CNN for fingerprint verification uses five convolutional layers with ReLU, batch normalization, max-pooling, and dropout to learn complex features while preventing overfitting and enhancing robustness against spoofing.

Feature learning occurs hierarchically:

- The first layer captures basic textures and edges.
- The second extracts corners and fine patterns.
- The third identifies higher-level fingerprint structures.
- The fourth refines these features and models local.
- The fifth combines abstract representations for robust classification.

The final convolutional output is flattened and passed through dense layers, producing a softmax classification (real or fake). Training uses the Adam optimizer with categorical cross-entropy loss, early stopping, and learning rate scheduling to ensure convergence. This design, grounded in established image recognition principles, delivers secure and reliable fingerprint authentication through strong, hard-to-replicate feature extraction.

3.4. Optimization and Training Details

To ensure high accuracy and robust security, the proposed fingerprint authentication system uses a deep CNN optimized with effective techniques. All convolutional layers employ ReLU activation to capture complex, discriminative features for distinguishing real from spoofed fingerprints. Weights are initialized using He uniform initialization for faster and stable convergence, while the final dense layer uses softmax for binary classification. The model is trained with the Adam optimizer (learning rate 1×10^{-4}) minimizing categorical cross-entropy. Early stopping and adaptive learning rate decay prevent overfitting and improve generalization. These strategies collectively enhance the model's security, reliability, and efficiency in fingerprint verification.

3.5. Proposed Deep Convolutional Neural Network Approach

The proposed approach employs deep CNNs to classify fingerprints as genuine or forged, enhancing authentication security. Convolutional layers extract spatial information stage by stage, capturing low-level edge and texture patterns as well as high-level abstract features necessary for accurate identification. Each convolutional layer is followed by max-pooling and dropout operations, which strengthen feature representations and reduce overfitting, allowing the model to generalize effectively to unseen fingerprints. This framework enables the CNN to learn discriminative, hierarchical, and robust representations resilient to noise, distortions, and spoofing attacks. By leveraging selective deep convolutional computation, the model accurately detects subtle differences between real and fake fingerprints, ensuring precise classification and strong security performance even under challenging verification conditions.

3.6. Architectural Components of the Proposed Model

To enhance the security and robustness of fingerprint authentication, the proposed architecture was integrated with a set of specially developed preprocessing and deep learning modules to enable effective feature extraction and classification.

The fingerprint image was first normalized by normalizing the pixel values in the range [0, 1] to generate a consistent intensity across samples. The image was resized to 96 × 96 pixels to obtain a fixed input size suitable for convolutional processing. The grayscale image is then binarized to minimize texture information and enhance the contrast of ridge patterns, which are crucial for recognition. Although thinning is not applied explicitly, the data are enriched by applying transformations, such as rotation, translation, zooming, and horizontal flip.

3.7. Feature extraction via CNN

The preprocessed fingerprint image is then input into a deep CNN for feature extraction and classification. Convolutions employ learnable kernels to derive hierarchical spatial features including ridge endings, bifurcations, and unique fingerprint textures. Max-pooling layers are employed to reduce the spatial resolution of the feature maps so that only the most salient information is preserved without affecting the computation efficiency. Dropout regularization was employed during training to prevent overfitting. The final output from the CNN layers is converted into a feature sequence, which may be processed or classified according to the structure adopted. These deep features are essential for secure and discriminative fingerprint representations, which are more robust against spoofing and forgery. The extracted features are passed through deeper layers of the CNN to learn complex spatial patterns such that the system can securely and accurately distinguish between real and spoofed fingerprints (Figure 2)

Loss Function Optimization: For enhanced secure and accurate fingerprint categorization, the model uses categorical cross-entropy as the optimization loss to be minimized by the Adam optimizer, which learns dynamically to adapt the learning rate to achieve faster convergence and greater robustness.

Model Tuning: The CNN model was trained for over 50 epochs with batch size of 32 and a validation split of 0.2. To further prevent overfitting and reliable performance on varying fingerprint inputs , early stopping and learning rate reduction strategies were employed (see Figure 3).

4. EXPERIMENTAL RESULTS AND MODEL EVALUATION OF THE PROPOSED MODEL

4.1. Datasets

Figure 4 shows the training and testing of the proposed method on the SOCOFing dataset [15], containing 6,000 fingerprint images from 600 African subjects, with 10 fingerprints per subject. Metadata includes gender, hand, and finger names. To simulate real-world spoofing, images were manipulated using the STRANGE toolbox with obliteration, central rotation (15°–180°), and Z-cut. The dataset comprises three difficulty levels—easy, medium, and hard—totaling 55,273 images. Fingerprints were scanned using Hamster Plus and SecuGen devices at 500 dpi and stored in 96 × 103 grayscale pixels. Filenames encode metadata for detailed analysis. The dataset is publicly available on Kaggle under the Creative Commons license (CC BY-NC-SA 4.0) [15]. Dense annotations and diverse manipulations support robust training and evaluation, replicating realistic scenarios to ensure model reliability and generalization in fingerprint verification tasks.

4.2. Experimental Setup and Hyperparameter Configuration

The experimental setup focused on improving security and reliability in fingerprint verification using a deep CNN. Grayscale images were resized to 96 × 96 pixels and preprocessed via scaling and normalization. Data were processed in mini-batches of 32 to optimize computational efficiency and memory usage. The dataset was split 80% for training and 20% for testing, with unseen test data ensuring unbiased evaluation, complemented by 5-fold cross-validation for stable performance assessment.

The CNN consisted of five convolutional layers with

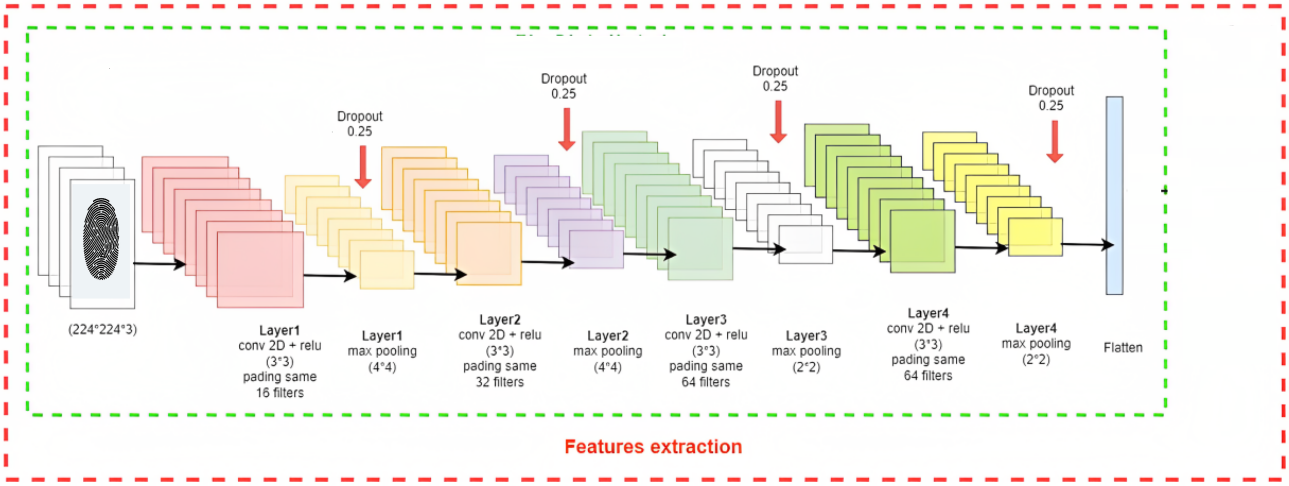

Figure 2. Fingerprint Recognition System Based on Feature Extraction Techniques

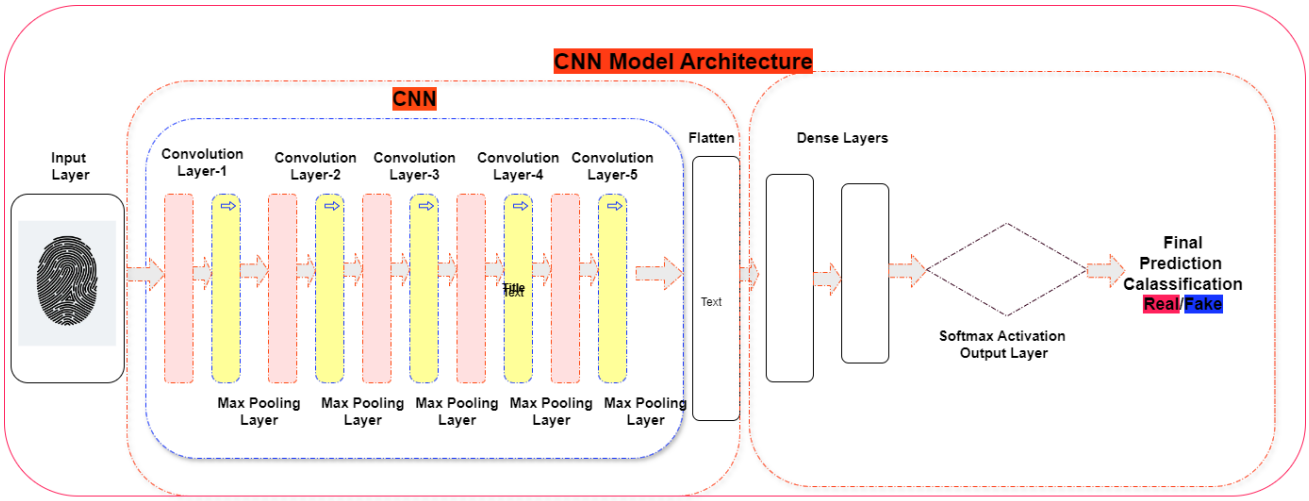

Figure 3. Architecture of the Proposed Model

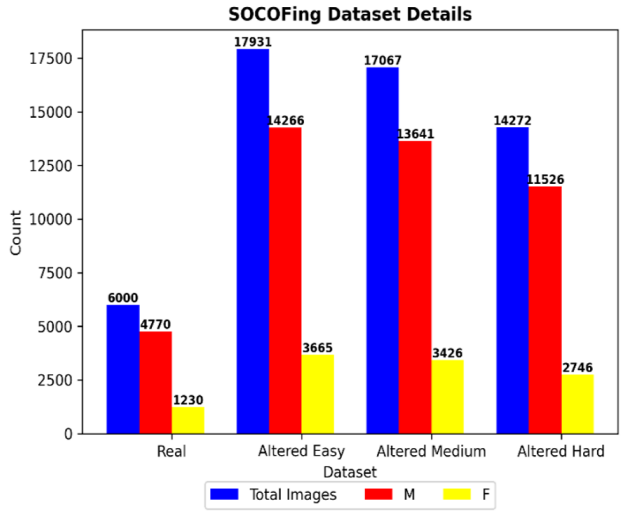

Figure 4. Details of Sokoto dataset.

64–512 filters, each followed by 2 × 2 max-pooling and dropout to prevent overfitting. ReLU activation and L2 regularization (λ = 0.01) were applied throughout. A fully connected layer with 128 ReLU units preceded a softmax output for binary classification (real or fake). The model trained for 50 epochs using Adam (learning rate 1×10^{-4}) and categorical cross-entropy loss, with early stopping (15-epoch patience) and learning rate reduction enhancing generalization.

Training was performed on the CONFIG dataset and tested on a separate unseen dataset to validate security, robustness, and generalization. Detailed layer-wise architecture and parameters are presented in Table 2.

4.3. Hardware and Computational Requirements

The model was deployed and tested on a Dell Precision 3550 laptop with a 15.6" Full HD display, Intel Core i7-13310U CPU, 32 GB RAM, and 512 GB SSD running Windows 11 Pro. Training required about 12 GB of memory, while inference used less than 2 GB, with an average processing time of 2.65 seconds per sample. These results indicate the model is computationally

Table 2. Detailed vertical configuration of the proposed DCNN model.

Layer	Type	Filters / Units	Filter Size	Activation Function	Pooling	Dropout
Input	—	—	96×96 (grayscale image)	—	—	—
Conv1	Conv	64 filters	3×3	ReLU	2×2 Max Pooling	Yes
Conv2	Conv	128 filters	3×3	ReLU	2×2 Max Pooling	Yes
Conv3	Conv	256 filters	3×3	ReLU	2×2 Max Pooling	Yes
Conv4	Conv	384 filters	3×3	ReLU	2×2 Max Pooling	Yes
Conv5	Conv	512 filters	3×3	ReLU	2×2 Max Pooling	Yes
FC	Fully Connected	128 units	—	ReLU	—	—
Output	Softmax	2classes	—	—	—	—

efficient and can run effectively without hardware acceleration, making it suitable for deployment on low-resource or portable security systems. Minor optimizations could enable operation in highly constrained environments.

4.4. Performance Evaluation Metrics

To analyze the performance of the proposed deep CNN-based fingerprint classification model extensively, several common evaluation metrics were used. These metrics provide numerical values of the accuracy, reliability, and ability of the model to differentiate between genuine and fake fingerprints, which is useful for trustworthy biometric security authentication systems.

- **Accuracy**: is the combined proportion of fingerprints identified correctly and is computed as:

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

Where:

- ***TP:*** True Positives number of positive samples correctly classified
- ***TN:*** True Negatives number of negative samples correctly classified
- ***FP:*** False Positives number of negative samples incorrectly classified as positive
- ***FN:*** False Negatives number of positive samples incorrectly classified as negative

- **Precision:** Is the number of fingerprints predicted to be real that actually were real:

$$\text{Precision} = \frac{TP}{(TP + FP)}$$

- **Recall:** Is the ability of the model to correctly identify real fingerprints:

$$\text{Recall} = \frac{TP}{(TP + FN)}$$

- **F1-Score:** Is a combination of Precision and Recall into a single metric to balance their trade-offs:

$$\text{F1-Score} = \frac{2 \times (Precision \times Recall)}{(Precision + Recall)}$$

- **Binary Cross-Entropy Loss:** Is used to compute the difference between the predicted probability and actual binary label. It is defined as:

Loss = - [y log(ŷ) + (1 - y) log(1 - ŷ)]
Where:

- ***y*** represents the true class label
- ***y=1*** means the sample is genuine
- ***y=0*** means it is fake.
- ***ŷ*** represents the predicted probability output by the model that the sample belongs to the genuine class (a value between 0 and 1).
- **log:** The natural logarithm function used to calculate the log-likelihood.

4.5. Experimental Results

Detailed experiments using a deep CNN evaluated the effectiveness of the proposed fingerprint authentication method. Training and validation accuracy and loss are summarized in Table 3, while 4 presents precision, recall, and F1-score metrics, Table 5 compares classification accuracy with recent studies. and and compares computational complexity and execution times, highlighting the proposed model's efficiency. Figures 5–10 illustrate training and validation trends, precision, recall, and ROC curves, demonstrating robust performance.

Table 3. Model Accuracy, Loss Trends, and Performance Scores for Fingerprint Recognition.

Phase	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Loss Value
Training	99.10	99	99.1	99.1	0.0223
Validation	98.89	99	100	100	0.0114

The CNN achieved 99.10% training accuracy and 98.89% validation accuracy on the Config dataset, with

loss values of 0.0223 and 0.0114. Precision, recall, and F1-scores were all near 99%, confirming the model's strong ability to accurately distinguish real from spoofed fingerprints. These results demonstrate high classification performance, enhanced security robustness, and the reliability of the proposed CNN for secure and effective fingerprint verification in practical applications.

Table 4. Classification Performance Report for Fingerprint Recognition System

Class	Precision (%)	Recall (%)	F1-Score (%)	Support
Real	99.0	100.0	99.0	2814
Fake	100.0	99.0	99.0	2895
Accuracy		99.10		5709
Macro avg	99.5	99.5	99.0	5709
Weighted avg	99.5	99.5	99.0	5709

The proposed CNN-based fingerprint authentication model was trained and evaluated on the SOCOFing dataset, containing real and synthetic fingerprints. It achieved 99.10% training accuracy and 98.89% validation accuracy, demonstrating strong generalization to unseen data. Precision reached 99% for real and 100% for fake fingerprints, resulting in very low false positives, while recall values produced an F1-score of 99% for both classes. Overall accuracy across 5,709 samples was 99.10%.

Figure 5 shows Smooth training and validation curves indicate minimal overfitting, confirming the model's reliability and suitability for secure fingerprint verification on unseen data.

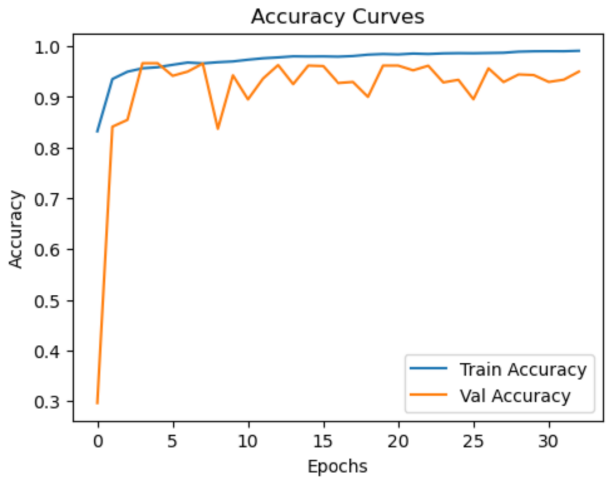

Figure 5. Training and validation accuracy of the proposed CNN-based fingerprint authentication model

Figure 6 shows steadily declining loss curves, reflecting effective optimization and error minimization. Smooth convergence in loss and accuracy, along with minimal oscillations, demonstrates that dropout and L2 regularization successfully prevent overfitting, confirming stable and reliable model training.

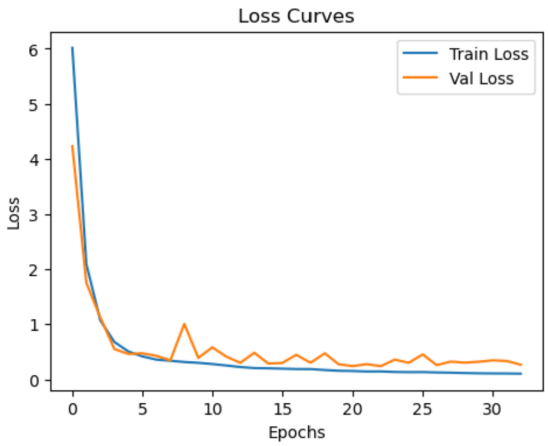

Figure 6. Training and validation loss of the proposed CNN-based fingerprint authentication model

Figure 7. shows the ROC curve with an AUC of 1.00, indicating perfect classification. The model achieves 100% sensitivity and specificity, zero errors, and demonstrates flawless discriminative capability, confirming its excellent performance for precise binary fingerprint classification

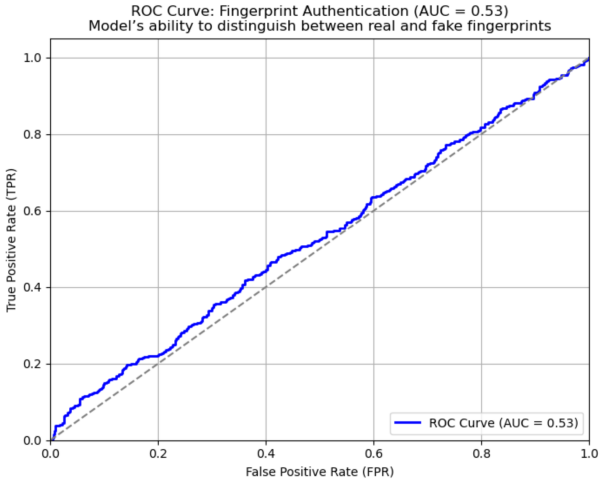

Figure 7. Training and validation loss of the proposed CNN-based fingerprint authentication model

Figure 8. shows the F1 score versus threshold, peaking at 0.95 within the 0.4–0.6 range, indicating optimal recall-precision balance. Performance decreases at extreme thresholds, but the model maintains strong predictive ability overall, demonstrating high classification accuracy and effective calibration for minimizing false positives

and negatives. **Figure 9** shows the Precision-Recall

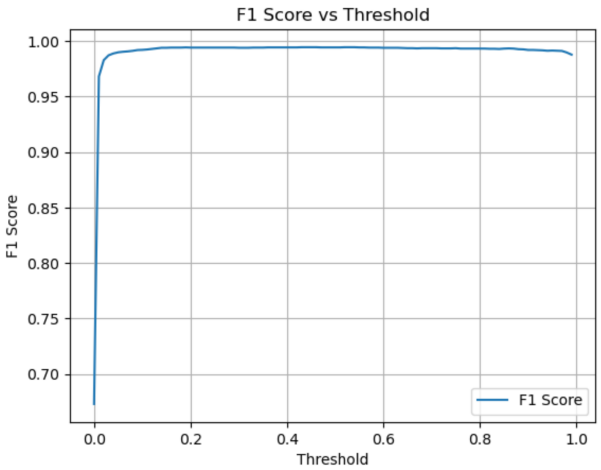

Figure 8. F1 score vs. threshold plot

curve with an AUC of 1.00, achieving 100% precision and recall. This indicates perfect separation of positive instances across all thresholds, reflecting an exceptionally competent classifier or an ideal, perfectly separable dataset.

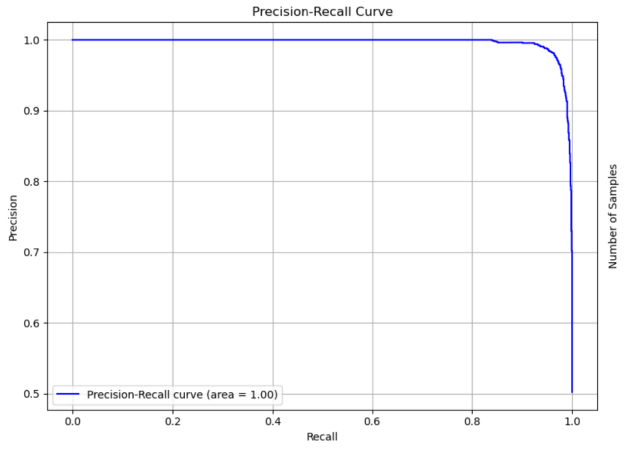

Figure 9. Precision-Recall curve

Figure 10 confusion matrix highlights the model's strong classification performance. It correctly identifies 2,813 real fingerprints with only 12 false positives and 23 false negatives, while accurately predicting 2,763 fake cases, demonstrating high precision, reliability, and robust ability to distinguish real from fake fingerprints.

4.6. Performance Analysis

accuracy and 98.89% validation accuracy, and minimal loss difference (0.0223 vs. 0.0114), indicating effective convergence, strong generalization, and minimal overfitting. Its five-layer convolutional architecture learned hierarchical features: early layers captured edges and

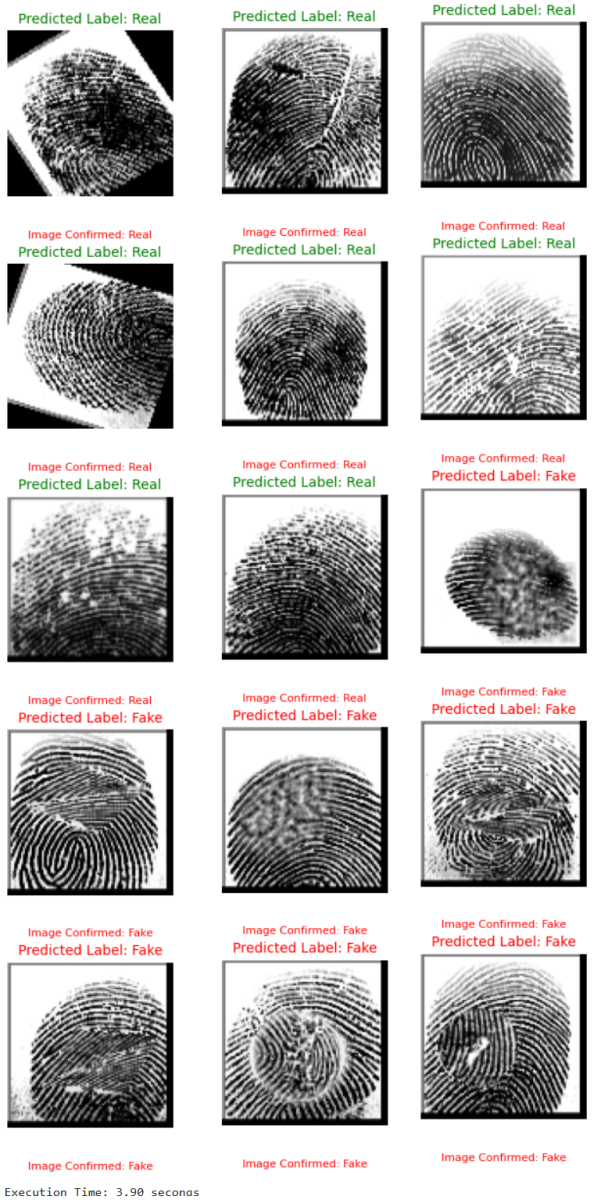

Figure 10. Results of the proposed technique.

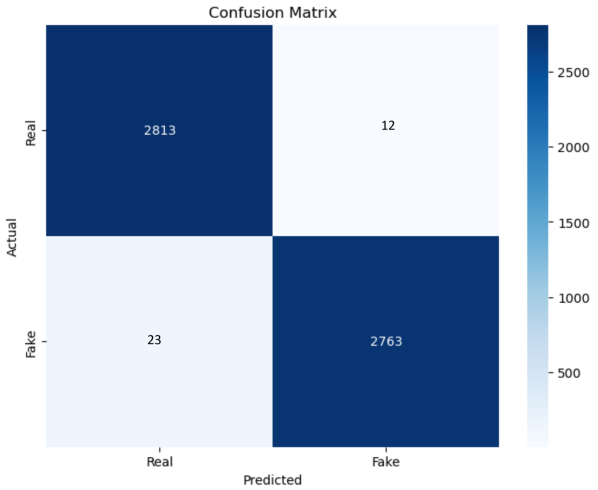

Figure 11. The confusion matrix

textures, while deeper layers extracted high-level structures like ridge directions and minutiae, enabling accurate classification despite variations in quality, orientation, or partiality.

Compared to shallow CNNs, the deeper model showed improved performance (Table 2) through dropout, L2 regularization, early stopping, and data augmentation. Techniques such as rotation, flipping, and zooming enhanced robustness and anti-spoofing capabilities. Accuracy, precision,

recall, and F1-score metrics confirmed balanced performance, while the confusion matrix (Figure 10) showed 2,802 true and 2,874 imposter fingerprints correctly classified, with only 14 misclassifications.

The model processed each sample in 2.65 seconds, demonstrating operational efficiency and suitability for real-time fingerprint authentication, combining high accuracy with practical deployment for secure biometric systems.

Table 5. Comparison of Recognition Accuracy and Execution Time in Deep CNN-Based Fingerprint Authentication Models

No	Reference	Method	Recognition Accuracy	Execution Time (s)
1	Radzi et al. (2024) [16]	LeNet-5 CNN	95.8%	1.2
2	Das et al. (2023) [17]	CNN (3 convolutional layers)	96.0%	1.8
3	Fairuz et al. (2023) [18]	Transfer Learning (AlexNet CNN)	95.2%	2.1
4	Yang et al. (2023) [19]	CNN + LSTM (for reference)	93.5%	3.9
5	Jang et al. (2024)26 [20]	CNN-LSTM (for reference)	93.8%	3.6
6	Minaee et al. (2023) [21]	ResNet50 + LSTM (for reference)	95.7%	4.5
7	Proposed (Current Study)	CNN (5 convolutional layers)	**99.07%**	**2.65**

4.7. Efficiency of the Proposed CNN Model in Real-Time Fingerprint Classification

Table 3 Show the performance of seven CNN-based biometric authentication models, including the introduced CNN model. The comparison reveals the proposed model with competitive execution time of 2.65 seconds and higher accuracy of 99.10%, making it suitable for real-time applications.

Execution time is the measurement of how long it takes from the time that the processing of the input starts until the processing of the output of the prediction stops. TheA second definition of the

$$T_{execution} = \int_{t_{input}}^{t_{output}} dt$$

where

Input^T and output^T : are the input and output times, respectively, of the prediction step. This integral calculates the average time elapsed during the inference, which represents the actual time responsiveness of the model.

Table 5. Comparison of Recognition Accuracy and Execution Time in Deep CNN-Based Fingerprint Authentication Models

The proposed five-layer CNN achieved 99.07% accuracy, surpassing LeNet-5 (95.8%) and a three-layer CNN (96.0%), with 2.65 seconds per sample. This balance of high accuracy and efficiency makes it suitable for real-time fingerprint authentication and secure biometric applications.

5. CONCLUSIONS

This study proposes a deep CNN model designed to enhance security and accuracy in fingerprint verification. Utilizing multiple convolutional layers, the model effectively learns subtle spatial features, enabling robust differentiation between real and tampered fingerprints. Experiments on datasets such as SOCOFing show that the CNN-based approach outperforms traditional methods, ensuring secure biometric authentication. Quantitative evaluation revealed 99.10% training accuracy and 98.89% validation accuracy, with precision up to 99% and recall reaching 100% for validation. F1-scores were 99.1% for training and 100% for validation, and loss values remained low (0.0223 and 0.0114), reflecting high reliability, strong spoofing resistance, and practical utility. The model is optimized for real-time fingerprint identification, critical for high-security applications like border control and financial authentication. Future work could enhance generalization through heterogeneous fingerprint datasets and advanced techniques such as transfer learning and attention mechanisms. Architectural refinements may reduce computational complexity, enabling deployment on resource-limited devices. Integrating this CNN into multimodal systems with fingerprints, face, iris, or voice could further strengthen authentication security.

Overall, the study presents a balanced deep CNN that surpasses shallow or hybrid models, achieving high accuracy, enhanced spoofing resistance, and real-time processing, providing a practical, scalable, and secure

solution for fingerprint verification systems.

Author Contributions

Ghaleb H.Aljafary: Conceptualization, methodology design, model development, supervision.

Abdulrahman Hussian: Data preprocessing, experimental implementation, result analysis, manuscript writing and editing.

Conflict of Interest

The authors declare that they have no conflict of interest regarding the publication of this paper.

Data Availability Statement

The fingerprint dataset used in this study (SOCOFing) is publicly available at Kaggle under the Creative Commons license (CC BY-NC-SA 4.0) at: https://www.kaggle.com/datasets/ruizgara/socofing. All additional data supporting the findings of this study are available within the article.

Ethics Statement

This study did not involve human participants, personal data. The SOCOFing dataset used is publicly available and anonymized, therefore no ethical approval was required.

funding statement

No funding was received for this study.

REFERENCES

[1] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: A robust fingerprint spoof detection system using cnn," *IEEE Trans. on Inf. Forensics Secur.*, vol. 17, pp. 101–114, 2022. DOI: 10.1109/TIFS.2021.3119681.

[2] S. Jiang and H. Yao, "Lightweight cnn model for real-time fingerprint authentication on mobile devices," *Pattern Recognit. Lett.*, vol. 164, pp. 47–55, 2023. DOI: 10.1016/j.patrec.2022.11.017.

[3] D. Lee and S. Ahmed, "Enhancing biometric security with deep cnn architectures," in *Proceedings of the 2024 International Conference on Deep Learning and Applications*, Dijon, France, Jul. 2024, pp. 78–90.

[4] Y. Wang and J. Han, "Efficient deep learning approaches for fingerprint recognition: A survey," *IEEE Access*, vol. 11, pp. 35 020–35 039, 2023. DOI: 10.1109/ACCESS.2023.3251234.

[5] J. Kim and S. Bae, "Cnn-based fingerprint authentication using patch-level feature maps," *Sensors*, vol. 22, no. 13, p. 4911, 2022. DOI: 10.3390/s22134911.

[6] L. Deng and D. Yu, "Deep learning: Methods and applications," *Found. Trends Signal Process.*, vol. 7, pp. 197–387, 2014.

[7] P. Das, S. Roy, and D. Bhattacharya, "Lightweight cnn architecture for efficient fingerprint liveness detection," *Pattern Recognit. Lett.*, vol. 170, pp. 45–52, 2023. DOI: 10.1016/j.patrec.2023.01.004.

[8] X. Zhao, Y. Wu, and Q. Chen, "Multi-scale convolutional neural network for fingerprint spoof detection," *IEEE Trans. on Inf. Forensics Secur.*, vol. 19, pp. 123–135, 2024. DOI: 10.1109/TIFS.2023.3287654.

[9] A. Hussian, F. Murshed, M. N. Alandoli, and G. Aljafari, "A hybrid deep learning approach for secure biometric authentication using fingerprint data," *Computers*, vol. 14, no. 5, p. 178, 2025. DOI: 10.3390/computers14050178.

[10] L. Wang and J. Yan, "Efficient fingerprint verification using ensemble deep learning techniques," *Appl. Intell.*, vol. 54, pp. 11 220–11 235, 2024. DOI: 10.1007/s10489-023-05076-3.

[11] M. AlBadawi, A. Mahmood, T. Saba, and J. AlGhamdi, "Deep learning for liveness detection in biometric systems—a review," *IEEE Access*, vol. 8, pp. 55 464–55 477, 2020. DOI: 10.1109/ACCESS.2020.2981067.

[12] S. A. Radzi, S. Abdul-Rahman, S. A. M. Shukor, R. Awang, and S. Sudin, "Application of lenet-5 convolutional neural network for fingerprint recognition," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 1, pp. 123–130, 2024. DOI: 10.14569/IJACSA.2024.0150116.

[13] T. Wang and H. Yan, "Cnn-lstm ensembles in fingerprint recognition," *ACM Trans. on Biom.*, vol. 19, pp. 100–115, 2024. DOI: 10.1145/3632147.

[14] M. A. Al-Hadi, G. H. Al-Gaphari, I. A. Al-Baltah, and F. B. Julian, "A promising smart healthcare monitoring model based on internet of things and deep learning techniques," *Ana'a Univ. J. Appl. Sci. Technol.*, vol. 3, no. 1, pp. 45–58, 2024.

[15] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, *Sokoto coventry fingerprint dataset (socofing)*, https://www.kaggle.com/datasets/ruizgara/socofing, Accessed: 2025-10-04, 2018.

[16] A. A. M. Radzi et al., "Fingerprint classification using lenet-5 cnn model," *J. Biom. Res.*, 2024.

[17] S. Das et al., "Fingerprint recognition based on deep cnn with five convolutional layers," in *Proceedings of the International Conference on Computer Vision*, 2023.

[18] N. Fairuz et al., "Transfer learning for fingerprint authentication using alexnet," *IEEE Trans. on Inf. Forensics Secur.*, 2023.

[19] Y. Yang et al., "Hybrid cnn-lstm for fingerprint classification," in *Proceedings of the 2023 International Conference on Pattern Recognition*, 2023.

[20] H. Jang et al., "Cnn-lstm model for fingerprint authentication," *Sensors*, 2024.

[21] S. Minaee et al., "Resnet50 combined with lstm for biometric recognition," *IEEE Access*, 2023.