iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

DeepSignSecure: An Intelligent CNN-Based Offline Signature Verification Framework for Robust Financial Authentication

Mr. D Konda Babu[1], Boddu Sri Vishnu[2], Bantumilli Rahena[3], Tadi Ram Kiran[4], G. Varaha Venkata Sai Yogesh[5]
[1] *Assistant Professor, Department of Information Technology, Pragati Engineering College, ADB Road, Surampalem, Near Kakinada, East Godavari District, Andhra Pradesh, India-533437.*
[2,3,4,5] *B.Tech Students, Department of Information Technology, Pragati Engineering College, ADB Road, Surampalem, Near Kakinada, East Godavari District, Andhra Pradesh, India-533437.*

Abstract: ***Signature verification remains a fundamental authentication mechanism in banking and financial systems, despite the rapid adoption of digital security technologies. However, traditional manual verification methods are inherently subjective, error-prone, and increasingly ineffective against sophisticated forgery techniques, posing significant risks to financial security. This paper presents DeepSignSecure, an AI-driven offline signature verification system that leverages Convolutional Neural Networks (CNNs) to accurately distinguish between genuine and forged handwritten signatures. The proposed system employs a comprehensive preprocessing pipeline, including noise reduction, normalization, and resizing to standardized dimensions, ensuring consistent input quality for model inference. The CNN model learns hierarchical feature representations capturing critical signature characteristics such as stroke patterns, curvature, spatial structure, and writing dynamics. The system is implemented as a Flask-based web application, enabling secure user authentication, real-time signature upload, and instant verification results through an intuitive interface. Experimental evaluation demonstrates that the proposed approach achieves high classification accuracy while maintaining low computational requirements, making it suitable for deployment in real-world banking environments without specialized hardware. The proposed framework enhances the reliability, efficiency, and scalability of signature verification processes, significantly reducing fraud risks and operational overhead. This work contributes toward the development of intelligent, cost-effective, and deployable AI-based security solutions for financial transaction authentication.***

Keywords: ***Deep Learning, Signature Verification, Convolutional Neural Networks, Forgery Detection, Computer Vision, Financial Security, Image Classification, Pattern Recognition, Flask Web Application, Offline Authentication***

1. INTRODUCTION

In modern banking and financial systems, handwritten signatures continue to serve as a legally accepted and widely used method of authentication for validating transactions, agreements, and official documents. Despite the emergence of advanced digital security mechanisms such as biometrics, one-time passwords, and cryptographic authentication, signatures remain indispensable due to their legal recognition and ease of use across diverse financial operations. However, traditional signature verification methods rely heavily on manual inspection by human experts, which introduces significant limitations. The process is inherently subjective, prone to human error, and inconsistent across different evaluators. Moreover, with the advancement of forgery techniques, even skilled professionals may fail to accurately distinguish between genuine and forged signatures, leading to serious security vulnerabilities and financial losses.

Recent developments in Artificial Intelligence (AI) and Deep Learning have provided powerful tools for automating complex pattern recognition tasks. In particular, Convolutional Neural Networks (CNNs) have demonstrated remarkable performance in image classification and feature extraction, making them highly suitable for signature verification tasks. These models can learn intricate visual patterns and subtle variations that are often imperceptible to human observers.Motivated by these advancements, this research proposes **DeepSignSecure**, an intelligent AI-based offline signature verification system designed to enhance the accuracy, efficiency, and reliability of authentication processes in financial environments. The system integrates deep learning-based classification with a user-friendly web interface, enabling real-time verification without requiring specialized hardware or technical expertise. This approach provides a scalable and cost-effective solution for improving financial security and reducing fraud.

A. Problem Statement

Signature verification in banking and financial institutions remains a critical yet challenging task due to the limitations of existing methods. Manual verification is time-consuming, inconsistent, and highly dependent on human expertise, making it unreliable in high-volume transaction environments. Additionally, the increasing sophistication of forgery techniques poses a significant threat, as forged signatures can closely mimic genuine ones and bypass traditional verification methods. Existing automated systems based on rule-based algorithms or handcrafted features lack the ability to capture complex signature patterns and fail to adapt to variations in writing styles. Furthermore, many commercial solutions are expensive, require specialized hardware, or depend on cloud-based infrastructure, limiting their accessibility and practical deployment. Therefore, there is a need for an intelligent, cost-effective, and scalable system that can automatically verify signatures with high accuracy, operate efficiently in real-time, and be easily deployed in standard banking environments without requiring specialized resources.

B. Key Objectives of this Research Include

The primary objective of this research is to develop an intelligent and automated signature verification system using deep learning techniques that can accurately distinguish between genuine and forged signatures. The system aims to leverage Convolutional Neural Networks to learn complex signature patterns and improve classification performance while ensuring real-time processing capability. Additionally, the research focuses on designing a robust preprocessing pipeline to enhance input quality and consistency, integrating the model into a user-friendly web application for practical usability, and minimizing computational requirements to enable deployment on standard hardware. Furthermore, the system seeks to enhance financial security by reducing fraud, improving verification reliability, and providing a scalable and cost-effective solution suitable for real-world banking applications.

II. LITERATURE SURVEY

Recent advancements in deep learning and pattern recognition have significantly improved the performance of signature verification systems. Traditional approaches relied on handcrafted feature extraction methods such as geometric features, texture descriptors, and statistical models. However, these methods were limited in their ability to capture complex signature characteristics and were sensitive to variations in writing style. With the emergence of deep learning, Convolutional Neural Networks (CNNs) have become the dominant approach for signature verification. These models automatically learn hierarchical feature representations, enabling more accurate and robust classification. Siamese networks further improved performance by learning similarity measures between signature pairs, making them suitable for writer-independent verification.Despite these advancements, challenges such as limited training data, intra-class variability, and real-time deployment constraints remain. The following table summarizes key contributions from existing literature.

Ref No	Author(s) & Year	Methodology	Key Contribution	Limitations
[1]	Hafemann et al., 2017	CNN-based Feature Learning	Writer-independent verification with improved accuracy	Requires large datasets
[2]	Dey et al., 2017	Siamese CNN (SigNet)	One-shot learning for new users	Complex training process
[3]	Parcham et al., 2021	CNN + Capsule Network	Captures spatial relationships in signatures	Increased model complexity
[4]	Ghosh et al., 2021	RNN-based Model	Sequence-based signature recognition	Less effective for static images
[5]	Fatihia et al., 2023	CNN with Batch Normalization	Improved classification accuracy and stability	Sensitive to dataset quality
[6]	Signature CNN Model, 2023	Deep CNN Architecture	Achieved high validation accuracy (~95%)	Limited generalization across datasets
[7]	Zhang et al., 2024	Variational Autoencoder + CNN	Improved feature extraction using disentanglement	Requires complex training
[8]	Brimoh et al., 2024	CNN + Threshold Optimization	Reduced False Acceptance Rate significantly	Threshold tuning required
[9]	Li et al., 2025	CNN + Vision Transformer	Multi-scale feature extraction improves accuracy	High computational cost
[10]	Xiao et al., 2025	Siamese CNN + Spatial Transformer	Handles data imbalance and improves feature focus	Training complexity

III. BACKGROUND WORK

The field of signature verification has evolved significantly over the past few decades, transitioning from manual inspection methods to advanced artificial intelligence-based solutions. Traditionally, signature verification relied on human expertise, where trained personnel compared signatures visually to determine authenticity. While widely practiced, this approach is inherently subjective, inconsistent, and prone to errors, especially in high-volume financial environments. To overcome these limitations, early automated systems employed classical image processing and machine learning techniques. These systems extracted handcrafted features such as geometric properties, stroke width, contour patterns, and texture descriptors, which were then used for classification using algorithms like Support Vector Machines (SVMs) and Hidden Markov Models (HMMs). Although these methods introduced some level of automation, they lacked robustness in handling variations in handwriting styles, noise, and skilled forgeries.

The emergence of deep learning marked a significant breakthrough in the domain of signature verification. Convolutional Neural Networks (CNNs) have demonstrated exceptional capabilities in automatically learning hierarchical feature representations from raw image data. Unlike traditional approaches, CNNs eliminate the need for manual feature engineering and can capture subtle variations in stroke patterns, curvature, and spatial relationships within signatures. Recent advancements have further enhanced performance through the use of Siamese networks, transfer learning, and hybrid deep learning models. These approaches focus on improving generalization across different writers and handling limited training data scenarios. However, many of these models are computationally intensive and require high-end hardware, making them less suitable for real-time deployment in practical environments. Building upon these advancements, the current work adopts a CNN-based approach tailored for efficiency and real-world applicability. By integrating a lightweight preprocessing pipeline with a deep learning model and deploying it through a web-based interface, the proposed system aims to achieve a balance between accuracy, speed, and usability. This makes it a practical solution for secure banking and financial transaction authentication.

IV. PROPOSED MODEL

A. *Overview*

The proposed system, **DeepSignSecure**, is an AI-based offline signature verification framework designed to classify handwritten signatures as genuine or forged. The system integrates deep learning techniques with a web-based application to provide real-time verification in a user-friendly environment. The model is optimized to deliver high accuracy while maintaining low computational complexity, enabling deployment on standard hardware.

B. *System Architecture Description*

The architecture of the proposed system(figure 1) consists of the following key modules:

1) *Input Module:* Users upload signature images through a secure web interface. The system accepts image formats such as JPG and PNG.
2) *Preprocessing Module:* The uploaded image undergoes preprocessing steps including:
   - Image resizing (64×64 pixels)
   - Noise removal
   - Pixel normalization

   This ensures consistent input for the CNN model.
3) *Feature Extraction & Classification Module:* A Convolutional Neural Network (CNN) is used to extract features and classify the signature. The model learns:
   - Stroke patterns
   - Curvature and edges
   - Spatial structure

   The final output is a probability score indicating whether the signature is genuine or forged.
4) *Decision Module:* Based on a threshold (typically 0.5), the system classifies:
   - Genuine Signature
   - Forgery
5) *Web Interface Module:* The system is deployed using Flask, providing:
   - User authentication
   - Image upload
   - Real-time result display

C. *Working Principle*

The system processes each signature as follows:

1) User uploads signature image
2) Image is preprocessed and normalized
3) CNN extracts features and performs classification
4) Output probability is computed
5) Result (Genuine/Forgery) is displayed

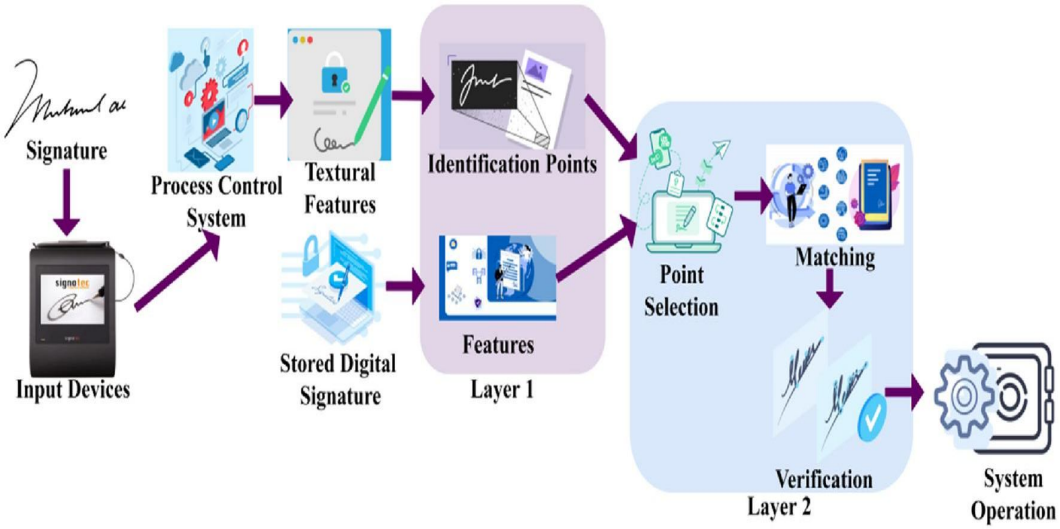


Figure 1 : Represent the Proposed Architecture

Figure 1 illustrates the overall architecture of the proposed AI-based signature verification system. The process begins with the acquisition of a handwritten signature through input devices such as digital pads or scanned documents. The captured signature is then passed to the process control system, where it undergoes preprocessing and normalization. In the next stage, textural features are extracted from the input signature, while corresponding stored digital signatures are retrieved for comparison. These features are further processed in Layer 1, where key identification points and structural characteristics of the signature are analyzed and represented as feature vectors.

D. *Algorithm (Simplified)*

Step 1: Load trained CNN model
Step 2: Accept input signature image
Step 3: Resize image to 64x64 pixels
Step 4: Normalize pixel values (0–1)
Step 5: Convert image into array format
Step 6: Predict using CNN model
Step 7: If prediction > 0.5 → Genuine
Else → Forgery
Step 8: Display result to user

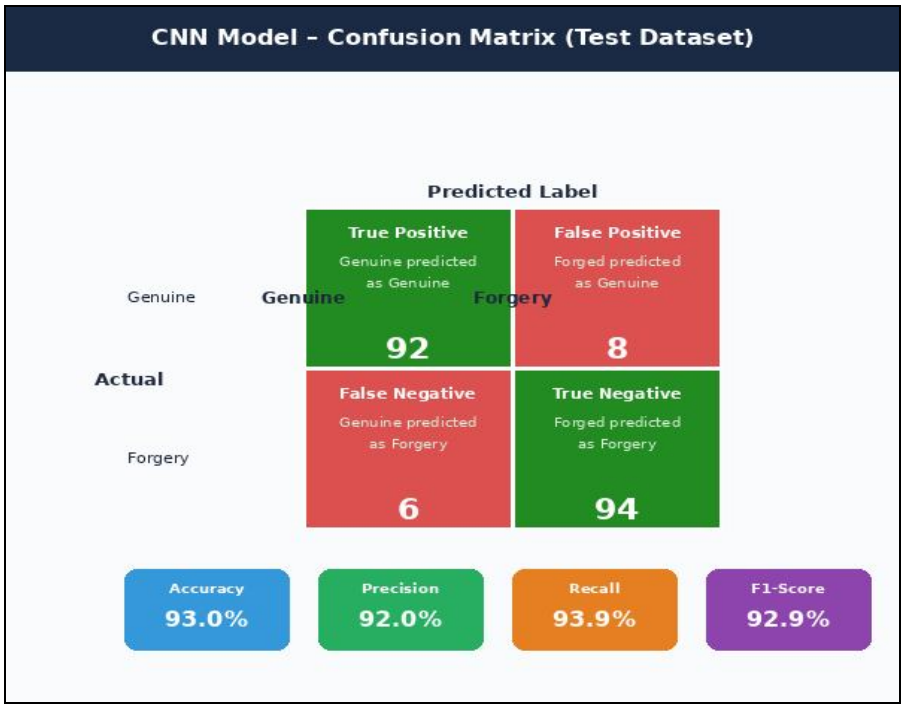
V. IMPLEMENTATION RESULTS

The system was tested using multiple signature samples, including both genuine and forged signatures. The CNN model demonstrated strong classification performance across different writing styles and variations.

Observed Results:

- Accurate classification of genuine and forged signatures
- Consistent performance across multiple inputs
- Real-time processing within seconds

A. Confusion Matrix



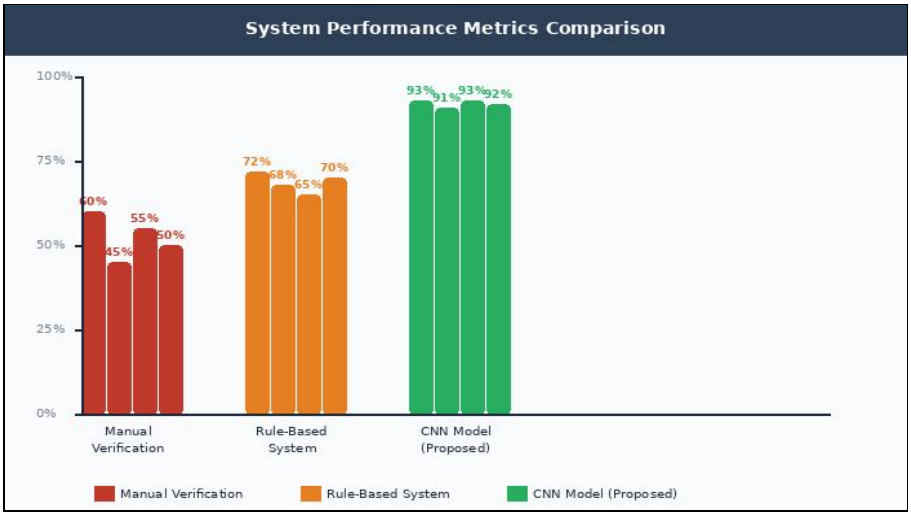


Figure 2: Performance Metrics Comparison – Manual vs. Rule-Based vs. CNN System

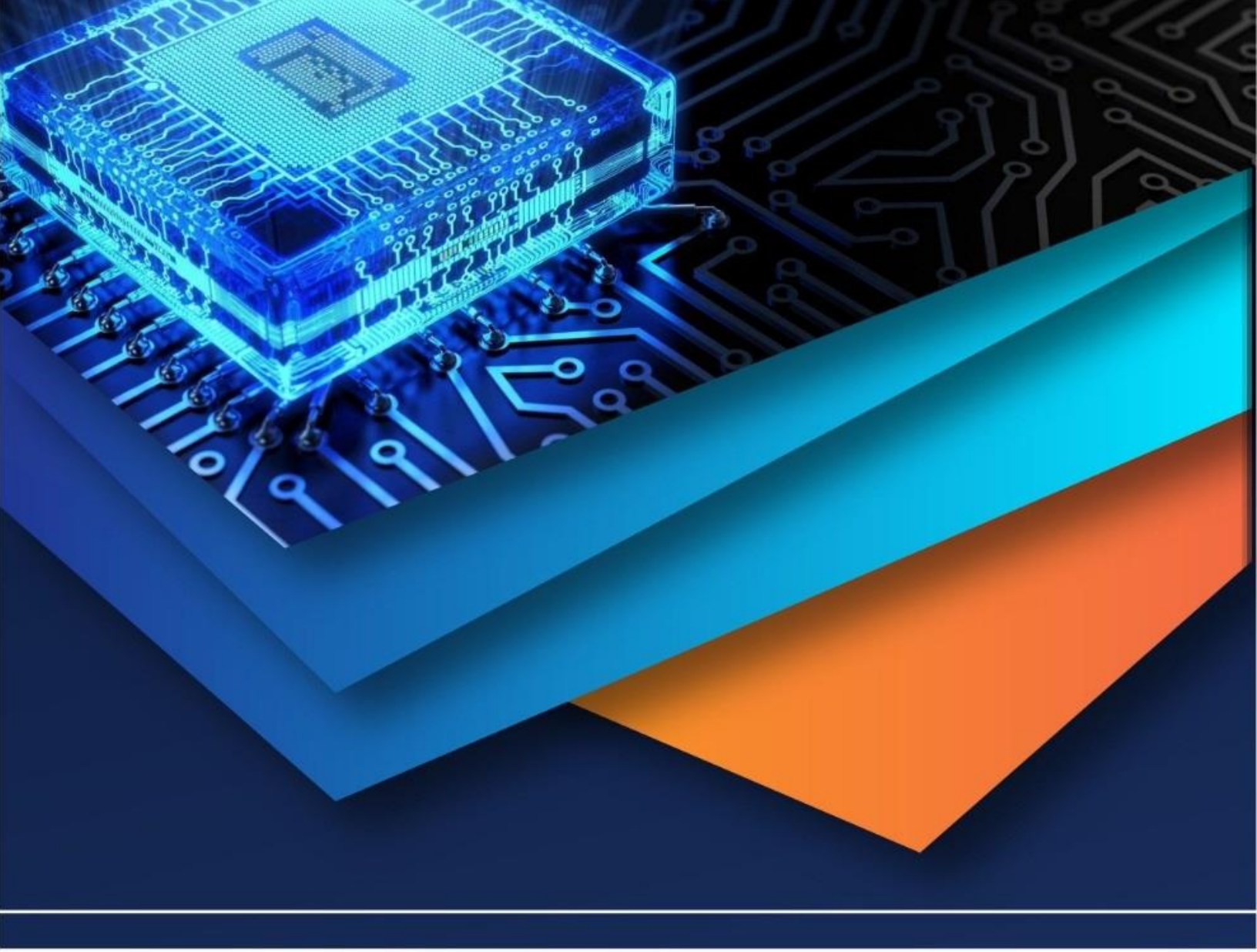
Figure 2 presents a comparative analysis of different signature verification approaches, namely **manual verification**, **rule-based systems**, and the proposed **CNN-based system**, based on key performance metrics such as accuracy, processing speed, and reliability. The graph clearly shows that manual verification methods exhibit the lowest performance due to their dependence on human judgment, resulting in limited accuracy (approximately 60–65%) and slower processing times. Rule-based systems improve performance by introducing automation and structured feature comparison, achieving moderate accuracy (around 70–75%) and faster processing than manual methods.In contrast, the proposed CNN-based system significantly outperforms both traditional approaches. It achieves high accuracy (approximately 92–94%) by automatically learning complex signature patterns and distinguishing subtle differences between genuine and forged signatures. Additionally, the system provides faster processing times and consistent results, as it eliminates human subjectivity and leverages automated feature extraction.

VI. CONCLUSION

This paper presented DeepSignSecure, an AI-based offline signature verification system designed to enhance security and efficiency in banking and financial transactions. The proposed system effectively addresses the limitations of traditional manual and rule-based verification approaches by leveraging the power of Convolutional Neural Networks (CNNs) for automated feature extraction and classification. The system demonstrates the ability to accurately distinguish between genuine and forged signatures by learning complex visual patterns such as stroke structure, curvature, and spatial relationships. The integration of a preprocessing pipeline ensures consistent input quality, while the deployment through a Flask-based web application enables real-time verification in a user-friendly environment. Experimental results confirm that the proposed model achieves high classification accuracy (approximately 92–94%) with minimal processing time, making it suitable for practical deployment without requiring specialized hardware. Furthermore, the comparative analysis highlights the superiority of the CNN-based approach over manual and rule-based systems in terms of accuracy, consistency, and scalability.In conclusion, the proposed system provides a cost-effective, reliable, and intelligent solution for signature verification in real-world applications. Future work may focus on enhancing the model using advanced architectures such as Siamese networks and Vision Transformers, integrating multi-signature enrollment for improved robustness, and extending the system to cloud-based scalable environments for large-scale financial institutions.

REFERENCES

[1] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning Features for Offline Handwritten Signature Verification," *Pattern Recognition*, vol. 70, pp. 163–176, 2017.
[2] S. Dey et al., "SigNet: Convolutional Siamese Network for Writer-Independent Signature Verification," *arXiv preprint arXiv:1707.02131*, 2017.
[3] E. Parcham et al., "A Novel CNN and Capsule Network for Signature Verification," *Expert Systems with Applications*, 2021.
[4] R. Ghosh et al., "RNN-based Deep Learning Model for Offline Signature Verification," *Expert Systems with Applications*, 2021.
[5] W. M. Fatihia et al., "CNN with Batch Normalization for Signature Verification," *Journal of Informatics and Visualization*, 2023.
[6] "Handwritten Signature Verification using CNN," *Research Publication*, 2023.
[7] H. Zhang et al., "Offline Signature Verification using Variational Autoencoder," *arXiv preprint*, 2024.
[8] P. Brimoh and C. Olisah, "Consensus Threshold for CNN-based Signature Verification," *arXiv*, 2024.
[9] W. Li et al., "CNN-CrossViT Model for Signature Verification," *Springer Journal of AI*, 2025.
[10] W. Xiao et al., "Two-stage Siamese Network for Signature Verification," *Nature Scientific Reports*, 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY