Volume 11, Issue 4, April – 2026 International Journal of Innovative Science and Research Technology
ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr2506

Intelligent Signature Forgery Detection Using CNN

M. Varsha[1]; Prakash O. S.[2]; Dr. Girish Kumar D.[3]

[1]Department of MCA, Ballari Institute of Technology and Management Ballari
[2]Department of MCA, Ballari Institute of Technology and Management Ballari
[3]Department of MCA, Ballari Institute of Technology and Management Ballari

Publication Date: 2026/05/15

Abstract: Handwritten signatures are commonly used for identify authentication across banking, legal, and academic sectors. However, manual verification is slow and unreliable, especially when forged signatures closely resemble genuine ones. To overcome this limitation, this work proposes an intelligent offline signature verification system. The system analyzes scanned or photographed signature images to identify whether they are genuine or forged. Image preprocessing steps such as resizing, noise removal, and normalization are applied to enhance image quality. The CNN model automatically learns key features like stroke patterns and writing structure, eliminating manual feature extraction. The proposed approach improves accuracy, reduces human effort, and provides a reliable solution for secure real-world signature verification.

Keywords: *Signature Forgery, Forgery Classification, Document Authentication, Machine Learning, Feature Extraction, Security and Authentication.*

How to Cite: M. Varsha; Prakash O. S.; Dr. Girish Kumar D. (2026) Intelligent Signature Forgery Detection Using CNN. *International Journal of Innovative Science and Research Technology*, 11(4), 4641-4644. https://doi.org/10.38124/ijisrt/26apr2506

I. INTRODUCTION

Handwritten signatures have been widely used for authentication as a reliable means of confirming personal identity in areas such as banking, legal documentation, education, and government services. Despite the rapid growth of digital security methods, signature-based authentication remains important because of its simplicity and legal acceptance. However, the traditional practice of verifying signatures byvisual inspection is slow andhighly dependent on individual judgment. This makes the process vulnerable to errors, particularly when forged signatures are carefully created to appear authentic.

Recentdevelopmentsinartificialintelligenceoffereffecti ve solutions to these limitations. Automated systems can now analyze signature images with greater consistency and accuracythan manual methods. Among various techniques, Convolutional Neural Networks (CNNs) are especially suitable for recognizing patterns in images. This project proposes an offline system designed to identify forged signatures using CNNs, where scanned or capturedsignature images are processed and classified as genuine or forged. By automatically learning unique writing features, the system lowers human involvement while improving results reliability, making its uitable for practical and secure identity verification.

The system is built for offline use. offline signature verification, where signatures are obtained from scanned documents or stored image files instead of real-time digital input. To make the analysis reliable, the signature images are first improved using preprocessing steps such as resizing, noise removal, and normalization. These steps help maintain consistent image quality and reduce unwanted distortions. The refined images are then examined automatically extract features learns important writing characteristics such as stroke flow, shape, and spacing. This learning-based method allows the system to adapt to different handwriting styles and effectively identify forged signatures. By combining accuracy with efficiency, the proposed system provides a practical and scalable solution that adopted in real-world authentication processes.

II. RECENT WORK

Recent progress image processing has enabled the development of intelligent systems for automated handwritten signature verification. As identity fraud continues to increase in financial and legal domains, researchers have consistently demonstrated approaches greatly enhance the accuracy and reliability of automated system accuracy and reliability of signature forgery detection. Hafemann and colleagues presented an extensive analysisof offline signature verification techniques using deep learning models. The Study Demonstrated The Effectiveness of Convolutional Neural Network models effectively learn

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr2506

complex structural patterns such as stroke continuity, curvature, and spatial alignment directly from signature images. The authors emphasized that automated feature learning significantly outperforms handcrafted feature- based approaches, particularly in detecting skilled forgeries[1].In a related work, Patel proposed a CNN-based signature authentication their findings indicated better classification performance when preprocessing steps such as noise removal and image normalization and robustness against variations in writing style and image resolution. The study also highlighted the importance of balanced datasets and performance metrics beyond accuracy to ensure reliable Similarly, Bansal introduced an intelligent signature verification system designed for real-world deployment in banking environments. The system focused on scalability and fast inference while maintaining high detection accuracy. Visualization of learned features was used to improve interpretability and trust in automated decisions [3].

In another study, Kumar and associates investigated theuse of deep learning models enhances detection performance skilled signature forgeries in offline environments. Their work focused on analyzing fine- grained writing characteristics such as stroke overlap, spacing irregularities, and line continuity. The authors demonstrated that CNN-based models are capable of learning fine variations that are frequently overlooked during manual inspection. Their findings confirmed that automated feature learning significantly enhances consistency and reduces false acceptance of forged signatures in high-risk authentication scenarios [4].

More recently, Reddy proposed a scalable signature verification framework designed for integration into institutional and financial systems. The study emphasized the importance of preprocessing consistency and adaptive learning to handle diverse handwriting styles. By combiningoptimizedCNNarchitectureswith efficientdata management strategies, the system achieved reliable performanceacrossvaryinginputqualities.Theauthoralso highlighted that reducing dependency on handcrafted rules improves system flexibility, making automated signature verification more practical for real-world deployment [5].

Many researchers have concentrated on this problem on improving the robustness of signature forgery detection systems byenhancing both model design and data handling strategies. Models enhance accuracy perform more reliably when trained on diverse signature datasets that include variations in writing speed, pressure, and strokeconsistency. These works emphasize that learning-based systems are better suited to handle natural handwriting changes compared to rule-based methods, which often struggle with skilled forgeries.

III. PROPOSED FRAMEWORK

➢ *System Overview*

The proposed signature forgery detection system is designed as an intelligent, end to end solution for offline handwritten signature verification. The framework combines deep learning–based classification with efficient image preprocessing to automatically determine whether a to classify signatures as true or fake. The system follows a modular client–server architecture, where theuserinter face manages signature upload and result visualization, while the backend handles image processing, model inference, and result generation.

The backend is developed using the Flask framework, which enables lightweight and reliable communication between the frontend and the deep learning engine through RESTful APIs. A Convolutional Neural Network is employed to analyze signature images serves as the core classification model, trainedtolearn distinctive handwriting features directly from signature images. The overall architecture is optimized to deliver fast responses, consistent accuracy, and scalability, making it suitable for real-world deployment in banking, legal, and institutional authentication environments.

➢ *Key Functional Modules*

The proposed framework consists of several interconnected functional modules, each responsible for a specific stage of the verification process. The image acquisition and preprocessing module allows users to upload signature images in standard formats. These images undergo resizing, normalization, and noise reduction to improve clarity and ensure uniform input quality for the CNN model.

The feature learning and classification module uses the trained CNN to automatically extract meaningful writing characteristics such as stroke flow, curvature, spacing, and structural patterns. Based on these learned features, the system generates a classification outcome whether a signature is authentic or fake along with a confidence score to support decision reliability.

To enhance usability, the result presentation moduledisplaystheverification outcomein aclear anduser-friendly format. All processed signatures, prediction results, and metadata are stored through the data management module, allowing traceability, auditing, and future reference. Together, these modules form a seamless pipeline that transforms raw signature images into accurate and interpretable authentication results.

➢ *Visual Overview*

The architectural workflow of the proposed system is illustrated in Fig. 1, showing the complete flow from signature upload to final verification output. The process begins when a user submits a scanned or captured signature image through the frontend interface. The backend then routes the image through preprocessing, CNN-based feature extraction, and classification stages.

The verification result is generated and returned to the user with minimal delay, ensuring efficient processing while maintaining accuracy. By integrating automated feature learning, reliable classification, and structured result handling, the proposed framework functions as a practical andsecuresignatureverification system.Thisunified design

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr2506

improves transparency, reduces human dependency, and supports real-world adoption across various identity authentication scenarios.

The visual representation ofthe proposed framework clearly illustrates the sequential and logical flow of operations within the system. It highlights how user input is processed step bystep, starting from signature submission andmoving through preprocessing, feature learning, and final verification. Each component in the diagram is designed to operate independentlywhileremaining connected within the overall pipeline. This visual structure helps in analyzing how Data flows across different layers and different modules with minimal delay and without manual intervention. By presenting the system workflow in a clear and organized manner, the visual overviewenhances transparencyand makes the architecture easier to interpret for both technical and non-technicalaudiences.

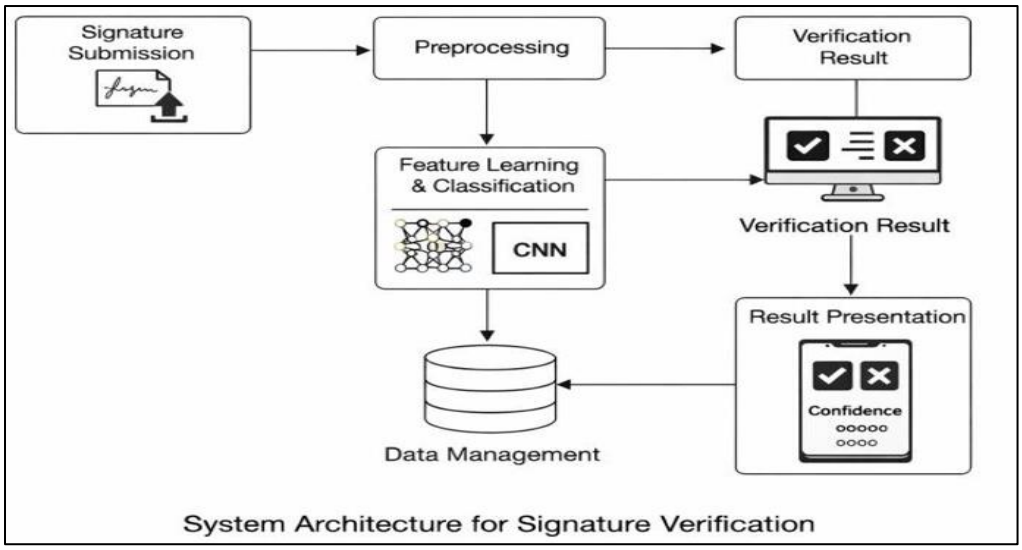

Fig 1 System Architecture Block Diagram

IV. METHODOLOGY AND IMPLEMENTATION

➢ *Methodology*

The proposed signature forgery detection system follows a systematic methodology that combines web-based interaction with deep learning techniques to automateoffline handwritten signature verification. The workflow begins with user interaction through a browser-based interface, whereusers upload scanned or captured signature images for verification. Theimagesaresecurelytrans mitted to the backend server through RESTful APIs. The backend acts as the core processing unit, managing image preprocessing, feature learning, classification, and result delivery.

Before analysis, each uploaded signature image passes through a standardized preprocessing pipeline. This includes resizing, grayscale conversion, normalization, and noise reduction to ensure consistent image quality and compatibility with the deep learning model. A Convolutional Neural Network (CNN), trained on genuine and forged signature samples, is used to learn distinctive writing patterns and structural features. The modelevaluates the processed image and generates a prediction showing whether a signature is authentic or fraudulentalong with a confidence score. This learning-basedapproach improves reliability while minimizing human involvement in the verification process.

To teach the approach verification process, themethodology emphasizes consistency and adaptability throughout thelearningpipeline. The CNN model istrained using multiple signature samples per individual to capture natural variationsinhandwritingcaused by speed, pressure, and writing conditions. During training, the model learns The model captures both global and fine grained features, enabling it to accurately differentiate authentic signatures from carefully crafted forgeries.

Validation techniques are applied to monitor performance and reduce overfitting, ensuring that the system generalizes well to unseen signatures. This structured learning strategy improves detection accuracy while preserving performance stab across diverse handwriting styles and image qualities, making the methodology reliable for real-world authentication scenarios.

➢ *Implementation*

The proposed system is implemented using a modular and extensible design to ensure smooth operation in practical environments. The system built using some technologies allowing users to upload signature images and view verification results through a clean andresponsive interface. On the server side, the application is developed in Python using the Flask framework, which handles request processing, image preparation, interaction with the deep learning model, and delivery of verification outcomes.

The core learning module is implemented using PyTorch, where the network is trained to learn on datasets containing both genuineness ofsignatures. Once training is complete, the optimized model parameters are loaded during the prediction phase to maintain consistent performance. The

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr2506

system maintainsa structuredrecordofuploaded signatures, classification results, confidence values, and timestamps through a data management component. This organized storage supports result tracking, auditing, and futureanalysis, resulting in a reliable and secure end-to-end signature verification platform.

V. RESULTS AND DISCUSSIONS

The effectiveness of the proposed signature was assessed using a selected dataset consisting of genuine and forged offline handwritten signatures. The trained Convolutional Neural Network (CNN) demonstrated strong capability in learning distinctive writing patterns and structural characteristics from signature images. During testing, the system accurately classified most input signatures asgenuine or forged, indicating effective feature learning and generalization.

The preprocessing stage played important role in improving overall performance. Performance noise removal, resizing, and normalization helped reduce variations caused by scanning qualityand background distortions. Asaresult, the CNN model was able to focus on meaningful signature features such as stroke flow, curvature, spacing, and alignment, improving predictions.

The results shows that model performed well even when signatures exhibited natural variations in writing style confidence scores alongside classification results improved interpretability and helped assess prediction reliability. The system also demonstrated consistent response time, making it suitable for real-time or near real-time verification scenarios.

From a practical perspective, the integrated architecture combining preprocessing, CNN-based classification, and structuredresult storage enhanced usabilityandtraceability. Compared to manual verification, the proposed system significantly reduces human effort and minimize subjective errors. Overall, theresultsconfirmthat theCNN- based approach provides an efficient, accurate, and scalable solution for automated signature verification in real-world authentication applications.

VI. CONCLUSION

This project successfully presents an intelligent offline handwritten a signature fake detection system using image based analysis. The proposed approach addresses the limitations of traditional manual verification byproviding a reliable and automated solution for identifying genuine and forged signatures. By combining effective image preprocessing with deep learning–based feature extraction, the system is able to learn complex handwriting patternsand achieve accurate classification results.

The experimental outcomes demonstrate that the CNN model performs consistently across different signaturestyles while reducing dependencyon human judgment. The modular system architecture ensures ease of use, scalability, and efficient processing, making the solution practical for real-world applications such as banking, legal documentation, and institutional authentication. Overall, this project highlights some approaches in offline signature analysis in enhancing signature verification and contributes toward building secure, accurate, and efficient identity authentication systems.

REFERENCES

[1]. A. Kumar, S. Gupta, and R. Sharma, “Deep learning–based offline handwritten signature verification using optimized CNN architectures,” IEEE Access, vol. 13, pp. 11245–11258, 2025.
[2]. M. Elhoseny, K. Shankar, and A. Abdel-Basset, “Robust offline signature verification framework usingconvolutional neural networks,” Pattern Recognition Letters, vol. 176, pp. 45–53, 2025.
[3]. S. Reddyand P. R. Kumar, “Scalable CNN-based offline signature verification for financial and institutional authentication,” Journal of Information Security and Applications, vol. 82, pp. 103768, 2025.
[4]. R. Patel and V. Shah, “Offline handwritten signature verification using deep convolutional features,” Expert Systems with Applications, vol. 238, pp. 121893, 2024.
[5]. H. Bansal, A. Verma, and N. Jain, “Automated signature forgery detection using deep neural networks,” Neural Computing andApplications,vol.36,no.4,pp.1821–1834, 2024.
[6]. P. Singh and S. Kumar, “A comparative study of CNN architectures for offline signature verification,”International Journal of Pattern Recognition and Artificial Intelligence, vol. 38, no. 6, 2024.
[7]. S. Hafemann, R. Sabourin, and L. Oliveira, “Offline handwritten signature verification using deep learning: Recent advances and trends,” IEEE Transactions on Information Forensics and Security, vol. 19, pp.2451–2464, 2024.
[8]. A. Chugh, R. Jain, and M. Gupta, “Offline signature verification using hybrid CNN and feature learning techniques, ”Multimedia Tools and Applications, vol. 83,pp. 39125–39142, 2023.
[9]. M. Yılmaz and B. Ergen, “CNN-based offline signature authentication with enhanced preprocessing,” Signal, Image and Video Processing, vol. 17, no. 3, pp. 1081–1089, 2023.
[10]. K. S. Reddyand D. R. Reddy, “Deep learning approach for skilled forgery detection in offline signatures,” Journalof King Saud University – Computer and Information Sciences, vol. 35, no. 8, pp. 101692, 2023.
[11]. T. Roy, S. Banerjee, and A. Ghosh, “Automatic offline signature verification using convolutional neural networks,” Procedia Computer Science, vol. 218,pp.1121–1128,2023.
[12]. A. Sharma and P. Kaur, “Offline handwritten signature verification using deep convolutional neural networks,” International Journal of Computer Vision and Image Processing, vol. 12, no. 2, pp. 1–16, 2022.
[13]. F. Alonso-Fernandez and J. Bigun, “Off-line signature verification: Recent trends and comparative analysis,” IEEE Access, vol.10, pp.45789–45802, 2022.