IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, November 2025
Impact Factor: 7.67

Signature Forgery Detection Using Deep Learning

Ashitha Raj V K and Thouseef Ulla Khan
Department of MCA
Vidya Vikas Institute of Engineering and Technology, Mysuru, India
ashitharaj2020@gmail.com and thouseef.khan@vidyavikas.edu.in

Abstract: *One of the most challenging problems of the biometric authentication is handwritten signature authentication due to the high disparity of writing style, signature and creation of forgery techniques. The proposed project offers an effective offline signature verification algorithm that will make use of a hybrid deep learning network that will help to integrate the advantages of the Convolutional Neural Networks (CNNs) and Vision Transformers (ViTs). Specifically, we propose two hybrid models that use ResNet-18 and a Vision Transformer as well as MobileNetV2 and a Vision Transformer. These models are supposed to capture the local (stroke, shape), and the global (spatial structure) content of signature images.*

To improve performance, we introduce a variety of innovations in this, by removing the last CNN layers into higher integration of the transformer, and by data augmentation and preprocessing to regularize the input with diversified datasets. We test our models using CEDAR datasets and show remarkable accuracy rates, including a

99.89 percent accuracy rate on CEDAR. Along with achieving low False Acceptance Rates (FAR) and False Rejection Rates (FRR), the suggested system maintains efficient execution durations, which makes it appropriate for mobile and real-time applications. In addition to providing a high- performing solution to the offline signature verification problem, this work demonstrates the usefulness of hybrid deep learning models in enhancing the security and dependability of digital authentication systems.

Keywords*:* Signature forgery detection, Deep Learning, Convolutional Neural Network (CNNs), Vision Transformers (ViTs), ResNet-18, MobileNetV2, Image Processing, PyMuPDF, Machine learning

I. INTRODUCTION

In today's digitally connected world, the demand for trustworthy and safe identity verification solutions has increased more critical than ever. The handwritten signature is grouped under other biometric traits that are still utilized in the authentication of identity during a financial transaction, legal institution, and administrative processes. However, the handwritten signature is extremely hard to verify due to intra- writer heterogeneity, inter- writer heterogeneity and better forging work. The signature verification systems which are classical tend to utilize either online or offline. Even though online systems are able to record dynamic writing patterns (pressure and speed of the stroke) the offline systems utilize only fixed aspects of an image and therefore the process is more complex. Further, the conventional approaches to machine learning do not necessarily succeed when tackling small variations and advanced fraud schemes.

In order to address these problems, the given project implies the use of hybrid deep learning-based convolutional neural network (CNNs) that is incorporated into this architecture, along with the Vision Transformers (ViTs) to achieve the higher accuracy and the greater strength of the offline signature verification. Specifically, the proposed system proposes two hybrid architectures, i.e., ResNet-18 + ViT and MobileNetV2+ ViT- that can both extract fine-grained local features and global patterns in signature images. The system can attain superior performance in classification using the Swish and Tanh functions of activation and integration optimization of models. The model is assessed and trained on benchmark datasets CEDAR achieving great precision and low error rates across diverse types of writing and languages. These results validate the system's effectiveness in distinguishing between both authentic and fake signatures, which makes it a valuable solution for enhancing security in practical uses such as mobile authentication platforms and document verification systems.

DOI: 10.48175/IJARSCT-30008

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

II. LITERATURE SURVEY

[1] The paper "Enhancing Security: Infused Hybrid Vision Transformer for Signature Verification" by Muhammad Ishfaq et al. proposes an innovative hybrid model that blends Vision Transformers (ViTs) with convolutional neural network (CNNs) to improve offline signature verification. By integrating local extraction of feature from CNNs with global attention from ViTs, the precision of this model is increased in detecting forged signatures, improving security and robustness in biometric authentication systems.

[2] The paper "MobileNetV2: Inverted Residuals and Linear Bottlenecks" by Sandler et al. (2018) presents an improved version of the MobileNet architecture designed for efficient deep learning on mobile and embedded devices. MobileNetV2 introduces two key innovations: inverted residual blocks, which connect thin bottleneck layers with shortcut connections, and linear bottlenecks, which avoid non-linear activations in narrow layers to preserve information. These design choices make the network lightweight and fast while keeping a high level of accuracy, which makes it suitable for real-time applications with limited computational resources.

[3] The paper "Deep Residual Learning for Image Recognition" by He et al. (2016) introduces ResNet, which is an deep neural network for architecture that uses residual connections to solve the vanishing gradient problem in very deep networks. By allowing gradients to flow through shortcut paths, ResNet enables the training of extremely deep models, significantly improving image recognition performance.

[4] The paper "Image Splicing-Based Forgery Detection Using DWT and Edge Weighted Local Binary Patterns" by Siddiqi et al. (2021) presents a technique that combines Edge Weighted Local Binary Patterns (EW-LBP) for texture analysis and for feature extraction the Discrete Wavelet Transform (DWT) to identify picture splicing forgeries. The precision of forgery detection in manipulated photos is increased by this hybrid technique, which efficiently gathers both frequency and edge information.

[5] The paper "Vision Transformer (ViT): the value of an image 16x16 Words" by Dosovitskiy et al. (2020) propose the Vision Transformer (ViT), which applies Transformer architecture directly to sequences of image patches without convolutional layers. By leveraging global self-attention, ViTs capture long-range dependencies and achieve state-of-the-art performance on large-scale image classification tasks. Although computationally expensive, the model demonstrates that pure Transformer-based architectures can outperform CNNs when trained on sufficiently large datasets, influencing research in biometrics and signature verification.

III. METHODOLOGY

The proposed model is a deep learning-based signature verification system designed to distinguish between genuine and forged signatures with high accuracy. It leverages a hybrid architecture that combines the feature extraction power of Convolutional Neural Networks (CNNs)—specifically, ResNet-18 and MobileNetV2—with the global context modeling capabilities of a Vision Transformer (ViT). This hybrid approach enables the model to analyze both local and global features of handwritten signatures, thereby enhancing its classification precision.

CNNs form the backbone of the feature extraction process. These networks utilize convolutional layers to learn and detect key features such as strokes, curves, and spatial patterns from signature images. The hierarchical nature of CNNs allows the model to start with basic patterns (e.g., lines and edges) and progressively identify more complex structures (e.g., loops, pressure variations) through deeper layers. These features are captured in the form of feature maps, which represent the spatial locations and importance of detected features.

To reduce dimensionality and computational complexity, the CNN modules incorporate pooling layers—primarily max pooling—to retain the most prominent features while discarding irrelevant noise. These pooled features are then passed through fully connected layers where feature representations are flattened and mapped to output classes— real or fake signatures.

To further enhance performance, the model integrates a Vision Transformer. After extracting local features using CNNs, the transformer applies self-attention mechanisms to model long- range dependencies across the entire signature image. This allows the model to learn global relationships and refine classification decisions. The transformer's architecture includes components such as multi-head self-attention layers, layer normalization, and positional encodings, enabling it to understand spatial significance and complex variations in signature styles.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

The final layers of the model consist of dense (fully connected) layers activated by non- linear functions like Swish and Tanh, improving the model's ability to generalize across diverse signature datasets. A softmax layer at the end converts logits into probabilities, outputting the likelihood of a signature being real or forged.

The hybrid system is trained on benchmark datasets including CEDAR. Preprocessing steps such as resizing to 224x224, normalization, and augmentation (like jittering and flipping) are applied to ensure consistency and robustness. This combination of CNN and Transformer not only enhances verification accuracy but also reduces false acceptance and rejection rates, making it ideal for real-world applications like document authentication, mobile banking, and digital forensics.

The working methodology of this project is based on a hybrid deep learning approach for verifying handwritten signatures. The process follows several systematic steps from data ac- quisition to result display

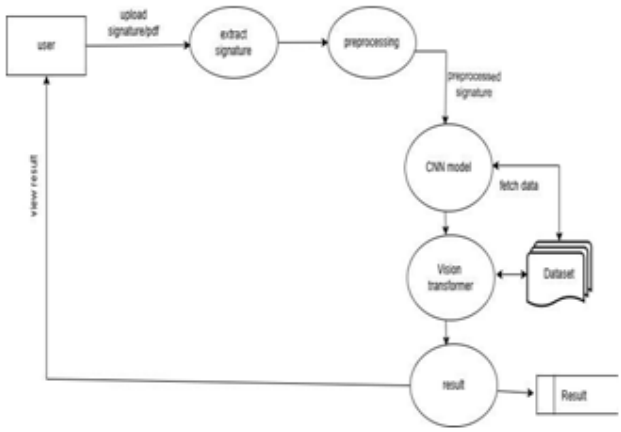

Fig 1 . Workflow Diagram

A. Data Collection

• The system uses signature images from datasets like CEDAR, categorized into genuine and forged.
• These images are stored in structured folders and are also optionally extracted from uploaded PDF documents.

B. Preprocessing

• Images are resized, converted to RGB format, and normalized using torchvision transforms.
• Invalid image formats are filtered out to ensure quality inputs.
• If uploaded in PDF format, signature images are extracted using the fitz (PyMuPDF) library and PIL.

C. Feature Extraction

• Convolutional Neural Networks (CNNs) are deep learning models designed for image- related tasks like classification, object detection, and signature verification. In signature verification, models such as ResNet-18 and MobileNetV2 are used to extract local features from input images. CNNs include convolutional layers (to detect edges, curves, and textures), pooling layers (to reduce dimensionality), activation functions (like Tanh and Swish to introduce non-linearity), and fully connected layers for final classification. These components help the network learn distinctive patterns in signatures, making CNNs highly effective for identifying subtle differences between genuine and forged signatures. Their strength lies in automatically learning detailed and hierarchical features, forming a reliable base for signature verification systems.

D. Vision Transformer Integration

• Vision Transformers (ViTs) offer a novel approach to image classification by using self-attention mechanisms instead of convolutional operations like CNNs. In ViTs, an image is divided into fixed-size patches, flattened, and projected

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

into embeddings, with positional encodings added to retain spatial information. These embeddings pass through transformer encoder layers that use multi-head self- attention and feed-forward networks to capture global relationships across the image. This allows ViTs to model the overall structure and long-range dependencies, which is especially useful in handling variations in writing styles for signature verification. While CNNs focus on local features, ViTs provide a broader context, making them effective for recognizing holistic patterns. In the hybrid model, ViTs are applied after CNNs to enhance the verification process by combining local detail with global understanding.

E. Classification

• A classifier head predicts whether a given signature is genuine (label 0) or forged (label 1) based on the ViT output.
• Cross-entropy loss is used during training, and performance is monitored using accuracy, precision, recall, and F1-score.

F. Prediction Interface

• A user uploads a signature through the React frontend.
• The image is sent to the Flask server for inference.
• The result ("Genuine" or "Forged") is returned and displayed on the web interface.

IV. RESULTS AND DISCUSSION

Several The hybrid signature verification system demonstrates promising results in improving identity authentication accuracy and addressing signature forgery challenges. Through its AI-powered architecture that combines ResNet-18 or MobileNetV2 with a Vision Transformer, the system is able to distinguish between genuine and forged signatures with high precision in real time.

The integrated feature extraction and classification pipeline streamlines the verification process by capturing both local and global features from signature images, enhancing the detection of skilled forgeries. A notable capability of the system is its ability to extract signatures directly from PDF documents and process them for verification, making it highly applicable to real-world use cases such as digital contracts, scanned forms, and official records.

In this work, a hybrid signature verification model was developed by integrating a ResNet-18 feature extractor with a Vision Transformer (ViT) to differentiate between authentic and counterfeit signatures. The model was trained on labeled signature data and evaluated using standard classification metrics. It achieved a loss of 0.0041, with an impressive accuracy of 99.89 percentage, indicating strong overall performance. A precision of 100 percentage and recall of 99 percentage reflect the model's effectiveness in minimizing both false positives and false negatives. The F1-score of 99.89 percentage further confirms a good balance between precision and recall. These findings suggest that the suggested model has a lot of promise for real-world applications .

V. CONCLUSION

This project developed a powerful system for verifying handwritten signatures using a combination of deep learning models specifically ResNet-18 or MobileNetV2 with a Vision Trans- former. By combining these models, the system was able to learn both small details and the overall structure of a signature, making it better at telling real signatures from fake ones. The model achieved high accuracy across several signature datasets, showing it works well for different writing styles and languages. This system can be useful for real-world applications like secure document verification and mobile banking, where signature-based authentication is needed.

REFERENCES

[1] Kaiming He, Shaoqing Ren, Xiangyu Zhang, and Jian Sun. Deep residual learning for image recognition. Proceedings of the IEEE Conference on Pattern Recognition and Computer Vision, pages 770–778, 2016.
[2] Muhammad Ishfaq, Ayesha Saadia, Faeiz M Alserhani, and Ammara Gul. Enhancing security: Infused hybrid vision transformer for signature verification. IEEE Access, 2024.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

[3] Rafael C. Gonzalez, Richard E. Woods. Digital Image Processing. Pearson, 4th edition, 2018.
[4] Sabri A. Mahmoud. Offline Signature Verification Using Graph matching. Pattern Recognition of Letters, 26(12):1770–1779, 2005.
[4] Hafiz Malik, Vir V. Phoha, and Rui Chen. Comparative study of off-line signature verification techniques. Pattern Recognition, 35(6):1329–1340, 2002.
[5] Vikas Bansal, Sanjay Kumar, and Ramesh Chandra. Offline Signature Verification Using CNN features. Procedia Computer Science, 167:2407–2416, 2020.
[6] Nalini K. Ratha, Ruud Bolle, and Sharath Pankanti. Automated signature verification. In developments in Biometrics, pages 137–148. Springer, 2007.
[7] Ahmed Soukupová and Jan Čech. Real-Time Eye Blink Detection Using Facial landmarks. In Twenty first Computer Vision Winter Workshop (CVWW), 2016. (Relevant for forgery detection / liveness).
[8] Lingxiao He, Wu Liu, Jia Jia, and Tao Mei. Forgery detection in images: A survey. ACM Computing Surveys (CSUR), 56(2):1–37, 2023.