Deep Learning-Based Detection of Skilled Signature Forgeries

Mrs. K. Menaka[1], Ms. S. Aarthi[2], Ms. K. Kaladevi[3], Ms. M. Kaviya[4]
[14]Assistant Professor, Dept of Computer Science and Engineering
[2, 3, 4]Dept of Computer Science and Engineering
[1, 2, 3, 4] Sree sowdambika college of Engineering, Virudhunagar, Tamilnadu, India.

Abstract- *Signature verification plays a critical role in authentication systems used in banking, legal documentation, and financial transactions. However, skilled signature forgeries pose a significant challenge for traditional verification techniques. This paper presents a deep learning-based approach for detecting skilled signature forgeries using a Convolutional Neural Network (CNN). The proposed system compares an original signature with a suspected signature and determines whether the signature is genuine or forged. The model is implemented using the PyTorch deep learning framework and deployed through a Flask-based web application. Image preprocessing techniques such as resizing, grayscale conversion, and normalization are applied before feeding the signatures into the CNN model. The system extracts discriminative features from signature images through multiple convolutional layers and predicts the authenticity of the signature with a confidence score. Experimental results demonstrate that the proposed approach effectively identifies forged signatures and provides reliable verification performance. The developed system can assist in preventing fraud in financial and authentication systems.*

Keywords: Deep Learning, Signature Forgery Detection, Convolutional Neural Network, Image Processing, Signature Verification

I. INTRODUCTION

- Signature verification is widely used as a method of personal authentication in banking systems, financial transactions, legal documentation, and identity verification. A handwritten signature is unique to each individual and serves as a common means of verifying identity. However, signatures can be easily forged, especially by skilled forgers who attempt to imitate the original signature closely.
- Traditional signature verification systems rely on manual inspection or basic image processing techniques. These approaches are often time-consuming and may produce inaccurate results when dealing with complex or skilled forgeries. As a result, there is a growing need for automated systems capable of detecting forged signatures.
- Recent advancements in **deep learning** have significantly improved the performance of image recognition systems. Convolutional Neural Networks (CNNs) are particularly effective in extracting complex features from images and have been successfully applied in various computer vision tasks. By learning unique patterns in handwritten signatures, CNN-based systems can distinguish between genuine and forged signatures more effectively.
- This research presents a **deep learning-based signature forgery detection system** designed to identify skilled signature forgeries. The proposed system compares an original signature with a suspected signature and determines whether the signature is genuine or forged. The system is implemented using the **PyTorch deep learning framework** and integrated into a web-based interface using **Flask**. Image preprocessing techniques such as resizing, grayscale conversion, and normalization are applied before the images are fed into the model.
- The developed system aims to provide a reliable and automated solution for signature verification that can assist in preventing fraud in banking, legal, and authentication systems.

II. LITERATURE REVIEW

- **Traditional Signature Verification Methods**
  Earlier systems used manual verification and basic image processing techniques to identify forged signatures. These methods relied on handcrafted features but often produced inaccurate results for skilled forgeries.
- **Feature-Based Approaches**
  Some studies used feature extraction techniques such as shape, texture, and stroke analysis to compare genuine and forged signatures. However, these methods required complex feature engineering.
- **Machine Learning-Based Methods**
  Machine learning algorithms such as Support Vector Machines (SVM) and Random Forest were used to

classify signature patterns. These methods improved automation but still depended on manually extracted features.

- **Deep Learning Approaches**
  Recent research focuses on deep learning models like Convolutional Neural Networks (CNNs) that automatically learn features from signature images. These approaches have shown better accuracy in detecting skilled signature forgeries.

III. EXISTING SYSTEM

Traditional signature verification systems mainly rely on manual verification or basic image processing techniques. In many cases, experts visually compare signatures to determine authenticity, which can be time-consuming and prone to human error. Some automated systems use simple feature extraction methods to analyze signature patterns, but they often struggle to detect skilled forgeries. These limitations reduce the accuracy and reliability of traditional signature verification methods.

IV. PROPOSED SYSTEM

The proposed system uses a deep learning approach to detect skilled signature forgeries. A Convolutional Neural Network (CNN) is used to analyze and extract important features from signature images. The system compares an original signature with a suspected signature and predicts whether it is genuine or forged. Image preprocessing techniques such as resizing, grayscale conversion, and normalization are applied before feeding the images into the model. The model is implemented using the PyTorch framework and integrated into a Flask-based web application to provide an easy-to-use interface for signature verification.

Avantages of the proposed system:

1) **Improved Accuracy** – The deep learning model can effectively detect skilled signature forgeries with better accuracy compared to traditional methods.
2) **Automation** – The system automatically verifies signatures, reducing the need for manual inspection.
3) **Fast Verification** – Signature comparison and prediction are performed quickly, saving time in authentication processes.
4) **User-Friendly Interface** – The Flask-based web application allows users to easily upload signatures and obtain verification results.

V. TOOLS AND TECHNOLOGIES USED

The development of the proposed signature forgery detection system involves several tools and technologies. Python is used as the main programming language for implementing the system. The deep learning model is developed using the PyTorch framework to build and train the Convolutional Neural Network (CNN). Flask is used to develop the web application that allows users to upload and verify signature images. Pillow (PIL) and NumPy are used for image processing and numerical operations. Additionally, HTML, CSS, and JavaScript are used to design the user interface of the web application.

VI. DATASET DESCRIPTION

- The dataset consists of genuine and forged signature images used for training and testing the model.
- It includes handwritten signatures from different individuals, containing both original and skilled forged signatures.
- The signature images are preprocessed by converting them into grayscale format to simplify feature extraction.
- The dataset is divided into training and testing sets to evaluate the performance of the CNN model.
- The dataset helps the model learn patterns and differences between genuine and forged signatures for accurate detection.

VII. METHODOLOGY

The proposed system follows several steps to detect signature forgeries. First, the user uploads two signature images: an original signature and a suspected signature. The images are then preprocessed by resizing, converting them to grayscale, and normalizing them to improve model performance. After preprocessing, the images are passed to a Convolutional Neural Network (CNN) model that extracts important features from the signatures. The model compares these features and predicts whether the signature is genuine or forged. Finally, the system displays the result along with a confidence score through a Flask-based web interface.

VIII. MODULES

The proposed system is divided into the following modules:

- **Image Upload Module**
  This module allows the user to upload two signature images: an original signature and a suspected signature through the web interface.
- **Image Preprocessing Module**

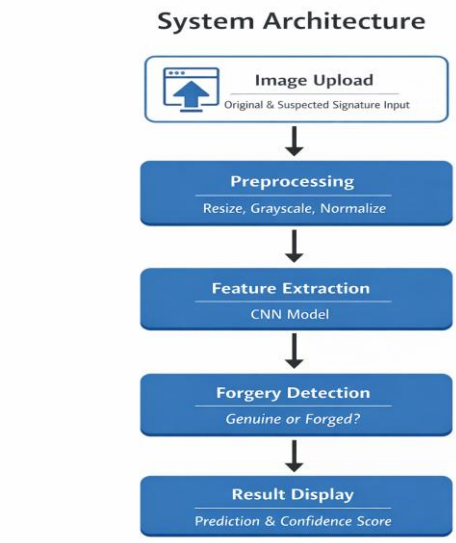
In this module, the uploaded images are resized, converted into grayscale, and normalized to improve the quality of the input data for the model.

- **Feature Extraction Module**
  The Convolutional Neural Network (CNN) extracts important features from the signature images to identify unique patterns**.**
- **Forgery Detection Module**
  The system compares the extracted features and predicts whether the signature is genuine or forged.
- **Result Display Module**
  The final prediction result along with the confidence score is displayed to the user through the web interface.

IX. SYSTEM ARCHITECTURE

The system architecture consists of several stages for detecting signature forgeries:

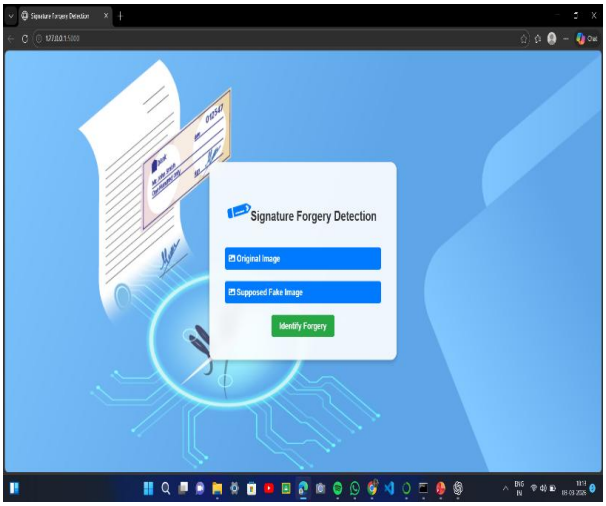
- Image Upload – The user uploads the original signature and the suspected signature through the web interface.
- Preprocessing – The images are resized, converted to grayscale, and normalized for better analysis.
- Feature Extraction – A Convolutional Neural Network (CNN) extracts important features from the signature images.
- Forgery Detection – The model compares the extracted features to determine whether the signature is genuine or forged.
- Result Display – The system displays the prediction result along with a confidence score to the user.

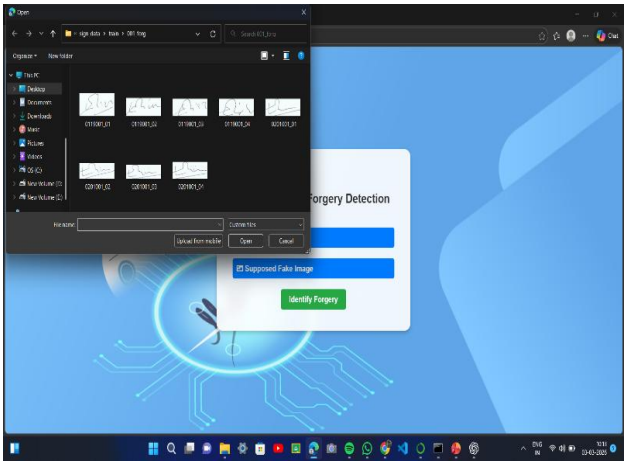


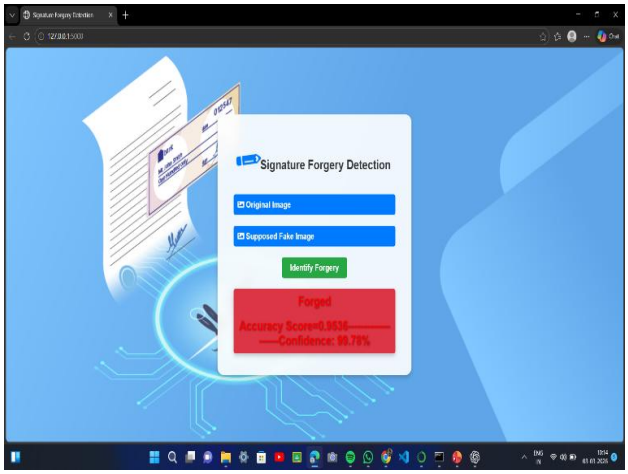
X. RESULTS AND OUTPUT

The proposed system was tested using multiple signature images to evaluate its performance. The user uploads an original signature and a suspected signature through the web interface. The system processes the images using the trained CNN model and predicts whether the signature is genuine or forged. The output result is displayed along with a confidence score. The screenshots below illustrate the input and output results of the system.

Then insert your screenshots with figure captions, for example:







XI. FUTURE SCOPE

The proposed system can be further improved by using larger and more diverse signature datasets to increase the accuracy of forgery detection. Advanced deep learning models such as ResNet or other deep neural networks can also be implemented to enhance feature extraction. The system can be extended to support real-time signature verification and integrated with mobile applications for easier accessibility. Additionally, the model can be deployed as an API service so that other applications, such as banking or authentication systems, can use the signature verification service.

XII. CONCLUSION

In this paper, a deep learning-based system for detecting skilled signature forgeries was presented. The proposed method uses a Convolutional Neural Network (CNN) to analyze signature images and identify whether a signature is genuine or forged. Image preprocessing techniques were applied to improve the performance of the model. The system was implemented using PyTorch and integrated with a Flask web application for easy user interaction. The results show that the proposed system can effectively assist in detecting signature forgeries and help improve authentication security in various applications.

REFERENCES

[1] L. Ni, J. Li, H. Xu, X. Wang, and J. Zhang, ‘‘Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection,’’ IEEE Trans. Computat. Social Syst., vol. 11, no. 2, pp. 1615–1630, Feb. 2024.

[2] W. Yu, Y. Wang, L. Liu, Y. An, B. Yuan, and J. Panneerselvam, ‘‘A multiperspective fraud detection method for multiparticipant e-commerce transactions,’’ IEEE Trans. Computat. Social Syst., vol. 11, no. 2, pp. 1564–1576, Feb. 2024.

[3] S. Lai, J. Wu, C. Ye, and Z. Ma, ‘‘UCF-PKS: Unforeseen consumer fraud detection with prior knowledge and semantic features,’’ IEEE Trans. Computat. Social Syst., vol. 11, no. 4, pp. 5454–5467, Aug. 2024

[4] S. Hafemann, L. Oliveira, and R. Sabourin, “Writer-independent feature learning for offline signature verification using deep convolutional neural networks,” *International Joint Conference on Neural Networks (IJCNN)*, 2016.

[5] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[6] D. Impedovo and G. Pirlo, “Automatic signature verification: The state of the art,” *IEEE Transactions on Systems, Man, and Cybernetics*, v l. 38, no. 5, pp. 609–635, 2008.

[7] R. K. L. Kennedy, F. Villanustre, T. M. Khoshgoftaar, and Z. Salekshahrezaee, ‘‘Synthesizing class labels for highly imbalanced credit card fraud detection data,’’ J. Big Data, vol. 11, no. 1, p. 38, Mar. 2024.

[8] G. Du, J. Zhang, M. Jiang, J. Long, Y. Lin, S. Li, and K. C. Tan, ‘‘Graphbased class-imbalance learning with label enhancement,’’ IEEE Trans. Neural Netw. Learn. Syst., vol. 34, no. 9, pp. 6081–6095, Sep. 20