Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338
Volume 14 Issue 01, 2025

Deep Learning-Based Automated Signature Verification for Fraud Detection

Prof. Pranali Faye[1], Ms. Arya Gawande[2], Ms. Chaitrali Raut[3], Ms. Deeksha Meshram[4], Ms. Khushi Jaiswal[5]

[1]Assistant Professor, Department of Computer Engineering, SCET, Nagpur, Maharashtra, India
[2,3,4,5] UG Student, Department of Computer Engineering, SCET, Nagpur, Maharashtra, India
[1]pranalifaye5739@gmail.com, 8668531298, [2]chaitraliraut2004@gmail.com, 9623432656,
[3]deekshameshram28@gmail.com, 7249705243, [4]khushdj001@gmail.com, 8010427557,
[5]aryagawande18@gmail.com, 7385340410

Peer Review Information

Submission: 07 Feb 2025
Revision: 16 Mar 2025
Acceptance: 18 April 2025

Keywords

Signature Detection
Signature Verification
Deep Learning
Fraud Prevention

Abstract

Every individual has a distinctive signature, making it a key element in personal identification and authentication for legal and financial transactions. However, manual signature verification is often labor-intensive and prone to errors, making it a challenge in combating document forgery and falsification.To address this, we have developed an automated online signature verification system utilizing Convolutional Neural Networks (CNNs), a powerful Deep Learning algorithm. The model is trained on over 100 signature samples per user, ensuring high accuracy in detecting forged signatures through extensive testing.The system is built using the Flask framework, combining HTML, CSS, and JavaScript for a user-friendly interface, while the backend integrates Python and a MySQL database for efficient data management and secure authentication. This approach provides a fast, accurate, and scalable solution for online signature verification, enhancing security in digital transactions.

Introduction

In the modern era of digital transactions, handwritten signatures continue to serve as a critical component of document authentication, playing a vital role in establishing identity and ensuring the validity of legal and financial agreements. However, traditional signature verification methods struggle to keep up with evolving threats posed by sophisticated forgery techniques and technological advancements.

This paper introduces "Deep Sign Verify," an advanced automated signature verification system that harnesses the power of Convolutional Neural Networks (CNNs) within the Flask framework. Designed to overcome the shortcomings of manual verification, Deep Sign Verify offers an intelligent, efficient, and scalable solution for authenticating signatures with greater precision. By leveraging deep learning, the system ensures high accuracy in detecting forgeries while maintaining ease of integration and usability.

This study presents an in-depth analysis of Deep Sign Verify's architecture, emphasizing the role of CNNs in feature extraction and classification, as well as the Flask-based implementation that enables a seamless user experience. Furthermore, the paper examines the testing methodology employed to evaluate the system's ability to differentiate between genuine and forged signatures. Through this exploration, it becomes clear that Deep Sign Verify has the potential to redefine document security, significantly reducing the risks associated with signature fraud in digital and physical transactions.

LITERATURE SURVEY

Malakappa Shirdhonkar [November 2010]"Off-Line Handwritten Signature Retrieval using Curvelet Transforms," ResearchGate. This paper introduces a novel approach for offline handwritten signature retrieval based on the Curve-let Transform. Many image processing applications require efficient image retrieval from large databases, making image indexing crucial for organized and accurate searches. This study focuses on a system designed for similarity retrieval within a database of handwritten signature images. The proposed method utilizes Curve let-based texture feature extraction to enhance retrieval accuracy. Experimental results demonstrate that the system effectively identifies signatures with high accuracy, even when portions of a signature are missing.

Suresh Pokharel [February 2020]"Deep Learning-Based Handwritten Signature," ResearchGate. This research explores a deep learning model using CNN architecture for signature verification. For experimental purposes, the feature extraction component of the GoogleNet model was utilized for transfer value computation, while the classification layer was retrained using backpropagation and transfer learning. The model was trained on a dataset containing 25 signature classes, each comprising 85 signature samples. After training, the model was tested using 15 signatures per class, achieving a mean testing precision of 85.2%, demonstrating its effectiveness in handwritten signature verification.

METHODOLOGY

The Deep Sign Verify system is designed to offer a comprehensive and secure solution for automated signature authentication. It incorporates a user authentication module that ensures safe storage of user credentials during registration and login. By leveraging the power of Convolutional Neural Networks (CNNs), the system enables users to compare two signature images—an original and a test signature—delivering real-time verification results through an intuitive web interface.

To maintain data integrity and security, the system integrates a MySQL database, allowing for efficient data management, future analysis, and system enhancements. DeepSignVerify prioritizes user experience by utilizing HTML, CSS, and JavaScript, ensuring a seamless and interactive interface. The CNN model undergoes extensive testing on a diverse dataset containing approximately 100 samples per signature, ensuring high accuracy in detecting forgeries.

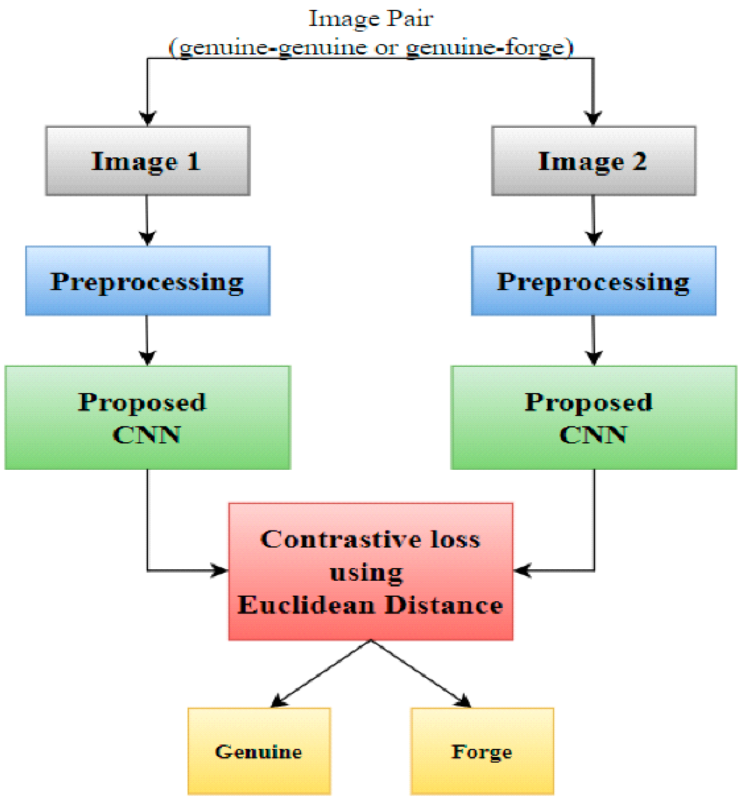


Figure 1. Block diagram of the proposed model.

System Modules & Functionality

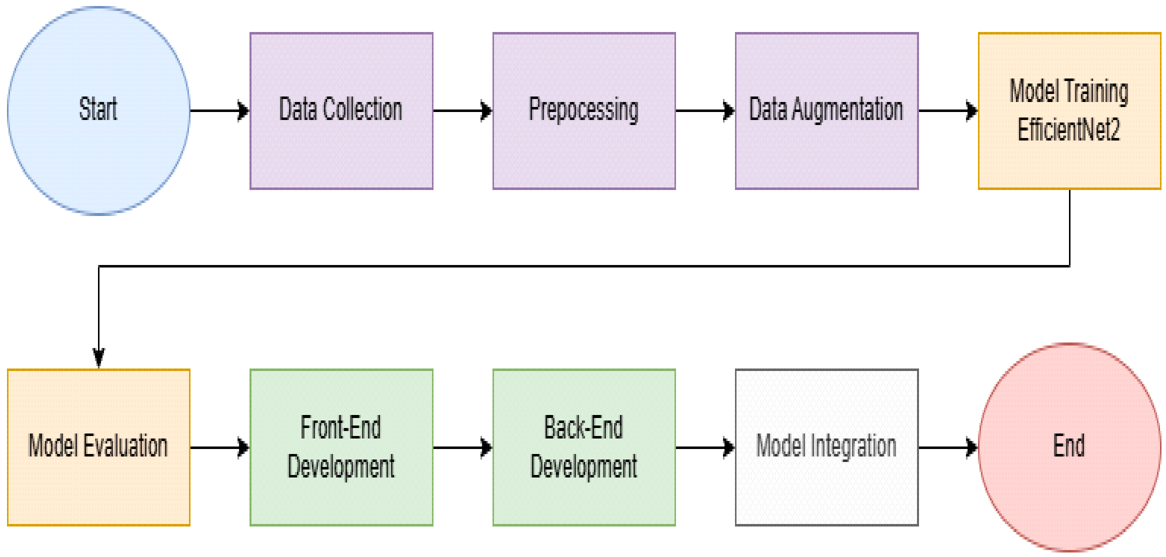
User Registration & Authentication

- Secure sign-up process requiring a username, email, and password.
- Login authentication for registered users, ensuring controlled access.

Signature Verification Process

- Image Upload: Users submit two signature images—one original and one for comparison.
- Processing & Analysis: The system preprocesses the images, extracts signature features using CNN, and performs classification.
- Result Display: Users are directed to a results page, where the system determines whether the signature is genuine or forged.

FLOWCHART



Dataset Description

To analyze our proposed signature verification approach, we considered three widely used benchmark databases: (1) GPDS Synthetic Signature Dataset (English), (2) BHSig260 (Hindi) signature corpus, and (3) BHSig260 (Bengali) signature corpus. Figure 2 shows some of the genuine and forged signatures from each dataset.

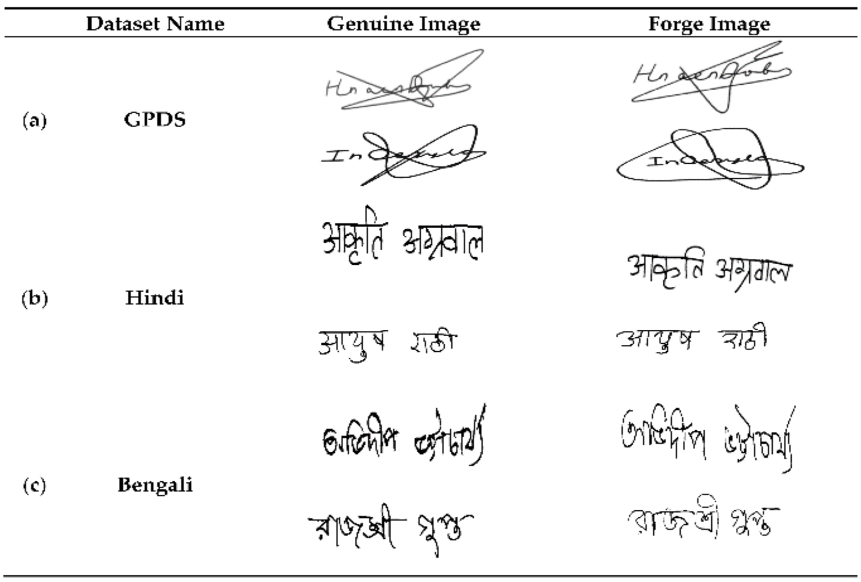
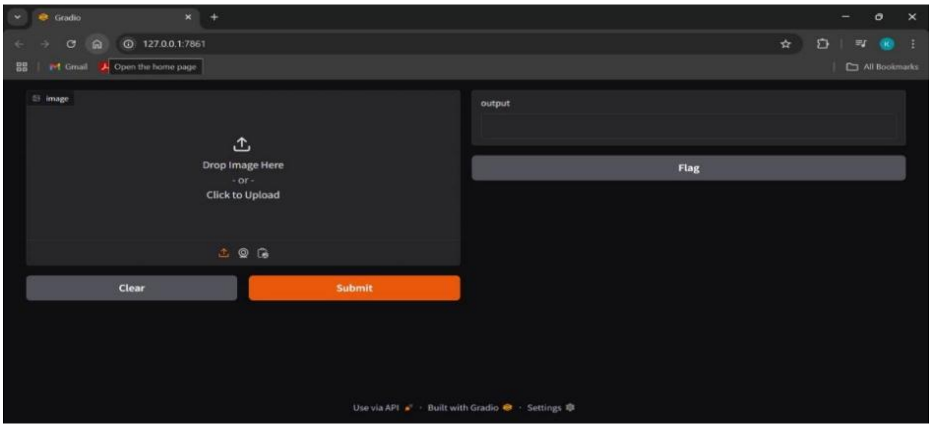
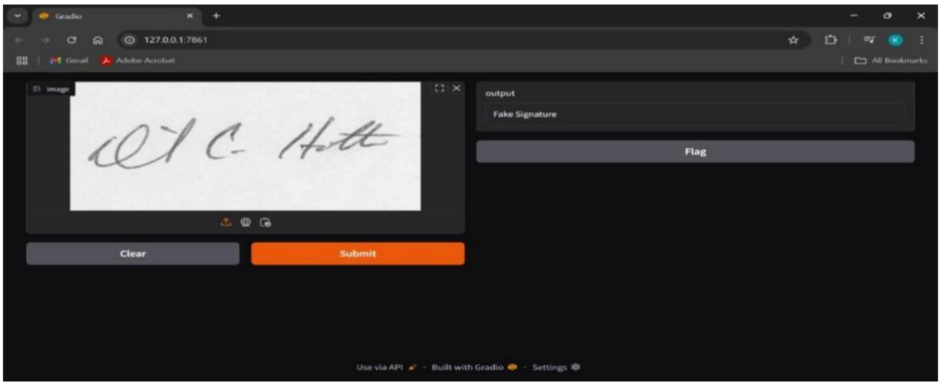


Figure 2. Sample genuine and forge images of datasets: (a) GPDS, (b) Hindi, and (c) Bengali.

RESULT





CONCLUSION

We have designed an intelligent signature fraud detection system powered by Convolutional Neural Networks (CNNs) to enhance the accuracy and reliability of signature authentication. Our algorithm efficiently identifies forgery patterns, delivering precise and consistent verification results. The system is built to ensure high accuracy, efficiency, and security, making it a robust solution for detecting fraudulent signatures.

To reinforce data protection and user trust, the system integrates a secure authentication module, safeguarding user credentials for seamless future logins and verifications. Through extensive testing on a diverse dataset of signature images, the model consistently demonstrates exceptional accuracy in distinguishing between genuine and forged signatures. DeepSignVerify sets a new standard in automated fraud detection, offering a fast, reliable, and secure approach to signature verification.

References

Elias N. Zois , Dimitrios, "A Comprehensive Study of Sparse Representation Techniques for Offline Signature Verification", 2637-6407 _c 2019 IEEE.

Victor L. F. Souza, Adriano L. I. Oliveira, "A writer-independent approach for offline signature verification using deep convolution neural networks features", 978- 1-5386-8023-0/18/$31.00 ©2018 IEEE DOI 10.1109/BRACIS.2018.00044.

Muhammed Mutlu Yapıcı, Adem Tekerek, "Convolutional Neural Network Based Offline Signature Verification Application", 978-1-7281-0472- 0/18/$31.00 ©2018 IEEE.

Elias N. Zois, Ilias Theodorakopoulos, "Parsimonious Coding and Verification of Offline Handwritten Signatures", Unrecognized Copyright Information DOI 10.1109/CVPRW.2017.92.

Wang Kai, Liu Jingzhi, Xu Shun, "Sparse representation classification for battlefield textual information", 978-1- 4673-8979-2/17/$31.00 ©2017 IEEE .

A. Hamadene and Y. Chibani, "One-Class Writer-Independent Off-line Signature Verification Using Feature Dissimilarity Thresholding", 1556-6013 (c) 2015 IEEE.

Shih-Chung, Hsu, Chung-Lin, "Object verification in two different views using sparse Representation", 978- 1- 4799-6100-9/15/$31.00 ©2015 IEEE.

Mrs. Madhuri R. Deore, Mrs. Shubhangi M. Handore, "A Survey on Offline Signature Recognition and Verification Schemes", 978-1-4799-7165-7/15/$31.00 ©2015 IEEE.

Amit Kishore Shukla, Pulkit Mohan, "Offline Signature Verification System Using Grid and Tree Based Feature Extraction", 978-1-4799-2900-9/14/$31.00 ©2014 IEEE.

Unnila A. Jain, Prof. Nitin N. Patil, "A Comparative Study of Various Methods for Offline Signature Verification", 978-1- 4799-2900-9/14/$31.00 ©2014 IEEE.

H. Firouzi, M. Babaie-Zadeh, A. Ghasemian Sahebi, C. Jutten, "A first step to convolutive sparse representation", 1-4244- 1484-9/08/$25.00 ©2008 IEEE.

H. Baltzakis and N. Papamarkos. A new signature verification technique based on a two-stage neural network classifier. Engineering applications of Artificial intelligence, 14(1):95–103, 12