Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

Dynamic forgery signature detection using CNN and PCA

[1]Ms. Deepali Narwade, [2]Omkar Pawale, [3] Mayur More, [4] Sachita Shelar

Department of Artificial Intelligence & Data Science Engineering, DYPCOEI, Varale, Pune, Maharashtra, India

Peer Review Information

Submission: 21 Feb 2025
Revision: 25 March 2025
Acceptance: 30 April 2025

Keywords

Forgery Detection
Dynamic Signature Data
CNN
PCA

Abstract

Signature verification plays a crucial role in identity authentication, with dynamic forgeries posing a significant threat to the reliability of security systems. This work presents a robust method for identifying forged signatures by leveraging the capabilities of Convolutional Neural Networks (CNNs) combined with Principal Component Analysis (PCA). CNNs are utilized to extract deep spatial features from signature images, effectively capturing intricate patterns and anomalies that often occur in forged samples.

To enhance computational efficiency and reduce feature dimensionality, PCA is applied to the extracted features. This technique retains essential information while streamlining the processing workload. The model is trained on a dataset comprising both authentic and forged signatures, enabling it to distinguish genuine signatures from those crafted by skilled forgers with improved precision.

Experimental analysis demonstrates that the integration of CNNs for feature extraction and PCA for optimization yields high accuracy while also reducing computational demands. This approach contributes to the development of reliable and scalable signature verification systems suitable for real-world applications.

INTRODUCTION

In recent years, Convolutional Neural Networks (CNNs) have emerged as powerful tools for image-based pattern recognition, offering exceptional accuracy in feature extraction and classification tasks. Their ability to automatically identify intricate patterns and subtle differences allows signature verification systems to effectively distinguish between genuine and forged signatures, reducing reliance on manually designed features.

However, one major drawback of CNNs is the generation of high-dimensional feature maps, which can lead to increased processing time and higher memory consumption, affecting the system's overall efficiency.

To address this challenge, Principal Component Analysis (PCA) is integrated into the verification pipeline. PCA helps reduce the dimensionality of the features while preserving the most important information. By eliminating redundant data and focusing on the most relevant characteristics, PCA significantly improves computational efficiency without compromising accuracy.

This combination of CNNs for deep feature extraction and PCA for optimization offers a balanced approach—enhancing both performance and resource management in signature verification systems. [1][2][3].

LITERATURE SURVEY

In the paper “Back to the Basics: Revisiting Out-of-Distribution Detection Baselines” by Johnson Kuan and Jonas Mueller, the authors explore straightforward methods for detecting out-ofdistribution (OOD) images that can be applied to any pre-trained classifier, relying solely on its predictions or learned representations. The study evaluates the OOD detection performance of various methods using ResNet-50 and Swin Transformer models. The findings suggest that methods based solely on model predictions can be easily surpassed by those that also incorporate learned representations. Based on their analysis, the authors advocate for a simple yet effective approach often overlooked in previous research: identifying OOD images by measuring the average distance to their K nearest neighbors in the classifier's representation space, specifically for images trained on in-distribution data [2].

In the paper "Handprinted Character and Online Signature Recognition Using Residual Convolutional Network: A Comparative Study" by Abdullah Basuhail, the effectiveness of residual convolutional networks (ResNets) in image and pattern recognition tasks is explored. The study highlights the strong performance of ResNets in handwriting recognition, particularly for handprinted characters and online signature verification. The paper references two prior studies that applied ResNet architectures to these tasks, achieving highly accurate results that rival current state-of-the-art methods [3].

J. Yang, K. Zhou, Y. Li, and Z. Liu, explores the challenge of identifying out-of-distribution (OOD) samples in machine learning systems. Detecting OOD inputs is essential for maintaining the reliability and robustness of these models, especially when they encounter data that differs significantly from their training distribution. This capability is particularly vital in safety-critical applications, where the presence of unfamiliar or abnormal inputs could lead to serious consequences if not properly handled [5].

S. Vaza, addressed the challenge of open-set recognition, an advanced form of classification that goes beyond traditional closed-set tasks. While closed-set classification assumes that all test samples belong to known classes, open-set recognition also requires the system to identify when a sample comes from an unknown or unseen class—commonly referred to as out-of-distribution data. The paper suggests that well-designed closed-set classifiers, with appropriate modifications, can be effectively adapted to perform open-set recognition tasks [6].

D. Y. Yeung, et. al. focused specifically on signature verification. This competition aimed to assess the effectiveness of different signature verification methods by providing a common platform with standardized datasets and evaluation criteria. The primary goal was to distinguish between genuine and forged signatures while promoting advancements and consistency in the development and comparison of verification techniques [9].

METHODOLOGY

Traditional retail systems often struggle to manage large volumes of customer data, resulting in poor inventory control and ineffective sales strategies. Similarly, signature forgery presents a serious threat to identity verification, particularly in financial services, legal documentation, and official recordkeeping.

Among the most challenging forms of forgery are dynamic forgeries, where individuals closely replicate genuine signatures. These are particularly hard to detect using conventional verification methods. Techniques that rely on manual inspection or hand-crafted feature-based algorithms frequently fall short in accurately distinguishing between authentic and forged signatures.

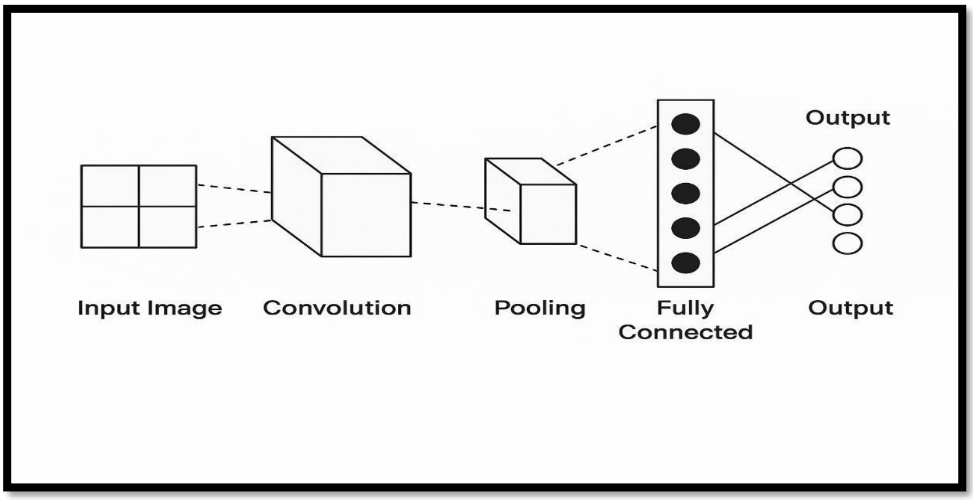


Figure 1. CNN Architecture

With advancements in deep learning, Convolutional Neural Networks (CNNs) have demonstrated exceptional performance in image-based pattern recognition tasks. These networks are widely used in computer vision, a branch of Artificial Intelligence that focuses on enabling machines to interpret and analyze visual data.

CNNs are designed to extract complex features from images, but they often generate highdimensional data, which can increase computational demands. To address this, Principal Component Analysis (PCA) is used to reduce the dimensionality of the feature space while preserving the most important information. This combination not only enhances processing efficiency but also maintains the accuracy of the model.

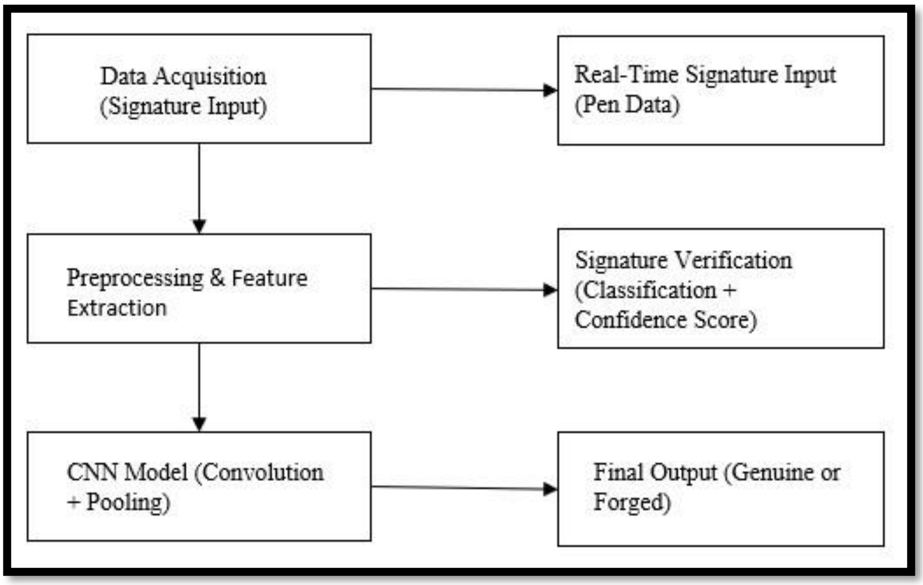

Data Acquisition (Signature Input)
Real-Time Signature Input (Pen Data)
Preprocessing & Feature Extraction
Signature Verification (Classification + Confidence Score)
CNN Model (Convolution + Pooling)
Final Output (Genuine or Forged)

Figure 2. System Architecture of Model

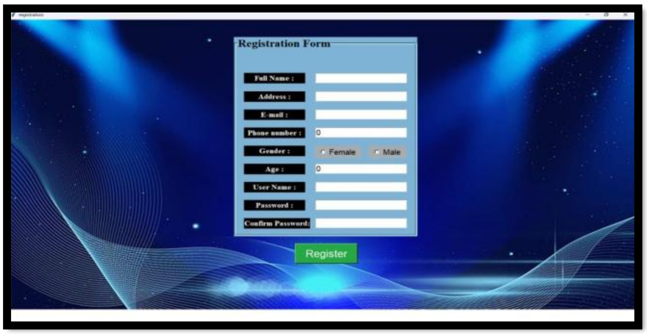
The primary motivation for this study is to develop an automated, reliable, and efficient signature verification system by combining Convolutional Neural Networks (CNNs) for deep feature extraction with Principal Component Analysis (PCA) for performance optimization. This approach aims to improve detection accuracy, reduce processing time, and strengthen protection against signature forgery in identity verification applications.

EXPERIMENTAL RESULTS

1. Title: The top says "Signature Detection System," indicating what the tool does.
2. Process Buttons: On the left, there are four buttons:
   - Select Image: To choose a signature image to analyze.
   - Image Process: To process the selected image (prepare it for analysis).
   - CNN Prediction: To use a Convolutional Neural Network (CNN), a type of AI, to predict if the signature is real or fake.
   - Exit: To close the program.

3. Image Stages: The three images in the middle show the steps of analyzing the signature:
- The first image is the original signature.
- The second image is after some processing (like adjusting brightness and contrast).
- The third image is a black-and-white version, likely used by the AI to make its prediction.

4. Result: The text at the bottom says:
- "Image Testing Completed..!!"
- "Selected Image Signature is Forged !!!" (meaning the signature is fake).
- "Execution Time: 9.755 seconds" (it took 9.755 seconds to finish the analysis).



Registration Form

Full Name :

Address :

E-mail :

Phone number : 0

Gender : ○ Female ○ Male

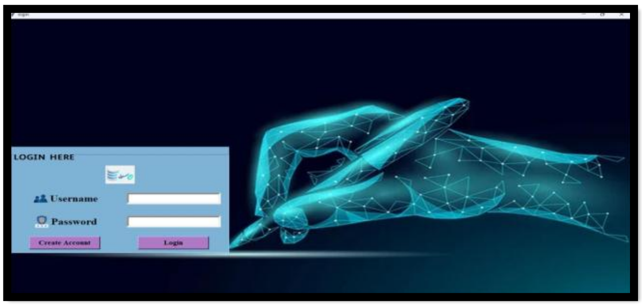
Age : 0

User Name :

Password :

Confirm Password:

Fig3. Registration Page



LOGIN HERE

Username

Password

Fig4. Login page

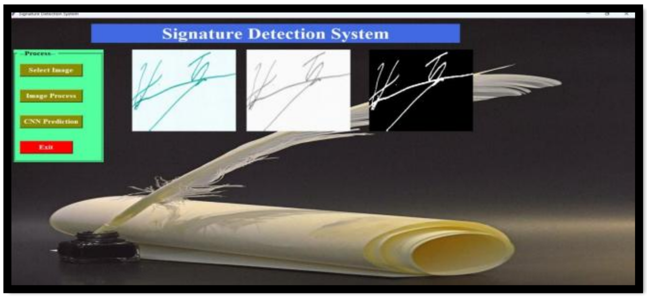


Fig 5. Image Processing

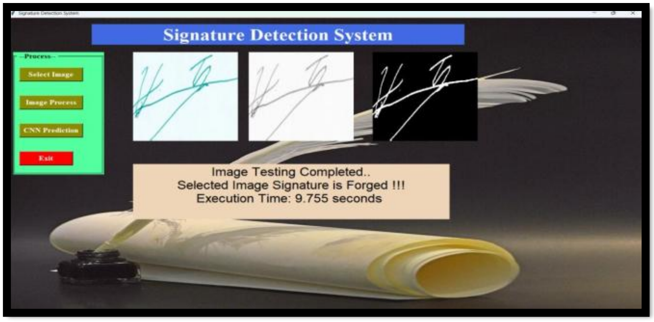


Image Testing Completed..
Selected Image Signature is Forged !!!
Execution Time: 9.755 seconds

Fig 6. Image Prediction

CONCLUSION

Signature verification is an evolving field with significant applications in areas such as banking, legal documentation, and identity verification. One of the key challenges is that a person's signature may vary slightly each time they sign, making it essential to develop a system that can accurately distinguish between genuine and forged signatures despite these inconsistencies.

In our approach, we focus on a single authentic signature due to the difficulty in obtaining multiple genuine samples. To train the system, we generate variations of this original signature by introducing minor changes. When the same user provides another signature later, the system compares it with the previously generated variants to determine its authenticity.

References

R. Averly and W.-L. Chao, "Unified out-of-distribution detection: A model-specific perspective,", Published in International

Conference on Computer Vision (ICCV 2023) 2023.

J. Kuan and J. Mueller, "Back to the basics: Revisiting out-of-distribution detection baselines," Published in International Conference on Computer Vision (ICCV 2022) 2022.

H. Oqaibi, A. Basuhail, and G. Abosamra, "Handprinted character and online signature recognition using residual convolutional network: A comparative study," in Proc. Int. Conf. Electr., Comput., Commun. Mechatronics Eng. (ICECCME), Oct. 2021, pp. 1–7.

G. Abosamra and H. Oqaibi, "Using residual networks and cosine distance-based K-NN algorithm to recognize on-line signatures," IEEE Access, vol. 9, pp. 54962–54977, 2021.

J. Yang, K. Zhou, Y. Li, and Z. Liu, "Generalized out-of-distribution detection: A survey," 2021, arXiv:2110.11334

S. Vaza, "Open-set recognition: A good closed-set classifier is all you need," OpenReview, 2021.

Bibi, S. Naz, and A. Rehman, "Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities," Multimedia Tools Appl., vol. 79, nos. 1–2, pp. 289–340, Jan. 2020.

X. Lu, Y. Fang, W. Kang, Z. Wang, and D. Freng, "SCUT-MMSIG: A multimodal online signature database," in Proc. 12th Chin. Conf. Biometric Recognit., Shenzhen, China, 2017, pp. 729–738.

D. Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, "SVC2004: First international signature verification competition," in Proc. 1st Int. Conf. Biometric Authentication, Hong Kong, 2004, pp. 16–22.