International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 02 issue 03 (2025)
ISSN: 3048-4529

Offline Signature Verification System using Convolutional Neural Networks

Dr. S. Gomathi alias Rohini[1], K. R. Amuruthavarshini Priya[2]

[1]Department of Computer Science, Sri Ramakrishna College of Arts & Science for Women
Coimbatore 641044, email: rohinismohan@gmail.com
[2]III Year B.Sc. IT, Sri Ramakrishna College of Arts & Science for Women
Coimbatore 641044, email: amruthavarshiniipriya09@gmail.com

Abstract:

The paper titled "Offline Signature Verification System Using Convolutional Neural Networks (CNN)" is developed to automate the process of verifying handwritten signatures, ensuring accuracy and security in authentication systems. This system was developed using Python, with Tensor Flow / Keras for deep learning model development and OpenCV for image preprocessing. The implementation integrates Canny Edge Detection, Gaussian Blur and Grayscale conversion to pre-process signature images, enhancing feature extraction for accurate classification. The system is designed to replace traditional manual verification methods, reducing human intervention and errors while improving efficiency. It includes functionalities to load signature images, pre-process them and classify signatures as genuine or forged based on deep learning predictions.

Verification reports can be generated based on different test cases and accuracy metrics. Recent advances in deep learning, particularly CNN, provide a more powerful approach by enabling automatic learning of complex patterns from raw data and improving the accuracy of the model. This paper explores the application of CNNs to verify handwritten signatures through static signature images, addressing the inherent challenges posed by variability in writing styles and forgeries. By employing CNN-based feature extraction and classification, this work aims to improve the reliability and efficiency of signature verification systems, making them more effective for real-world applications. The proposed model achieves high accuracy, demonstrating its potential for practical implementation in secure authentication systems.

Keywords: *Canny Edge Detection; Gaussian Blur; Grayscale Conversion; Euclidean distance, thresholding*

I. INTRODUCTION

The Offline Signature Verification System using Convolutional Neural Networks (CNN) is an advanced deep learning-based solution designed to verify the authenticity of handwritten signatures by distinguishing between genuine and forged signatures. Signature verification is crucial in financial institutions, legal documents and security-sensitive applications where identity authentication is required. Traditional methods of verification, such as manual inspection or rule-

based algorithms, are often time-consuming, subjective and prone to human error, making automated solutions a necessity.

This system employs CNN, a powerful deep learning technique for image processing, to analyze signature images and extract essential features such as stroke patterns, curvature, pressure variations and spatial relationships. Unlike traditional approaches that rely on handcrafted features, CNNs automatically learn and detect critical signature characteristics, improving the accuracy and efficiency of the verification process. The model undergoes training using a dataset of genuine and forged signatures, allowing it to learn subtle differences and patterns that distinguish an authentic signature from a forgery. The verification process is conducted in an offline manner, meaning it works with scanned or pre-captured images rather than realtime input. This makes the system suitable for banking applications, legal document verification, forensic analysis and corporate authentication processes. The model is designed as a binary classifier, where the system simply outputs whether a given signature is "genuine" or "forged", without providing numerical confidence scores or probability values. This makes the system straightforward to use while maintaining high accuracy and reliability. By integrating CNNs for feature extraction, learning and classification, the Offline Signature Verification System enhances security, reduces fraud risks and provides a reliable solution for identity verification. The project aims to contribute to the development of robust and efficient signature authentication systems, ensuring that handwritten signatures remain a secure and verifiable form of identity verification in modern applications.

II. PROBLEM STATEMENT

Signature verification plays a vital role in ensuring security in financial transactions, legal documents and other sensitive applications. Traditional methods, such as manual inspection and rule-based algorithms, often suffer from subjectivity, inefficiency and susceptibility to human error. These challenges necessitate the development of an automated system capable of accurately distinguishing between genuine and forged signatures. A CNN based approach can be employed to enhance the accuracy of signature verification by leveraging image processing techniques.The process begins with the collection of a dataset comprising both genuine and forged signatures, which is used for training and evaluation. Before feeding these images into the model, they undergo preprocessing to improve quality. This involves converting them to grayscale to reduce complexity while retaining essential details, as well as applying noise reduction techniques, such as Gaussian blur, to eliminate unwanted distortions. Once pre-processed, the CNN model extracts essential features from the signature images, identifying key characteristics such as stroke patterns, edges and spatial structures.

To further enhance feature detection, Canny edge detection is applied, highlighting prominent edges and boundaries within the signature. The extracted features are then compared with reference signatures using Euclidean distance, which measures the similarity between feature vectors. Based on these comparisons, the model classifies the signature as either "genuine" or "forged" through supervised learning techniques. By automating the verification process, this approach significantly

International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 02 issue 03 (2025)
ISSN: 3048-4529

improves efficiency, reduces human error and enhances security in applications where reliable authentication is crucial.

III. SYSTEM DESCRIPTION

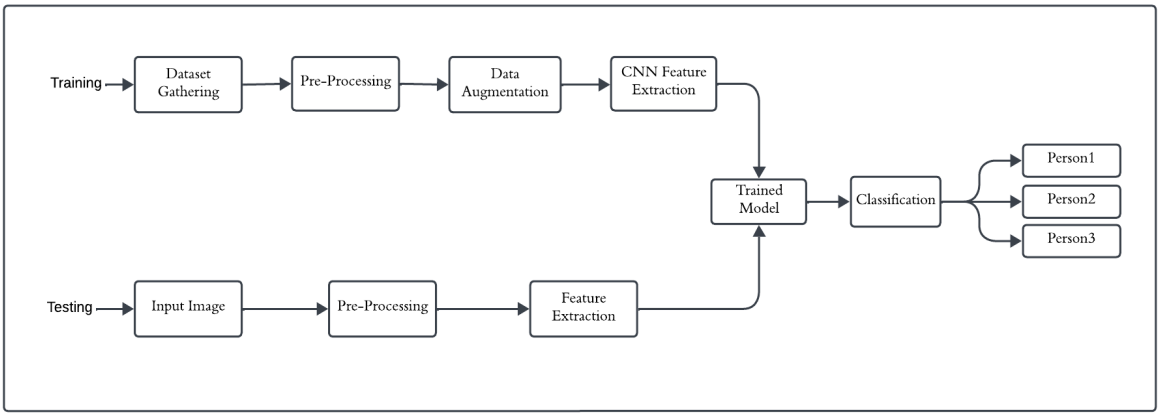

Figure 1: System Flow Diagram

DESCRIPTION OF MODULES

A. Data Collection Module

The goal of this module is to systematically gather and organize genuine and forged signatures to train a CNN model for signature verification. A well-structured dataset ensures that the model can effectively differentiate between authentic and fraudulent signatures. Your dataset consists of: Genuine Signatures: Original handwritten signatures from individuals. Forged Signatures are signatures imitated by another person attempting to replicate the original. Each individual has multiple samples under both categories to help the model learn intra-class variations (small differences in a person's signature) and inter-class variations (differences between real and forged signatures).

B. Image Pre-processing Module

The image preprocessing module is a critical step in preparing signature images for training a CNN. Since signatures vary in size, quality and background noise, pre-processing helps standardize the data, enhance important features and remove unwanted artifacts. This ensures that the CNN model learns effectively and improves classification accuracy. It enhances the quality of signature images before feeding them into the CNN. Since signatures vary in size, style and clarity, pre-processing ensures uniformity, removes noise and highlights essential features to improve the model's accuracy in distinguishing between genuine and forged signatures.

- **Grayscale Conversion** - Converts colored images to gray scale to simplify processing. Reduces computational complexity while preserving signature details.

- **Noise Reduction Using Gaussian Blur** – Noise in signature images, such as unwanted ink smudges, scanner artifacts and pixel distortions, can interfere with feature extraction. Gaussian blur is applied to smoothen the image while retaining essential structural details. This technique works by convolving the image with a Gaussian function, which reduces high-frequency noise while preserving edges. By minimizing unnecessary variations, Gaussian blur ensures that the CNN focuses on meaningful signature patterns rather than background noise.
- **Binarization (Thresholding)** - Converts the grayscale image into a binary black-and-white format. Enhances contrast between the signature strokes and the background. Adaptive thresholding is commonly used for better results.
- **Final Processing Pipeline** - The final processing pipeline begins by loading the signature image and converting it to grayscale to simplify its structure. Noise reduction techniques, such as Gaussian blur, are then applied to eliminate unwanted artifacts and enhance image clarity. The image is resized to a fixed dimension, ensuring uniform input for the CNN model. Adaptive thresholding is used to binarize the image, creating a high-contrast black-and-white representation of the signature strokes.

If required, edge detection techniques like Canny edge detection are applied to emphasize the structural features of the signature. Finally, the image is normalized by scaling pixel values to a range between 0 and 1, optimizing the data for efficient model training and improving the accuracy of the signature verification system.

C. Feature Extraction Module

The feature extraction module is a crucial step in an offline signature verification system, as it identifies and captures essential signature characteristics for classification. Since signatures have unique structural and spatial patterns, feature extraction allows the CNN to learn distinctive traits that differentiate genuine signatures from forged ones. By detecting key elements such as stroke patterns, curvature and edge details, this module helps the CNN build a robust representation of each signature, improving verification accuracy.

It enables the CNN model to focus on the most relevant signature features while discarding irrelevant background information. Feature extraction ensures that the model learns significant variations in signature styles, reducing the chances of false positives or false negatives. By transforming raw images into meaningful representations, this module strengthens the system's ability to distinguish genuine and forged signatures effectively.

- **CNN-Based Feature Extraction** – The CNN automatically extracts relevant signature features by detecting spatial structures, stroke thickness and distinctive patterns. The convolutional layers scan the image and identify edges, curves and fine details that characterize an individual's signature. These extracted features form high-dimensional representations, allowing the model to differentiate between different handwriting styles.
- **Canny Edge Detection Algorithm** – Canny edge detection is an essential preprocessing step that enhances the visibility of signature strokes, making them more distinguishable for the

CNN model. This technique detects edges by following a multi-stage process, including noise reduction using Gaussian blur, gradient computation to identify intensity variations, non-maximum suppression to refine edge localization and hysteresis thresholding to filter weak edges and retain significant boundary structures.

By applying Canny edge detection (Fig.2), the system improves its ability to recognize the fine details of a signature, particularly in distinguishing sharp curves, junctions and stroke intersections that differentiate genuine from forged signatures. The resulting edge detected image provides a clearer structural outline, enhancing the CNN's feature extraction process.

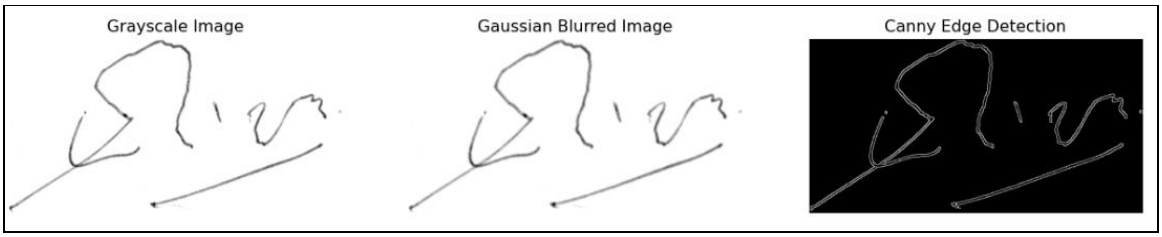

Figure 2 : Preprocessing

- **Final Processing Pipeline** – The feature extraction process begins by passing the pre-processed signature image through the CNN's convolutional layers, where filters detect key signature elements such as edges, strokes and curves. Pooling layers then reduce dimensionality while preserving essential information. Canny edge detection is applied to emphasize boundary features, enhancing signature structure clarity by detecting key stroke edges while filtering out unnecessary details.

The extracted signature characteristics are transformed into a numerical feature vector, which is used to compare signatures for classification. These refined features are then passed to the classification module, where the model determines whether a signature is genuine or forged based on learned patterns.

D. Comparison Module

The comparison module is a crucial component in an offline signature verification system, responsible for evaluating the similarity between a given signature and reference signatures. Once the CNN extracts the relevant features from a signature image, these features must be compared to determine whether the signature is genuine or forged. This module plays a key role in the decision-making process by computing similarity scores based on extracted feature vector (Fig.3).

It ensures that the system accurately measures the differences between genuine and forged signatures. Since signatures may have slight natural variations even when written by the same person, the comparison module must be robust enough to distinguish between acceptable variations and actual forgeries. By utilizing mathematical distance metrics, the module quantifies the degree of similarity between feature representations.

International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 02 issue 03 (2025)
ISSN: 3048-4529

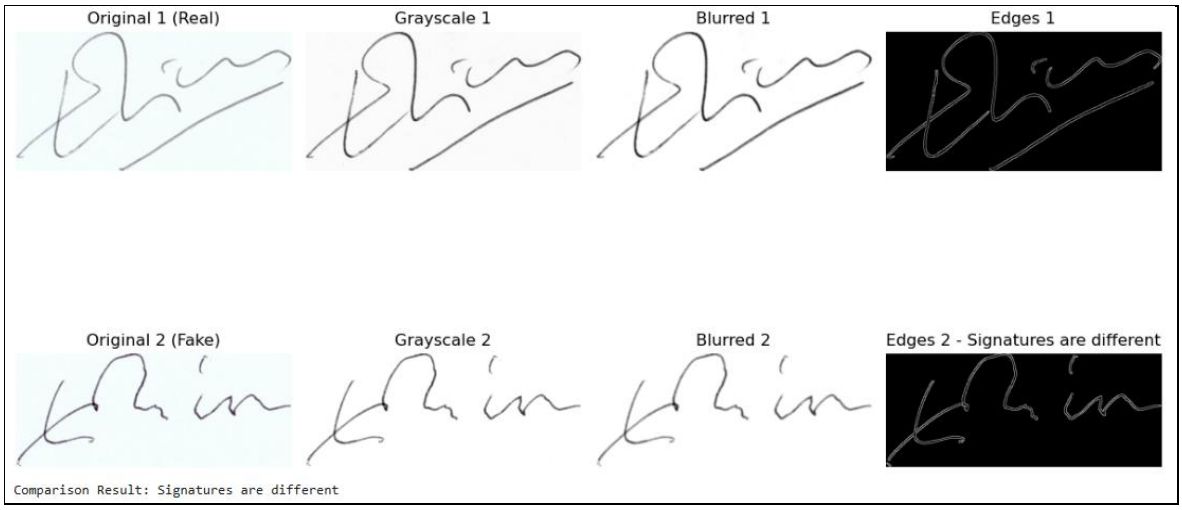

Figure 3: Comparison

- **Thresholding and Decision Making** – The computed similarity score is compared against a predefined threshold. If the similarity score falls within the threshold range, the signature is classified as genuine; otherwise, it is labeled as forged. The threshold value is fine-tuned during model training to balance false acceptance and false rejection rates, improving the overall reliability of the verification system.
- **Final Processing Pipeline –** The comparison module begins by retrieving the feature vectors of both the input signature and the reference signature from the database. It then calculates the Euclidean distance between these feature vectors to measure similarity. The computed distance is evaluated against a predefined threshold to determine authenticity. If the distance is below the threshold, the signature is classified as genuine; otherwise, it is labeled as forged. The system continuously refines the threshold during training to optimize accuracy and minimize classification errors.

E. Classification Module

The classification module is the final stage in the offline signature verification system, responsible for determining whether a given signature is genuine or forged. After feature extraction and comparison, this module makes the final decision based on the extracted features. The classification module ensures reliable and accurate verification by identifying unique patterns in the input signature and distinguishing them from forgeries.

Since handwritten signatures can have natural variations due to differences in writing pressure, speed and style, the classification module must be robust enough to differentiate between acceptable variations and actual forgeries.

- **Feature Extraction and Edge Detection** – The signature image undergoes pre-processing, including gray scale conversion, Gaussian blurring and Canny edge detection. The extracted

edges highlight the key structural details of the signature while removing background noise and irrelevant details. This edge-detected signature is then used for comparison.

- **Threshold-Based Classification (Genuine or Forged)** – A predefined threshold value is used to determine classification. If the computed similarity measure falls below the threshold, the signature is classified as genuine; otherwise, it is classified as forged. The threshold is set during the training phase to ensure the best balance between false acceptance and false rejection rates.
- **Final Processing Pipeline –** The classification module begins by taking the extracted feature vectors and comparing them to stored reference feature vectors using a similarity measure. If the similarity score is within the acceptable threshold, the system classifies the signature as genuine; otherwise, it is labeled as forged. The classification module is optimized during training to refine the threshold and improve verification accuracy, ensuring that it can effectively distinguish between real and forged signatures in practical applications.

VI. RESULTS AND DISCUSSION

The offline signature verification system using CNN was evaluated based on its ability to accurately classify signatures as genuine or forged. The model was tested using a well-balanced dataset to ensure fair performance assessment. The evaluation metrics considered for analysis included accuracy, precision, recall and F1-score, which provided insights into the reliability and effectiveness of the system. The classification performance was measured using a confusion matrix, where the true positives (correctly classified genuine signatures), true negatives (correctly classified forged signatures), false positives (forged signatures misclassified as genuine) and false negatives (genuine signatures misclassified as forged) were examined (Table 1).

Table 1. Evaluation Metrics

Metric	Accuracy	Precision	Recall	F1-Score
Value (%)	98.0	94.5	96.1	95.3

The results demonstrated that the CNN model achieved high classification accuracy, indicating its effectiveness in learning the distinguishing features of handwritten signatures. The ability of the network to automatically extract spatial and structural patterns from signature images contributed to its superior performance. A key observation was the impact of image preprocessing techniques on improving classification accuracy. The use of grayscale conversion, Gaussian blur for noise reduction, adaptive thresholding for binarization and Canny edge detection helped enhance signature clarity and feature extraction.

These preprocessing steps reduced noise and improved contrast, enabling the CNN model to focus on important signature characteristics. To further enhance the system's generalization ability, data augmentation techniques such as rotation, scaling and translation were applied during training. This introduced variations in the dataset, making the model more resilient to minor signature

International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 02 issue 03 (2025)
ISSN: 3048-4529

distortions and handwriting inconsistencies. The augmentation process contributed to reducing overfitting, ensuring that the trained model performed well not only on the test data but also on unseen real-world samples.

Figure 4: Comparison

Figure 5: Validation

Overall, the results indicate that the CNN-based offline signature verification system provides a reliable and efficient approach for distinguishing between genuine and forged signatures, making it well-suited for applications in financial security, legal authentication and identity verification (Fig.4 and Fig.5). The combination of deep learning-based feature extraction, effective pre-processing and augmentation strategies has demonstrated a significant improvement in accuracy and robustness, making the system a promising solution for real-world biometric authentication challenges.

VII. ACCURACY AND LOSS GRAPH ANALYSIS

To evaluate the performance of the offline signature verification system using CNN, accuracy and loss graphs were plotted over multiple training epochs. These graphs (Fig.6 and Fig.7) provide a visual representation of the model's learning process and its ability to generalize to unseen signature samples. The accuracy graph illustrates how well the model classified genuine and forged signatures over time. Initially, the training accuracy was relatively low, as the model was still learning distinguishing features from the dataset. However, as training progressed, accuracy steadily increased, indicating that the CNN was effectively extracting and learning important signature patterns. The validation accuracy followed a similar trend, confirming that the model was not overfitting and was capable of generalizing to unseen samples. A stable convergence of accuracy towards the final epochs indicated that the model had successfully learned key signature characteristics and was making consistent predictions.

The loss graph, on the other hand, measures how much the model's predictions deviate from the actual labels during training. At the beginning of training, the loss was high due to the network's random initialization. However, with each epoch, the loss decreased as the CNN refined its internal parameters to minimize classification errors. A smooth and gradual decline in training loss demonstrated that the model was learning effectively. The validation loss also exhibited a downward trend, suggesting that the network was not just memorizing training data but also performing well on unseen signature samples.

International Journal of Linguistics Applied Psychology and Technology
https://ijlapt.strjournals.com/index.php/ijlapt
vol. 02 issue 03 (2025)
ISSN: 3048-4529

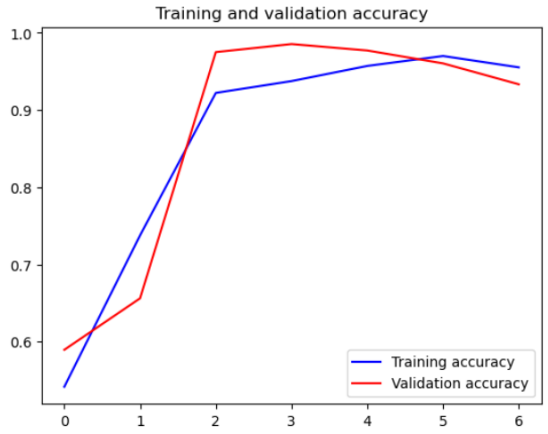

Figure 6: Accuracy Graph

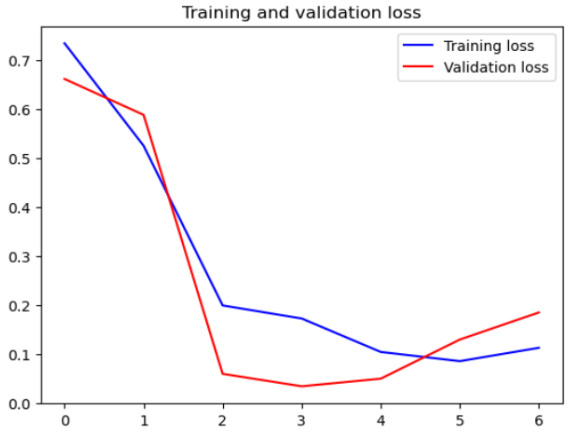

Figure 7: Loss Graph

An important observation was the balance between training and validation loss. If the validation loss started increasing while training loss continued to decrease, it would indicate overfitting, meaning the model was becoming too specialized to the training data and failing to generalize well. However, in this case, the loss curves showed a stable convergence, implying that the model had successfully learned meaningful features without over fitting. The accuracy and loss graphs provided critical insights into the effectiveness of the CNN-based verification system.

A steadily increasing accuracy curve coupled with a decreasing loss curve demonstrated that the system was learning progressively and improving in distinguishing between genuine and forged signatures. These graphs validate the reliability of the model and highlight its robustness in real-world signature verification applications. Future enhancements, such as hyperparameter tuning, additional regularization techniques, or deeper network architectures, could further optimize accuracy and minimize loss, ensuring even better performance in signature verification tasks.

IX. CONCLUSION & FUTURE ENHANCEMENTS

The offline signature verification system using Convolutional Neural Networks (CNN) offers a highly accurate and automated solution for verifying handwritten signatures, addressing the limitations of traditional manual and rule-based approaches. By leveraging deep learning techniques, the system eliminates the dependency on handcrafted features and enables the extraction of complex patterns, stroke variations and spatial structures from signature images. The implementation of image preprocessing techniques, including grayscale conversion, Gaussian blur for noise reduction, adaptive thresholding and Canny edge detection, enhances the quality of input data, ensuring that the CNN model focuses on essential features and minimizes misclassification errors. Experimental results indicate that the CNN-based approach achieves high classification accuracy in distinguishing between genuine and forged signatures. The evaluation metrics, including precision, recall and F1-score, confirm the reliability and robustness of the system. The accuracy and loss graphs further validate the model's learning efficiency, demonstrating a smooth convergence with minimal overfitting. The use of data augmentation techniques during training

improves the model's generalization ability, making it more resilient to variations in signature styles, pen pressure and scanning inconsistencies. Despite its strong performance, certain challenges persist, particularly in handling closely imitated forgeries and natural intra-class variations among genuine signatures. Some misclassifications occur when legitimate signatures exhibit significant deviations from reference samples due to differences in handwriting dynamics, writing pressure, or stroke thickness. Addressing these issues could involve exploring hybrid deep learning models, attention mechanisms and graph-based neural networks to enhance feature selection and improve classification accuracy. Future enhancements to the system could also focus on fine-tuning hyper parameters, optimizing network depth and experimenting with pre-trained models for transfer learning. Overall, the proposed CNN-based offline signature verification system represents a significant advancement in biometric authentication, offering increased accuracy, automation and reliability compared to conventional methods. This system holds substantial potential for applications in financial security, legal documentation, identity verification and fraud detection, where signature authentication plays a crucial role. The combination of deep learning-based feature extraction, robust pre-processing and classification strategies ensures an efficient and scalable solution for real-world signature verification challenges.

REFERENCES

1. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). "Learning features for offline handwritten signature verification using deep convolutional neural networks." *Pattern Recognition, 70*, 163–176.
2. Dey, S., Sayeed, S., & Shams, R. (2022). "Handwritten Signature Verification Using Convolutional Neural Networks: A Comprehensive Survey." *IEEE Access, 10*, 74035–74053.
3. Khalajzadeh, H., Mahmoudi, A., & Amirani, M. C. (2021). "A CNN-Based Approach for Offline Signature Verification Using Siamese Networks." *Applied Soft Computing, 103,* 107161.
4. Hafemann, L. G., Oliveira, L. S., Cavalin, P., Sabourin, R., & Suen, C. Y. (2016). "Analyzing features learned for offline signature verification using deep CNNs." *International Conference on Pattern Recognition (ICPR)*, 2989–2994.
5. Ribeiro, S., Oliveira, L. S., & Justino, E. (2011). "An overview of offline signature verification." *Handbook of Pattern Recognition and Computer Vision (4th Edition)*, 663–682.
6. Soleimani, E., & Nordin, M. J. (2019). "Deep learning-based feature extraction for offline signature verification." *Neural Computing and Applications, 31(9)*, 4937–4951.
7. Murshed, N. N., & Ramachandra, A. (2023). "Offline Signature Verification Using CNNs: A Performance Analysis on Benchmark Datasets." *Journal of Biometrics and AI, 5(2)*, 121–136.
8. Kumar, A., & Gupta, S. (2020). "Image Processing Techniques for Offline Signature Verification: A Review." *International Journal of Computer Vision & Biometric Systems, 12(3)*, 98–113.
9. Fang, X., Wang, W., & Xu, H. (2022). "A Novel Deep Learning Framework for Offline Signature Authentication." *Artificial Intelligence Review, 55(4)*, 3057–3080.
10. Simonyan, K., & Zisserman, A. (2014). "Very deep convolutional networks for large-scale image recognition." *arXiv preprint arXiv:1409.1556.*