IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Inkcheck & Auth: Signature Fraud Detection Using Deep Learning

Mr. M .VeeraBabu [1], Mrs. M. Madhuri [2], Madiki Belishia Rani [3], Devarakonda Vyasa Vamsi Vardhan [4], Kunche Rashmi [5]

[1, 2] Assistant Professor, [3, 4, 5] B.Tech Students,
Department of CSE (Artificial Intelligence),
Pragati Engineering College, ADB Road, Surampalem, Near Kakinada, East Godavari District, Andhra Pradesh, India 533437.

ABSTRACT:

Companies need signature fraud detection systems to prove valid signatures on official documents across various industries. Fraudulent signatures harm many different sectors by causing damage to finances and creating identity theft problems along with legal problems. Forensic experts who check signatures by hand take too long and produce results that depend on their own feelings and mistakes. Digital platforms need an automatic security system that accurately spots fake signatures because of growing document threats and rising electronic transactions. This project creates a system that uses CNNs to identify irregular signatures through deep learning technology. CNNs show remarkable results when classifying images which make them good at differentiating real signatures from frauds. The application runs on the web through a Flask framework and lets users add signature images for evaluation. The deep learning model needs processed images first which means the system prepares the images by adjusting their size and quality while removing noise for optimal performance. Our model works with diverse data to examine signature images and inform users if their input is an original or a fake. This system working model fits different industries including bank, law, business security, and official government use as they all depend on accurate signature verification. Using advanced machine learning helps our system identify signatures better which reduces document fraud risk and creates a reliable solution for organizations that need secure verification. The system can develop additional security features by adding electronic signature tracking alongside multiple security checks and block chain network connections.

KEYWORDS:

Fraudulent Signatures, Flask Framework, Machine Learning, Deep Learning Model, Block Chain.

1. INTRODUCTION

Secure paper documents require effective signature screening methods to protect against scams. Signatures written by hand serve as proof throughout different professional sectors including money banks banking groups law courts business enterprises and public administration entities. Manual signature verification no longer works properly because advanced technology has made it easier for fraudsters to create fake authentications. Traditional verification by expert analysts depends on their detailed assessment of handwriting strokes plus pressure changes and the rate of writing. These verification processes work properly for certain cases but take too long to complete and people making them can make errors. Also multiple experts might give opposite findings when examining the same signature. Manual signature verification becomes hard to use when organizations need to process many documents throughout the day.

Modern deep learning technologies replace manual signature verification works by achieving precise results with artificial intelligence. Due to their natural suitability with image classification CNNs become an excellent selection for automated signature recognition. CNN networks excel at finding signature patterns in handwritten digits to spot fake signatures with only small human interaction. When trained with large sets of signature details from real and duplicated sources CNNs can spot minute marking differences invisible to human vision.

The suggested system brings together Flask web application and a deep learning model to verify signatures. Users upload their signature pictures through the system which processes the input data to prepare it for analysis. The deep learning system checks signature images to tell whether they are authentic or fake while showing the results straight away to users. Our approach brings better results than standard methods while doing checks faster than before which makes the system work well in busy digital settings.

2. OBJECTIVES OF STUDY

This research project creates an AI system to check signature authenticity better and safer in financial, legal, and government settings. The AI system uses deep learning technology especially CNN networks to check handwritten signatures and replace manual processes that lead to mistakes and variation. Our research trains an effective model with genuine and forged signatures while creating an easy-to-use web verification tool and adapting to different deployment sizes. Our main objective is to develop a consistent and dependable way to stop signature fraud.

Main Objectives

1. Our system will apply deep learning to ensure exact recognition between real and fake signatures.
2. Automatic security tools protect banking providers and companies from security threats when they verify authenticated documents.
3. Our computer system should replace manual signature reviews through CNN-based image classification tools.
4. Our system provides online access to instant authentication feedback through a webbased application.
5. Trained system data should contain samples of different handwriting styles plus multiple stroke varieties and abnormal writing pressure levels to make it more effective.
6. The system should work with businesses that require advanced signature authentication solutions at scale.

3. BACKGROUND WORK

The most crucial phase in software development is the background work. Numerous writers conducted preliminary studies on this relevant topic, and we will consider key papers to expand our work. The field of signature verification has witnessed significant advancements, particularly with the integration of deep learning techniques. Below is a literature survey table summarizing recent research papers published in IEEE and Springer that focus on signature verification using deep learning methods.

Author(s) and Year	Paper Title	Findings and Problem Gap
Veena V. G, J. R. Jeba (2024)	Unveiling the Future of Signature Verification: Deep Learning Insights	Proposed a deep learning approach for offline signature verification using a novel method to enhance model's capacity to extract detailed and high-level semantic information from signature images. Achieved 97.39% accuracy, demonstrating the effectiveness of deep learning in signature verification.
Madhushree, Poornima G J, Roopa Banakar (2023)	Survey on Online Signature Verification Using Deep Learning Models	Introduced a time-aligned recurrent neural network (TARNN)-based method for online signature verification, capturing both static and dynamic aspects of signatures. Achieved state-of-the-art performance, highlighting the potential of deep learning in online signature verification.
Pharos University in Alexandria (2023)	Signature Verification Based on Deep Learning	Evaluated five pre-trained deep learning models on various datasets, with InceptionV3 achieving up to 100% accuracy. Demonstrated the potential of deep learning models in revolutionizing signature verification techniques.
Poddar, J., Parikh, V., Bharti, S. K. (2020)	Offline Signature Recognition and Forgery Detection using Deep Learning	Proposed methods for signature recognition and forgery detection using CNN, Crest-Trough method, SURF algorithm, and Harris corner detection. Achieved 90-94% accuracy for signature recognition and 85-89% for forgery detection, indicating the effectiveness of deep learning in these tasks.
Tuncer, T., Aydemir, E., Ozyurt, F., Dogan, S. (2022)	A Deep Feature Warehouse and Iterative MRMR Based Handwritten Signature Verification Method	Introduced a method combining deep feature extraction with iterative Minimum Redundancy Maximum Relevance (MRMR) for signature verification. Achieved high verification accuracy, demonstrating the effectiveness of feature selection in deep learning-based signature verification.
Li, G., Sato, H. (2020)	Handwritten Signature Authentication Using Smartwatch Motion Sensors	Utilized smartwatch motion sensors for signature authentication, achieving promising results. Highlighted the potential of

		wearable devices in enhancing signature verification methods.
Mukherjee, P., Viswanath, P. (2019)	A Lightweight and Hybrid Deep Learning Model Based Online Signature Verification	Developed a hybrid deep learning model for online signature verification, balancing accuracy and computational efficiency. Addressed the need for lightweight models in resource-constrained environments.
Ren, Y., Wang, C., Chen, Y., Chuah, M. C., Yang, J. (2019)	Signature Verification Using Critical Segments for Securing Mobile Transactions	Proposed a method focusing on critical segments of signatures for verification, enhancing security in mobile transactions. Addressed challenges in mobile-based signature verification.
Jain, A., Singh, S. K., Singh, K. P. (2020)	Handwritten Signature Verification Using Shallow Convolutional Neural Network	Utilized a shallow CNN for signature verification, achieving competitive accuracy with reduced computational complexity. Highlighted the trade-off between model depth and performance.
Xia, Z., Shi, T., Xiong, N. N., Sun, X., Jeon, B. (2018)	A Privacy-Preserving Handwritten Signature Verification Method Using Combinational Features and Secure kNN	Introduced a privacy-preserving method combining various features and secure k-Nearest Neighbors for signature verification. Addressed privacy concerns in signature authentication.

4. EXISTING SYSTEM

Manual signature verification previously required the examination of experts along with rule-based software programs for authenticity assessment. Signature verification under manual assessment depends on forensic analysts who compare handwriting features through stroke analysis with pressure testing to check signature authenticity. Usage of this widely practiced approach faces problems of subjectivity together with operational inefficiency. The challenges required solution through the implementation of rule-based software programs with defined algorithms for matching features. Botanical evaluation frequently encounters difficulties when diagnosing natural handwriting changes and modern forgery patterns because these algorithms rely on edge detection with geometric analysis in their evaluation process. Basic mismatches are detectable with this technique but it does not possess the capability to detect sophisticated forgeries.

Limitations of the Existing System

1. The process of manual verification through human operators generates unreliable authentication results because it produces inconsistent screening of samples especially when skilled forgers are involved.
2. The specialized signature examination procedure operates at a pace which contradicts the operational requirements of banking institutions and government departments and law enforcement agencies that process numerous documents.
3. The limitations of traditional systems include their inability to handle big document quantities efficiently which results in poor performance when applied to big-volume organizational transactions.
4. The rule-based system faces challenges to recognize new forgery techniques because its static parameters fail to evolve against evolving forgery methods.
5. Centralized signature template storage locations create a security hazard through vulnerable data systems which can lead to both cyberattacks and unauthorized access as well as potential data breaches.
6. The verification system for signatures requires the implementation of Convolutional Neural Networks (CNNs) under deep learning because these frameworks eliminate previous technical limits to enhance both accuracy and safety as well as scalability of verification procedures.

5. PROPOSED SYSTEM

The system proposes deep learning functionality to automate signature verification improving its process effectiveness. The current signature verification methods face challenges because experts perform manual verification and rule-based software requirements are limited in accuracy and efficiency. The system adopts Convolutional Neural Networks (CNNs) to address these challenges because these neural networks are known for their successful classification and recognition of images. The CNN model processes both authentic and fraudulent signatures in the training data so it acquires detailed knowledge about signature characteristics which helps it identify real signatures from forged ones effectively.

A Flask-based web application delivers the system which enables transparent signature verification through a user-friendly interface. The preprocessing step with OpenCV applies to signature images that utilize

three procedures: clarity enhancement, noise removal and dimensional normalization. The CNN model analyzes the refined image and provides real-time Genuine or Forgery classification without requiring any human involvement in the process.

Advantages of the Proposed System

1. **High Accuracy**

Through automatic operation the CNN model develops its own understanding of signature features that encompass pen pressure together with stroke consistency along with curvature characteristics. Deep learning models improve their accuracy through data processing since their operations lead to continuous enhancement as they analyze greater amounts of information.

2. Automation and Efficiency

The system eliminates manual verification tasks which decreases human mistakes. The authentication system enables real-time banking processes as well as digital contract and forensic applications to run much faster.

3. Scalability for Enterprise Applications

From a technical standpoint the system delivers comprehensive verification of thousands of documents which qualifies it for deployment at banks and government agencies along with multinational corporations.The solution merges seamlessly with all current authentication systems.

4. Continuous Learning and Adaptability

The model maintains the ability to receive updated training data for staying on top of new forgery methods.The addition of data augmentation techniques based on rotation and scaling and noise addition helps the system recognize handwriting from various styles better.

5. Security Enhancements and Data Protection

Features robust security measures such as encryption, secure session management, and role-based authentication. The cloud-based formula provides practical secure verification services from remote locations that defend sensitive data against cyber attacks.

Using deep learning along with automation and real-time processing capabilities enables the proposed system to handle established verification problems effectively. The system can be enhanced in the future with biometric authentication systems along with block chain digital signature implementation and real-time stylus-based signature capture to improve both document security and fraud prevention measures.

6. PROPOSED MODEL

Algorithm for Signature Fraud Detection System Using CNN

Step 1: Preprocessing

1. **Convert Image to Grayscale** → Remove color information to reduce complexity.
2. **Resize Image to 64×64 Pixels** → Ensure uniform input size and prevent distortions.
3. **Normalize Pixel Values** → Scale pixel values to [0,1] for better training convergence.

Step 2: Feature Extraction (CNN Layers)

1. **Apply Convolutional Filters** → Extract signature patterns such as strokes, edges, and curves.
2. **Use ReLU Activation Function** → Introduce non-linearity for better feature learning.
3. **Perform Max Pooling** → Reduce spatial dimensions while retaining key features.

Step 3: Classification

1. **Flatten Feature Maps** → Convert extracted features into a 1D vector.
2. **Pass Through Fully Connected Layers** → Learn deeper relationships between signature patterns.
3. **Apply Sigmoid Activation** → Generate probability scores for classification.

Step 4: Prediction and Decision Making

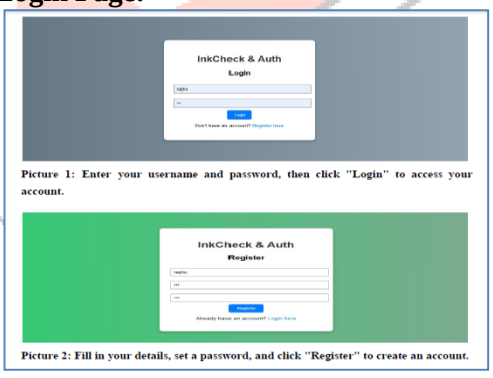
1. **Compare Probability Score Against Threshold (0.5)**
   - If score > **0.5** → Signature is **Genuine**.
   - If score ≤ **0.5** → Signature is **Forgery**.
2. **Output Confidence Score** → Indicate certainty of classification.

This streamlined CNN-based approach automates signature verification, improving accuracy, efficiency, and scalability.

7. EXPERIMENTAL RESULTS

In this project, we utilized Python as the programming language to develop the proposed application, which is executed on Uses Flask to serve dynamic HTML templates for user interaction.

Login Page:

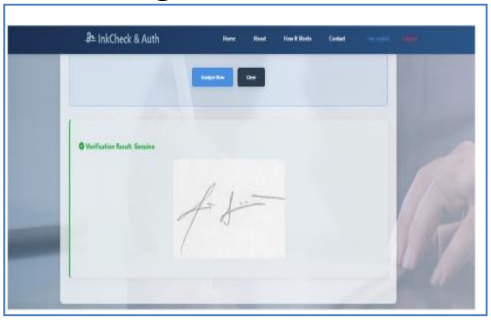


Picture 1: Enter your username and password, then click "Login" to access your account.

Picture 2: Fill in your details, set a password, and click "Register" to create an account.

Explanation: This interface defines admin login to access his dash board.

List of Users Page



Explanation: Upload a signature image and click "Analyze Now" to verify authenticity. If genuine, the result is displayed in green**.**

8. CONCLUSION & FUTURE WORK

The Signature Fraud Detection System effectively leverages deep learning techniques to enhance signature verification, offering a reliable and automated approach to fraud detection. By utilizing a Convolutional Neural Network (CNN) integrated with a Flask-based web application, the system ensures real-time verification, reducing reliance on error-prone manual methods. The model accurately analyzes stroke consistency, pen pressure, and spatial patterns, improving detection accuracy. Through comprehensive testing, the system has demonstrated high precision in distinguishing genuine signatures from forgeries. Its scalability and efficiency make it a valuable solution for banking, legal, and corporate applications, significantly enhancing document security and fraud prevention.

Future Work

Future enhancements can further improve the system's accuracy, security, and adaptability. Incorporating real-time signature analysis using stylus-based devices will enable dynamic fraud detection. Multi-factor authentication, integrating biometric techniques such as fingerprint and facial recognition, can enhance security. Cloud-based implementation will improve scalability, remote access, and data security. Supporting multiple languages and handwriting styles will expand global usability. Blockchain integration can provide immutable, tamper-proof authentication records, ensuring transparency. Additionally, developing a mobile application will allow users to verify signatures on the go, making the system more accessible for businesses, legal firms, and financial institutions.

9. REFERENCES

1. **Veena V. G. and J. R. Jeba**, "Unveiling the Future of Signature Verification: Deep Learning Insights," *International Journal of Intelligent Systems and Applications in Engineering*, 2024. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/5782.

2. **Madhushree, P. G. J., and R. Banakar**, "Survey on Online Signature Verification Using Deep Learning Models," *International Journal of Human-Computer Interaction*, 2023. [Online]. Available: https://milestoneresearch.in/JOURNALS/index.php/IJHCI/article/view/106

3. **Pharos University in Alexandria**, "Signature Verification Based on Deep Learning," *Alexandria Journal of Science and Technology*, 2023. [Online]. Available: https://ajst.journals.ekb.eg/article_329159.html

4. **J. Poddar, V. Parikh, and S. K. Bharti**, "Offline Signature Recognition and Forgery Detection using Deep Learning," *Procedia Computer Science*, vol. 167, pp. 1681-1690, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920305731

5. **T. Tuncer, E. Aydemir, F. Ozyurt, and S. Dogan**, "A Deep Feature Warehouse and Iterative MRMR Based Handwritten Signature Verification Method," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 6313-6332, 2022. [Online]. Available: https://link.springer.com/article/10.1007/s11042-021-11726-x

6. **G. Li and H. Sato**, "Handwritten Signature Authentication Using Smartwatch Motion Sensors," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3225-3238, 2020.

7. **P. Mukherjee and P. Viswanath**, "A Lightweight and Hybrid Deep Learning Model Based Online Signature Verification," *IEEE Access*, vol. 7, pp. 168293-168305, 2019.

8. **Y. Ren, C. Wang, Y. Chen, M. C. Chuah, and J. Yang**, "Signature Verification Using Critical Segments for Securing Mobile Transactions," *IEEE Transactions on Mobile Computing*, vol. 18, no. 11, pp. 2656-2668, Nov. 2019.

9. **A. Jain, S. K. Singh, and K. P. Singh**, "Handwritten Signature Verification Using Shallow Convolutional Neural Network," *International Journal of Computer Vision and Image Processing (IJCVIP)*, vol. 10, no. 3, pp. 1-12, 2020.

10. **Z. Xia, T. Shi, N. N. Xiong, X. Sun, and B. Jeon**, "A Privacy-Preserving Handwritten Signature Verification Method Using Combinational Features and Secure kNN," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 324-336, 2018.