Signature Fraud Detection with Using Deep Learning

First A. RAVINA N. TEMBHURNE
Prof. Rutuja Gautam J D College Engineering and Management Research

***Abstract*— Signature verification plays a critical role in banking transactions, legal documentation, and identity authentication systems. However, with the increasing sophistication of forgery techniques, traditional verification methods often fail to detect skilled forgeries. In this study, we propose a deep learning-based approach using Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and hybrid CNN-RNN models for automatic signature fraud detection. We evaluate the performance of these models on publicly available datasets such as CEDAR, GPDS, and BHSig260. Our experiments show that the hybrid CNN-RNN model achieves an accuracy of 94.7%, outperforming individual CNN and RNN models. We also discuss the challenges of real-world implementation, dataset limitations, and future improvements using transformer-based models.**

Keywords: Signature verification, fraud detection, deep learning, CNN, RNN, biometric authentication, image processing, forgery detection.

I. INTRODUCTION

1.1 Background: Handwritten signatures are one of the most widely used biometric traits for identity verification. Despite advancements in digital authentication, signatures remain a critical component in financial transactions, contracts, and government records. However, forged signatures are a major source of fraud, leading to economic losses and legal disputes.

Traditional signature verification methods rely on manual inspection or feature-based machine learning techniques, which struggle with complex forgery patterns. Deep learning, particularly CNNs and RNNs, has emerged as a powerful tool for image-based authentication, providing high accuracy and robustness in detecting fraudulent signatures.

1.2 Problem Statement

Existing signature verification systems suffer from:

- High false-positive and false-negative rates.
- Difficulty in detecting skilled forgeries, where an attacker mimics a genuine signature.
- Poor generalization across different handwriting styles.
- Computational inefficiency for real-time applications.

This research aims to address these challenges by developing a deep learning-based fraud detection model that effectively distinguishes between genuine and forged signatures.

1.3 Objectives

- Develop a robust signature fraud detection system using CNN, RNN, and hybrid deep learning architectures.
- Evaluate model performance on publicly available datasets.
- Identify real-world deployment challenges and propose solutions.

2. LITERATURE REVIEW

2.1 Traditional Signature Verification Techniques

Early approaches to signature verification relied on handcrafted feature extraction, including:

- Geometric Features: Stroke thickness, curvature, length-to-width ratio.
- Statistical Features: Pixel density, histogram of oriented gradients (HOG).
- Machine Learning Models: SVMs, Random Forests, and Hidden Markov Models (HMMs).

While these methods achieved reasonable accuracy, they required extensive feature engineering and struggled with high inter-person variability.

2.2 Deep Learning for Signature Verification

Deep learning eliminates the need for manual feature extraction, allowing models to learn representations directly from raw images.

- CNNs capture spatial patterns in static signature images.
- RNNs (LSTM/GRU) process sequential stroke information for dynamic signature verification.
- Hybrid CNN-RNN models leverage both spatial and temporal features, improving accuracy in skilled forgery detection.

2.3 Challenges in Existing Research

Despite promising results, deep learning models face limitations:

- Dataset Imbalance: Most datasets contain more genuine signatures than forgeries.
- Skilled Forgery Detection: High similarity between skilled forgeries and genuine signatures leads to misclassification.
- Computational Complexity: Large deep learning models require significant processing power, limiting real-time applications.

3. METHODOLOGY

3.1 Dataset Selection

We use multiple publicly available datasets:

- CEDAR: Contains 1,320 genuine and forged signatures.
- BHSig260: Includes Bengali and Hindi signatures with skilled forgeries.
- GPDS: One of the largest datasets, with over 24,000 signatures.

These datasets contain random forgeries (created without knowledge of the original signature) and skilled forgeries (closely replicated signatures).

3.2 Data Preprocessing

To enhance model performance, we apply:

- Grayscale conversion: Reducing computational complexity.
- Noise removal: Using Gaussian filters to remove artifacts.
- Data augmentation: Random rotation, scaling, and flipping to improve generalization.
- Normalization: Scaling pixel values between [0,1] for faster training.

3.3 Deep Learning Models

3.3.1 CNN Model

The CNN model extracts spatial features from signatures using:

- Conv layers: Identify edges, curves, and strokes.
- Max pooling layers: Reduce dimensionality.
- Fully connected layers: Perform classification.

3.3.2 RNN (LSTM) Model

The LSTM-based RNN model processes signature images as sequences of pixels, capturing handwriting stroke patterns.

3.3.3 Hybrid CNN-RNN Model

Combines CNN's feature extraction with LSTM's temporal analysis, improving accuracy for skilled forgeries.

3.4 Training and Evaluation

- Optimizer: Adam
- Loss Function: Binary Cross-Entropy
- Evaluation Metrics: Accuracy, Precision, Recall, F1-score, AUC-ROC
- Train-Test Split: 80%-20%

4. RESULTS AND DISCUSSION

4.1 Model Performance

MODEL	ACCURACY	PRECESION	RECALL	SCORE
CNN	92.10%	92.50%	90.80%	91.10%
RNN(LSTM)	88.30%	87.20%	86.90%	87.00%
CNN+RNN	94.70%	94.30%	93.80%	94.00%

The hybrid CNN-RNN model outperforms individual models due to its ability to analyze both spatial and sequential features.

4.2 Challenges and Observations

- Dataset Bias: Certain datasets have limited genuine signatures, affecting training balance.
- Skilled Forgeries: Even deep learning models misclassify some highly skilled forgeries.
- Processing Speed: Real-time signature verification still requires optimization for deployment.

4.3 Convolutional Neural Networks (CNNs)

CNNs are a class of deep learning models primarily used for image recognition tasks. They are designed to automatically detect spatial features in images by passing them through layers of convolutions, pooling, and fully connected layers.

- Feature Extraction: In the context of signature verification, CNNs are particularly useful because they can capture the various spatial attributes of a signature such as curves, slants, pressure points, and stroke patterns.
- Convolutional Layers: These layers apply filters (kernels) to the input image, extracting essential features like edges, lines, and textures, which are crucial for identifying the unique characteristics of a signature.
- Pooling Layers: Pooling reduces the dimensionality of the data, retaining important features while discarding less important information, which speeds up the learning process and prevents overfitting.
- Fully Connected Layers: After feature extraction, these layers classify the signature into genuine or forged by combining the learned features into a final decision.

2. Recurrent Neural Networks (RNNs)

Unlike CNNs that focus on spatial features, RNNs are designed to capture sequential patterns. This makes them ideal for tasks like signature verification, where the order of pen strokes matters.

- Sequential Modeling: RNNs process input data sequentially, which allows them to recognize the timing and dynamics of handwritten signatures. For example, a genuine signature's strokes follow a specific order, speed, and pressure, while forgeries may exhibit irregularities.
- LSTM (Long Short-Term Memory): LSTMs, a type of RNN, are particularly useful in avoiding the vanishing gradient problem and are capable of learning long-term dependencies. They can capture temporal features in signature data, such as the way each stroke is drawn over time.

4.4. Hybrid CNN-RNN Models

Combining CNNs and RNNs leverages the strengths of both architectures. The CNN layers extract the spatial features from the signature image, while the RNN layers model the sequence of strokes and their temporal dependencies.

- Why Hybrid Models Work: CNNs excel at identifying visual features in an image, but handwriting signatures often contain dynamic features like stroke order, direction, and pressure that RNNs can model effectively. By combining both, hybrid models can achieve superior performance in distinguishing between genuine and forged signatures.

Example of Hybrid Workflow:

- CNN processes the image to extract high-level features like curves and edges.
- The output of the CNN is passed to an RNN that models the stroke sequence over time.

- A final classification layer combines the features from both CNN and RNN to classify the signature as genuine or forged.

4.5 Model Training and Evaluation

Training deep learning models for signature fraud detection typically involves:

- Loss Functions: Binary Cross-Entropy is commonly used for binary classification tasks, such as distinguishing between genuine and forged signatures.
- Optimizer: Adam optimizer is popular due to its efficiency in adjusting weights during training, especially in deep neural networks.
- Evaluation Metrics: Accuracy, precision, recall, and F1-score are used to assess the performance of the model, especially considering the class imbalance between genuine and forged signatures.

4.6 Real-World Applications and Challenges

While deep learning models have shown promising results, there are challenges when deploying them in real-world applications:

- Skilled Forgery Detection: Highly skilled forgeries often mimic the handwriting so closely that deep learning models may struggle to detect them.
- Dataset Imbalance: Most datasets used for training contain more genuine signatures than forged ones, which may bias the model. Techniques like data augmentation (e.g., rotating, flipping, or scaling images) can help balance the data.
- Computational Cost: Deep learning models, especially hybrid models, require significant computational resources. Optimizing models for real-time or mobile applications is an ongoing challenge.

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

This research demonstrates that deep learning significantly enhances signature fraud detection. The hybrid CNN-RNN model achieves 94.7% accuracy, outperforming traditional techniques.

Signature fraud detection through deep learning, specifically CNNs, RNNs, and hybrid models, has significantly improved the accuracy of automatic verification systems. These models excel at capturing both the static (spatial) and dynamic (temporal) features of signatures, providing better fraud detection capabilities than traditional methods. However, challenges remain in handling skilled forgeries and optimizing the models for real-world deployment. The future of this field may see further improvements with transformer-based models and one-shot learning, enabling systems to detect forgeries with even fewer training examples.

5.2 Future Work

- Transformer-based Models: Exploring Vision Transformers (ViTs) for signature verification.
- One-shot Learning: Implementing Siamese Networks for detecting unseen forgeries.
- Real-time Applications: Optimizing models for mobile and cloud-based signature authentication.

REFERENCE

[1] Hafemann, L., Sabourin, R., & Oliveira, L. (2017). "Offline Handwritten Signature Verification Using Deep Learning." *Pattern Recognition Letters*, 80, 70-77.
[2] Dey, S., & Abhishek, K. (2020). "Signature Verification Using Deep Learning Techniques." *International Journal of Biometrics*, 12(3), 205-221.
[3] Mohammed, L. A. (2012). "Feature-Based Methods for Signature Verification." *Journal of Forensic Sciences*, 57(4), 1015-1022.