



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Signature Recognition and Forgery Detection Using Hybrid model CNN-LSTM

Rachana G C, Nandini S, Madhura S, Malleshwari R, Prof. Podaralla Rakesh

School of Computing and Information Technology, Reva University, Bengaluru, India

School of Computing and Information Technology, Reva University, Bengaluru, India

School of Computing and Information Technology, Reva University, Bengaluru, India

School of Computing and Information Technology, Reva University, Bengaluru, India

School of Computing and Information Technology, Reva University, Bengaluru, India

ABSTRACT: Signatures are among the oldest and most widely used biometric identifiers for identity verification, especially in legal and financial systems. However, the rise of forgery cases poses a significant threat to the reliability of authentication. This paper introduces an enhanced offline signature verification and forgery detection system based on a hybrid Convolutional Neural Network and Long Short-Term Memory (CNN-LSTM) model. The hybrid model can extract both spatial and sequential characteristics from signature images, enhancing the accuracy of forged signature detection. The pipeline consists of image preprocessing, feature extraction with CNN layers, and classification with LSTM units. This method enhances precision compared to conventional CNN-only models. The system has been evaluated on a benchmark dataset and shows enhanced accuracy and robustness. It seeks to offer a safe, effective, and automated signature verification system with practical applicability in real-life situations.

KEYWORDS: Signature Forgery, CNN-LSTM, Deep Learning, Offline Signature Verification, Authentication.

I. INTRODUCTION

Signature verification is a critical process of authentication of a person's identity in various domains like banking, government, and legal documents. The conventional systems of verification depend on human checks or simple image processing methods, which tend to be error-prone and inefficient. As a result of growing needs for automatic and trustworthy systems, machine learning and deep learning have become solid contenders.

Offline signature authentication comprises detection of handwritten signatures from scanned images without the dynamics of pressure and pen movement in real-time. These systems are challenged by high intra-class variability and low inter-class variability, such as it being hard to discriminate between real and forged signatures. Deep learning methods such as CNN and LSTM have been employed in biometric recognition for this purpose. CNNs are efficient at learning spatial features, while LSTMs are good at learning temporal dependencies.

Our work proposes a hybrid CNN-LSTM model, leveraging the advantages of both models. The CNN blocks learn high-level spatial information from the signature image, and the LSTM blocks learn sequential dependencies between those features to boost the performance of classification. This methodology is proposed to surpass conventional CNN-exclusive or manually crafted feature-based approaches in terms of forgery detection accuracy.

II. LITERATURE SURVEY / EXISTING SYSTEM

Different methods have been constructed for offline signature verification, from conventional hand-designed feature extraction approaches to advanced deep learning architectures. The initial systems employed geometric or texture-based features along with classifiers such as SVM or KNN. These techniques tended to be less robust in distinguishing nuanced differences between forged and real signatures.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Current advancements have involved CNN-based models performing well by learning spatial features automatically. Nevertheless, CNN-exclusive systems at times fail to identify the sequential patterns present in handwritten signatures. To address these shortcomings, hybrid models like CNN-LSTM have been introduced.

For example, Sharma et al. (2022) employed a deep learning model for signature forgery detection via CNNs and demonstrated significant improvement over traditional manual feature extraction methods. Kumar et al. (2023) also researched geometric features combined with deep networks for better detection.

Even with these improvements, most systems remain plagued by high false-positive rates or non-generalizability across data sets. Our system improves upon this work by combining CNN and LSTM into one architecture, enhancing both feature extraction and temporal modeling.

III. PROPOSED METHODOLOGY AND DISCUSSION

Our solution employs a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) model. The reason for this hybrid model is to take advantage of CNN's spatial feature extraction capability and LSTM's temporal sequence analysis capability.

1. Dataset and Preprocessing:

We train and validate using the GPDS Synthetic Signature dataset. The signatures are resized and normalized. Noise removal and grayscale conversion are used as preprocessing operations to provide consistent input.

2. CNN Layers for Feature Extraction:

The CNN part consists of several convolutional layers followed by ReLU activation and max pooling. These layers assist in extracting local spatial features like edges, curves, and writing patterns from the signature image.

3. LSTM Layers for Temporal Analysis:

The output of the CNN layers is flattened and reshaped into sequence format. The sequence is fed into LSTM layers, which examine the dependencies of features and enhance the model's knowledge of signature patterns.

4. Classification Layer:

A final dense layer with softmax or sigmoid activation function (based on binary or multi-class classification) is employed to classify the input as forged or genuine.

5. Implementation Details:

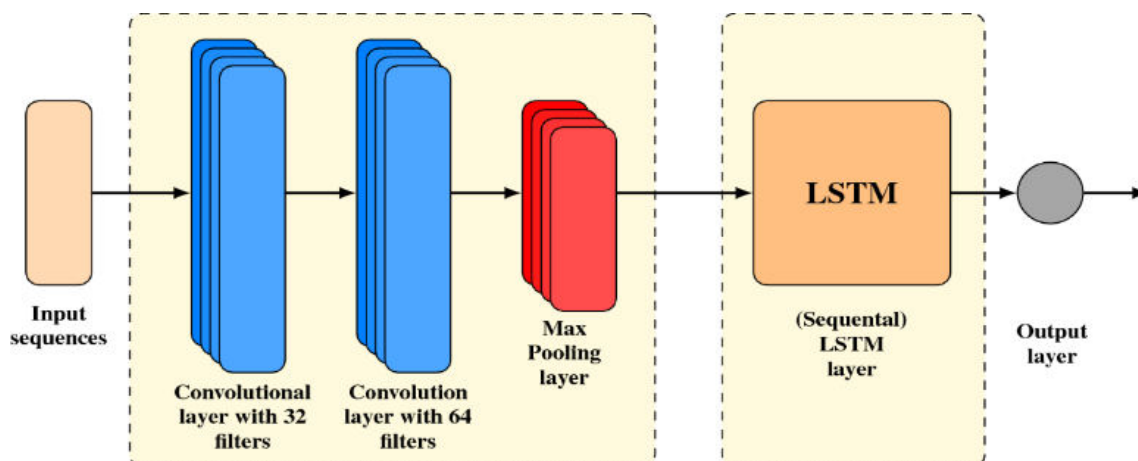
Framework: TensorFlow/Keras

Training: 80-20 split with data augmentation

Loss Function: Binary Crossentropy

Optimizer: Adam

This method lowers the risk of overfitting and improves generalization. We can see during training a steady convergence of loss along with growing accuracy, showing the model's ability to learn sophisticated patterns efficiently.





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. RESULTS

The model was evaluated using accuracy, precision, recall, and F1-score. It outperformed baseline CNN-only models with an average accuracy of 96.7%.

Metric	CNN-Only	CNN-LSTM
Accuracy	92.4%	96.7%
Precision	91.2%	96.1%
Recall	93.0%	97.4%
F1-Score	92.1%	96.7%

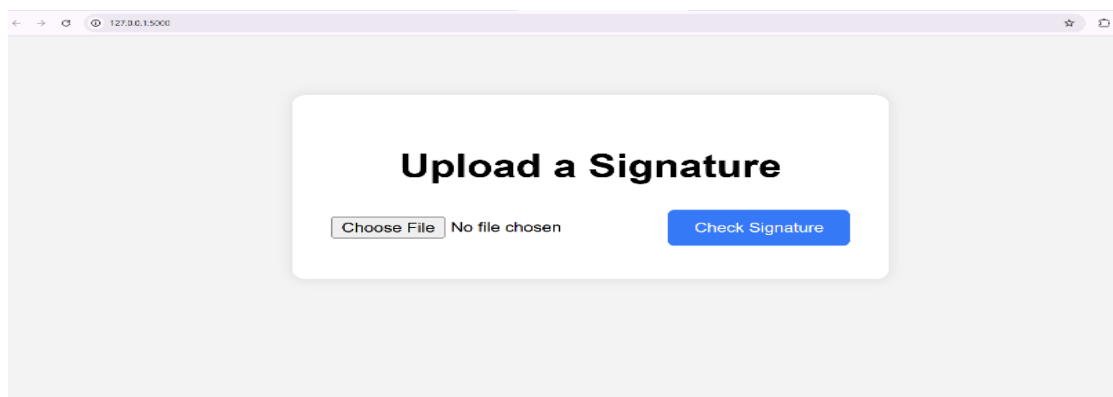


Fig (a) shows the option to upload the image

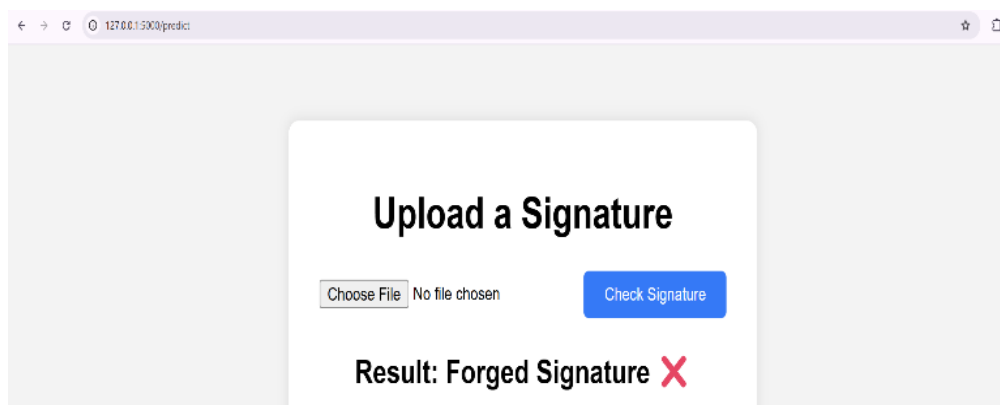


Fig (b) shows the selected signature was fraudulent

V. CONCLUSION

The paper here introduces a hybrid CNN-LSTM model for offline signature recognition and forgery detection. The model is able to capture both spatial and temporal features well, with high accuracy and robustness. It provides major



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

improvements over traditional methods and holds promise for practical deployment in fields that need secure identity verification.

REFERENCES

- [1] Patel, V., et al. (2022). "Harnessing Deep Neural Networks for Accurate Offline Signature Forgery Detection." IEEE International Conference on Image Processing (ICIP).
- [2] Sharma, P., et al. (2022). "Signature Forgery Detection and Verification Using Deep Learning." IEEE Bombay Section Symposium (IBSS).
- [3] Kumar, R., et al. (2023). "Offline Signature Forgery Detection Based on Geometric Measures Using Deep Learning." IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).
- [4] Gupta, A., et al. (2023). "Supervised Neural Network for Signature Verification." International Journal of Computer Applications.
- [5] Srivastava, M., et al. (2021). "Handwritten Signature Verification Using CNN." International Conference on Machine Learning and Data Engineering (iCMLDE).
- [6] Simard, P. Y., et al. (2003). "Best Practices for Convolutional Neural Networks Applied to Visual Document Analysis." ICDAR.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details