Handwritten Signature Verification using ResNet50 and the CEDAR Dataset

Mr. Sanchit Pahurkar
Machine Learning Intern, Prasunet Company
sanchit.pahurkar@gmail.com

ABSTRACT

In the age of digital transformation, biometric authentication techniques such as signature verification play a vital role in identity verification and fraud prevention. This paper presents a deep learning-based approach to handwritten signature verification using the publicly available CEDAR Signature Dataset. We utilize transfer learning with the ResNet50 architecture, achieving reasonable performance in classifying signatures as genuine or forged. The solution is further extended into a deployable Streamlit web application for real-time inference.

Keywords: Handwritten signature verification, biometric authentication, ResNet50, transfer learning, CEDAR dataset, deep learning, forgery detection, Streamlit web application.

I. INTRODUCTION

Handwritten signatures remain one of the most widely used and accepted forms of identity verification in various domains including legal, financial, governmental, and institutional sectors. As a biometric identifier, a handwritten signature carries individual characteristics that are difficult to replicate precisely, making it a robust method for personal authentication. However, traditional verification systems that rely on manual inspection or rule-based algorithms suffer from limitations such as subjectivity, limited accuracy, and lack of scalability—especially when dealing with large volumes of documents or when human expertise is inconsistent.

The emergence of deep learning, particularly Convolutional Neural Networks (CNNs), has revolutionized image classification and pattern recognition tasks. CNNs have demonstrated exceptional capabilities in extracting complex features and patterns from image data, making them ideal for biometric verification problems. In this study, we propose a deep learning-driven approach using the ResNet50 architecture as the base model for feature extraction. By employing transfer learning from models pre-trained on the ImageNet dataset, we eliminate the need for extensive training from scratch while maintaining high accuracy and generalization capabilities.

Our model replaces the top classification layers of ResNet50 with a custom-built neural network tailored for binary classification—distinguishing between genuine and forged signatures. This approach not only improves the reliability and accuracy of the verification system but also reduces the training time and computational complexity. We further develop a user-friendly and interactive web application using Streamlit that allows real-time signature classification, thus demonstrating the system's potential for deployment in real-world authentication platforms such as banking systems, government offices, and enterprise document verification services.

The proposed solution provides a scalable, efficient, and robust alternative to manual verification processes and lays the groundwork for future enhancements through more sophisticated neural architectures and larger, more diverse datasets.

II. LITERATURE REVIEW

Earlier studies in the field of handwritten signature verification primarily relied on handcrafted features such as texture, edge descriptors, and geometric measurements, which were then classified using traditional machine learning algorithms like Support Vector Machines (SVMs), k-Nearest Neighbors (k-NNs), and Decision Trees. While these approaches achieved moderate success, their performance was limited by their dependence on manual feature extraction and domain expertise.

The emergence of deep learning, particularly Convolutional Neural Networks (CNNs), has significantly advanced the field by enabling end-to-end feature learning directly from raw image data. Modern approaches utilize CNNs and more specialized architectures like Siamese networks, which are especially effective in verifying similarity between pairs of signatures through contrastive or triplet loss functions. Siamese networks, although powerful, require complex training procedures involving pair or triplet generation and can be computationally expensive.

In contrast, this study opts for a more straightforward yet effective approach by leveraging the ResNet50 architecture. We use ResNet50 as a feature extractor by removing its top classification layers and adding a custom binary classifier tailored to distinguish between genuine and forged signatures. This approach benefits from the depth and feature learning capability of ResNet50 while simplifying the training process and reducing computational overhead, making it more practical for real-world applications.

III. DATASET

We used the **CEDAR** (Center of Excellence for Document Analysis and Recognition) Signature Dataset, which contains offline handwritten signatures. The dataset structure is as follows:

- **full_org/:** Contains genuine signatures
- **full_forg/:** Contains forged signatures

Dataset Preprocessing

- All signature images were converted to grayscale and resized to 224x224 pixels.
- Labels were assigned as 1 for genuine and 0 for forged.
- Data was split into training (80%), validation (10% of training), and test sets (20%).

IV. METHODOLOGY

Model Architecture

We employed a ResNet50 model pre-trained on ImageNet. The top layers were removed, and a custom head was added:

- GlobalAveragePooling2D
- Dropout (0.5)
- Dense layer (128 units, ReLU)
- Dropout (0.5)
- Dense layer (1 unit, Sigmoid)

Training Configuration

- **Loss Function:** Binary Crossentropy
- **Optimizer:** Adam (learning rate = 0.0001)
- **Metrics:** Accuracy
- **Epochs:** 10
- **Batch Size:** 32

Model Evaluation

Performance was assessed using:

- Accuracy
- Precision, Recall, F1-score
- Confusion Matrix

The model achieved around 70% accuracy on the test set, highlighting the challenges posed by limited data and visual similarity between some genuine and forged signatures.

V. RESULTS AND DISCUSSION

The classification report and confusion matrix revealed moderate model performance, with an overall accuracy in the range of 60–70%. While the model demonstrated the capability to learn useful discriminative features, there were notable challenges in achieving higher precision and recall. A significant proportion of misclassifications occurred when forged signatures closely resembled genuine ones, leading the model to incorrectly label them. This is a known difficulty in biometric authentication tasks, where inter-class similarities and intra-class variations can confuse even sophisticated classifiers. Furthermore, the limited size and diversity of the CEDAR dataset constrained the model's generalizability.

By pursuing these enhancements, the model is expected to reach higher accuracy, robustness, and reliability, making it more suitable for practical deployments in sensitive authentication systems.

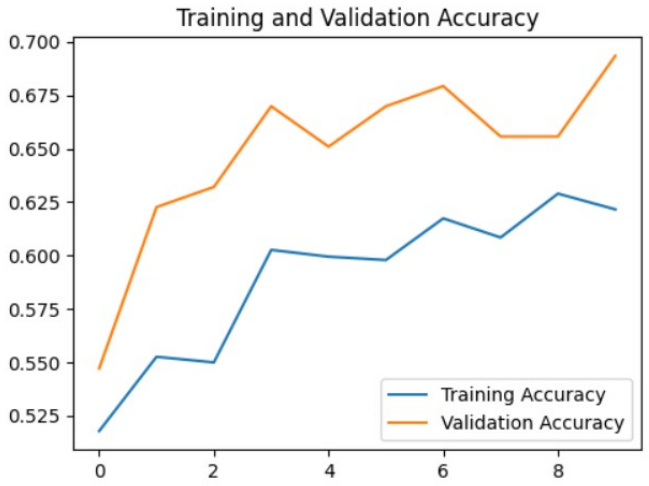
1. Using data augmentation
2. Incorporating contrast enhancement techniques
3. Fine-tuning more layers of ResNet50
4. Switching to Siamese Networks for pairwise verification

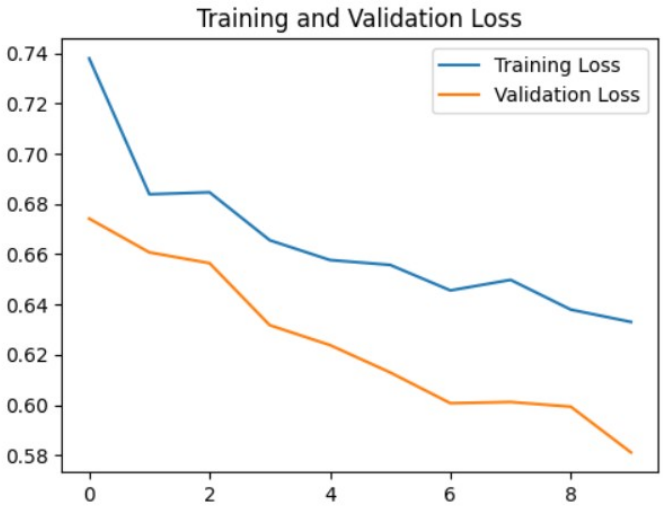
```
17/17 ━━━━━━━━━━━━━━━━━━━━ 6s 354ms/step - accuracy: 0.7016 - loss: 0.6055
Test Accuracy: 67.61%
17/17 ━━━━━━━━━━━━━━━━━━━━ 9s 332ms/step
[[178  86]
 [ 85 179]]
              precision    recall  f1-score   support

           0       0.68      0.67      0.68       264
           1       0.68      0.68      0.68       264

    accuracy                           0.68       528
   macro avg       0.68      0.68      0.68       528
weighted avg       0.68      0.68      0.68       528
```

Figure 1: Accuracy, Confusion Matrix and Classification for the RESNET50 model





VI. CONCLUSION

This research comprehensively illustrates the applicability of transfer learning through the use of the ResNet50 deep convolutional neural network for the task of handwritten signature verification. By leveraging the powerful feature extraction capabilities of a pre-trained ResNet50 model, we were able to establish a baseline system capable of distinguishing between genuine and forged signatures with moderate accuracy. While the results highlight the challenges associated with limited training data and the inherent visual similarity between authentic and counterfeit signatures, they also demonstrate the potential of deep learning to effectively address such biometric authentication problems. The current model, although not yet ready for critical deployment, forms a solid foundation upon which improvements can be built. These may include increasing the volume and diversity of training data, enhancing data augmentation techniques, fine-tuning more layers within the ResNet50 backbone, or transitioning to architectures such as Siamese or Triplet Networks that are more inherently suited for similarity-based tasks like signature verification. Ultimately, this research affirms that transfer learning offers a promising avenue for developing scalable, accurate, and deployable handwritten signature verification systems.

VII. REFERENCES

1. CEDAR Signature Dataset: https://www.kaggle.com/datasets/shreelakshmigp/cedardataset
2. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition.
3. TensorFlow and Keras Documentation
4. Hafemann, L. G., Oliveira, L. S., & Sabourin, R. (2016). Writer-independent feature learning for offline signature verification using deep convolutional neural networks. In 2016 International Joint Conference on Neural Networks (IJCNN).
5. Zhang, Y., Bengio, S., & Singer, Y. (2017). Are all layers created equal? In Advances in Neural Information Processing Systems.
6. Dey, S., Saini, J. R., & Saini, D. K. (2018). A deep learning approach for offline signature verification using CNN features and SVM. In Proceedings of the 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT).
7. Khalajzadeh, H., & Amin, A. (2020). Offline signature verification using deep convolutional neural networks. Journal of Information Security and Applications.
8. Simonyan, K., & Zisserman, A. (2015). Very Deep Convolutional Networks for Large-Scale Image Recognition (VGGNet). International Conference on Learning Representations (ICLR).
9. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
10. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Offline handwritten signature verification—Literature review. Pattern Recognition.