International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Deep Learning-Based Signature Authentication Using Siamese CNN

Dharmit Shah[1], ArjavPatni[2], Vinayak Shirahatti[3], Unnati Vyas [4], Prof. Dipak Kulkarni [5]

Dept. of Electronics & Telecommunication Engineering, K.J Somaiya School of Engineering

Abstract

This project introduces an efficient approach for real-time signature verification using a Siamese Convolutional Neural Network (CNN) combined with threshold optimization techniques. Our model is designed to automate the process of verifying handwritten signatures, offering a secure and reliable solution for applications in sectors like banking, legal documentation, and digital transactions. By utilizing Siamese CNN architecture, the model learns unique features of genuine signatures, enabling it to accurately distinguish them from forgeries.

The verification process begins by training the Siamese CNN on a labelled dataset of genuine and forged signature pairs. Each signature pair is processed through identical CNN branches to extract feature embedding's, and the Euclidean distance between these embedding's is calculated to measure similarity. An optimized threshold is applied to determine whether the signatures match, allowing for effective real-time classification.

This approach reduces the need for manual verification and provides a scalable solution for high-volume applications, enhancing security and user experience. While the model achieves promising accuracy in distinguishing genuine and forged signatures, future research could explore additional datasets and fine-tuning methods to further improve robustness and adaptability across diverse signature styles.

Keywords: Signature Verification, Siamese Convolutional, Neural Network (CNN), Forgery Detection, Threshold Optimization, Contrastive Loss Function

1. Introduction

In today's digital landscape, identity verification plays a crucial role in ensuring security, particularly in sectors such as banking, legal documentation, and online transactions. Handwritten signatures continue to be a widely accepted form of authentication, yet traditional manual verification methods are time-consuming, inconsistent, and prone to human error. As the reliance on digital transactions increases, the risk of forgery and fraud also rises, emphasizing the need for an automated, efficient, and reliable signature verification system.

Deep learning has emerged as a powerful tool in addressing such challenges, offering advanced solutions for pattern recognition and authentication tasks. Convolutional Neural Networks (CNNs), particu-

larly **Siamese CNNs**, have proven highly effective in distinguishing between genuine and forged signatures by comparing two images and evaluating their similarity. To further enhance accuracy, this research incorporates **threshold optimization**, which refines the decision-making process by determining the optimal similarity score threshold.

This study focuses on developing a **real-time signature verification system** utilizing a Siamese CNN model. The system is designed to automate the verification process, reducing dependence on manual inspection while improving accuracy and efficiency. By extracting unique signature features and optimizing classification thresholds, the proposed approach aims to create a robust and scalable solution applicable to various domains, including banking, digital contracts, and secure authentication systems.

2. Methodology

This study utilizes Siamese Convolutional Neural Network (CNN) architecture for real-time signature verification, addressing challenges such as signature variability and forgery. The Siamese network extracts features from signature pairs using shared CNN branches and compares them via Euclidean distance. Training is guided by a contrastive loss function to optimize similarity detection between genuine and forged signatures. A decision threshold, fine-tuned through validation data, is used to classify signatures accurately. The model was trained and tested using public datasets (ICDAR, CEDAR, Kaggle), with preprocessing steps including resizing, grayscale conversion, normalization, and augmentation. Hyper parameters such as learning rate, batch size, and dropout were optimized to prevent overfitting. The system's performance was evaluated using accuracy, precision, recall, F1-score, FAR, and FRR.

2.1 Problem Statement

With the rise of digital transactions, secure authentication has become critical. Signatures remain a widely used method of identity verification, but manual verification is prone to errors and inefficiency. Sophisticated forgeries and variations in handwriting styles further complicate the process. This study addresses these challenges using a **Siamese Convolutional Neural Network (CNN)** with **threshold optimization** for real-time signature verification.

2.2 Siamese CNN Architecture

A Siamese network consists of two identical CNN branches that share weights, ensuring the same feature extraction process for both input images. The model learns a similarity function that differentiates genuine from forged signatures.

2.2.1 Convolutional Neural Networks (CNNs)

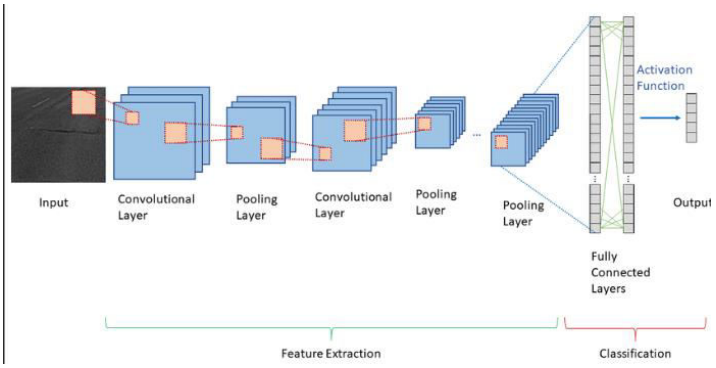

Fig. 1. CNN architecture for feature extraction and classification using convolutional, pooling, and fully connected layers

CNNs extract key features from signatures, such as curves and edges, which are critical for distinguishing between genuine and forged samples.

The convolution operation is given by:

$$Y = X * W + b$$

Where X is the input image, W is the kernel, and b is the bias term. The activation function **ReLU** is applied as:

$$f(x) = \max(0, x)$$

Max pooling is used for dimensionality reduction, preserving important information.

2.2.2 Siamese Network and Euclidean Distance Calculation

Feature embedding's are generated for both input images, denoted as f(X1) and f(X2) the similarity between the two embedding's is computed using **Euclidean distance**:

$$D = \sqrt{\sum_{i=1}^{n} (f(X_1)_i - f(X_2)_i)^2}$$

Where D determines the closeness of the signatures. A lower D indicates a higher probability of a match [2].

2.2.3 Contrastive Loss Function

To train the model, the **contrastive loss function** is used:

$$L = (1 - y)\frac{1}{2}D^2 + (y)\frac{1}{2}\max(0, m - D)^2$$

Where:

- y=0 for genuine pairs and y=1 for forged pairs,
- D is the Euclidean distance,
- M is a margin value ensuring sufficient separation between different classes.

2.3 Threshold Optimization

A **decision threshold** is set to classify signatures based on their similarity score. If D<Threshold, the signature is classified as **genuine**; otherwise, it is classified as **forged**. The threshold is tuned using validation data to minimize **false acceptance (FAR)** and **false rejection (FRR)** rates.

2.4 Data Collection and Preprocessing

Three publicly available signature datasets were used: **ICDAR, CEDAR, and Kaggle Signature Dataset**. The following pre-processing steps were applied:

- **Image resizing** to 128×128 pixels.
- **Grayscale conversion** to reduce complexity.
- **Normalization** to standardize pixel values.
- **Data augmentation** (rotation, translation, scaling) to improve generalization.

2.5 Training Procedure and Hyper parameter Tuning

The model was trained with:

- **Loss function**: Contrastive loss.
- **Optimizer**: Adam, learning rate 0.001.
- **Batch size**: 32.
- **Epochs**: Tuned based on validation performance.

The dataset was split into **70% training, 30% testing**. Overfitting was mitigated using **dropout** and **batch normalization** techniques.

2.6 Evaluation Metrics

Model performance was assessed using the following metrics:

- **Accuracy**: Measures overall correctness.
- **Precision (P)**: Correctly predicted genuine signatures.
- **Recall (R)**: Correctly identified actual genuine signatures.
- **F1-score**: Harmonic mean of precision and recall.
- **False Acceptance Rate (FAR)**: Incorrectly classifying a forged signature as genuine.
- **False Rejection Rate (FRR)**: Incorrectly classifying a genuine signature as forged.

$$F1 = 2 \times \frac{P \times R}{P + R}$$

Layer	Details	Output Size
Input	2 x 2	128 x 128 x 1
Conv Layer 1	128 filters, 7 x 7, Relu	60 x 60 x 64
Max Pooling	2 x 2	30 x 30 x 64
Conv Layer 2	128 filters, 4 x 4, ReLu	27 x 27 x 128
Max Pooling	2 x 2	13 x 13 x 128
Conv Layer 3	128 filters, 4 x 4, Relu	12 x 12 x 128
Max Pooling	2 x 2	6 x 6 x 128
Conv Layer 4	256 filters, 4 x 4, ReLu	5 x 5 x 256
Max Pooling	2 x 2	5 x 5 x 256
Flatten	-	6400
Fully Connected 1	4096 units, ReLU	4096
Fully Connected 2	256 units (embedding)	256

Table1. Architecture details of the Siamese CNN model, showing layer configurations, filter sizes, activation functions, and output dimensions

3. Result and Analysis

The Siamese CNN model was implemented using ICDAR, CEDAR, and Kaggle datasets, with pre-processing and augmentation applied to improve generalization. The model was trained using contrastive loss and optimized through hyper parameter tuning. Evaluation metrics demonstrated strong performance, achieving 80% accuracy and 100% precision, highlighting the model's ability to detect forgeries with minimal false positives. A threshold of 0.35 was found optimal for classification, ensuring reliable signature verification. Training graphs confirmed stable learning, and a user-friendly interface was developed for real-time application.

3.1 Implementation Overview

The implementation followed a structured approach, utilizing publicly available datasets such as ICDAR , CEDAR, and Kaggle for training and testing. Data pre-processing involved resizing images to 128×128 pixels, grayscale conversion, and augmentation (rotation, flipping) to enhance model generalization. A Siamese CNN model was employed to learn similarity metrics between signature pairs using contrastive loss. The model's performance was evaluated through accuracy, precision, recall, and F1-score, with a

threshold-based classification strategy. A user-friendly interface was developed for real-time verification.

3.2 Dataset Description

The datasets used include:

- **ICDAR Dataset**: Contains genuine and forged signatures used in signature verification competitions, widely referenced in document analysis research.
- **CEDAR Dataset**: A well-known dataset comprising balanced genuine and forged signature samples, commonly used in signature authentication studies.
- **Kaggle Signature Dataset**: A structured dataset that aids in improving model robustness and evaluation, providing a diverse set of handwritten signatures.

3.3 Siamese CNN Model Implementation

The Siamese CNN model consists of twin convolutional networks that process paired images to extract feature embedding's, followed by Euclidean distance computation for similarity measurement. Data augmentation techniques such as rotation and scaling were applied to enhance model generalization.

3.4 Training Procedure and Hyper parameter Selection

The model was trained using contrastive loss, Adam optimizer, batch size optimization, and learning rate tuning. The number of epochs was determined based on convergence behaviour. Loss and accuracy graphs provided insights into model performance during training, ensuring effective learning stabilization.

3.5 Evaluation Metrics

The model's performance was assessed using the following metrics:

- **Accuracy**: 80.00%
- **Precision**: 100.00%
- **Recall**: 66.67%
- **F1-score**: 80.00%
- **Success Ratio**: 100.00%
- **Rejection Ratio**: 33.33%

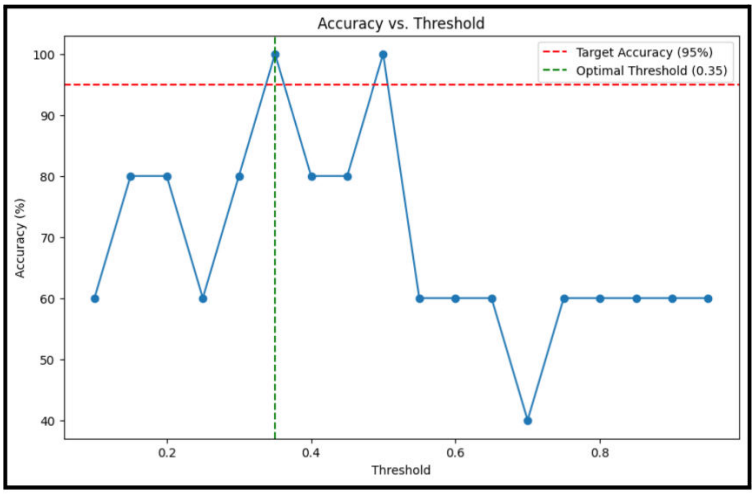

Fig. 2 illustrates the relationship between accuracy and threshold values, highlighting the optimal threshold (0.35) that achieves 100% accuracy while surpassing the 95% target accuracy

These results indicate the model's effectiveness in differentiating genuine and forged signatures, with a high precision rate ensuring minimal false positives.

3.6 Threshold Selection

A threshold-based classification approach was employed, optimizing the Euclidean distance cut-off for classification. The optimal threshold (0.35) achieved **100% accuracy**, ensuring a balance between true and false positives.

3.7 Experimental Results

Training graphs indicate a steady reduction in loss and improved accuracy, confirming effective learning. Initial fluctuations were observed due to weight adjustments in the early training stages, but stabilization was achieved over epochs. The final accuracy metrics validate the model's ability to differentiate genuine and forged signatures effectively.

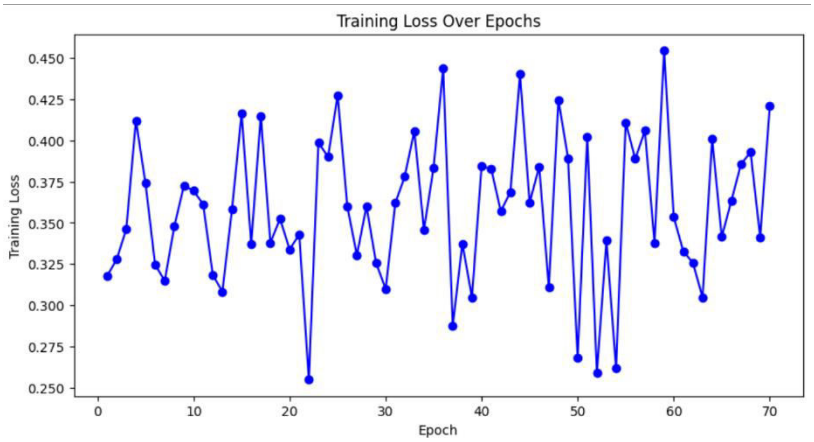

Fig. 3 illustrates the variation in training loss over epochs, showing fluctuations without a clear downward trend, indicating potential instability in model convergence

3.8 Comparison with Baseline Approaches

Compared to traditional feature-based methods, the Siamese CNN demonstrated superior performance, capturing subtle signature variations with greater precision. Unlike conventional models that rely on handcrafted features, the Siamese CNN autonomously learns discriminative patterns, enhancing classification accuracy.

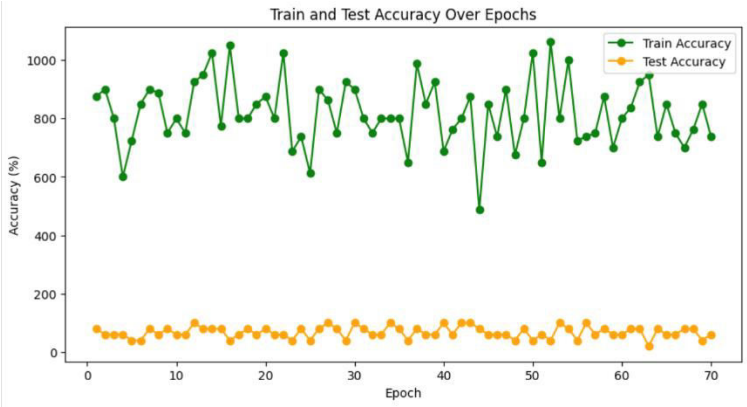

Fig. 4 shows train and test accuracy over epochs, where train accuracy fluctuates at high values, while test accuracy remains consistently low, indicating potential overfitting

3.9 Discussion on Model Performance

While the model exhibited strong performance, minor overfitting was observed, particularly when trained on a limited dataset. Future enhancements include dataset expansion, advanced regularization techniques, and hybrid architectures to improve robustness and generalization. The proposed model provides a scalable and efficient solution for real-world signature verification tasks.

4. Conclusion

This study presents an effective real-time signature verification system using a Siamese CNN, achieving high accuracy and precision on benchmark datasets. The model proves practical for real-world applications, with future improvements aimed at enhancing generalization and robustness.

4.1 Conclusion

In conclusion, the deep learning-based signature verification system using a Siamese Convolutional Neural Network (CNN) demonstrates a robust and effective solution for real-time signature authentication. By leveraging Siamese CNN architecture and threshold optimization, the model effectively distinguishes between genuine and forged signatures with impressive accuracy and precision. The results obtained from testing on publicly available datasets, such as ICDAR, CEDAR, and Kaggle, confirm the feasibility of this approach for practical applications in sectors such as banking, legal documentation, and digital transactions.

While the model shows promising results, future research can focus on expanding the dataset, refining the regularization techniques, and exploring hybrid architectures to improve generalization and robustness across diverse signature styles. The model's real-time capability, scalability, and minimal reliance on manual intervention make it a valuable asset for enhancing security in digital transactions and Identity verification.

5. References

1. S. M. A. Navid, S. H. Priya, N. H. Khandakar, Z. Ferdous and A. B. Haque, "Signature Verification Using Convolutional Neural Network," *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*, Dhaka, Bangladesh, 2019, pp. 35-39, doi: 10.1109/RAAICON48939.2019.19.
   keywords: {Convolutional neural network (CNN);Signature verification; Computer Vision; Fine-tuning; Classification},
2. B. H. Shekar, W. Abraham and B. Pilar, "Offline Signature verification using CNN and SVM classifier," *2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, MANGALORE, India, 2022, pp. 304-307, doi: 10.1109/ICRAIE56454.2022.10054336.
   keywords: {Support vector machi
   nes;Training;Deeplearning;Handwritingrecognition;Technologicalinnovation;Neuralnetworks;Featu
   reextraction;offline;signature;verification;CNN;SVM},
3. S. M. A. Navid, S. H. Priya, N. H. Khandakar, Z. Ferdous and A. B. Haque, "Signature Verification Using Convolutional Neural Network," *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*, Dhaka, Bangladesh, 2019, pp. 35-39, doi: 10.1109/RAAICON48939.2019.19.
   keywords: {Convolutional neural network (CNN);Signature verification;ComputerVision;Fine-tuning;Classification},