Signature Verification System by using Convolutional Neural Network (CNN)

Vipin Koshe[1], Ashwin Kadawey[2], Nikita Parihar[3], Yash Solanki[4], Pratik Pawar[5], Prof. Sonali Rathore[6]

[1, 2, 3, 4, 5] B. Tech Scholar, [6]Assistant Professor
Department of Artificial Intelligence & Data Science
Shri Balaji Institute of Technology & Management
Betul, RGPV University M.P, India

Abstract

One of the most popular verification biometrics is the signature[2], which uses handwritten signatures in cheques, applications, letters, forms, minutes, etc. A person's handwritten signature must be individually identified because each individual's signature is unique by nature. Verifying signatures is a popular technique for verifying someone while they are away. Human verification can be inaccurate and occasionally unsure. The most common method for confirming a person or a private is with a signature. A person's signature is used to identify them in all social, professional, and commercial contexts[2]. The word "signature verification" is extremely important because it could be misused and lead to significant losses. The signature may be a behavioral biometric trait that combines the signer's neuromotor characteristics (e.g., how our brain and muscles, among other things, shape how we tend to sign) as well as sociocultural influences (e.g., the differences between Western and Asian styles). Through the ages, United Nations agency experts have constructed signature examinations to verify the validity of sample-supported rhetorical analysis.

Keywords: CNN (Convolutional Neural Network), Signature Verification, Support Vector Machine, Biometric Analysis.[1]

Introduction

Signature verification is widely used in a variety of industries, particularly for authentication purposes in banking, legal cases, and digital criminals[1]. While signatures can be considered unique biometric properties, verification of their authenticity creates several problems, including in-direct variation and false experts. Traditional test methods rely on manual methods of extracting properties, such as histograms of orientation gradients (HOG), invariant transformations of properties (SIFT), and matrix of initial joint arrivals to grey levels (GLCM)[3]. However, these features are manually limited in accuracy when distinguishing between genuine and counterfeit signatures. Signature verification is widely used for authentication purposes in a variety of industries, including banking, legal, and digital offenders. While signatures can be considered a unique biometric line, verification of their authenticity poses several challenges, including within-person variation and professional counterfeiting. Traditional test methods depend on manual methods of extracting features, such as a histogram of oriented gradients (HOG), scale-invariant transformation of features (SIFT), and a matrix of a joint first arrival at the gray level (GLCM). Nevertheless, these functions manually have limited accuracy when distinguishing between subtle differences in genuine and forged signatures. Recent advancements in deep learning have enabled the

automation of signature verification. Convolutional Neural Networks (CNNs) have been particularly successful due to their ability to learn complex spatial patterns directly from raw images. In this article, we investigate various CNN-based approaches for offline and online validation. This includes unique model architectures and hybrid models that incorporate federated learning. Recent advances in detailed learning have made it possible to automate signature verification. The deleted neural network (CNN) has completed the ability to directly study complex spatial models from raw images, particularly successfully. This article covers a variety of approaches based on offline and online signatures, CNNs. This includes unique model architectures, including federal training and hybrid models.

Literature Review

The area of Handwritten Signature Verification has been broadly lyre search in the last decades and remains as an open research problem. This project focuses on offline signature verification, characterized by the usage of static(scanned)images of signatures, where the objective is to discriminate if a given signature is genuine. We present an overview of how the problem has been handled by several researchers in the past few decades and their recent advancements in the field.[4]

Machine Learning:

Machine learning is fundamentally built upon data, which serves as the foundation for training and testing models. Data consists of inputs (features) and outputs (labels). A model learns patterns during training and is tested on unseen data to evaluate its performance and generalization. In order to make predictions, there are essential steps through which data passes in order to produce a machine-learning model that can make predictions.

Convolutional Neural Network (CNN):

A Convolutional Neural Network (CNN) is a specialized deep learning model designed for image processing, pattern recognition, and spatial data analysis. Unlike traditional neural networks, CNNs automatically verification.

- Convolutional Layers: These layers apply convolutional operations to input images, using filters (also known as kernels) to detect features such as edges, textures, and more complex patterns. Convolutional operations help preserve the spatial relationships between pixels.[1]
- Pooling Layers: They downsample the spatial dimensions of the input, reducing the computational complexity and the number of parameters in the network. Max pooling is a common pooling operation, selecting the maximum value from a group of neighboring pixels.
- Activation Functions: They introduce non-linearity to the model, allowing it to learn more complex relationships in the data.extract features from input data, making them highly effective for tasks like image classification, object detection, and signature
- Fully Connected Layers: These layers are responsible for making predictions based on the high-level features learned by the previous layers. They connect every neuron in one layer to every neuron in the next layer.

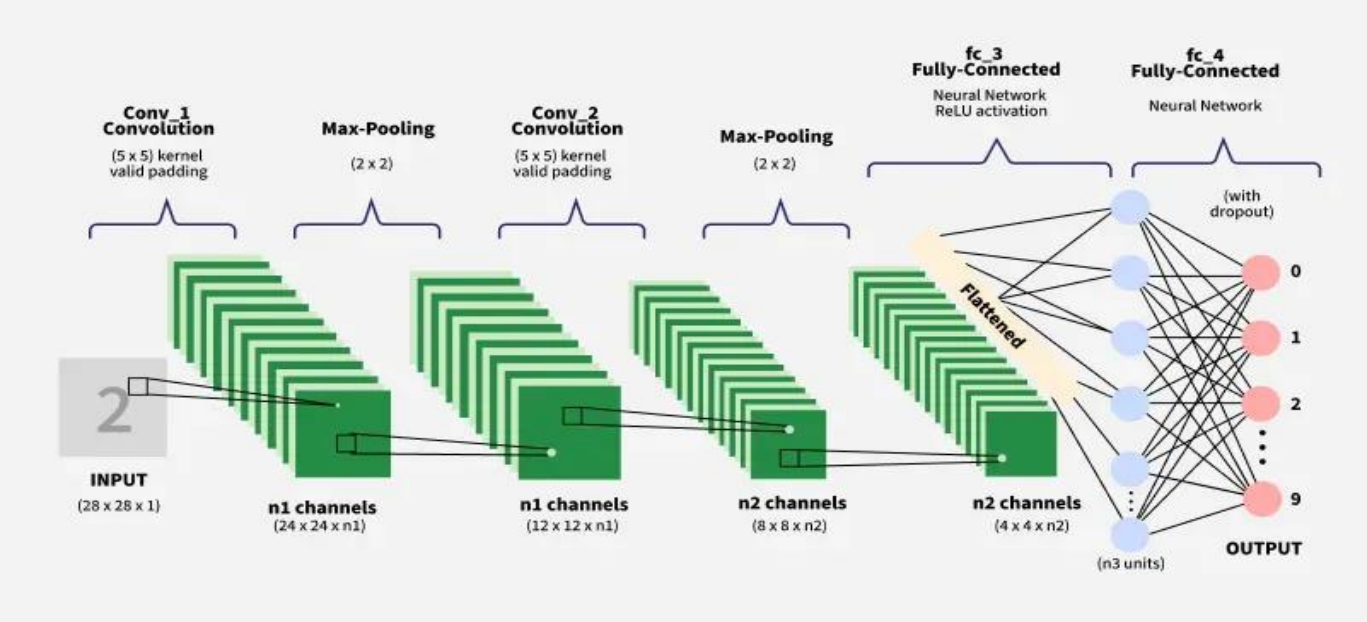
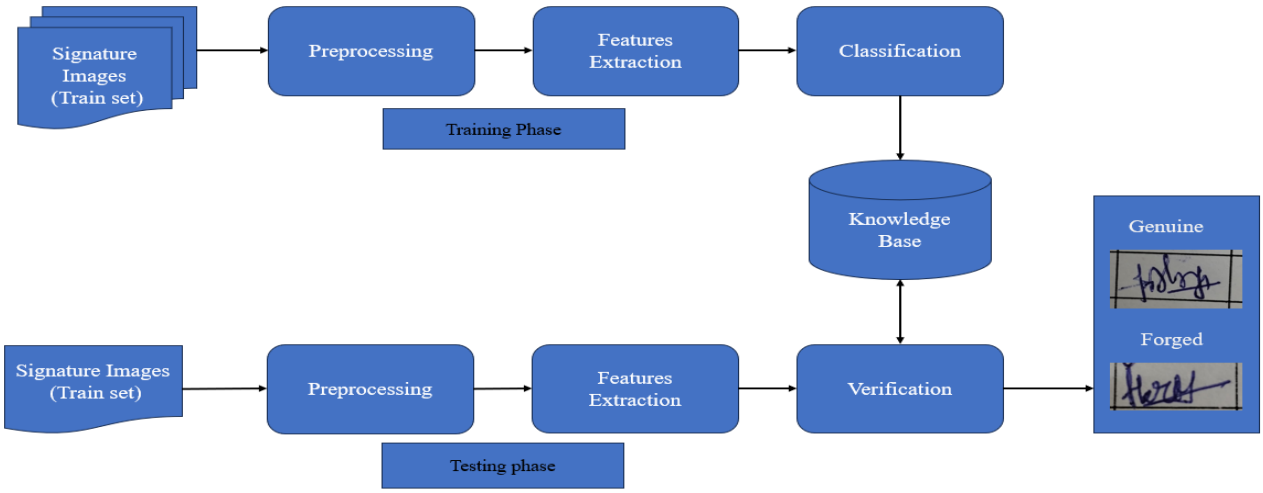


Fig: CNN Work

System Architecture and design

The signature verification system is structured to ensure efficient processing, feature extraction, and classification using a Convolutional Neural Network (CNN). The architecture comprises multiple interconnected modules that handle data collection, preprocessing, model training, and real-time verification.



System Architecture

The system follows a modular design consisting of:

Data Acquisition Module

Collects genuine and forged signatures from various sources.

Ensures high-quality images through preprocessing (grayscale conversion, noise reduction, normalization).

Feature Extraction Module

Uses CNN layers to extract relevant spatial features from the input signature images. Detects edges, textures, and other distinguishing elements through convolutional operations.

Classification Module

Comprises a fully connected neural network that classifies the signature as genuine or forged.

Supports additional verification techniques, such as Support Vector Machine (SVM) for robustness.

Dataflow:

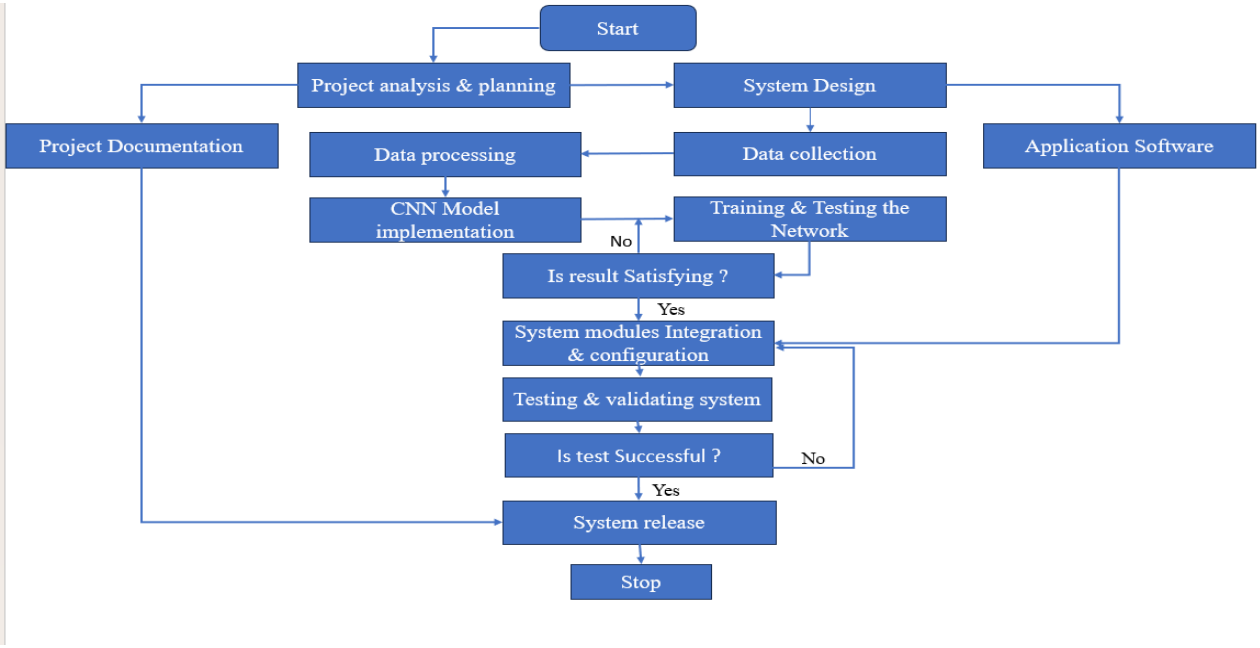


Fig: Dataflow

Data Collection and Preparation:

The process of collecting and preparing signature images for training the models involves several steps to ensure the availability of a diverse and representative dataset. Firstly, a dataset containing genuine and forged signature images is compiled from various sources, including public repositories, legal documents, and financial records. Care is taken to include signatures from different individuals with varying handwriting styles and characteristics.

Once the dataset is curated, preprocessing techniques are applied to standardize and enhance the quality of the signature images. This typically includes steps such as grayscale conversion, noise reduction, and normalization to ensure consistency across images. Additionally, data augmentation techniques may be employed to increase the variability of the dataset, such as rotation, scaling, and translation, to simulate real-world variations in signatures.[3]

Training and Evaluation:

The training process involves feeding the preprocessed signature images into the CNN models and iteratively adjusting the model parameters to minimize the classification error. During training, the models learn to differentiate between genuine and forged signatures by optimizing a predefined loss function, typically categorical cross-entropy. Hyperparameter tuning is performed to optimize the performance of the models, including parameters such as learning rate, batch size, and number of epochs. Additionally, techniques such as early stopping and dropout regularization may be employed to prevent overfitting and improve generalization. Once trained, the models are evaluated using a separate validation dataset to assess their performance in terms of accuracy, precision, recall, and other relevant metrics. The models are then

tested on unseen data to measure their effectiveness in real-world scenarios. Evaluation results are analyzed to identify areas for improvement and refinement of the signature verification system.[3]

Machine Learning Algorithms Used:**

1. Convolutional Neural Network (CNN)*

- Primary model for feature extraction and classification.
- Architecture includes convolutional layers, pooling (max-pooling), ReLU activation, and fully connected layers**.**

2. ***Support Vector Machine (SVM)****

- Referenced for robustness validation (hybrid approach or comparative analysis).

Note: The core algorithm is CNN, with SVM mentioned in the paper's keywords and referenced for validation

Result

Fig: Interface

In this system we detect the Signature is Fraud or Genuine.

Conclusion

Python machine learning for signature validation provides an automatic and effective method of confirming the legitimacy of signatures.

Enhancing security protocols and fraud detection is made feasible by accurately differentiating between real and fake signatures through the use of machine learning methods and methodologies. The steps involved in implementation include gathering a variety of trademark picture datasets, enhancing their quality through preprocessing, extracting significant features, and utilizing the right methods to train a machine learning model. In conclusion, we presented a unique architecture for signature comparison that holds potential for use in future signature verification studies, particularly when comparing known authentic signatures of a certain signer against a potentially faked signature. The task is appealing since it simulates a real-world scenario where signature verification is used. Despite our lackluster performance on this assignment, our method appears promising based on the literature on signature verification. We should be able to perform better on this Endeavor if we had greater

access to data and processing power. We could train our model on bigger datasets and let more Layers train for longer epochs if we had access to these.

FutureScope:

- Enhanced Generalization: Further research and development efforts will focus of improving the generalization capabilities of the models, enabling them to effectively handle variations in signature images from diverse sources.
- Scalability and Efficiency: Optimization techniques will be explored to enhance the scalability and efficiency of the system, allowing for seamless operation with larger datasets and increased user traffic.
- Integration of Advanced Techniques: Integration of advanced techniques such as ensemble learning, attention mechanisms, and domain adaptation will be explored to further enhance the performance and robustness of the system.
- User Feedback and Iterative Improvement: Continuous solicitation of user feedback and iterative testing cycles will guide the refinement and enhancement of the Signature Verification System, ensuring its effectiveness and usability in real-world scenarios.

References

1. R. K. Mohapatra, K. Shaswat and S. Kedia, "Offline Handwritten Signature Verification using CNN inspired by Inception V1 Architecture," 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India, 2019, pp. 263-267,doi: 10.1109/ICIIP47207.2019.8985925
2. HrishikeshMhaske, RushikeshBhalerao, SanketWalke, VaibhavGholap, Prof. Puja Lingampalli,"Signature Verification using CNN" 2023 International Journal of Advanced Research in Science, Communication and Technology (IJARSCT),ISSN (Online) 2581-9429.
3. AnupDhoble ,Ankit Bhardwaj ,Ajay Mahato ,SuhaniTaran,Prof. Bhagyashree S. Madan."Signature Verification System Using CNN" 2024,
4. Dr.R.Palson Kennedy , Nithish Kumar , Vinodh Kumar, Yogesh," Human Signature Verification Using CNN With Tensorflow, 2022 IJCRT | Volume 10, Issue 6 June 2022 | ISSN: 2320-2882
5. Sujith, K., et al. "Signature Verification Using Python." International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 1, International Journal for Research in Applied Science and Engineering Technology (IJRA-SET), Jan. 2023, pp. 891–96. Crossref, https://doi.org/10.22214/ijra-set.2023.48643.
6. Fierrez-aguilar, J., Krawczyk, S., Ortega-garcia, J. & Jain, A. K.(2005), `Fusion of Local and Regional Approaches for On-Line Signature Verification', Iwbrs 2005 LNCS 3781, 188-196.