



SIGNATURE VERIFICATION SYSTEM USING KNN & CNN ALGORITHM

Kaveri Santosh Ahire

Master's Student, Data Science, Dr. D.Y. Patil Arts, Commerce & Science College, Pimpri, Pune

ABSTRACT

Biometric authentication systems have gained significant importance in secure identity verification, with handwritten signatures remaining a widely accepted behavioral biometric in banking, financial, and legal domains. However, the inherent variability in individual writing styles and the prevalence of skilled forgeries make signature verification a challenging task, particularly in offline scenarios where only static images are available.

This paper presents an offline handwritten signature verification system that integrates Convolutional Neural Networks (CNN) for automated feature extraction and k-Nearest Neighbors (KNN) for classification. The proposed approach leverages CNN's capability to learn discriminative spatial features such as stroke patterns, texture, and structural characteristics directly from signature images, eliminating the need for manual feature engineering. The extracted feature vectors are subsequently classified using the KNN algorithm, which determines the authenticity of a signature based on similarity measures with stored reference samples.

The performance of the system is evaluated using standard metrics such as accuracy, precision, and false acceptance/rejection rates. Experimental results demonstrate that the hybrid CNN-KNN model achieves improved classification accuracy and robustness compared to traditional methods, making it suitable for practical deployment in fraud detection systems. The study also highlights the effectiveness of combining deep learning-based feature extraction with classical machine learning classifiers for enhanced signature verification performance.

KEYWORDS: Handwritten Signature Verification, Biometric Authentication, Convolutional Neural Networks (CNN), k-Nearest Neighbors (KNN), Offline Signature Verification, Feature Extraction, Pattern Recognition, Image Processing, Forgery Detection, Machine Learning, Deep Learning, Classification Algorithms, Behavioral Biometrics, Signature Authentication System.

INTRODUCTION

Handwritten signatures continue to be one of the most widely used methods for personal authentication in banking, legal documentation, and financial transactions. Due to their convenience and long-standing acceptance, signature verification systems have become an important area of research in biometric authentication. However, accurate verification remains a challenging task because of significant intra-class variations in genuine signatures and the increasing sophistication of forged signatures.

Signature verification can be broadly classified into two categories: online and offline systems. Online signature verification captures dynamic information such as writing speed, pressure, and stroke order, which generally results in higher accuracy. In contrast, offline signature verification relies solely on static images of signatures, making it more complex due to the absence of dynamic features. Despite these challenges, offline systems are more practical and widely used because they do not require specialized input devices.

With the growing incidence of fraud, signature forgery has become a major concern, necessitating the development of robust and automated verification systems. Traditional approaches often depend on handcrafted feature extraction techniques, which may fail to capture complex patterns present in signature data.

In this study, we propose an offline signature verification approach that combines Convolutional Neural Networks (CNN) and k-Nearest Neighbors (KNN). CNN is employed to automatically extract discriminative features from signature images, capturing structural and textural characteristics effectively. These features are then used by the KNN classifier to determine the authenticity of a signature based on similarity measures with stored reference samples. The integration of deep learning-based feature extraction with a classical machine learning classifier aims to improve verification accuracy and robustness in detecting forged signatures.

LITERATURE REVIEW

Handwritten signature verification has been extensively studied as a reliable behavioral biometric for identity authentication. Over the years, researchers have proposed various approaches ranging from traditional machine learning techniques to advanced deep learning models.

Early studies in signature verification primarily focused on handcrafted feature extraction methods combined with classical classifiers. Features such as geometric properties, texture, stroke direction, and statistical measurements were commonly used. Algorithms like Support Vector Machines (SVM), k-Nearest Neighbors (KNN), and Hidden Markov Models (HMM) were widely applied for classification. Although these methods provided reasonable accuracy, their performance was highly dependent on the quality of manually extracted features



and often failed to generalize well for complex or skilled forgeries.

Subsequently, researchers introduced texture-based and transform-based feature extraction techniques, including Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), Wavelet Transform, and Fourier Transform. These methods improved the representation of signature characteristics; however, they still required domain expertise and were limited in capturing high-level abstract patterns.

With the advancement of deep learning, Convolutional Neural Networks (CNN) have emerged as a powerful tool for image-based classification tasks, including signature verification. CNN models automatically learn hierarchical feature representations from raw signature images, eliminating the need for manual feature engineering. Several studies have demonstrated that CNN-based approaches significantly outperform traditional methods in terms of accuracy and robustness, especially in offline signature verification. In addition to deep learning models, hybrid approaches combining CNN with classical machine learning algorithms have gained attention. In such systems, CNN is used for feature extraction, while classifiers like KNN, SVM, or Random Forest are employed for final decision-making. Among these, KNN is particularly effective due to its simplicity and ability to classify signatures based on similarity measures, making it suitable for small and medium-sized datasets.

Recent research highlights that combining deep learning feature extraction with lightweight classifiers can achieve a balance between computational efficiency and classification performance. Therefore, in this work, a hybrid CNN-KNN approach is adopted to leverage the strengths of both methodologies for improved signature verification accuracy and reliable forgery detection.

PROBLEM STATEMENT

Handwritten signature verification remains a challenging task in biometric authentication systems due to the presence of high intra-class variability and inter-class similarity. Genuine signatures of the same individual may vary significantly because of factors such as writing speed, mood, and environmental conditions, while skilled forgeries can closely resemble original signatures, making accurate classification difficult.

In offline signature verification, the problem becomes more complex as only static images are available, without dynamic information such as pen pressure, stroke order, and writing speed. Traditional verification methods rely heavily on handcrafted feature extraction techniques, which are often insufficient to capture complex and subtle patterns present in signature images.

Furthermore, many existing systems struggle to achieve a balance between high accuracy and computational efficiency, especially when dealing with large datasets or real-time applications. There is a need for an automated and robust system

that can effectively extract meaningful features and accurately distinguish between genuine and forged signatures.

Therefore, the main problem addressed in this study is to develop an efficient offline signature verification system that utilizes advanced feature extraction and classification techniques, specifically combining Convolutional Neural Networks (CNN) and k-Nearest Neighbors (KNN), to improve accuracy, reduce false acceptance and rejection rates, and enhance overall system reliability.

OBJECTIVE

The main objective of this research is to develop an efficient and accurate offline handwritten signature verification system using machine learning and deep learning techniques.

The specific objectives are:

1. To design a signature verification system using Convolutional Neural Networks (CNN) for automatic feature extraction
2. To implement k-Nearest Neighbors (KNN) for effective classification of signatures as genuine or forged
3. To improve the overall accuracy of signature verification by reducing false acceptance rate (FAR) and false rejection rate (FRR)
4. To eliminate the dependency on manual feature extraction by utilizing deep learning techniques
5. To analyze and compare the performance of the proposed model using evaluation metrics such as accuracy, precision, and recall
6. To develop a robust and reliable system suitable for real-world applications such as banking and legal authentication

METHODOLOGY AND DATASET

Methodology

The proposed system follows a structured pipeline for offline handwritten signature verification. The major stages include preprocessing, feature extraction, classification, and evaluation.

1. Data Preprocessing

1. The input signature images are preprocessed to improve quality and consistency. This step includes:
2. Noise removal using filtering techniques
3. Conversion to grayscale
4. Image resizing and normalization
5. Binarization to separate foreground (signature) from background
6. These steps ensure that the input data is standardized for further processing.

2. Feature Extraction using CNN

1. A Convolutional Neural Network (CNN) is used to automatically extract meaningful features from signature images. CNN captures:
2. Stroke patterns
3. Edge information
4. Texture and structural details
5. Unlike traditional methods, CNN eliminates the need for manual feature engineering and learns hierarchical representations directly from data.

3. Classification using KNN

1. The extracted feature vectors are passed to the k-Nearest Neighbors (KNN) classifier.
2. KNN compares the input signature with stored reference signatures
3. It calculates similarity using distance metrics (e.g., Euclidean distance)
4. Based on nearest neighbors, the signature is classified as genuine or forged

4. Performance Evaluation

1. The system performance is evaluated using standard metrics:
2. Accuracy
3. Precision
4. Recall
5. False Acceptance Rate (FAR)
6. False Rejection Rate (FRR)

Dataset

The dataset consists of scanned images of handwritten signatures, including:

1. Genuine signatures of individuals
2. Forged signatures created by imitators

The dataset is divided into:

1. Training set (used to train CNN and store features)
2. Testing set (used to evaluate system performance)

System Architecture



RESULTS AND ANALYSIS

The proposed signature verification system based on the hybrid CNN-KNN approach demonstrates significant improvement in performance for offline handwritten signature authentication. The Convolutional Neural Network (CNN) effectively extracts discriminative features such as stroke patterns, edge details, and structural characteristics from the input signature images. These extracted feature representations are then utilized by the k-Nearest Neighbors (KNN) classifier to perform similarity-based classification, enabling accurate differentiation between genuine and forged signatures.

Experimental evaluation shows that the system achieves high accuracy while maintaining a balanced trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR). The reduction in FAR indicates that the system is capable of minimizing the acceptance of forged signatures, whereas the lower FRR ensures that genuine signatures are correctly identified. Additionally, the model exhibits strong precision and

recall values, highlighting its effectiveness in handling both genuine and forged samples.

Compared to traditional signature verification methods that rely on manual feature extraction, the proposed approach provides better generalization and robustness due to the automatic feature learning capability of CNN. The integration of KNN further enhances classification reliability by leveraging distance-based similarity measures. Overall, the results confirm that the hybrid CNN-KNN model offers an efficient and accurate solution for offline signature verification, making it suitable for practical applications in banking and security systems.



The Signature Verification System was successfully developed using machine learning to classify signatures as genuine or forged. The system uses preprocessing and feature extraction techniques before applying KNN and CNN models for prediction. The KNN model provides quick results for smaller datasets, while the CNN model offers better accuracy for complex image patterns. The system is fast, user-friendly, and reduces manual effort. However, its performance depends on the quality of the dataset and images. Overall, the project demonstrates an effective and practical use of machine learning



for signature verification, with scope for further improvement using advanced models and real-time applications.

CONCLUSION

This paper presents an efficient online handwritten signature verification system based on a hybrid approach combining Convolutional Neural Networks (CNN) and k-Nearest Neighbors (KNN). The proposed method effectively addresses the challenges associated with signature variability and forgery by utilizing CNN for automatic feature extraction and KNN for accurate classification. The system eliminates the need for manual feature engineering and improves overall performance by capturing complex patterns present in signature images.

The experimental results demonstrate that the proposed model achieves high accuracy while reducing both False Acceptance Rate (FAR) and False Rejection Rate (FRR), making it reliable for practical applications. The integration of deep learning and machine learning techniques enhances the robustness and efficiency of the verification process. Therefore, the proposed system can be effectively deployed in real-world domains such as banking, legal documentation, and identity authentication systems to ensure secure and reliable verification.

Future Scope

Although the proposed CNN-KNN based signature verification system demonstrates effective performance in detecting forged signatures, there are several opportunities for further improvement and enhancement. One potential direction is the use of larger and more diverse datasets, which would help improve the generalization capability and robustness of the model. Incorporating advanced deep learning architectures such as ResNet, VGG, or transformer-based models could further enhance feature extraction and improve classification accuracy.

Additionally, the system can be extended to support online signature verification by incorporating dynamic features such as pen pressure, writing speed, and stroke sequence, which would significantly increase reliability. Another promising direction is the development of real-time verification systems that can be integrated into banking applications, mobile devices, and cloud-based platforms for faster and more secure authentication.

Furthermore, combining CNN-KNN with other machine learning techniques or ensemble models could improve performance in complex forgery cases. The integration of Explainable Artificial Intelligence (XAI) methods can also help in understanding model decisions, making the system more transparent and trustworthy. Overall, future research can focus on improving accuracy, scalability, and real-world deployment of signature verification systems.

REFERENCES

1. *Handwritten signature attributes for its verification*, Anastasia Beresneva;Anna Epishkina;Darina Shingalova, 2018
2. *New Local Difference Feature for Off-Line Handwritten Signature Verifica-tion*, Naouel Arab;Hassiba Nemmour;Youcef Chibani, 2019
3. *Handwritten Signature Verification System Using Sound as a Feature*, Mustafa Semih Sadak;Nihan Kahraman;Umut Uludag, 2020
4. *Handwritten Signature Verification using TensorFlow*, Rahul D Rai; J.S Lather, 2018
5. *Improved Multi-Scale Local Difference Features for Off-Line Handwritten Signature Verification*, Naouel Arab;Hassiba Nemmour;Youcef Chibani, 2020
6. *Improved Multi-Scale Local Difference Features for Off-Line Handwritten Signature Verification*, Naouel Arab;Hassiba Nemmour;Youcef Chibani, 2020
7. *Handwritten Signature Verification via Deep Sparse Coding Architecture*, Dimitros Tsourounis; Ilias Theodorakopoulos; Elias N. Zois;George Economou; Spiros, 2018
8. *A handwritten signature verification method employing a tablet*, Micha l Lech;Andrzej Czyzewski, 2016
9. *Angle features extraction of handwritten signatures*, Osama Mohamed Elra- jubi;Idris S. El-Feghi, 2015
10. *Parallel Gpu Based Offline Signature Verification Model*, Amit Kumar Kar;Saroj Kumar Chandra;Manish Kumar Bajpai, 2019