Handwritten Signature Validation and Counterfeit Detection Framework with KNN, Backpropagation, and Convolutional Neural Networks

Mr Jadhav U B[1], Prof. Kharat Y. D[2], Prof. Tirmakhe V. R[3], Prof. Bhmabare A. V[4], Prof. Bansode D. K[5]

[1]Principal, [2, 3, 4,5]Assistant Professor
[2,3,4,5] Department of Computer Engineering
Computer Engineering, SND Polytechnic, Yeola, Nashik

Abstract

Biometrics has gained global prominence as a reliable method for identifying and verifying individuals, including their handwritten signatures. A person's handwritten signature is a distinct and personal identifier, widely utilized in banking, financial, and legal operations. However, handwritten signatures have become increasingly susceptible to forgery due to their historical and legal significance. The Signature Verification System (SVS) aims to determine the authenticity of a signature, identifying whether it is genuine (created by the claimed individual) or forged (produced by an imposter).

Verifying signatures using static images of scanned signatures, without dynamic information about the signing process (such as speed and pressure), poses significant challenges, particularly in offline scenarios. Over the past decade, deep learning algorithms have demonstrated their effectiveness in extracting and learning the unique features of signature images. This field of research has seen continuous progress, and recent developments provide insight into how signature verification has evolved, along with promising directions for future exploration.

Key Words: Signature Verification, KNN, CNN, Backproagation.

INTRODUCTION

The widespread and continuing usage of signatures for personal authentication, signature verification has been a focus of the current study. Despite this, it is still a difficult process due to wide intra-class variances and sophisticated forgeries. Depending on how the signature is obtained, signature verification can either be online or offline. Because more informational dimensions are accessible, online signature verification methods typically outperform offline systems in terms of performance. One of the most popular methods in use today to authenticate someone is signature verification. Because of this, attackers frequently attempt signature forging. Online and offline signature verification are the two categories under which signature verification is categorized. This study concentrates on identifying online signature verification forgeries. In the suggested method, we applied the discrete Fourier transform, which is used to extract information that can be used to distinguish a fake signature from a real one. Next, we classified data using the Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) methods of recurrent neural networks.

Because we know both past and future results in this situation, we used bidirectional LSTM and bidirectional GRU

MOTIVATION

Even in the digital age, customers still use their signatures as a primary form of authentication for a range of transactions. Their signatures authorize checks, new account paperwork, loan documents, and more, and to minimize the risk of fraud, your financial institution needs the right solutions to detect forgeries quickly and accurately

OBJECTIVE

- To improve accuracy of existing signature verification/recognition methods.
- To reduce the time required for correct identification of original signatures from forged ones.
- Reduce fraudulent activities by recognition of signatures in legal documents and cheques used in banks
- To overcome and decrease the risk of financial loss

EXISTING SYSTEM

The system consists of major steps preprocessing, feature extraction, and classification. In the testing phase verification is done with pertained sample signatures.

•Preprocessing: The motivation behind the pre-processing stage is to make signature standards and prepared for include extraction. The pre-preprocessing stage basically includes noise, resizing, Binarization, thinning, clutter removal, and normalization

•Feature Extraction: Features extraction is required when input information to an algorithm is excessively huge and repetitive. This excess information is then changed into the brief and fundamental arrangement of features. This technique is called feature extraction. Features compared with offline signatures may incorporate.

•Classification : Classification is the process where input information is sorted. Another piece of information when contributing to the framework tends to be effectively recognized as having a place with a specific class

•Verification : In this step prepared classifier verify the test signature against a set of test sample signature it has pertained to during the classification stage. If the match is found over a certain threshold, then the signature is considered original else it is considered forged.

LITERATURE SURVEY

A. Beresneva, A. Epishkina, and D. Shingalova, ”Handwritten signature attributes for its verification,”[1] 2018 - This paper examines authentication systems based on handwritten signature and the main informative parameters of signature such as size, shape, velocity, pressure, etc. The authors analyzed their statistical characteristics and considered methods to extract them using Wavelet transform, discrete Radon, and Fourier transform. To design an effective verification algorithm, handwritten signature data acquisition methods were investigated

R. D. Rai and J. S. Lather, ”Handwritten Signature Verification using TensorFlow,”[2] 2018 – The proposed system was designed using TensorFlow, which is used widely for deep learning. The Convolutional Neural Network (CNN) used in the designed system is capable of accurately verifying the characters unique to the original signature. The effectiveness of the system is measured using two parameters which are False Rejection Rates (FRR) and False Acceptance Rates (FAR). The proposed system showed FAR and FRR

values as 5 percent and 5 percent respectively while testing and the overall accuracy of the system is 90 percent

N. Arab, H. Nemmour and Y. Chibani, ”New Local Difference Feature for Off-Line Handwritten Signature Verification,”[3] 2019 - In this work, authors propose a new textural feature for solving offline handwritten signature verification. The proposed feature is called Local Difference Feature (LDF) is an LBP-like texture descriptor. PDF calculates differences between a central pixel and eight neighbors taken on a specific neighborhood radius

S. Soisang and S. Poomrittigul, ”New Textural Features for Handwritten Signature Image Verification,”[4] 2021 - In this work, a new textural feature for solving offline handwritten signature verification is proposed. A new textural features method is developed by combining a Local Binary Patterns (LBP) method and a Gradient Quantization Angle (GQA) method. This proposed method is called Local Binary Patterns with Gradient Quantization Angle (LBPGQA), as developed by the heuristic method to improve the precision of verification of the offline signature image. The hypothesis for this study is to classify the distinctive handwritten signature individually with the actual signature angle and refraction for enhancing signature fraud detection. The verification step is achieved by Artificial Neural Network (ANN) classifier trained on genuine signatures. Furthermore, the test stage is performed on genuine signatures and skilled forgeries. The experiments are conducted on CEDAR datasets. The experimental results show that the LBPGQA method outperforms classical features such as Histograms of oriented gradients and local binary patterns. Conclusively, this proposed method can verify the individual and distinctive handwritten signature and help to protect the signature fraud by skilled forgeries.

A. Sharmila, Tejaswini Desai, Ritusree Samanta, Siddharth Sarkar, “Signature Verification and Forgery Recognition”. [4] 2021- Signature verification is behavioral biometric and is most widely used among other types of biometric recognition system like fingerprint, voice, iris etc. There are many biometric verification systems like finger print scanning, face recognition, iris scanning, and voice recognition etc. But cost of deploying for some systems is extremely high and some of the systems are not portable. Inorder to find a middle ground between efficiency, effectiveness in mass quantity and portability, we take a deeper look into signature verification system which can be deployed to produce fruitful results. In this project there is development of various algorithms to verify the signature and to analyze if it is genuine or not. It involves implementation of KNN, CNN and Backpropagation

ALGORITHMS

Convolution Neural Networks (CNN): CNNs are a pivotal compo nent of the project’s machine learning and computer vision techniques. CNNs
are well-suited for feature extraction and pattern recognition tasks, which are
critical for analyzing the unique traits within signatures. They excel at identi fying stroke patterns, pressure points, pen angles, and other distinctive features
that differentiate one person’s authentic signature from a forgery. By training
the CNN on a large dataset of genuine and forged signatures, the system can
learn to discern these intricate details with a high level of accuracy, thereby
enhancing the reliability of the verification process.
Department of Computer Engineering,PVGCOE and SSDIOM,Nashik.
Signature Verification and Forgery Recognition System Using KNN, Backpropagation and CNN. 10.

k-Nearest Neighbors (k-NN): The k-NN algorithm is instrumental.

for the project in terms of the verification process. Once the CNN extracts.
and encodes the unique signature traits, the k-NN algorithm can be employed.
to compare these features with reference signatures in the database. The k-NN algorithm categorizes a signature as genuine or a forgery by measuring the
similarity between the signature's encoded characteristics and those of known
authentic signatures. The "k" in k-NN represents the number of nearest neighbros to consider, and it can be adjusted to achieve the desired trade-off between
accuracy and computation time. By leveraging k-NN, the system can make
real-time determinations about signature authenticity, ensuring a high level of
accuracy in the verification process..

SYSTEM ARCHITECTURE

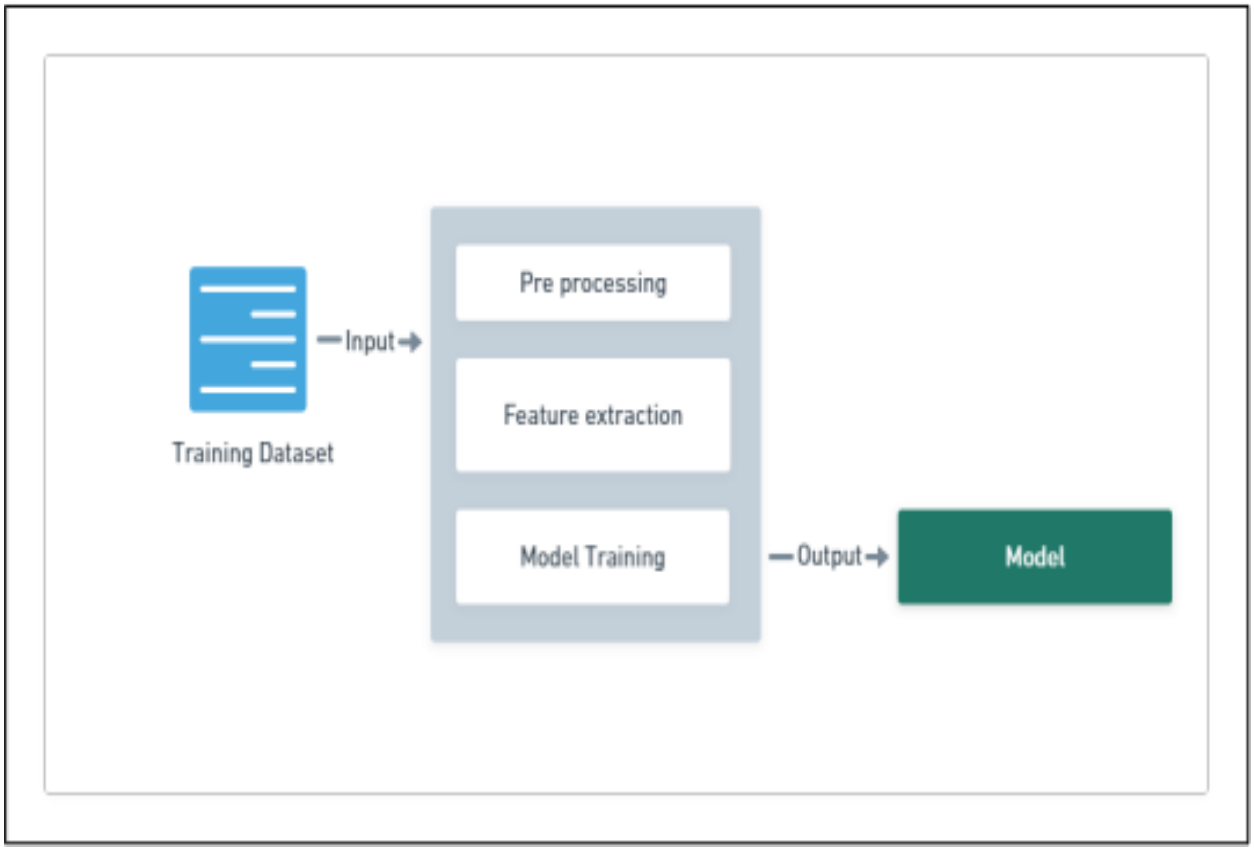

Fig -1: **System Architecture Diagram**

ADVANTAGES

- Easy to used system
- Control system from anywhere
- Centralized system

APPLICATION

- Student sector
- Government Sector

CONCLUSION

A detailed overview of the process of verification of the handwritten signatures system is done enabling the user to do the image processing and classification together in one application. It can be used as an integrated tool for different do- mains such as the internal system of a bank or an inventory and sales management system of a retail shop.

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