Signature Verification and Forgery Recognition System Using Machine Learning

Abhijeet Gaikwad[1], Onkar Mandlik[2], Aniket Madiwale[3], Gauri Gunwant[4], Prof. A.S. Pingle[5]

Department of Information Technology Engineering,
Pune Vidyarthi Girah's College of Engineering & S.S.D. Institute of Management, Nashik

Abstract

Biometrics is now widely used all over the world for the identification and verification of people and their signatures. A person's handwritten signature is a unique identifying work of human that is primarily used and recognized in banking and other financial and legal operations. Handwritten signatures, on the other hand, are becoming increasingly valuable due to their historical significance as a target of deception. The Sign Verification System (SVS) tries to determine whether a sign is genuine (created by the specified individual) or forged (produced by an impostor). Using images of scanned signatures and other documents without dynamic information about the signing process has proven difficult, especially in offline (static) situations. The use of Deep Learning algorithms to learn feature signature picture representations has been well-documented in the literature over the last five to ten years. Here, we examine how the subject has been studied throughout the last few decades, as well as the most recent developments and future study plans.

***Keywords*: Offline handwritten signature, classification, algorithms, artificial intelligence, CNN.**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 6, Nov. – Dec. 2023

INTRODUCTION

Because of 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.

1. PURPOSE

- **Identify need of Project**

The problem of automatic handwritten signature verification is commonly modeled as a verification task given a learning set L, that contains genuine signatures from a set of users, a model is trained. This model is then used for verification: a user claims an identity and provides a query signature. The model is used to classify the signature as genuine (belonging to the claimed individual) or forgery (created by someone else). To evaluate the performance of the system, we consider a test set T, consisting of genuine signatures and forgeries. The signatures are acquired in an enrollment phase, while the second phase is referred to operations (or classification) phase.

OBJECTIVE OF SYSTEM

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

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.

F. Boudamous, H. Nemmour, Y. Serdouk and Y. Chibani, ”An-open system for off-line handwritten signature identification and verification using histogram of templates and SVM,” 2017 – In this work author proposes a new writer- independent system for signature identification and verification. Besides, a new feature generation scheme is proposed by using the Histogram Of Templates (HOT). The identification and verification step are performed by SVM. Experiments are conducted on a standard dataset that contains off-line signaturesof 55 persons. The results obtained are very promising.

PROPOSED SYSTEM

The system consists of major steps preprocessing, feature extraction, and classification. In the testing phase verification isdone 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.

SYSTEM ARCHITECTURE

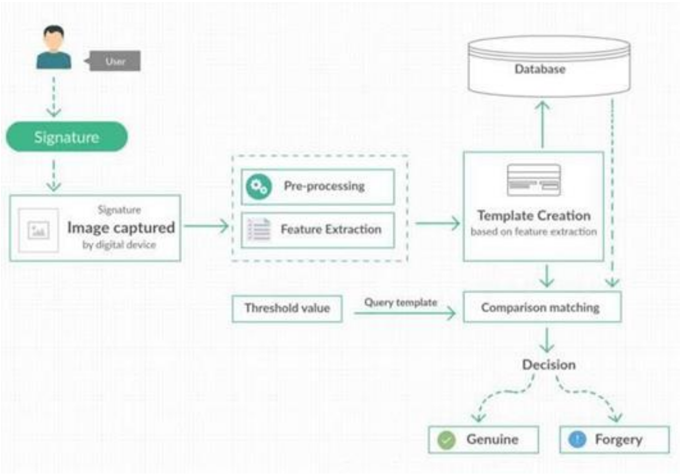

Fig -1: System Architecture Diagram

SYSTEM REQUIREMENTS

- **Software Used:**

1. Programming Language – Python

2. Libraries – NumPy, TensorFlow, Keras, OpenCV,Streamlit
3. Database – SQLite
4. Tools – Visual Studio Code
5. Algorithm – CNN.

- **Hardware Used:**

1. Processor – i3 or above
2. Hard Disk – 150 GB
3. Memory – 4GB RAM

ALGORITHMS

CNN(Convolutional Neural Network) - Convolutional Neural Networks (CNNs) have proven successful in recent years at a large number of image processing-based machine learning tasks. Many other methods of performing such tasks revolve around a process of feature extraction, in which hand-chosen features extracted from an image are fed into a classifier to arrive at a classification decision. Such processes are only as strong as the chosen features, which often take large amounts of care and effort to construct. By contrast, in a CNN, the features fed into the final linear classifier are all learned from the dataset. A CNN consists of a number of layers, starting at the raw image pixels, which each perform a simple computation and feed the result to the next layer, with the final result being fed to a linear classifier. The layers' computations are based on a number of parameters which are learned through the process of backpropagation, in which for each parameter, the gradient of the classification loss with respect to that parameter is computed and the parameter is updated with the goal of minimizing the loss function. Exactly how this update is done and what the lossfunction is are tunable hyperparameters of the network.

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 domains 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 Verification, 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 Elrajubi;Idris S. El-Feghi, 2015
10. Parallel Gpu Based Offline Signature Verification Model, Amit Kumar Kar;Saroj Kumar Chandra;Manish Kumar Bajpai, 2019