

OFFLINE HANDWRITTEN SIGNATURE VERIFICATION

¹Purvesh Kulkarni ²Jay Kolhe, ³Prof-S.A.Pawar

¹⁻³Department of Computer Engineering, TSSMs Bhivarabai Sawant College of Engineering and Research, Pune-411028, Maharashtra, India

Abstract: The most common application of a signature is to verify an individual or a private document. All social, business, and business operations use signatures as a mark of identify. That the word signature verification is extremely important because it might be exploited and lead to losses. The signature could be a behavioural biometric property that comprises the signer's neuromotor characteristics (e.g., our brain and muscles, among other things, delineate the ways we tend to sign) as well as socio-cultural influences (e.g., the Western and Asian styles). Throughout history, consultants for the United Nations have created signature examinations to check the credibility of the sample backed by rhetorical analysis. Angle, categorical attributes, scalar measurements, alignment to the baseline, length of strokes, slant of strokes, shape, punctuation, order, text loops, character spacing, and other forensic possibilities for author identification were used throughout this investigation. These characteristics that aid in the examination of the signature verification largely aid in the identification of the author. For the purpose of experimentation and testing, a larger dataset is required for signature analysis. As a result, the signature datasets are taken for further investigation.

Keywords: Signature, Verification, Support Vector Machine, Biometric, Analysis.

I INTRODUCTION

A signature is a representation of a person's name that is used to verify his or her identification. The primary mechanism for authentication and authorization in a vast number of transactions is a handwritten signature, which is a widely accepted biometric for identity verification. As a result, one of the most difficult tasks in biometrics and document forensics is signature verification. It's possible that the signature will be forged. As a result, the authenticity and verification of a signature are required. The challenge of signature verification can be defined as follows: given a set of signatures, the goal is to learn a model that can distinguish between authentic and forgery signatures. A typical signature verification system focuses on detecting one or more types of fraudulent signatures. When a forger

has unfettered access to one or more examples of the writer's actual signature, it is called skilled forgery. When a forger knows the writer's identity but does not have access to a sample of the actual signature, the result is a casual forgery. Any random scribble, a real signature, or a high-quality forgery for another writer can be considered a random forgery. The identification of a signature involves distinguishing one person's signature from that of others, whereas the verification of a signature involves determining whether or not a particular signature is an authenticate signature of the claimed identity. Signature identification and verification systems are designed to allow for the automatic identification of a person as well as the verification of the signature's authenticity.

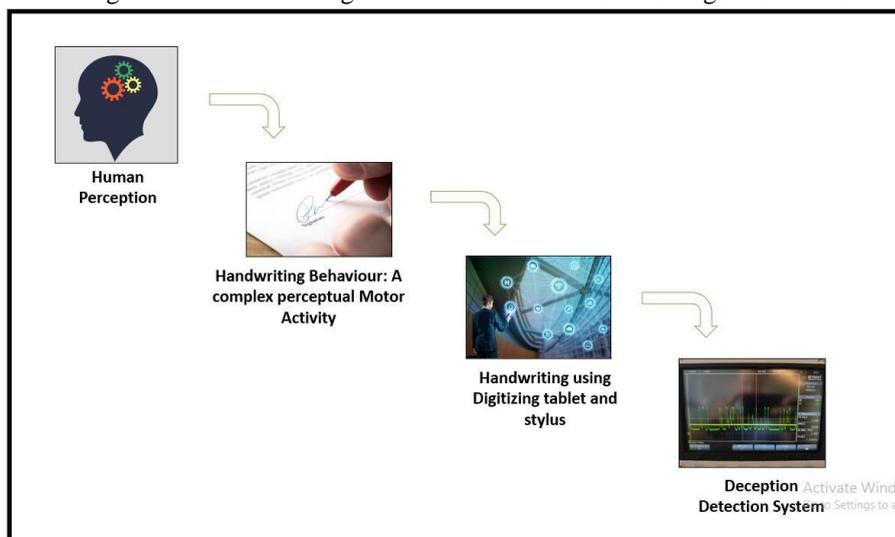


Fig. 1.1.1 Signature verification

Signatures can be forged using a variety of methods. One way is the "freehand method," in which the forger copies the signature freehand after meticulous practise. Although difficult to master, this strategy frequently yields the most convincing results. The "trace-over approach" involves

placing the sheet of paper with the real signature on top of the paper where the forgery is needed. The signature is traced over the piece of paper underneath, leaving a tiny impression.

This indentation can then be used as a guide for a signature. A number of characteristics can suggest to an examiner that a signature has been forged, mostly stemming from the forger focusing on accuracy rather than fluency. These include:

- Shaky handwriting
- Pen lifts
- Signs of retouching

- Letter proportions
- Very close similarity between two or more signatures

Forgery is considered a felony in all fifty states and is punishable by a range of penalties including jail or prison time, significant fines, probation, and restitution (compensating the victim for money or goods stolen as a result of the forgery).

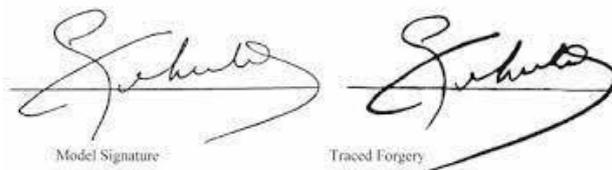


Fig. 1.1 Real vs Forged Signature

II. PROPOSED SOLUTION

A) SUPPORT VECTOR MACHINE

- The Support Vector Machine, or SVM, is a common Supervised Learning technique that may be used to solve both classification and regression issues. However, it is mostly utilised in Machine Learning for Classification difficulties.
- The SVM algorithm's purpose is to find the optimum

line or decision boundary for categorising n-dimensional space into classes so that additional data points can be readily placed in the correct category in the future. A hyperplane is the name for the optimal choice boundary.

- SVM selects extreme points/vectors that aid in the formation of the hyperplane. Support vectors are the extreme instances, and the algorithm is called a Support Vector Machine. Consider the diagram below, which shows how a decision boundary or hyperplane is used to classify two different categories:

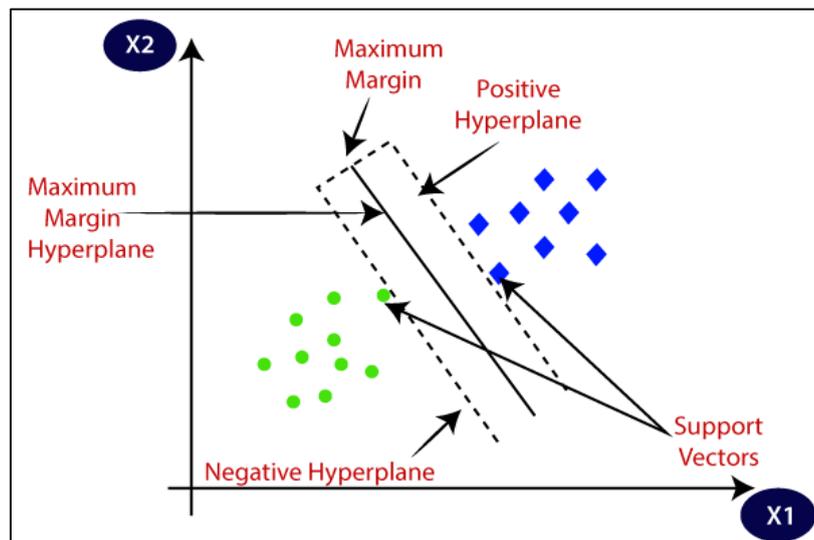


Fig. 2.1.1 Image processing using SVM

In n-dimensional space, there can be several lines/decision boundaries to separate the classes, but we must choose the optimum decision boundary to help classify the data points. The hyperplane of SVM refers to the best boundary. For two-group classification issues, a support vector machine (SVM) is a supervised machine learning model that uses classification techniques. SVM models can categorise new

text after being given sets of labelled training data for each category. Support Vector Machines, on the other hand, are like a sharp knife: they function on tiny datasets, but they can be considerably stronger and powerful in developing machine learning models on larger datasets..

B) CONVOLUTIONAL NEURAL NETWORK

Artificial Neural Networks are quite effective when it comes to Machine Learning. Artificial Neural Networks are utilised for a variety of classification tasks, including picture, audio, and word categorization. For example, we utilise Recurrent Neural Networks, more exactly an LSTM, for predicting the

sequence of words, and we use Convolution Neural Networks for image categorization. We will construct basic CNN building blocks in this blog.

Before we get into the Convolution Neural Network, let's go over some basic neural network ideas. There are three sorts of layers in a standard Neural Network:

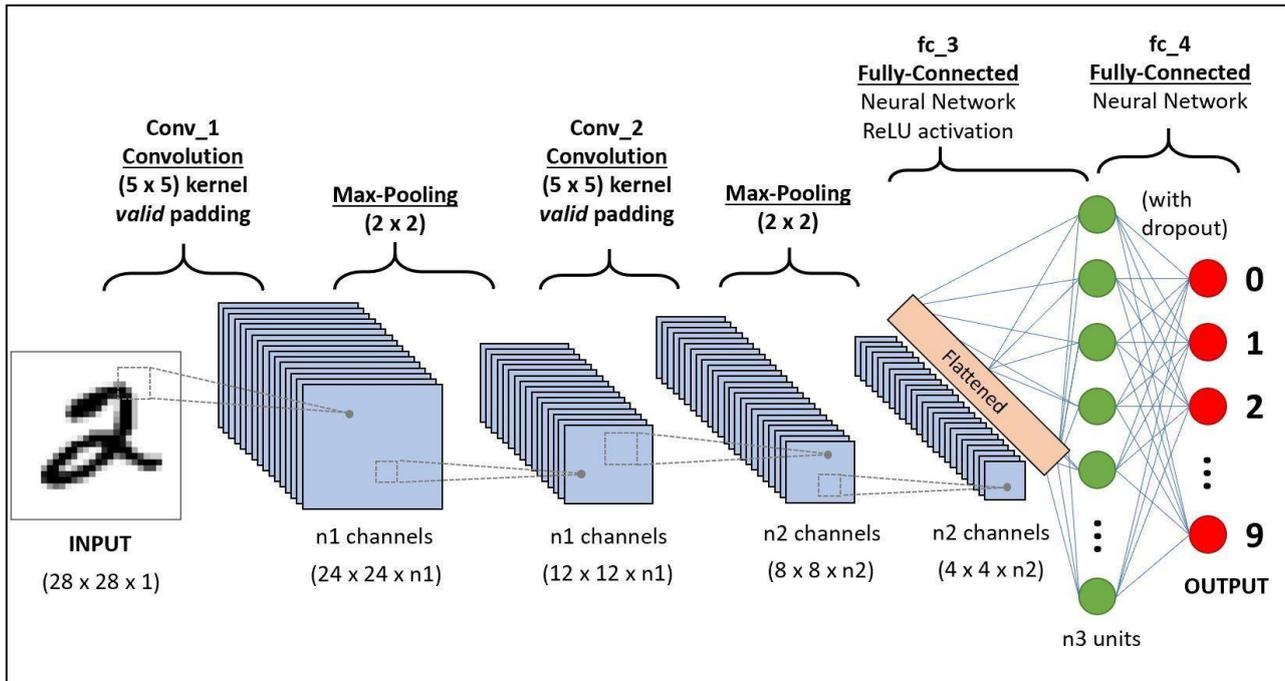


Fig. 2.2.1 Classification using CNN

Input Layers: This is the layer where we offer our model input. The entire number of characteristics in our data is equal to the number of neurons in this layer (number of pixels in case of an image).

Hidden Layer: The hidden layer receives the input from the input layer. Depending on our model and data size, there could be a lot of hidden layers. The number of neurons in each hidden layer can vary, however they are usually more than the number of characteristics. The output from each layer is produced by matrix multiplication of the preceding layer's output with that layer's learnable weights, then addition of

learnable biases, and finally activation function, which makes the network nonlinear.

Output Layer: The hidden layer's output is then input into a logistic function like sigmoid or SoftMax, which translates each class's output into a probability score for each class.

The CNN operates in following way:

1. Take input Signature.
2. Apply Algorithm on obtained signature.
3. Result stating signature is real or forged.

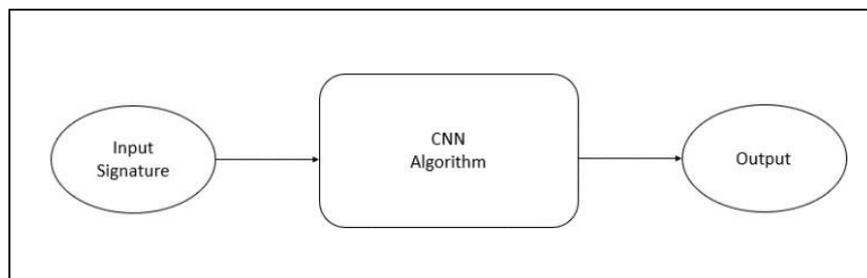


Fig. 2.2.2 Proposed System

C) PROPOSED METHOD

There are several steps included in preprocessing,

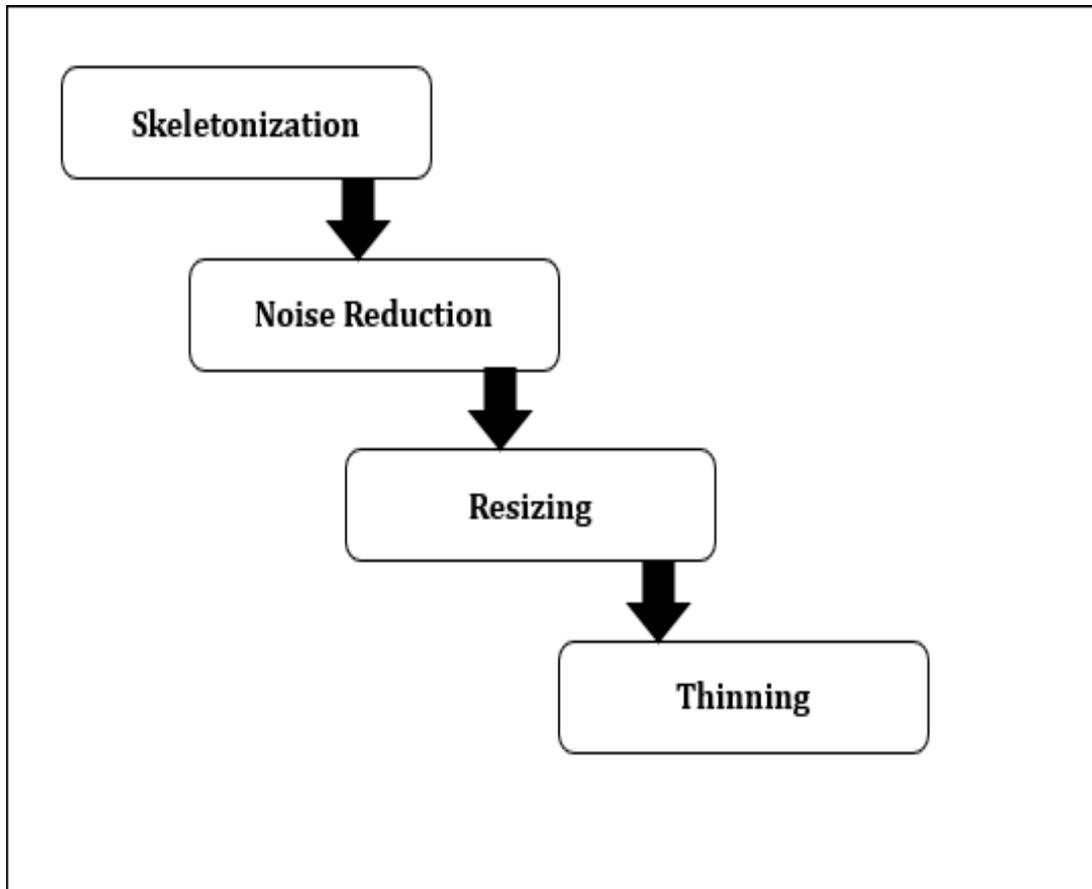


Fig. 2.3.1 Preprocessing

Skeletonization: The goal of skeletonization is to extract a region-based shape characteristic that represents an object's overall form. Skeletonization is a method of reducing foreground portions in a binary image to a skeletal residue that keeps the original region's extent and connection while discarding the majority of the foreground pixels.

Noise reduction: During the acquisition, coding, transmission, and processing of digital images, noise is constantly present. Without prior understanding of filtering procedures, removing noise from digital photos is extremely difficult.

Resizing: Picture resizing is required when the total number of pixels needs to be increased or decreased, whereas remapping is required when correcting for lens distortion or rotating an image. When you zoom in on an image, the number of pixels increases, allowing you to see more detail.

Thinning is the process of converting a digital image into a simpler but topologically identical version. Thinning is mostly used to create picture descriptor skeletons and to reduce the output of edge detectors to a one-pixel thickness, among other things.

Scanned Image Input: Images of handwritten signatures are scanned digitally using a digital scanner. The signature image is scanned through a scanner and the scanned image input is further used for preprocessing.

Preprocessing: This phase is to make the images of handwritten signatures ready for feature extraction. There are several steps in preprocessing.

Feature Extraction: For the verification of signature, the feature extraction is done. Feature extraction includes various attributes such as categorical attributes, scalar measures, shape, proportionality, text-loops, order, punctuation, alignment to the base, slant of the strokes, strokes length, character spacing, etc.

Training and Recognition: After the scanned image is taken as input and further preprocessed, feature extraction of the processed input is done and the next step to perform is training and recognition of the signature input is done.

Recognized Signature: The aim of the system is to recognize the signature whether it is genuine or forged and identify the author based on the signature verification.

III. SYSTEM DEVELOPMENT

A) SYSTEM ARCHITECTURE

The proposed system uses Convolutional Neural Network and Support Vector Machine Algorithm to classify obtained signature into real or forged.

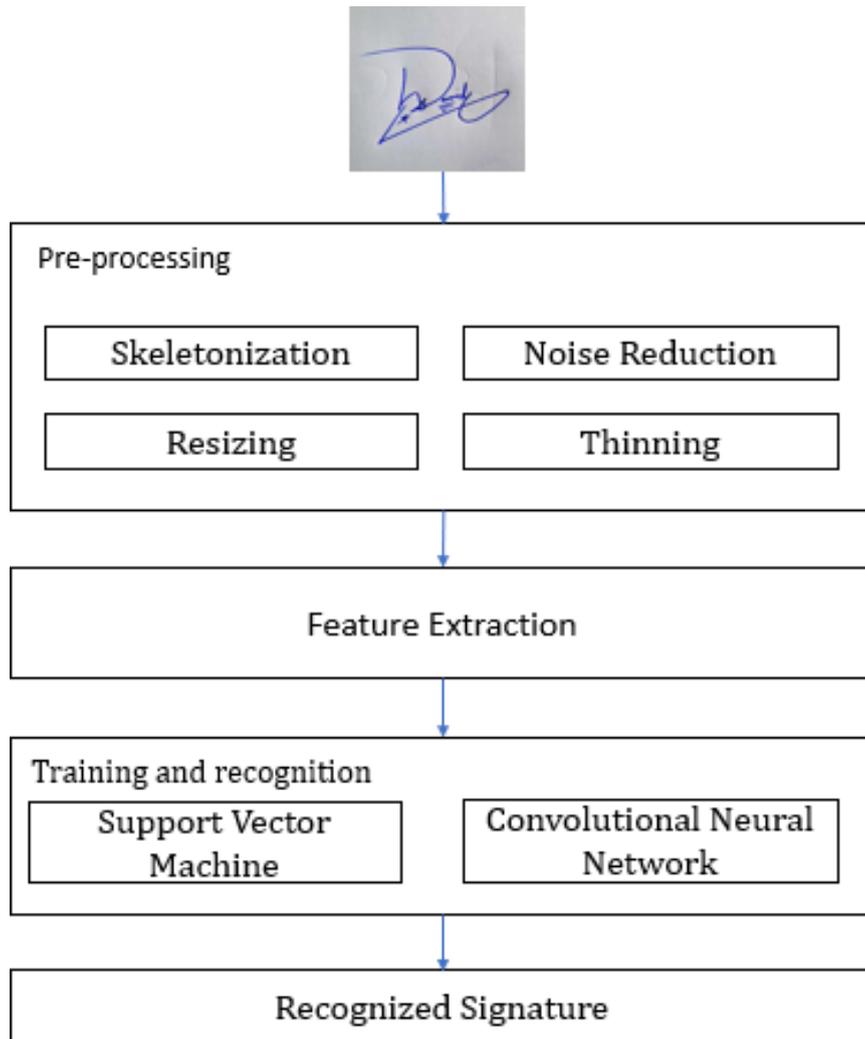


Fig. 3.1.1 System Architecture

B) USE CASE

A use case diagram is a graphical depiction of a user's possible interactions with a system. A use case diagram shows various

use cases and different types of users the system has and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses.

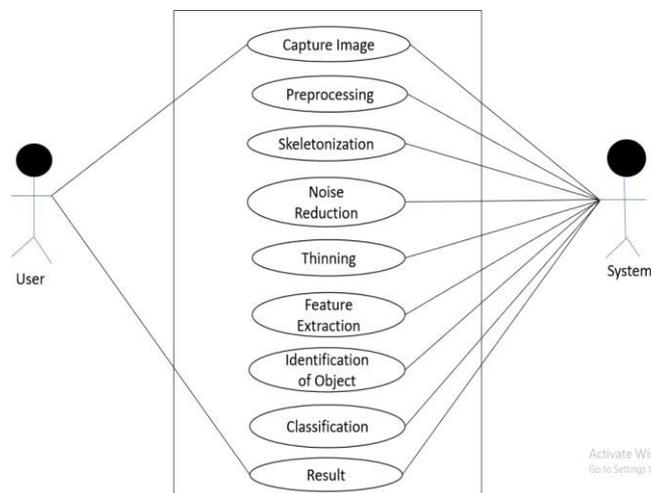


Fig. 3.2.1 Use Case Diagram

IV. CONCLUSION

As a result, in order to prevent signature fabrication, complete author identification is supported by signature analysis and verification. As a result, it will be possible to determine whether or not the signature belongs to the author. It will also lead to the conclusion that the signature has not been cast.

V Acknowledgment

We take this opportunity to thank our project guide Dr. S. V. Todkari sir and head of the department Dr. J. S. Patil for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the department of Information Technology of Jayawantrao Sawant College of Engineering, Pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, internet access and important books.

REFERENCES

- [1]Offline Handwritten Signature Verification Using Low Level Strokes Features, India, IEEE, 978-4799-8792-4/15 by Mohit Kumar A. Joshi, Mukesh M. Goswami, Hardik H. Adesara (2015).
- [2]Image processing-based signature verification technique to reduce fraud in financial institutions by Keigo Matsuda, Wataru Ohyama and Tetsushi Wakabayashi.
- [3]Offline forgery detection of handwritten signature using Gaussian empherical rule by Charu Jain, Preeti Rana, Priti Singh.
- [4]Derlin Morocho, Aythami Morales, Julian Fierrez, Reuben Vera Rodriguez, Human Assisted Signature Recognition based on Comparative Attributes (2017).
- [5]Offline Signature Verification through Machine Learning by Avani Rateria, Suneeta Agarwal (2018).