# Digital Signature Using Neural Network Bannar Amman Institute of Technology

Aathishasan S, Kawin M, Gugan M, Kavin S
*Computer Science And Engineering Bannari Amman Institute Of Technology*

## 1.INTRODUCTION

Digital signatures serve as the main means of authorization and authentication in legal transactions, there is a greater need for effective automated solutions for signature verification [1].In contrast to identification information like a password, PIN, PKI, or key cards that may be misplaced, stolen, or exchanged, the handwritten signature's captured values are specific to each person and nearly impossible to replicate. Verification of signatures is intuitive and natural. The technology is trustworthy and simple to understand. The fact that signatures are already widely recognized as the standard technique for identity verification is the main advantage that signature verification systems have over other kinds of technologies [2].

A signature verification system and the strategies used to solve this challenge are classified into two classes. Both offline and online [3].The online method extracts information about a signature using a pen and an electronic tablet that is connected to a computer. It also gathers dynamic data, such as pressure, velocity, writing speed, etc., for verification purposes. Verification of off-line signatures uses signature images taken by a camera or scanner and requires less electronic management. Features taken from a scanned signature image are used in an offline signature verification method. The offline signature verification features are considerably more straightforward. Only the pixel image needs to be assessed in this case.

However, designing off-line systems is challenging since many desirable features, like stroke order, velocity, and other dynamic information, are unavailable in the off-line scenario [4, 5]. Only the features that can be gleaned from the trace of the static signature images can be used in the verification procedure. The horizontal axis is used to calculate the center of gravity's position. A collection of 2106 signatures, comprising 936 authentic and 1170 fakes, is used to compare two methods for classification and verification: the Radial Basic Function (RBF) and the Resilient Back Propagation (RBP) neural network. The correct verification rates for these two classifiers are 91.21% and 88%, respectively.

### 1.1 Template matching approach

Fang et al. [8] offered two approaches for detecting competent forgeries through template matching. Elastic matching of the strokes in two-dimensional signature patterns is the basis of one approach, while optimum matching of the one-dimensional projection profiles of the signature patterns is the basis of the other. A choice is made based on a distance measure after the positional variations are compared with the training set's statistics for a test signature that needs to be validated. Grey-level and binary signature images are both examined. When comparing grey-level signature images using the local peaks of their vertical projection profiles and incorporating the whole calculated covariance matrix, an average verification error rate of 18.1% was obtained.

For many years, researchers have conducted extensive research on handwriting analysis and pattern matching. Various technologies have been employed in the field of Handwritten Signature Verification (HSV), particularly offline HSV, and research is still ongoing. We examine a few recent papers on offline HSV in this part. The kind of characteristics that are extracted, the training strategy, and the classification and verification model that are employed vary throughout researchers.

### 1.2 Hidden Markov Models Approach

A handwritten signature is a series of value vectors that correspond to each point in the signature's trajectory. Thus, the creation of an effective signature verification system may result from a carefully selected set of feature vectors for HMM. The stochastic nature of these models allows them to take into account both the similarities and differences between patterns. Stochastic matching between the model and the signature occurs in HMM. Steps of the probability distribution of the features included in the signatures or the probability of how the original signature was computed are used to accomplish this matching. The signature is by the original individual if the findings indicate a greater probability than the test signatures probability; if not, the signatures are rejected.The paper [6] presents a system that solely makes use of global features. Using non-overlapping beams per angle for X number of angles, a discrete random transform, or sinograph, is computed for every binary signature image in the range of 0 to 360. This transform is a function of the total number of pixels in the image and the intensity per individual pixel. This periodicity makes it invariant to shift, rotation, and scaling. The model for each writer's signature is an HMM. For an AER of 18.4%, the technique compares a set of 440 authentic signatures from 32 authors with 132 expert forgeries.

1.3 Neural Networks Approach

Neural networks (NNs) are widely used in pattern recognition due to their strength and user-friendliness. Using many samples from various signers, a straightforward method is to first extract a feature set that represents the signature (details like length, height, duration, etc.). Learning the connection between a signature and its class—either "genuine" or "forgery"—is the second stage. After learning this association, test signatures that can be categorized as belonging to a specific signer can be offered to the network. As a result, NNs are ideal for simulating the global features of handwritten signatures.

The suggested technique in [7] divides a signature into two parts and employs structure features from the signatures' contour, modified direction feature, and other features including surface area, length skew, and centroid feature.

1.4 Statistical approach

It is simple to determine the relationship, deviation,etc., between two or more data pieces using statistical expertise.To determine the connection between some set of data items, we typically adhereTo the correlation coefficient notion. refers to the separation of two variables from independence in mainstream statistical usage. This method uses the idea ofcorrelation to determine the degree of divergence between the entered signature and the average signature that is derived fromthe collection of previously gathered signatures.

A novel approach is presented in [9]. This method extracts a number of information, such as geometric and topographical descriptors like local correspondence to the signature trace, statistical features derived from a signature's pixel distribution, and global features like image gradient. The categorization process entails establishing a distribution in distance space as well as differences among the same writer's signatures. A statistical Kolmorogorv-Smirnov test is used to determine the probability of similarity between the distribution that the approach obtains for each questioned signature and the known distribution. The approach achieves 84% accuracy with only 4 real examples for learning, and 89% accuracy with a larger sample set of authentic signatures.

1.5 Support Vector Machine

In order to generalize unseen data, machine learning algorithms known as Support Vector Machines (SVMs) use a high dimensional feature space to infer differences between classes of provided data. For classification and verification, the system in [10] makes advantage of the signature's global, directional, and grid properties as well as SVM. Seventy writers use the 1320 signatures in the database. A total of 320 signatures are used for training, with 40 writers contributing eight signatures apiece. The method obtains FRR 2% and FAR 11% in first testing using 8 original signatures and 8 forgeries.

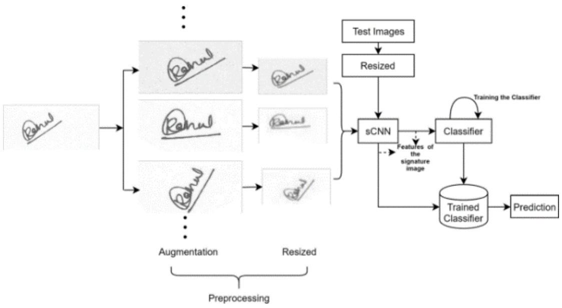
Contribution:

In this paper, we present a model that verifies the model using a neural network classifier. Database signatures are pre-processed prior to feature extraction. Features are extracted from the pre-processed signature image. These features are then retrieved and used to train a neural network. During the verification step, test signatures undergo pre-processing and feature extraction.Following their retrieval, these characteristics are fed into a trained Neural network, which establishes if the signature is realor fraudulent.

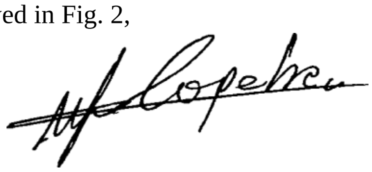
Structure of the paper: This is how the remainder of the paper is structured. The model for verifying signatures is explained in section 2. The algorithm is introduced in section 3.Section 4 presents the results produced by the system, and Section 5 concludes

## 2.TECHNIQUES

This section discusses the system's block diagram. The block diagram of the suggested signature verification system, which confirms the legitimacy of a person's provided signature, is shown in Fig. 1. Two phases comprise the design system:




1) The training phase 2) Phase of testing
Four main steps make up a training stage. 1) Getting a signature image out of a database 2) Pre-processing images 3) The extraction of features 4) Training neural networks
There are five main steps in a testing stage. 1) Finding a signature in a database to test 2) Preparing an image 3) Extracting features 4) Using a trained neural network with extracted features 5) Verifying the results produced by a neural network.
One of the original signature images from a database is displayed in Fig. 2,



and each of the following figures displays the final signature image that was produced by following the instructions in an algorithm.

### 2.1.InitialPreparation

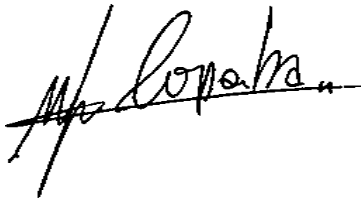
Both the training and testing phases use the preprocessing step. Grayscale scans of signatures are used. This phase's goal is to standardize signatures and prepare them for feature extraction. The pre-processing step enhances the image's quality and prepares it for feature extraction [11].

### 2.1.1 Image conversion to binary

To facilitate feature extraction, a grayscale signature image is transformed to binary.

### 2.1.2 Resizing images

Since the signatory's signatures vary in size, scaling is done to make them uniform in size. This will result in signatures that are 256*256 in size, as seen in Fig. 3.

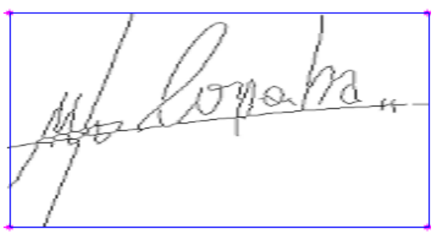


### 2.2 Extraction of Features

Selecting a robust feature set is essential for systems that verify signatures. A feature vector is produced using the features that are extracted during this stage. A candidate signature has been uniquely characterized using a feature vector of dimension 24. The following is how these features extracted:
1) Maximum histogram in both horizontal and vertical directions By counting the amount of black pixels in each row of the signature image, the horizontal histogram is computed. The maximum horizontal histogram is the row with the most black pixels. In a similar manner, a vertical histogram is computed by identifying the column in the signature image that contains the greatest amount of black pixels.
2) The center of mass Divide the signature picture into two equal pieces, then determine each part's center of mass.
3) Normalized signature area
It is the proportion of the signature image's area to the signature's area inside a bounding box. The number of pixels that make up a signature is its area.

### 2.1.3 The signing box's boundaries:

Create a rectangle that encloses the signature in the signature image. This saves time by reducing the region of the signature that needs to be processed further. A bounding box containing a signature is depicted in Figure 4.



### 2.2.4 Feature vector creation

As mentioned in section 2, all of the retrieved features are combined to create a feature vector of size 24.2. 2.2.5 Neural network training To place the extracted 24 feature points within the range of 0 to 1, they are normalized .The neural network receives these normalized features as input.

2.3 Confirmation

In order to acquire a feature vector of size 24, the verification stage involves preprocessing a test signature and performing feature extraction on the pre processed test signature image, as detailed in section 2.2. A feature vector is normalized before being fed into a trained neural network, which determines if a signature is authentic or fake.

## RESULT

The Digital Signature Using Neural network is prepared to characterize the marks into real or manufactured with the objective qualities 1 for certified and 0 for fashioned marks. Veritable marks will have a brain network yield esteems more like 1 and manufactured mark to 0.