Abstract: Signature Authentication is one of the popular biometric technique. This paper discusses Signature verification & recognition using neural network. In this we are recognizing whether the signature of an individual is original or fraud. There are two major classes of signature authorization: 1. Online Signature Verification & Recognition 2. Offline Signature Verification & Recognition. This paper deals with Offline Signature Verification & Recognition and there are 3 major steps:
1. Image pre-processing.
2. Feature Extraction
3. Neural Network Training
The process starts with scanning image & then we modify its quality by using various image enhancements & noise reduction techniques. Which comes under image pre-processing? Then we extract various features of signature image which are used later in neural network training.
Finally authenticates the user in neural network training

Keywords: Biometric, Image pre-processing, Feature Extraction, Neural Network Training, Signature Verification & Recognition
1. Introduction:

Signature is an act of writing one’s name. It may contain alphabet, letters, and special symbols/characters. Therefore most of the time we are unable to read it. Hence we treat signature as an image. Image is an array or matrix of pixels. Now, this signature image can be recognized using trained neural network.

Signature authentication contains 2 parts:

- Signature recognition
- Signature verification

Signature recognition scans the signature of a person and matches it with the signature stored in database.

In Signature verification the test signature (The signature to be authenticate) must be compared with all the signature in the database. In short it verifies whether the test signature is original or fraud/forged. There are two major classes:

- Online signature Verification & Recognition
- Offline Signature Verification & Recognition.

In Online signature Verification & Recognition, signature is recognized by measuring 2 characteristics speed & pressure given by a person during signing the signature. In Offline Signature Verification & Recognition, image pre-processing & feature extraction technique are used mainly to recognized the text sign.

The need for signature Authentication is to differentiate between original signature and forgery. Forgery is nothing but an attempt to make false sign of other individual to get unauthorized access. Forgery are of 3 types:

![Figure 1: Types of Forgeries](image)
- **Hit-Or-Miss Forgery**: Hit-Or-Miss Forgeries are the simple forgery that can be uncovered effortlessly. Forger creates a signature in its own style or without having any knowledge of original signature.

- **Well-Versed Forgery**: Forger may be master in imitating original signature. Here, forger have knowledge about original sign i.e. how it looks like.

- **Amateur Forgery**: In this forger keep an eye on original signature and tries to create sign. Here the forger is not experienced person.

![System Architecture](image)

*Figure 2: System Architecture*

This paper is organized as follows:

- Part-1 describes literature survey.
- Part 2 introduces proposed system.
- Part 3 Represent architecture of proposed system.
- Part 4 Concludes the topic.
2. Literature Survey:

TECHNIQUES

There are many methods that have been developed in the area of signature verification. We are describing some of the convenient approaches here.

2.1 Hidden Markov Model:

One of the approach is Hidden Markov Model[8] for offline signature verification developed by Justino, Bortolozzi and Sabourin to detect or discover, hit-or-miss, well-versed, Amateur forgeries. This method depends upon grid segmentation scheme which extract 3 features: Pixel density feature, Pixel distribution feature and an axial slant feature for detecting forgeries, a database of 1600 genuine signature is used. Signature of 60 writers with 40 training signature, 10 genuine test signatures, 10 hit-or-miss forgeries and 10 well-versed forgeries per signer is used in another data set for experimentation. This method gives False Acceptance Rate of 2.83% and False Rejection Rate of 1.44%, 2.50%, 22.67% are obtained for hit-or-miss, well-versed, Amateur forgeries respectively.

2.2 Shape Descriptors Method:

Another approach for signature verification system is using shape descriptors and multiple neural networks proposed by Mehdi Dehghan, Karim Faez and Mahmood Fathi. In this descriptors some of the shape descriptors are skeleton, upper and lower envolops of the signature and high pressure region of the signatures. Multiple multilayer perceptron neural network model was used to verify signature. This neural network makes use of fuzzy integral voter. A multiple multilayer perceptron was selected as a signature classifier for each different signature descriptor. Modified BP (Back Propagation) algorithm was used to trained this neural network. Here from 50 persons approximately 1000 signatures were taken and stored in database with hit-or-miss and well-versed forgeries. This approach gives 96% accuracy for hit-or-miss and 90 % for well-versed forgeries. The overall accuracy obtained is 98%[9].

2.3 Modified Direction Feature(Mdf):

Nguyen et al. developed an offline signature verification system which was based on 3 global features and a Modified Direction Feature (MDF).

An MDF Feature extraction technique employs the location of transitions from background to foreground pixels and the direction at transition in the vertical and horizontal directions of the boundary representation of an object. The Location of Transitions (LT) and Direction Transition (DT) values are recorded at each transition. 12 genuine and 400 hit-or-miss forgeries are taken publicly available database. The Support Vector Machine (SVM) classifier gives an Average Error Rate (AER) of 17.25% [10].

2.4 Back Propagation Neural Network:

Signature recognition system developed by Abbas used a Back Propagation neural network prototype. It was based on Multilayer Feed forward Structure and 3 different algorithms were used vanilla, enhanced and batch. This method obtained FAR between the range of 10-40% for amateur forgeries. Hanmanlu proposed a neuro-fuzzy system in which angles made by the signature pixels are compute with respect to reference points.

2.5 Moment Invariant Vector:

One of the method for signature verification and recognition moment invariant method and ANN[1]. 2 separate neural networks were designed one for the signature recognition and another for signature verification (i.e. for detecting forgery) both the network uses 4 step process.

First step is to separate the signature from its background. Second step performs normalization and digitization of the original signature. Third step calculates moment invariant vectors. And the last step implements signature recognition and verification. 10 signatures were taken for training: 5 true signature and 5 forgeries. This method detected 4 true signature and 5 forgeries correctly. It gives 100% success rate by identifying correctly all of the 30 signature that it was trained for but gives poor performs when it was present with signature that it was not trained for.

3. Proposed System

The proposed system consists of 3 major tasks:

- Image pre-processing.
- Feature extraction.
- Neural network training for pattern recognition.
Let us discuss this tasks in detail:

3.1 **Image Pre-Processing:**

After an image is acquired it goes through different levels of processing before applying it to the next step i.e. feature extraction. The image pre-processing is an important task because of the following reasons:

- It creates a level of similarity in terms of general features of an signature image such as size, sharpness, etc. This helps to compare two signature images easily.
- Signature can vary according to the tools we are using to write. Various other factors can vary signature such as pen, pencil, ink, pressure of hand, etc. In offline signature recognition we are not that important in this case and have to be eliminated. Instead of this we are extracting features for matching two signatures.
- Image pre-processing reduces noise, defects enhances the image. It also improves the quality of image information.
- The techniques used in image pre-processing are:
  i. Grey scaling.
  ii. Thresholding.
  iii. Bluring.
  iv. Thinning.
  v. Cropping

3.2 **Feature Extraction:**

Feature extraction is the next step in signature recognition & verification. It is an important step in signature verification system, as it is the key to identify & differentiate a user’s signature from another. If we want to compare two signatures there should be some measurement on which the comparison can be based. In this step, we are generating features which are used as comparison measurements. As signature verification is highly sensitive process we need more than one feature to be extracted. More extracted features contributes in enhancing the accuracy of the results.

Feature is nothing but a characteristic of an image that can be measured with the help of some designed algorithms. These features can be retrieved later by extraction.
Feature extraction involves two types of features:

- Global feature.
- Texture feature.

We are only focusing on global features here.

**Global Feature Extraction:**

1. **Signature height-to-width ratio:**
   This feature can be obtained by simply dividing signature height to signature width. Height to width ratio of one person’s signature are approximately equal.

2. **Signature Area:**
   Signature can be obtained by calculating no. of pixels belonging to the signature. This gives information about signature density.

3. **Maximum Horizontal and Maximum Vertical Histogram:**
   Horizontal histogram can be calculated for each row. The row which has the highest value is maximum horizontal histogram. Similarly the vertical histograms are calculated for each column. The column having highest value is maximum vertical histogram.

4. **Horizontal and vertical centre of signature:**
   For each column, those row index values, which are having black pixels are added in row_index_sum. The counter is incremental for each black pixel encountered.
   Calculate Cx by using formula:
   \[ Cx = \frac{\text{row}_\text{index}_\text{sum}}{\text{total black pixels encountered}} \]
   Similarly Calculate column_index_sum &
   \[ Cy = \frac{\text{column}_\text{index}_\text{sum}}{\text{total black pixels encountered}} \]
   Finally center is obtained by
   \[ \text{Center} = (Cx+1)\times\text{total column in signature} + Cy \]

5. **Edge point number of signature:**
   Edge point is the pixel which has only one neighbour which belongs to the signature in 8- neighbour region.

These features are given to trained neural n/w for pattern recognition.
3.3 Neural Network Training for Pattern Recognition:

Neural network is a computational model which is inspired by the biological nervous system. It is an interconnected group of artificial neurons. Neurons are processing elements working in unison to solve specific problem. Neural networks are known for being very accurate and efficient technique for pattern recognition. Neural network is a application of artificial intelligence. This computer application is trained to think like a human being or even better.

Neural networks like human beings adopt the idea of learning in order to achieve any task. The learning involves training on a large amount of data, which enables to create a pattern that will be used to verify signatures. Neural networks are very useful in discovering patterns which are difficult to derive by humans. It can be used in application where high security is required.

In this we are using Multi Layer perceptrons MLP’s neural network. This has a multi layer feed forward structure, where all the nodes of one layer have connection to all the nodes of the next layer and so on. But the nodes do not have connections to its previous layers. For this purpose we have to modify the function as a back propagation neural network using BP algorithm.

The inputs to trained neural network are signature and its extracted features. The output layer consists of a single node which calculates the weighted sum of the connections coming to the output layer. The final output of MLP neural network is a confidence value. Confidence value indicates the likelihood whether the test signature is original or fraud. This confidence value is compared with thresholding value which is user defined. If confidence value is greater than threshold value it is accepted otherwise rejected.

4. Recognition:

A trained neural network compares the features of a given signature with the features of signature in the database. The differences between these signatures are calculated. A tag of the signature having least differences is returned with a number that shows percentage of
similarity. Based on percentage of similarity the decision is taken whether the signature is original or not.

i. Signature is considered original: If the percentage of similarity ranges between 85-100%. This is because there are natural differences in the signature of a single person in multiple attempts.

ii. Signature is considered relatively doubtful: If the percentage of similarity ranges between 75-85%.

iii. Signature is considered highly doubtful: If the percentage of similarity is lower than 75%.

5. Conclusion:

This paper presents a method for offline signature identification using MLP neural network which uses global features: Signature area, signature height-to-width ratio, horizontal and vertical centre of signature, max horizontal and max vertical histogram, number of edge points of the signature which can be extracted by image processing. The neural network was trained using Back Propagation algorithm.
References:

1. C. Oz, F. Ercal, and Z. Demir, “Signature Recognition and Verification with ANN”, in Proc. of Third International Conference on Electrical and Electronics Engineering, (ELECO'03), Bursa, Turkey, December 2003.


5. Rajesh Kumar, Member, IEEE, Nikhil R. Pal, Fellow, IEEE, Bhabatosh Chanda, and J. D. Sharma, "Forensic Detection of Fraudulent Alteration in Ball-Point Pen Strokes", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

6. Debasish Jena, Banshidhar Majhi, Sanjay Kumar Jena, "Improved offline Signature Verification Scheme Using Feature Point Extraction Method", National Institute of Technology Rourkela, Orissa, India.


