

# Image Processing for Signature Verification

Pallavi V. Hatkar, Zareen J Tamboli

*Abstract* As signature is the primary mechanism both for authentication and authorization in legal transactions, the need for efficient auto-mated solutions for signature verification has increased [3].

Unlike a password, PIN, PKI or key cards – identification data that can be forgotten, lost, stolen or shared – the captured values of the handwritten signature are unique to an individual and virtually impossible to duplicate. The primary advantage that signature verification systems have over other type's technologies is that signatures are already accepted as the common method of identity verification [4]. A signature verification system and the techniques used to solve this problem can be divided into two classes Online and Off-line [5]. On-line approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc. for verification purpose. Whereas Off- line signature verification involves less electronic control and uses signature images captured by scanner or camera. An off-line signature verification system uses features extracted from scanned signature image. In this only the pixel image needs to be evaluated.

*Index Terms*— Artificial Neural Network, Average Error verification rate, Handwritten Signature Verification Probabilistic Neural Network.

## I. INTRODUCTION

For any legal transactions the authorization is done by the signature. So the need of the signature verification increases. The handwritten signatures are unique for individuals and which is impossible to duplicate. The technology is easy to explain and trust. The primary advantage that signature verification systems have over other type's technologies is that signatures are already accepted as the common method of identity verification. The handwritten signature verifications are of two types Online and the offline. On-line method uses an electronic technique and a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc. for the purpose of verification. In off-line signature verification involves less electronic control and uses signature images captured by scanner or camera.

An off-line signature verification system uses features extracted from scanned signature image. The features used for offline signature verification are much simpler. In this only the pixel image needs to be evaluated. But, the off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature images. In the area of Handwritten Signature Verification (HSV), specially offline HSV, different technologies have been used and still the area is being explored.

## II. NEURAL NETWORKS

The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power and ease of use. A simple approach is to firstly extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. The second step is for the NN to learn the relationship between a signature and its class (either "genuine" or "forgery"). Once this relationship has been learned, the network can be presented with test signatures that can be classified as belonging to a particular signer. NNs therefore are highly suited to modeling global aspects of handwritten signatures. The proposed system in uses structure features from the signatures contour, modified direction feature and additional features like surface area, length skew and centroid feature in which a signature is divided into two halves and for each half a position of the centre of gravity is calculated in reference to the horizontal axis. For classification and verification two approaches are compared the Resilient Back propagation (RBP) neural network and Radial Basic Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively. In this paper we present a model in which neural network classifier is used for verification. Signatures from database are pre-processed prior to feature extraction. Features are extracted from pre-processed signature image. These extracted features are then used to train a neural network. In verification stage, on test signatures pre-processing and feature extraction is performed. These extracted features are then applied as input to a trained neural network which will classify it as a genuine or forged signature.

**Manuscript received May 18, 2015**

**Pallavi V. Hatkar**, Department of E& TC Engineering, Sanjay Ghodawat Group of institutions, Atigre, India

**Zareen J Tamboli**, Department of E& TC Engineering, Sanjay Ghodawat Group of institutions, Atigre, India

### III. METHODOLOGY

In this section, block diagram of system is discussed. Fig. 1 gives the block diagram of proposed signature verification system which verifies the authenticity of given signature of a person. The design of a system is divided into two stages;

- A) Training stage
- B) Testing stage

#### A Training Stage Consist Of Four Major Steps

- i. Retrieval of a signature image from a database
- ii. Image pre-processing
- iii. Feature extraction
- iv. Neural network training.

#### B. Testing Stage Consists Of Five Major Steps

- i. Retrieval of a signature to be tested from a database
- ii. Image pre-processing
- iii. Feature extraction
- iv. Application of extracted features to a trained neural network
- v. Checking output generated from a neural network.

### IV. BLOCK DIAGRAM

- Block Diagram

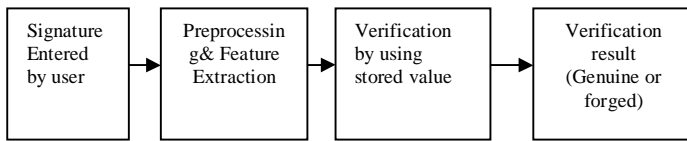


Figure 1: Block Diagram.

### V. FLOW CHART

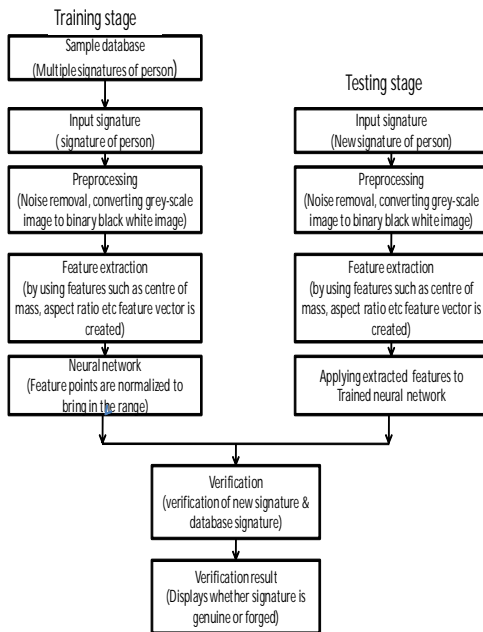


Figure 2: Flow Chart



Figure 3: Signature Image from the database

Fig. 3 shows one of the original signature image taken from a database and all the subsequent figures show the resultant signature image obtained after performing the steps mentioned in an algorithm.

The pre processing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signature standard and ready for feature extraction. The pre-processing stage improves quality of the image and makes it suitable for feature extraction. The preprocessing stage includes. A gray scale signature image is converted to binary to make feature extraction simpler. The signatures obtained from signatory are in different sizes so, to bring them in standard size, resizing is performed, which will bring the signatures to standard size 256\*256 as shown in Fig. 3. Thinning makes the extracted features invariant to image characteristics like quality of pen and paper. Thinning means reducing binary objects or shapes to strokes that are single pixel wide. In the signature image, construct a rectangle encompassing the signature. This reduces the area of the signature to be used for further processing and saves time.

The choice of a powerful set of features is crucial in signature verification systems. The features that are extracted in this phase are used to create a feature vector. A feature vector of dimension 24 has been used to uniquely characterize a candidate signature. These features are extracted as follows:

#### A. Maximum horizontal and vertical histogram

Horizontal histogram is calculated by going through each row of the signature image and counting number of black pixels. A row with maximum number of black pixels is recorded as maximum horizontal histogram. Similarly, a vertical histogram is calculated by going through each column of the signature image and finding a column with maximum number of black pixels.

#### B. Center of Mass

Split the signature image in two equal parts and find center of mass for individual parts.

#### C. Normalized area of signature

It is the ratio of area of signature image to the area of signature enclosed in a bounding box. Area of a signature is the number of pixels comprising it.

#### D. Aspect Ratio

It is the ratio of width of signature image to the height of the image. This is done because width or height of person's signature may vary but its ratio remains approximately equal.

#### E. Tri surface feature

Two different signatures may have same area .so; to increase the accuracy of the features three surface feature has been used.

#### F. The six fold surface feature

Divide a signature in three equal parts and find bounding box for each part. Then calculate centre of mass for each part. Draw a horizontal line passing through centre of mass of each part and calculate area of signature above and below centre of mass within a bounding box. This provides six features.

#### G. Transition feature

Traverse a signature image in left to right direction and each time there is a transition from 1 to 0 or 0 to 1, calculate a ratio between the position of transition and the width of image traversed and record it as a feature. Repeat a same process in right to left, top to bottom and bottom to top direction. Also calculate total number of 0 to 1 and 1 to 0 transitions. This provides ten features.

### VI. ALGORITHM

Input: signature from a database Output: verified signature classified as genuine or forged

1. Retrieval of signature image from a database.
2. Pre-processing the signatures.
3. Converting image to binary.
4. Image resizing.
5. Thinning.
6. Finding bounding box of the signature.
7. Feature extraction
8. Maximum horizontal and vertical histogram
9. Centre of mass
10. Normalized area of signature
11. Aspect ratio
12. The tri surface feature
13. The six fold surface feature
14. Transition feature
15. Creation of feature vector by combining extracted features.
16. Normalizing a feature vector.
17. Training a neural network with a normalized feature vector.
18. Steps 1 to 17 are repeated for testing signatures.
19. Applying normalized feature vector of test signature to trained neural network.
20. Using a result generated by the output neuron of the neural network declaring a signature as a genuine or forged.

### VII. RESULT AND DISCUSSION

For training and testing of the system many signatures are used. The results provided in this research used a total of 1000 signatures. Those 1000 signatures are comprised of 100 sets (i.e. from 100 different people) and, for each person there are 5 samples of genuine signatures and 5 samples of forgeries. To train the system, a subset of this database was taken comprising of 5 genuine samples taken from each of the 100 different individuals and 5 forgeries made by different person for one signature. The features extracted from 5 genuine signatures and 5 forged signatures for each person were used to train a neural network. After applying a feature vector of test signature if the output neuron generates value close to +1 test signature is declared as genuine or

if it generates value close to -1 it is declared as forged. The Accuracy of system is 86.25%

### REFERENCES

1. R. Plamondon and S.N. Srihari, "Online and Offline Handwriting Recognition: A Comprehensive Survey", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.22 no.1, pp.63-84, Jan.2000
2. B. Herbst, J. Coetzer, and J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," EURASIP.Journal on Applied Signal Processing, vol. 4, pp. 559-571, 2004.
3. JunLin chen; wen, jing; "Video-Based Signature Verification by Tracking Pen Tip Using Particle Filter Combined with Template Matching" IEEE Conference 2009 , vol. 1 PP. 83 - 88
4. Martinez, L.E., Travieso, C.M, Alonso, J.B., and Ferrer, M. Parameterization of a forgery Handwritten Signature Verification using SVM. IEEE 38th Annual 2004 International Carnahan Conference on Security Technology ,2004 PP.193-196
5. Vielhauer.c, Mayerhoper.A "Biometric hash based on statistical features of online signatures" IEEE Conference 2002, vol. 1 PP. 123 - 126
6. Prashanth CR,KB Raja,KR Venugopal, LM Patnaik,"Standard Scores Correlation based Offline signature verification system", International Conference on advances in computing, control and telecommunication Technologies 2009
7. M. Blumenstein, S. Armand, and Muthukkumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification," International Joint Conference on Neural Networks, 2006.
8. Prasad A.G. Amaresh V.M. "An offline signature verification system"
9. Ramachandra A. C ,Jyoti shrinivas Rao"Robust Offline signature verification based on global features" IEEE International Advance Computing Conference ,2009.
10. Ashwini Pansare, Shalini Bhatia "Handwritten Signature Verification using Neural Network" International Journal of Applied Information Systems (IJ AIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 1– No.2, January 2012

### ACKNOWLEDGMENT

We take the opportunity to express our reverence to Sanjay Ghodawat group of Institutes, Atigre, Kolhapur for the support and available facilities during the course of this work. The encouragement and enthusiasm given by the Institute in research has motivated us. Dr. V.A.Raikar, the Academic Advisor and Mr. Vinayak Bhosale, Trustee deserve special thanks for encouraging us to do Research work. We thank all our teachers and colleagues for their contribution in our studies and research work.



Ms.Pallavi V Hatkar, Working as Assistant Professor in E& TC Dept. in Sanjay Ghodawat Group of Institution for 2 years and AMGOI for 1.5 years. Worked as R& D Engineer in Innlink Technology, Mudshingi



Ms.Zareen J. Tamboli, Working as Assistant Professor in E& TC Dept. in Sanjay Ghodawat Group of Institution for 3 years