

## Proposed Method for Off-line Signature Recognition and Verification using Neural Network

Dhananjay S. Rakshe<sup>1</sup>, Prof. D.B. Kshirsagar<sup>2</sup>

<sup>1</sup>Computer Department, SRES College of Engineering Kopergaon

<sup>2</sup>Computer Department, SRES College of Engineering Kopergaon

**Abstract**— Computers have become common and are used in almost every field including financial transactions, thus providing additional security measures is necessary. According to consumer's expectations, these security measures must be cheap, reliable and un-intrusive to the authorized person. The technique which meets these requirements is handwritten signature verification. Signature verification technique has advantage over other biometric techniques: including voice, iris, fingerprint, palm etc. as it is mostly used for daily routine procedures link banking operations, document analysis, electronic funds transfer, access control and many other. Most importantly, it's easy and people are less likely to object it. Proposed technique involves using a new approach that depends on a neural network which enables the user to recognize whether a signature is original or a fraud. Scanned images are introduced into the computer, their quality is modified with the help of image enhancement and noise reduction techniques, specific features are extracted and neural network is trained, The different stages of the process includes: image pre-processing, feature extraction and pattern recognition through neural networks.

**Keywords**-Feature Extraction; Neural Network; Signature Verification and Recognition; Image Processing; Grid Based Feature Extraction

### I. INTRODUCTION

In the business world we sign things such as accounts and other official documents. Personal signature lends itself well for biometric verification in state-of-the-art electronic devices. Unfortunately, one drawback of signature is that people do not always sign documents in exactly the same manner. For example, the angle at which they sign may be different due to seating position or due to hand placement on the writing surface. Other affecting factors can be variety of pens, different inks used to make signature; but these things can be eliminated with the help of image enhancement and noise reduction techniques.

In this era of automation, automatic person identification is a major challenge, not that it's a new problem to the society but with this significant development of internet; interactions are becoming more and more automatic and thus the problem of identity of individual has become more important. Handwritten signatures are most easy and preferable because they are used to carry out daily transactions, they are less controversial, every individual's signature is unique and people are less likely to object it.

According to the studies that were done on signatures and types of signatures, forged signatures [1] fall into following three categories:

- **Random:** These signatures are not based on any knowledge of the original signature. Means the person who is trying to make a fake signature does not have any knowledge of what the original signature looks like or how it's made, forger simply tries to make one randomly and this signature can be easily identified as fake.

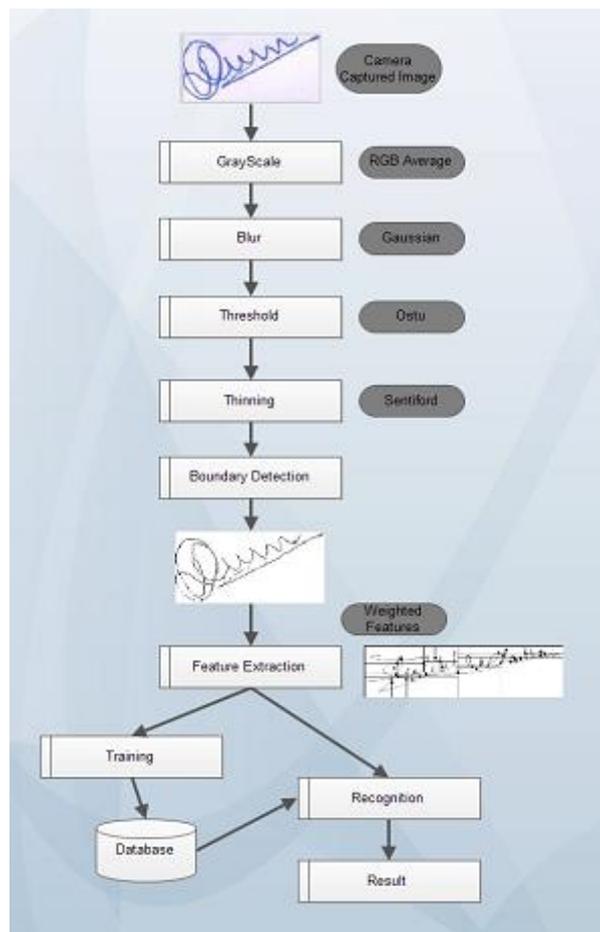
- Simple: These signatures are based on an assumption of how the signature looks like by knowing the name of the signer. By having knowledge of the name of the signer, the possibilities are limited about how the signer would have made his sign. Most of the people simply write their name. So the chances of faking a signature are increased by some amount.
- Skilled: An imitation of the original signature, which means that the person knows exactly how the original signature looks like. Here, forger knows exactly how the original sign looks like. Therefore, a perfect imitation can be made if the forger is good at copying.

We can tell that skilled signatures are the most difficult ones to detect as they can be very similar to the original signature and the error rate might be very small.

## II. SYSTEM OVERVIEW

The system mainly focuses on following areas-

- Image Pre-processing
- Feature Extraction
- Neural Network Training



**Figure 1. System Overview**

Figure 1 shows the offline signature recognition and verification system. As illustrated in the design, Scanned signature is taken as an input (using camera or scanner) and is provided to the system for pre-processing. Image will be processed using different image enhancement and noise reduction techniques. These techniques involve converting input image into grayscale, making it blur so that to

make it smoother, binarizing the image to achieve black and white image, detecting boundaries to remove unnecessary portions of image and thinning the image etc. Reason behind using these techniques is to enhance the image to a suitable form so that it can be properly used. As different people make signatures in different ways, pens and ink used to create these signatures varies too. So it becomes essential to enhance the input image first. Next step involves extracting different types of features from the input image and storing them in the database for future use. These features are used for comparison with the features that will be extracted from input signatures while authenticating them. Meanwhile, they are also used to train the neural network. After successful training of neural network, it can be used in recognition process to authenticate whether provided signature is authentic or a forgery.

### **III. SIGNATURE RECOGNITION AND VERIFICATION**

#### **3.1. Image Pre-Processing**

Image pre-processing has a wide range of techniques that exists for the manipulation and modification of images. It is the first step in signature verification and recognition. A successful implementation of this step produces improved results and higher accuracy rates. Following are the reasons why image pre-processing is important:

- It creates a level of similarity in the general features of an image, like the size aspect. This enhances the comparison between images.
- Signatures vary according to the tool that was used in writing; the type of pen/pencil, the ink, the pressure of the hand of the person making the signature, and so on. In off-line signature recognition, these facts are not important, and have to be eliminated and the matching should be based on more important offline features.
- Noise reduction, defects removal and image enhancement.
- Improves the quality of image information.
- It eases the process of feature extraction on which the matching depends mainly.

Following image pre-processing techniques can be used:

**RGB average:** RGB average algorithm can be used to convert an image into grayscale. This method separates Red, Green and Blue values from 24 bit image and averages them i.e. grayscale component is calculated. Then it simply replaces every original pixel value with its grayscale component.

**Otsu (threshold):** Pixel intensity ranges from 0 to 255. User defined threshold is used to compare pixels and accordingly black or white values are assigned to them and vice versa to achieve pure black and white image.

**Gaussian (Blur):** Blurring can be used to make images smoother. This method helps when images are too sharp. We simply adjust the intensity of surrounding pixels for e.g. 25 pixels (considering window size 5\*5) to make them blur.

**Stentiford (thinning):** Thinning is the most important part and can be done successfully using Stentiford algorithm. Outputs will be as shown in figures 2, 3, 4 below-

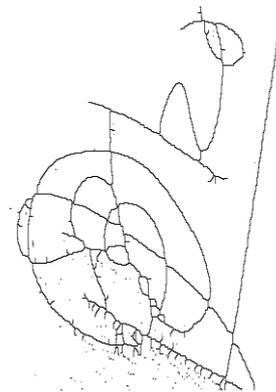
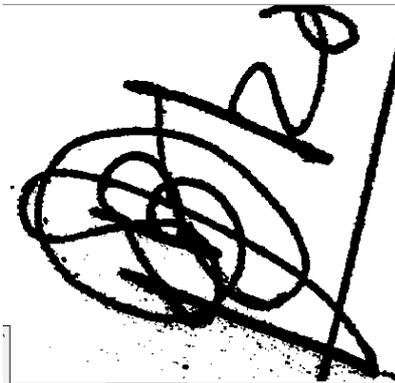
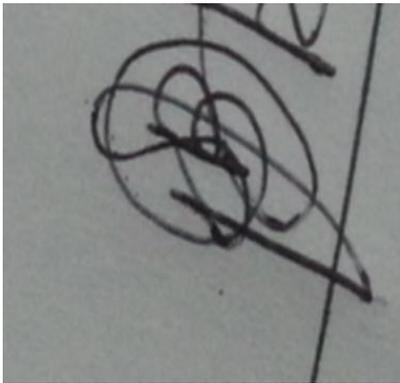


Figure 2. Blur and Grayscale  
 Figure 3. Threshold  
 Figure 4. Thinning

### 3.2 Feature Extraction

Objective of this phase is to extract the features [2] of the test image that will be compared to the features of training image for verification purpose.

- 1) After preprocessing we have a signature of size 100x200(pixels). Then we make a grid of  $m \times n$  where  $m < n$ ,  $m \ll 100$  and  $n \ll 200$ , over a pre-processed signature as shown in Figure 5. Let's say we take  $m=10$  and  $n=20$ . Thus, a signature image is divided into 200 square cells where each cell is having 100 pixels.
- 2) Now we find the cells of a row of a grid that contains signature content. Signature content is calculated in terms of black pixels, therefore only those cells should be considered which are having 3 or more black pixels. Repeat the process for all rows of a grid. Thus we have all those cell positions which are part of the signature image. Now we create a matrix of size  $m \times n$  corresponding to the grid of size  $m \times n$  i.e. one cell of a grid corresponds to one element of a matrix. The matrix element is equal to 1 if the cell of same position in the grid is the part of signature, otherwise the matrix element will be 0. Thus, as a result of this step, we have a matrix having elements 0 or 1 accordingly as shown in Figure 6.

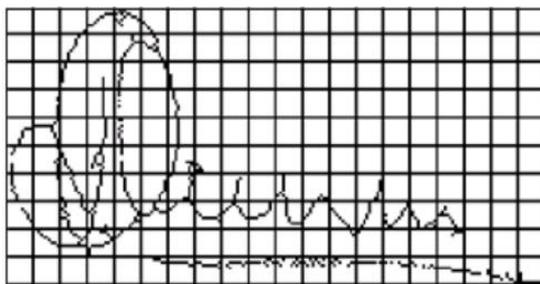


Figure 5. Grid over image

0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	0	1	0	1	1	0	1	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Figure 6. Corresponding matrix

- 3) We calculate the number of black pixels in cells of a row containing signature content. Repeat the process for all rows. Then we put the values of  $m$  rows in an array. Similarly, the same process can be applied to columns. Thus we get another array having  $n$  elements corresponding to each column.

Thus we extract three features: (i)  $m \times n$  matrix as described above corresponding to an  $m \times n$  grid. (ii) An array of size  $m$  where first element is the number of black pixels in first row of a grid, second element is the number of black pixels in second row and so on, (iii) An array of size  $n$  where the first element is the number of black pixels in first column of the grid, second element is the number of

black pixels in second column and so on. These features are further used in verification process. We have to compare these features of the test and reference signature images and then classify them as genuine or forge.

### 3.3 Neural Network Training

#### a) Calculate Column Matching Score (CMS)

(i) Let  $M_1$  and  $M_2$  be the matrices of reference image and test image respectively. Compare the columns of the matrix  $M_2$  with  $M_1$ . Each column is having  $m$  elements. If at least  $\beta$ , where  $\beta \geq 7$ , elements are same then that column is said to be matched and increase the column count  $C_1$  (say) by one.

(ii) Let  $A_1$  and  $A_2$  be the arrays of reference image and test image respectively containing number of black pixels in each column. Compare the corresponding elements of array  $A_2$  with  $A_1$ . Now check the following condition:

$$\sigma_{Ref} - \alpha < \sigma_{Test} < \sigma_{Ref} + \alpha$$

Where,  $\sigma_{Ref}$  is the element of reference array  $A_1$ ,  $\sigma_{Test}$  is the corresponding element of the test array  $A_2$  and  $\alpha$  is the tolerable factor which is the allowed variation in number of pixels. Tolerable factor is a dynamic value as it varies for different columns depending on the signature content in that column. Tolerable factor can be calculated as:

$$\alpha = \frac{P * \sigma_{ref}}{100}$$

Where,  $p$  is percentage of black pixels in a column of a grid and  $\sigma_{Ref}$  is the number of black pixels in that column. Width is the distance between two points in the horizontal projection and must contain more than 3 pixels in a cell, height is the distance between two points in the vertical projection and must contain more than 3 pixels in a cell.

If condition (1) satisfies then that column is acceptable and increase the counter  $C_2$  (say) by one.

(iii) If  $C_1 = n$  and  $C_2 = n$ , then CMS is said to be 100%.

Similarly for  $C_1 = n-i$  and  $C_2 \geq n-i$  where  $i=1, \dots, 8$ , CMS will be signatures up to 60% CMS are considered for further processing. If CMS is below 60% then the test signature will be classified as forgery at this step itself.

#### (b) Calculate Row Matching Score (RMS)

If  $CMS \geq 60\%$  then only we are interested in calculating Row Matching Score (RMS). It can be obtained same as CMS. All comparisons have to be done row wise. For RMS,  $\beta \geq 14$ . Calculate  $C_1$  and  $C_2$  for this case.

#### (c) Calculate the Average of CMS and RMS

#### (d) Threshold

Here the threshold is the security level which the user wants to achieve in the target application. If the user wants 100% security then input will be 100 and if the average of the CMS and RMS is 100% then the signature will be accepted. If the user wants 95% security then input will be 95 and if the average is greater or equal to 95% then the signature will be accepted. Threshold range is from 100 to 65 i.e. lowest security level for which results can be obtained in the proposed system, is 65. If average is below 65% then that signature will be classified as forge. Since the proposed technique works for a range of security levels, it can be used in various applications in which different level of security is required for different applications.

### III. CONCLUSION

In this paper, we have discussed an offline signature verification technique using grid based feature extraction. The preprocessed signature i.e. resized, gray scaled, binarized, and thinned signature is segmented into grid of size 10x20 cells where each cell is having 100 pixels. Matrix corresponding to grid is formed and arrays containing number of black pixels in rows and columns formed. For verification, these two features for training and test images can be compared both row wise and column wise and then the test signature can be classified accordingly. As far as database is concerned, one can simply use scanned images or camera captured images, also a freely available database at <http://www.vision.caltech.edu/mariomu/research/data> can be used.

### REFERENCES

- [1] Suhail M. Odeh, Manal Khalil, Off-line signature verification and recognition: Neural Network Approach, 978-1-61284-922-5/11/\$26.00 2011 IEEE.
- [2] Swati Srivastava, Suneeta Agarwal, Offline Signature Verification using Grid based Feature Extraction International Conference on Computer Communication Technology (ICCCCT)-2011
- [3] Devshri Satyarthi 1 , Y.P.S. Maravi 2 , Poonam Sharma 3 , R.K. Gupta, Comparative Study of Offline Signature Verification Techniques, International Journal of Advancements in Research Technology, Volume 2, Issue2, February-2013
- [4] Vaishali M. Deshmukh, Sachin A. Murab, Signature Recognition Verification Using ANN, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-6, November 2012

