International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-5)

Research Article | **May 2015**

Robust Signature Verification and Recognition Using Weighted Features Point

Nikita S. Wani, S. P. Patil
Electronics and Telecommunication &
North Maharashtra University,
Maharashtra, India

Abstract—

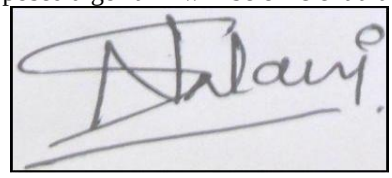
This review paper robust signature verification and recognition using weighted features point that depends on a artificial neural network which discriminate between two classes (i) forgery and (ii) original signature. The proposed scheme is based on the technique that applies pre-processing on the signature, feature point extraction and neural network training and finally verifies the authenticity of the signature. The objective of the proposed scheme is to reduce two vital parameters False Acceptance Rate (FAR) and False Rejection Rate (FRR). That means results are expressed in terms of FAR and FRR and subsequently comparative analysis has been made with existing techniques. The Proposed technique will give more efficient result than most of the existing techniques.

Keywords— Signature verification, Forgeries, Feature extraction, Neural network, FAR (False Acceptance Rate), FRR (False Rejection Rate), weighted feature points.

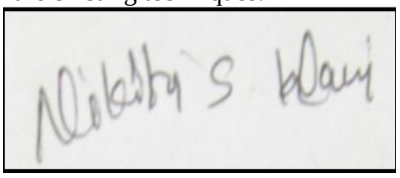
I. INTRODUCTION

Signature verification is an important research area in the field of personal authentication. The recognition of human handwriting is important concerning about the improvement of the interface between human beings and computers. If the computer is intelligent enough to understand human handwriting it will provide a more attractive and economic man-computer interface. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. Online data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation.

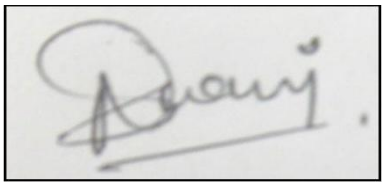
A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries. In this area signature is a special case that provides secure means for authentication, attestation authorization in many high security environment. The objective of the signature verification system is to discriminate between two classes: the original and the forgery, which are related to intra and interpersonal variability. The variation among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation . Problems of signature verification are addressed by taking into account three different types of forgeries: random forgeries, produced without knowing either the name of the signer nor the shape of its signature; simple forgeries, produced knowing the name of the signer but without having an example of his signature; and skilled forgeries, produced by people who, after studying an original instance of the signature, attempt to imitate it as closely as possible. Clearly, the problem of signature verification becomes more and more difficult when passing from random to simple and skilled forgeries, the latter being so difficult a task that even human beings make errors in several cases. The method takes care of simple and random forgeries and the skilled forgeries are also eliminated in greater extent. The threshold used in the proposed technique can be dynamically changed according to the target application. Basically, the threshold here is the security level which the user can input as per his requirement. The objective of the work is to reduce two vital parameters, False Acceptance Rate (FAR) and False Rejection Rate (FRR). So the results are expressed in terms of FAR and FRR and subsequently comparative analysis has been made with standard existing techniques. Results obtained by our proposed algorithm will be efficient than most of the existing techniques.



(a) Original Signature



(b) Random Forgery


(c)Simple Forgery

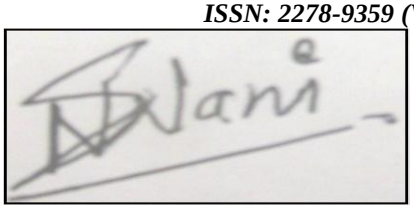

(d) Skilled Forgery

Fig.1 Types of Forgery

II. SIGNATURE DATABASE

The testing has been performed on images which are stored in file system. The file system contains small set of images for 2 to 5 individuals of 30 to 40 images. The forgeries were produced from the static images of the genuine signatures. Each forger was allowed to practice the signature for as long as she/he wished. Each forger imitated 3 signatures of 5 signers in a single day writing session. The genuine signatures were shown to each forger and were chosen randomly from the 10 genuine ones. Therefore, for each genuine signature, 10 skilled forgeries were produced by 10 forgers, from 10 different genuine specimens.

III. PROPOSED METHOD

From existing techniques, it has been observed that an offline signature verification process consist of pre-processing on signature. It is necessary to pre-process on signature because it helps to verify a signature correctly. Proposed system consists of following steps:

1. Signature Acquisition
2. Signature Pre-processing
3. Feature point Extraction
4. Neural Network Training
5. Signature Testing
6. Signature Verification

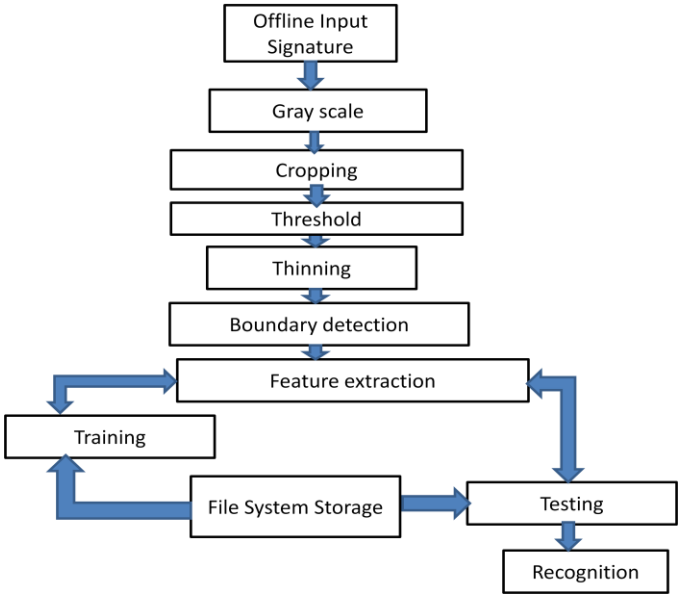


Fig.2 Block Diagram of Proposed System

1.Signature Acquisition: The proposed scheme is based on off-line signature verification so signature made on paper were acquired by scanner having 300dpi and saved in Portable Network Graphics (PNG) format.
Signatures are scanned in gray. Following fig. (ii) shows some sample signature from database.

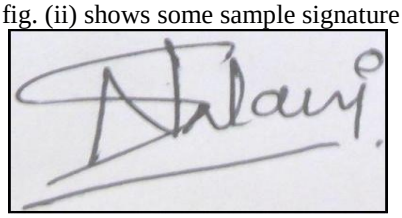


Fig.3 Sample Signature

Signature Pre-processing: To verify signature correctly, pre-processing phase is required. After signature acquisition, image may contain noise (extra pen dots), blurriness. It is necessary to remove these extra pixel or blurriness. Noise can be removed by using median filter. The pre-processing stage includes five steps: Gray Scale, Threshold and invert, Thinning, Boundary Detection and Auto cropping.

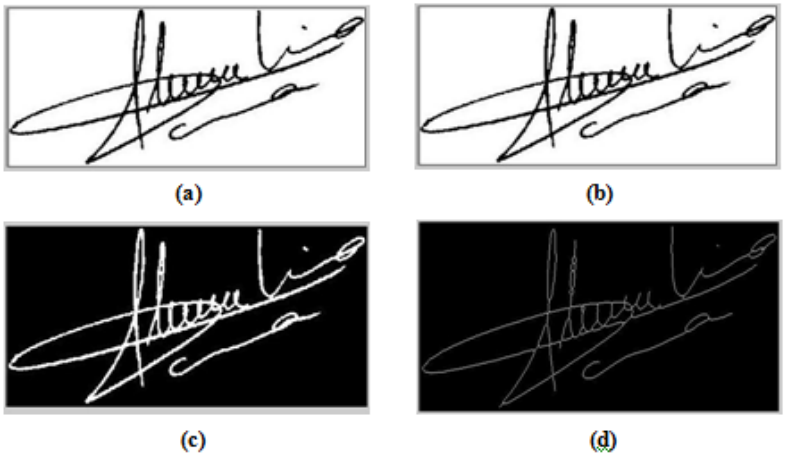


Fig.4 (a) Gray scale(b) Cropping (c) Threshold (d) Thinning and boundary detection

(a) Gray Scale
In signature verification, scanned image is converted in gray scale. It also called as monochromatic image in which each pixel carries only intensity information.
(b) Cropping
Cropping is the method of removing outer part of an image to get well bordered thin image. This image is ready for feature extraction.
(c) Threshold
Thresholding is the method of converting gray scale image to binary image. i.e. image with only black or white colours. Threshold image is used for feature extraction.
d) Thinning and boundary detection
Thinning eliminate the thickness differences of pen Due to the nature of variation of the signatures, because of age, illness, geographic location etc. by making the image one pixel thick. Boundary detection helps to get necessary part of scanned image .

Feature Extraction: This is the most important phase in any signature verification system since it is the key to identifying and differentiating a user‘s signature from another. Features extracted in proposed system are based on geometric centre of signature image. Geometric features are based on dimensions of the signature image, shape and depth of signature image. Here geometric features are based on two set of points in 2 dimensional planes. The vertical splitting of the image results thirty features points (v1,v2,v3,……,v30) and the horizontal splitting results thirty features points (h1,h2,h3,……,h30). Geometric centre of image split image in two halve left and right portion of image. Then again find out geometric centre of left and right part of image and calculate the total number of black pixel. Then divide the two parts in four parts with respect to the black pixel. This process gives 30 features in vertical splitting and 30 features in horizontal splitting.
Horizontal splitting of signature image: Horizontal feature points give thirty feature points by splitting image horizontally w. r. t. geometric centre point (h0). Here the geometric centre plays important role. After finding geometric centre of signature image, split the image with horizontal line passing through the geometric centre (h0). Splitting gives two part top and bottom. Find geometric centre point of top and bottom portion say h1 and h2 correspondingly. Split the top and bottom portion with vertical lines through h1 and h2 to divide the two parts into four parts: Left-top, Right-top and Left-bottom, Right bottom parts from which we obtain h3, h4 and h5, h6. We again split each part of the image through their geometric centers to obtain feature points h7, h8, h9,…, h13, h14. Then we split each of the parts once again to obtain all the thirty vertical feature points .

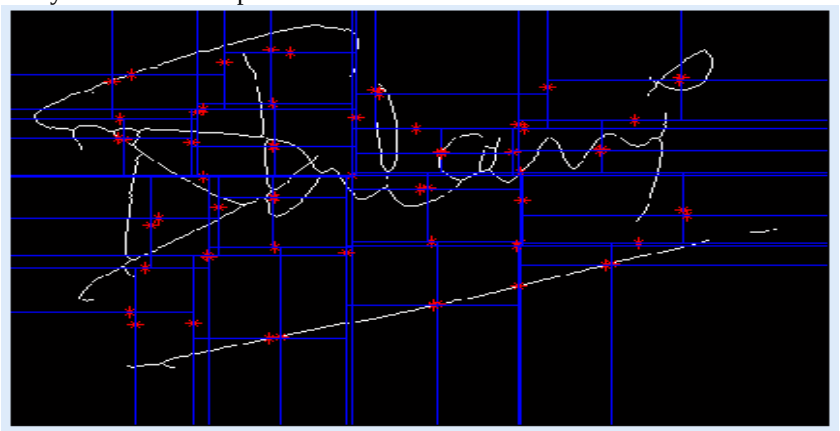


Fig.5 Horizontal and Vertical splitting of signature image

Vertical splitting of signature image: Vertical feature points give thirty feature points by splitting image vertically w. r. t. geometric centre point (v0). After finding geometric centre of signature image, split the image with vertical line passing through the geometric centre (v0). Splitting gives two part left and right. Find geometric centers v1 and v2 for left and right parts correspondingly. Split the left and right part with horizontal lines through v1 and v2 to divide the two parts into four parts: Top-left, Bottom-left and Top-right, Bottom right parts from which we obtain v3, v4 and v5, v6. Again split each part of the image through their geometric centers to obtain feature points v7, v8, v9,…, v13, v14. Then split each of the parts once again to obtain all the thirty vertical feature points.

Neural Network Training: original signature's extracted 60 features points are then fed to neural network using back propagation algorithm.

Signature Testing: Here signature to be tested is firstly scanned in gray then pre-processed it. After pre-processing feature extraction is performed to obtain 60 feature points. These 60 features are then fed to trained neural network using multiple layer feed forward algorithm.

Signature Verification: In proposed system, we get total 60 features based on vertical splitting and horizontal splitting. These features helps to classify signature is genuine or fake.

Here geometric centre plays important role to obtain features. So we use Euclidean distance model for classification. This model states that distance between a pair of feature points. following Eq. 1 is used to find out distance between pair of feature points. Let V (v1, v2, v3,…., v30) and H (h1,h2,h3,…..,h30) are two set of features points based on vertical and horizontal features point respectively. Here x and y is horizontal and vertical coordinator of pixel.

$$\text{Distance (d)} = \sqrt{(Y_2 - Y_1)^2 - (X_2 - X_1)^2} \quad (1)$$

After getting Euclidean distance, we calculate weighted average by multiplying with depth of feature point. Here in proposed system depth is set to maximum 5 i.e. geometric centers calculate upto depth 4 in horizontal and vertical splitting. This calculated average will help to classify the signature. Let d1, d2, d3, d4 and d5 are distances calculated by Euclidean distance model based on depth. Individual weighted average (W_a) is calculated for horizontal splitting and vertical splitting. Weighted distance average is given by following Eq. 2.

$$\text{Weighted Average } (W_a) = d1*5+d2*4+d3*3+d4*2+d5*1 \quad (2)$$

IV. PERFORMANCE EVALUATION

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the two parameters used for measuring performance of any signature verification method. FAR and FRR are calculated by the equations given below: *False Acceptance Rate (FAR):* Falseacceptance ratio is the total number of fake signature accepted by the system with respect to the total number of comparison made.

$$\text{FAR} = \frac{Number\ of\ forgeries\ accepted}{Number\ of\ forged\ tested} * 100$$

False Rejection Rate (FRR): False rejection ratio is the total number of original signature rejected by the system with respect to the total number of comparison made.

$$\text{FRR} = \frac{Number\ of\ originals\ rejected}{Number\ of\ originals\ tested} * 100$$

V. RESULT AND DISCUSSION

The proposed system will give better result in terms of FAR and FRR than existing techniques. In training section, ANN is trained by original signature's 60 features based on horizontal and vertical splitting. As mentioned earlier Euclidean distance model help to calculate the distance between pair of feature point of original signature and testing signature. In testing section, total error is calculated based on Euclidian distance and depth of point. If total error is less than threshold then new signature is acceptable. New signature i.e. test signature have to satisfy error rate to threshold comparison to be stated as verified or rejected.

VI. CONCLUSION

The proposed system will give better result in terms of FAR and FRR than existing techniques. The proposed system has higher accuracy than existing system in terms of identifying forged signatures as the technique accurately identifies false signatures with great accuracy and minimum FAR (False Acceptance Rate) as it works on 60 horizontal and vertical feature points extracted from signature image which helps signature verification at very micro level. The technique boosts of a high FRR and very low FAR.

REFERENCES

[1] Banshidhar Majhi, Y. Santhosh Reddy and D. Prasanna Babu, 2006. Novel features for offline signature verification. Int. J. Comput. Commun Control, 1: 17-24.

[2] Debasish Jena, Centre for IT Education, Bhubaneswar, Orissa, India, _Improved Offline Signature Verification Scheme Using Feature Point Extraction Method', Journal of Computer Science 4 (2): 111-116, 2008.

[3] K. Bowyer, V. Govindaraju, N. Ratha, _Introduction to the special issue on recent advances in biometric systems', IEEE Transactions on Systems, Man and Cybernetics—B 37(5)(2007)1091–1095.

[4] Manoj Kumar / International Journal on Computer Science and Engineering (IJCSE), _Signature Verification using Neural Network', Vol. 4 No. 09 Sep 2012.

[5] Meenakshi K. Kalera, Sargur Srihari and Aihua Xu, ―Offline Signature Verification and Identification using Distance Statistics‖,International Journal of Pattern Recognition and Artificial Intelligence, Vol.18, No.7, pp.1339-1360, 2004.

[6] Qi.Y, Hunt B.R., 'Signature Verification using Global and Grid Features', Pattern Recognition, Vol. 27, No. 12, 1994, pp. 1621-1629.

[7] Suhail M. Odeh, Manal Khalil, ‗Off-line Signature Verification and recognition: Neural Network Approch‘,2011.

[8] Swati Srivastava, Suneeta Agarwal, ‗Offline Signature Verification using Grid based Feature Extraction‘, 2011.

[9] Vahid Kiani, Reza Pourreza, Hamid Reza Pourezza, ―Offline Signature Verification Using Local Radon Transform and Support Vector Machines‖, International Journal of Image Processing (IJIP), Vol.3, No.5, pp.184-194, 2010.

