

Robust Signature Verification and Recognition using Weighted Features Point

Nikita S. Wani¹, S. P. Patil²

P.G. Student, E&TC Department, D. N. Patel College of Engineering, Shahada, India¹

Professor of E&TC Department, D. N. Patel College of Engineering, Shahada, India²

Abstract: This paper robust signature verification and recognition using weighted features point that applies artificial neural network which discriminates between two types of signature (i) forged and (ii) original signature. The proposed scheme performs pre-processing on the signature, feature point extraction and neural network training and finally verifies the authenticity of the signature. The aim here is to reduce two vital parameters False Acceptance Rate (FAR) and False Rejection Rate (FRR). Results are also maintained in terms of FAR and FRR and parallel comparative analysis is made with existing techniques. The Proposed technique provides more accurate and precise results than most of the existing technique in this field.

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 for 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 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. Signature is a special case that provides secure means for authentication, attestation authorization in many high security environments. The objective of the signature verification system is to discriminate between two signature types: 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. 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. Signature verification becomes more and more difficult with each forgery type making it so difficult that even human make errors in many cases. In the proposed technique threshold is calculated from the error rate multiplied with the depth of the ANN verification. 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 comparative analysis has been made with standard existing techniques.



Fig.1 Types of Forgeries

II. PROPOSED SYSTEM

From existing techniques, of offline signature verification process involves 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

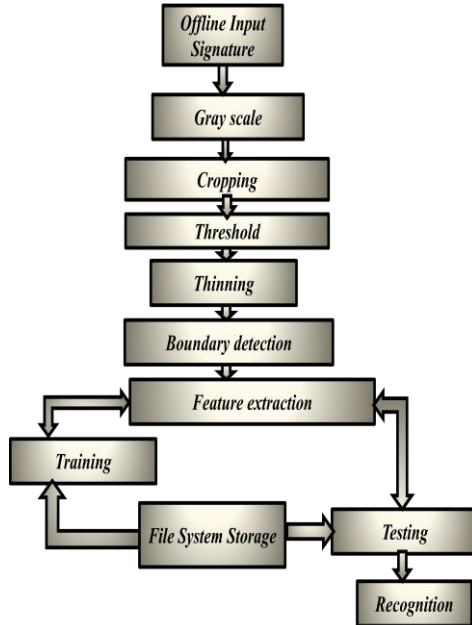


Fig.2 Proposed Verification System

1. Signature Acquisition: For the proposed scheme which is based on off-line signature verification signatures made on paper were acquired by scanner having and saved in Portable Network Graphics (PNG) format. Signatures were scanned in gray background. Following fig.3 shows some sample signature from database.

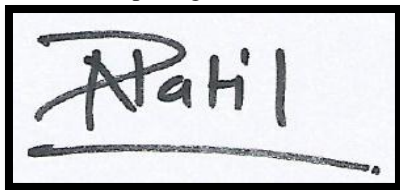


Fig.3 Sample Signature

2. Signature preprocessing: pre-processing phase is required for better signature verification. After signature acquisition, noise (extra pen dots), blurriness all such anomalies are taken care by the signature pre-processing step. Noise is to be removed by using median filter. The pre-processing stage includes five steps: Gray Scale, Threshold and invert, Thinning, Boundary Detection and Auto cropping.

(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 method involves removing of outer part of an image to get well bordered thin image. This image is ready for feature extraction.

(c) Threshold

Thresholding is the technique of converting gray scale image to binary. Image with only black or white colors.

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

3.Feature Extraction: This is the most significant phase in the lifecycle phase of signature verification system as it plays a key role in identifying and differentiating one user's signature from another. Extracted features 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 ($v_1, v_2, v_3, \dots, v_{30}$) and the horizontal splitting results thirty features points ($h_1, h_2, h_3, \dots, h_{30}$). Geometric center splits image into 2 halves left and right halves. Then again geometric half of respective left and right halves is calculated. This recursive process is performed until 30 black pixel points are extracted 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 (h_0). 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 (h_0). Splitting gives two part top and bottom. Find geometric centre point of top and bottom portion say h_1 and h_2 correspondingly. Split the top and bottom portion with vertical lines through h_1 and h_2 to divide the two parts into four parts: Left-top, Right-top and Left-bottom, Right bottom parts from which we obtain h_3, h_4 and h_5, h_6 . We again split each part of the image through their geometric centers to obtain feature points $h_7, h_8, h_9, \dots, h_{13}, h_{14}$. Similarly we split the image vertically to extract another set of 30 black pixel points from vertical splitting of the image.

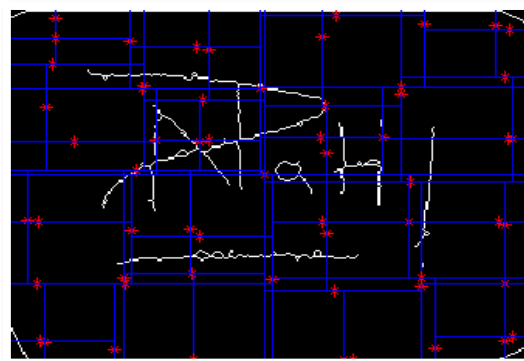


Fig.4 Horizontal and Vertical splitting of signature image
Vertical splitting of signature image: Vertical feature points give thirty feature points by splitting image vertically w. r. t. geometric centre point (v_0). After finding

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.

4. Neural Network Training: Original signature's extracted 60 features points are used in neural network which uses back propagation algorithm and feed forward algorithm to train the neural network for further image recognition while testing.

5. Signature Testing: Here signature to be tested is scanned in grey then pre-processed as mentioned in above steps. Post 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 to obtain the authenticity of the signature.

6. Signature Verification: The proposed signature verification methodology retrieves 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 retrieving Euclidean distance from above equation, we calculate weighted average by multiplying Euclidean distance with depth of feature point. Here in proposed system depth is set to maximum 5 i.e. geometric centers calculate up to 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.

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

III. PERFORMANCE EVALUATION

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the two parameters which define standard method to verify the performance of any Signature verification method. FAR and FRR are calculated by the equations given below: False

Acceptance Rate (FAR): False acceptance ratio is the total number of fake signature accepted by the system with respect to the total number of comparison made.

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

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.

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

IV. RESULT AND DISCUSSION

The proposed technique of signature verification with weighted feature point and ANN gives better results in comparison to most techniques present in the field of signature verification in terms of FAR and FRR. Training is performed by pre-processing images acquired and extracting 60 feature points via horizontal and vertical splitting which are feed to ANN thereafter and ANN is trained. Also Euclidean distance is used to calculate distance between 2 feature points of original and the signature under testing. Total error in testing phase is calculated based on product of Euclidean distance and depth of a feature point. The signature under testing is deemed acceptable if the error rate of test signature is below the threshold. Thus every test signature must satisfy the equation between the error rate and threshold value to be deemed accurate or original or to be accepted as valid as such.

REFERENCES

- [1] Manoj Kumar / International Journal on Computer Science and Engineering (IJCSSE), 'Signature Verification using Neural Network', Vol. 4 No. 09 Sep 2012.
- [2] Suhail M. Odeh, Manal Khalil, 'Off-line Signature Verification and recognition: Neural Network Approach', 2011.
- [3] Banshidhar Majhi, Y. Santhosh Reddy and D. Prasanna Babu, 2006. Novel features for offline signature verification. Int. J. Comput. Commun. Control, 1: 17-24.
- [4] Swati Srivastava, Suneeta Agarwal, 'Offline Signature Verification using Grid based Feature Extraction', 2011.
- [5] Vahid Kiani, Reza Pourreza, Hamid Reza Pourreza, '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.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] Qi.Y, Hunt B.R., 'Signature Verification using Global and Grid Features', Pattern Recognition, Vol. 27, No. 12, 1994, pp. 1621-1629.