Signature Verification Using Neural Network

Manoj Kumar
Department of Information Technology
JSS Academy of Technical education
Noida India
manojkumar@jssaten.ac.in

***Abstract*— In this paper we present new improved off-line signature verification system using global and texture features of signatures. This scheme is based on the technique that applies preprocessing on the signature to get a binary image and then calculate the global and texture features points from it and maintain a feature vector. All calculations are done on the basis of these feature points. The feature vector obtained from the global and texture features is used to compare with the feature vector of incoming testing signature. Based on the values obtained, the network will decide the appropriateness of the signature. The suggested scheme discriminates between original and forged signatures using artificial neural network (ANN) for training and verification of signatures. The method takes care of simple and random forgeries and the skilled forgeries are also eliminated in greater extent. 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 are more efficient than most of the existing techniques.**

Keywords — **Offline signature, forgeries, FAR (False Acceptance Rate), FRR (False Rejection Rate).**

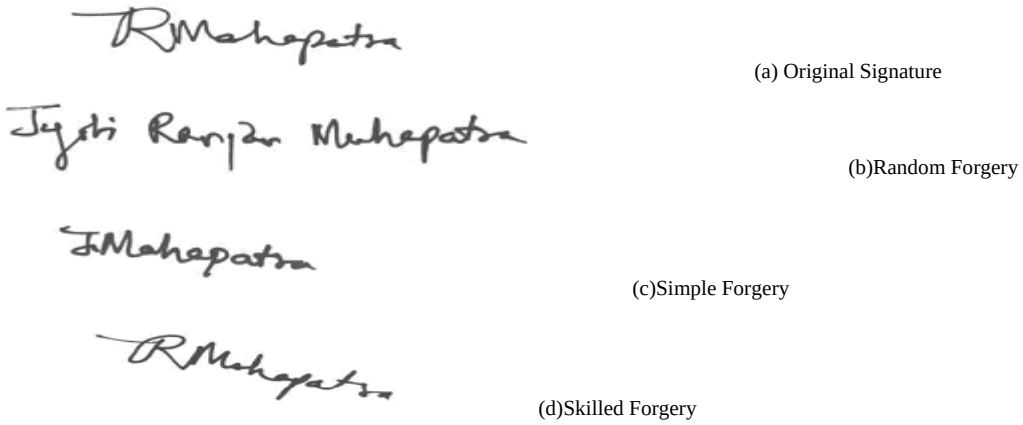
1.INTRODUCTION

Signature has been a distinguishing feature for person identification through ages. Even today an increasing number of transactions, especially financial, are being authorized via signatures; hence methods of automatic signature verification must be developed if authenticity is to be verified on a regular basis. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. On-line 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 [1]. 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 [2]. The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR).

It is also true that the track of the pen shows a great deal of variability. No two genuine signatures are ever exactly the same. Actually, two identical signatures would constitute legal evidence of forgery by tracing. The normal variability of signatures constitutes the greatest obstacle to be met in achieving automatic verification. Signatures vary in their complexity, duration, and vulnerability to forgery .Signers varies in their coordination and consistency. Thus, the security of the system varies from user to user. A short, common name is no doubt easier to forge than a long, carefully written name, no matter what technique is employed. Therefore, a system must be capable of ‘‘degrading’’ gracefully when supplied within consistent signatures, and the security risks must be kept to acceptable levels [3].

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 be comes 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. Indeed, exercises in imitating a signature of ten allow us to produce forgeries so

similar to the originals that discrimination is practically impossible; in many cases, the distinction is complicated even more by the large variability introduced by some signers when writing their own signatures [4].



(a) Original Signature

(b)Random Forgery

(c)Simple Forgery

(d)Skilled Forgery

Fig 1.1:Types of Forgery

2. PROPOSED SYSTEM

The overall architecture of our signature recognition system follows: Signature acquisition, Preprocessing,Feature extraction, and Classification. Offline signatures are the signatures made on papers. This requires specifying the resolution, image type and format to be used in scanning each image. To this effect, a number of existing offline signature databases [6], [7] was studied. So in any offline signature verification system, the first step is to extract these signatures from papers using scanners. The sheet on which signature is made is provided to scanner which gives scanned image of the signature.

In pre-processing stage, the RGB image of the signature is converted into grayscale and then to binary image. Thinning is applied to make the signature lines as single thickness lines and any noise present in scanned images are removed thus making the signature image ready to extract features. Features available to extract in offline signatures can be either global features or texture feature i.e. features extracted from whole images . In this system, the features extracted are Aspect ratio, Signature Area, Maximum horizontal

And Maximum vertical histogram, End point number of the signature, texture Homogeneity, Texture contrast, Entropy. These extracted features Form the basis to compare and there by classify Signatures either genuine or forge. The features extracted from atabase are compared with the features extracted from test signatures and based on the classification criteria the signatures are classified either genuine or forged.

3. PREPROCESSING

Signatures are scanned in gray. The purpose in this phase is to make signatures standard and ready for feature extraction. The preprocessing stage includes four steps: Background elimination, noise reduction, width normalization and thinning **.**The preprocessing steps of an example signature are shown in Fig. .

Fig 3. Preprocessing steps: (a) scanning, (b) background elimination, (c) noise reduction, (d) width normalization, (e) thinning applied signatures.

a) Background Elimination
Data area cropping must be done for extracting features. P-tile thresholding was chosen to capture signature from the background. After the thresholding the pixels of the signature would be "1" and the other pixels which belong to the back-ground would be "0".

b) Noise Reduction
A noise reduction filter is applied to the binary image for eliminating single black pixels on white background. 8-neighbors of a chosen pixel are examined. If the number of black pixels is greater than number of white pixels, the chosen pixel will be black otherwise it will be white.

c) Width Normalization
Signature dimensions may have intrapersonal and interpersonal differences. So the image width is adjusted to a default value and the height will change without any change on height-to-width ratio.

d) Thinning
The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick.

4. FEATURE EXTRACTION

Feature extraction process is an important step in developing any signature verification system since it is the key to identifying and differentiating a user's signature from another. The features extracted in this system is based on shape and texture of an image. The features in this system are global features and texture features. While global features provide information about specific cases concerning the structure of the signature, texture features are intended to provide overall signature appearance information.

4.1 GLOBAL FEATURES EXTRACTION

a) Signature height-to-width ratio: It is obtained by dividing signature height to signature width. Signature height and width can change. Heights-to- width ratio of one person's signature are approximately equal.

Steps:-
1. Read the pre-processed signature image.
2. For width calculation, first by going column wise calculate the column which has the left most pixel as black and similarly the column which has the right most black pixel is calculated. Width is the difference of those two column values.
3. For height calculation by scanning the image row wise check for the rows that encounters first black pixel and similarly the row which has the last black pixel.
4. Height to width ration is to be calculated.

b) Signature Area: It is the number of pixels which belong to the signature. This feature provides information about the signature density.

Steps:-
1. Read the preprocessed signature image.
2. Scan the image row wise and total number of black pixel is to be counted.

c) Maximum horizontal and maximum vertical histogram: The horizontal histograms are calculated for each row and the row which has the highest value is taken as maximum horizontal histogram. The vertical histograms are calculated for each column and the column which has the highest value is taken as maximum vertical histogram.

Steps:-
1. Read the preprocessed signature image.
2. Scan the image row wise and calculate the number of black pixels in each row.
3. Scan the image column wise and calculate the number of black pixels in each column.
4. The row which has maximum number of black pixels stored as maximum horizontal histogram.
5. The column which has the maximum number of black pixels column number is stored as Maximum vertical histogram.

d) Horizontal and vertical centre of the signature: To calculate the horizontal and vertical centre of the signature, we have proposed the following algorithm.

Steps:-

1. Read the preprocessed signature image.
2. Scan column wise. For each column, those row index values, which are having black pixels, are added in the row_index_sum. Also a counter is incremented each time a black pixel in any row is found for that particular column.
3. The same step is performed for all the columns.
4. Cx=row_index_sum / total black pixels encountered.
5. Scan row wise. For each row those column index values, having black pixels are added in column_index_sum. Also the counter is incremented each time a black pixel is encountered.
6. The same step is performed for all the rows.
7. Cy= column_index_sum/total black pixels encountered.
8. Centre is calculated by formula-
   (Cx+1) * total column in signature + Cy.
9. This centre as cell value is stored as centre feature.

e) Edge point number of the signature: Edge point is the pixel which has only one neighbor, which belongs to the signature, in 8-neighbor.

Steps:-

1. Read the preprocessed image.
2. Scan the image row wise. For each pixel no. of black pixels in 8 neighbors are to be counted.
3. If no. of black pixels in 8-neighbors is one. That pixel is recognized as edge pixel.
4. Total no. of such edge black pixel is counted.

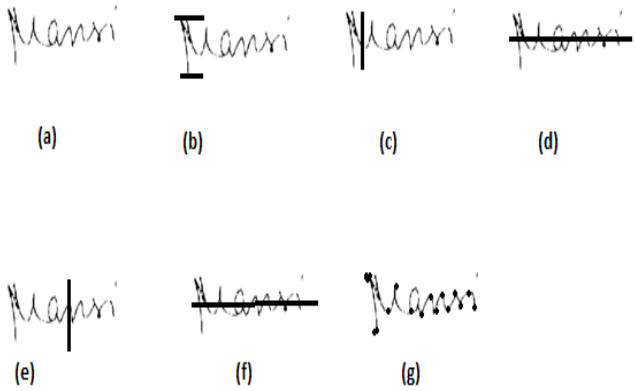


Fig 4.1 Feature extraction steps: (a) preprocessed signature, (b) height, (c) maximum vertical histogram, (d) maximum horizontal histogram, (e) horizontal centre, (f) vertical centre, (g) edge points

4.2 TEXTURE FEATURES EXTRACTION

a) Texture homogeneity H:

$$H = \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} \{P(i,j)\}^2$$

A homogeneous scene will contain only a few grey levels, giving a GLCM with only a few but relatively high values of $P(i, j)$. Thus, the sum of squares will be high.

b) Texture contrast C:

$$C = \sum_{n=0}^{G-1} \left\{ n^2 \cdot \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} P(i,j) \right\}, |i-j| = n$$

This measure of local intensity variation will favour contributions from $P(i, j)$ away from the diagonal, i.e $i \_= j$.

c) Texture entropy E:

$$E = \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} P(i,j) \cdot \log \{P(i,j)\}$$

Non-homogeneous scenes have low first order entropy, while a homogeneous scene reveals high entropy.

d) Texture correlation O:

$$O = \sum_{i=0}^{G-1} \sum_{j=0}^{G-1} \frac{i \cdot j \cdot P(i,j) - (m_i \cdot m_j)}{\sigma_i \cdot \sigma_j}$$

where *mi* and *σi* are the mean and standard deviation of *P*(*i*, *j*) rows, and *mj* and *σj* the mean and standard deviation of *P*(*i*, *j*) columns respectively. Correlation is a measure of grey level linear dependence between pixels at the specified positions relative to each other.

.5. SIGNATURE DATABASE

For training and testing of the signature recognition and verification system 310 signatures are used. The signatures were taken from 40 persons. For training the system 40 persons' signatures are used. Each of these persons signed either 8 original signatures or 6 original signatures; other 16 persons imitated the signatures. For each person 1 forgery signature of each type is signed. In the training set the total number of signatures is 290 = (original) = (25x8 + 15x6). For testing 250 forgeries of each type were taken and to test original signatures we took total 25 signatures.
In order to make the system robust, the signatures are collected at different times without seeing other signatures they signed before.

6. DESIGNING OF ANN

No. of neurons in input layer = 9
No. of neurons in hidden layer=10
Learning rate=0.4
No. of epoch=200
Initial weight= 1

7. TRAINING AND TESTING

A training stage consist of four major steps :

1. Retrieval of a signature image from a database
2. Preprocess the signature by the steps discussed earlier.
3. Extract the features of the signature by the feature extraction techniques discussed earlier.
4. Back propagation neural network training.

A Testing stage consists of five major steps :

1 Retrieval of a signature to be tested from a database
2. Pre-process the signature by the steps discussed earlier.
3. Extract the features of the signature by the feature extraction techniques discussed earlier.
4. Application of extracted features to a trained neural network
5. checking output generated from a neural network declaring signature as genuine or forged..

8. 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:

$$FAR = \frac{number\ of\ forgeries\ accepted}{number\ of\ forgeries\ tested} \times 100$$

$$FRR = \frac{number\ of\ originals\ rejected}{number\ of\ originals\ tested} \times 100$$

The table 4.1 shows the False Acceptance Rate of our proposed technique for different types of forgeries and the False Rejection Rate for original Signatures.

Table 8.1: FAR and FRR

No. of signatures	FAR	FRR
60	6.67%	13.33%

9. FUTURE WORK

The future work of this project is to verify the signature database using other efficient verification methods like Conic Section Function Neural Network (CSFNN), Multi Layer Perceptron (MLP) Neural Network, and RBF Neural Networked and compares the results of Back Propagation Neural Network with these results. The signature verification can also be changed by changing the features that can be extracted from a signature. So, the future work of the verification of signature can be done with the same Neural Network methods but using different signature features and compares the results with results of the present paper.
The precepts of this paper can be used in not only directly related applications like biometric identification, but also in a broad swath of fields of image processing especially. Relating to identification and comparison of images. The concepts in this project can be extended to other biometric identification systems like handwriting and when combined with other biometric aspects, such as speech and face recognition, can present a far better result than any individual system.

10. REFRENCES

[1] Plamondon.R., Brault J.J., 'A Complexity Measure of Handwritten curves: Modeling of Dynamic Signature Forgery', IEEE Trans. on Systems, Man and Cybernetics, Vol. 23, No.2, 1993, pp. 400-413.
[2] Qi.Y, Hunt B.R., 'Signature Verification using Global and Grid Features', Pattern Recognition, Vol. 27, No. 12, 1994, pp. 1621-1629.
[3] N. Herbst, C. Liu, 'Automatic signature verification based on accelerometry, Tech. Rep.', IBM Journal of Research Development, 1977.
[4] C. Sansone, M. Vento, 'Signature verification: increasing performance by a multi- stage system', Pattern Analysis & Applications, Springer 3 (2000) 169–181.
[5] 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.
[6] D.Zhang ,J . Campbell , D . Maltoni , R . Bolle , Special issue on biometric systems, IEEE Transactions on Systems ,Manand Cybernetics—C 35(3)(2005)273–275.
[7] S.Prabhakar ,J .Kittler , D . Maltoni , L . O ' Gorman ,T .Tan , 'Introduction to the special issue on biometrics : progress and directions , PAMI 29 (4)(2007)513–516.
[8] S.Liu , M . Silverman, 'A practical guide to biometric security technology' ,IEEE IT Professional3(1)(2001)27–32.
[9] R . Plamondon , S .Srihari , 'On-line and off-line handwriting recognition: a comprehensive survey' ,IEEE Transactions on Pattern Analysis and Machine Intelligence 22(1)(2000)63–84.
[10] K. Franke, J. R. Del Solar, M. K¨ open, 'Soft-biometrics: soft computing for biometric-applications', Tech.Rep.IPK, 2003.
[11] S.Impedovo, G.Pirlo, 'Verification of hand written signatures : an overview ,in: ICIAP '07:Proceedings of the 14th International Conference on Image Analysis and Processing' , IEEE Computer Society , Washington , DC , USA, 2007, pp.191–196,doi:http://dx.doi.org/10.1109/ICIAP.2007.131.
[12] R. Plafond, 'Progress in Automatic Signature Verification, World Scientific Publications', 1994.
[13] M.Fairhurst, 'New perspectives in automatic signature verification', Tech .Rep. 1, Information Security Technical Report, 1998.
[14] R.W. Canners , C.A. Harlow, 'A theoretical comparison of texture algorithms, IEEE Transactions on Pattern Analysis and Machine Intelligence '2 (3) (1980) 204–222.
[15] H B Kekre, 'Gabor Filter Based Feature Vector for Dynamic Signature Recognition', *International Journal of Computer Applications (0975 – 8887)Volume 2 – No.3, May 2010 pp-1023-1031.*

[16] Swati Srivastava and Suneeta Agarwal,"offline Signature Verification using Grid based Feature Extraction'',In :International Conference on computer & Communication Technology (ICCCT)-2011.pp 185-190.
[17] Katsuhiko Ueda,"Investigation of Off-line Verification using a pattern matching",In proceedings of the seventh International Conference on Document Analysis and Recognition(ICDAR'03). pp.201-206.
[18] Guangyu Zhu "Signature Detection & Matching for Document Image Retrieval " in Pattern Analysis & Machine intelligence" IEEE Transaction on Nov 2009, Vol 2002 pp.2015-2013.
[19] K,K Radhika, M.K Venkatesh G.W.Sekha "Signature authentication based on Subpattern analysis", Applied soft computing vol.11, issue 3, April 2011, pp-3218-3228.
[20] Ali Karan, Bassam Raya, Sania Bahtak "Offline Signature Recognition using neural networks approach" , Proceeding Computer Science Vol3, 2011, PP-151-161.
[21] Tjhi W.C,Lee Kee Khoon "Clustering based methodology with minimal user supervision for displaying cell- phenotype signature in image based Screening" in Bioimformatics & Biomedicine workshops 2010 IEEE International conference 2010 pp 252-257.
[22] Bi-Rubai, Jen Wei Huang " Adaptive Clustering for Multiple evolving stream" in Knowledge & Data Engineering,IEEE Transactions Sept,2006, Vol 18 issue 9 PP 1166-1180.
[23] Y.Rekik, N. Houmani, M.A Yacoubi, S.Garcia Salicetti and B. Dorizzi"A Comparison of Feature Extraction Approaches for offline signature verification" In: IEEE 2011.
[24] NG Geok See and Ong Hee Seng, " A neural Network Approach for offline Signature Verification, IEEE TENCON,93.