OFFLINE SIGNATURE VERIFICATION AND RECOGNITION

M. V. KANAWADE & S. S. KATARIYA

Department of Electronics, Amrutvahini College of Engineering, Sangamner, Maharashtra, India

ABSTRACT

Now a day’s Signature verification is one of the most widely used biometrics for authentication in bank transactions, passports etc. The fact that the signature is widely used as a means of personal verification emphasizes the need for an automatic verification system. Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature captured at the time the signature is made. Offline systems work on the scanned image of a signature. In this paper we present a method for Offline Verification of signatures using a grid base feature extraction. Before extracting the features, preprocessing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present.

The system is initially trained using a database of signatures obtained from those individuals whose signatures have to be authenticated by the system. For each subject a mean signature is obtained integrating the above features derived from a set of his/her genuine sample signatures. This mean signature acts as the template for verification against a claimed test signature. The paper discusses the different stages of the process including: data acquisition, image preprocessing, feature extraction and verification.

KEYWORDS: Signature Verification, Forgery, Data Acquisition, Preprocessing

INTRODUCTION

Biometrics can be classified into two broad categories-- behavioral and physiological. Handwritten signature is a behavioral biometric. It is amongst the first few biometrics to be used even before the advent of computers. Handwritten signature has long been used in the financial domain for identity verification. In most of the places the verification is done manually either by a person who is familiar to the signature or by matching it against a few signature templates. A signature recognition and verification (SRVS) is a system capable of efficiently addressing two individual but strongly related tasks (I)identification of the signature owner, and , (II) decision whether the signature is genuine or forger.

Depending on the actual needs of the problem at hand, SRVSs are often categorized in two major classes: on-line SRVSs and offline SRVSs.On–line verification requires a stylus and an electronic tablet connected to a computer to collect dynamic signature information. Offline verification, on the other hand, deals with signature information which is in a static format. On-line data records the motion of the stylus while the signature is produced/generates, 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. Offline data is a 2-D image of the signature.

Forgerys

Forgery means a person is trying another persons signature illegally to become authenticate.Forgerys is mainly divided in to three types.
Random Forgery

The signer uses the name of the victim in his own style to create a forgery known as the simple forgery or random forgery. This forgery is very easy to detect with eyes.

Unskilled Forgery

In this type the signer copy the signature in his own style without any knowledge of the spelling and does not have any previous experience. The copy is made by observing the signature closely for a while.

Skilled Forgery

It is the most difficult of all forgeries is created by professional impostors or persons who have experience in copying the signature. For achieving this one could either trace or copy the signature by hard way.

RELATED WORK

A lot of research has been done in the field of Off-line signature recognition. This is a convenient approach and various optimization techniques are applied to address the problem. Sabourin [12] used granulometric size distributions for the definition of local shape descriptors in an attempt to characterize the amount of signal activity exciting each retina on the focus of an superimposed grid. He then used a nearest neighbor and threshold-based classifier to detect random forgeries. A total error rate of 0.02% and 1.0% was reported for the respective classifiers. A database of 800 genuine signatures from 20 writers is used. [8]. The main approach to this work is to show the feasibility of such implementation, introducing the new scheme for the tasks.Abbas [10] used a back propagation neural network prototype for the offline signature recognition. He used feed forward neural networks and three different training algorithms Vanilla, Enhanced and batch were used. In [10] he reported FAR between the range of 10-40 % for casual forgeries. A neuro-fuzzy system was proposed by Hanmandlu , they compared the angle made by the signature pixels are computed with respect to reference points and the angle distribution was then clustered with fuzzy c-means algorithm. Back propagation algorithm used for training neural network.

The system reported FRR in the range of 5-16% with varying threshold. Baltzakis [11] developed a neural network-based system for the detection of random forgeries. The system uses global features, grid features (pixel densities), and texture features (co occurrence matrices) to represent each signature. For each one of these feature sets, a special two-stage perception one-class-one-network (OCON) classification structure is implemented. In the first stage, the classifier combines the decision results of the neural networks and the Euclidean distance obtained using the three feature sets. The results of the first stage classifier feed a second-stage radial basis function (RBF) neural network structure, which makes the final decision. Armand, Blumenstein and Muthukkumarasamy used combination of the Modified Direction Feature (MDF) in conjunction with additional distinguishing features to train and test two Neural Network-based classifiers. A Resilient Back Propagation neural network and a Radial Basis Function neural network were compared. Using a publicly available database of 2106 signatures containing 936 genuine and 1170 forgeries, they obtained a verification rate of 91.12%.

OBJECTIVE

The aim of off-line signature verification is to decide, whether a signature originates from a given signer based on the recorded image of the signature and a few images of the original signs of the signer. Signature is a special case of handwriting which includes special characters and flourishes. As many signs can be unreadable. They are a kind of artistic
handwriting objects. However, a signature can be handled as an image, and hence, it can be recognized using computer vision. Signature recognition and verification involves two separate but strongly related tasks: I) Identification of the owner of signature, II) Whether the signature is original or forged.

**SCHEME OF IMPLEMENTATION**

There are 4 major steps in achieving signature verification and recognition, and each of these steps consists of many methods to improved results. These steps are follows:

- Data Acquisition/Signature Database
- Image Pre-Processing
- Feature Extraction
- Classification/Verification

**Data Acquisition/Signature Database**

In On line signature verification system Data acquisition process is a process where the real time inputs of signature from the digitizing tablet and the special pen are read into the CPU for processing and to store the signature in to the database. The digitizing tablet is sending the real time inputs to the CPU for further processing and storage. For offline signature verification signatures from individual person are taken on A4 size paper and then scanned with scanner.

The database can be taken from individuals or database is available on internet. The signature image used in the paper is taken from internet. The database contains data from individuals, including genuine signatures from individuals, and forgeries. The signatures are collected using either black or blue ink, on a white A4 sheet of a paper, with four signatures per page. Using the scanner the four signatures are digitized. The signatures to be processed by the system should be in the digital image format.

The forgeries were produced from the static images of the genuine signatures. The original signatures were shown to each forger and were chosen randomly from the original ones. Therefore, for each original signature, skilled forgeries were produced by forgers, from 10 different genuine specimens. Access to the mentioned database was authorized for the use of these signatures for research and academic work only, and not for commercial use.

**Image Pre-Processing**

Preprocessing is used to improve the quality of signature image. Preprocessor processes the raw signature samples to make them usable by the feature extracting unit. The scanned signature image may contain spurious noise and has to be removed to avoid errors in the further processing steps. The following were the process that was carried out on the signature.
• **Conversion from RGB Image to Black and White (Logical) Image**

Original signature is converted in to black and white image.

For signature verification the color of ink has no significance at all. Instead the form of two signatures must be compared. Hence all the scanned images were converted to black and white images where white is represented by 1 and black by 0. Hence the signature part was represented by 0 and the blank part of the image (without any signature) by 1. This conversion makes future coding easier. A gray scale signature image is converted to binary to make feature extraction simpler.

![Segmented and Binarized Signature](image)

**Figure 2: Segmented and Binarized Signature**

• **Conversion of the Image from Black on White Back Ground to White on the Black Background**

For this conversion MATLAB software is used. This conversion can be easily done by using the inbuilt inversion function ( ~ ) of MATLAB. Now the signature part becomes coded by 1 while blank spaces are coded by 0. This makes logical comparison a lot easier.

• **Finding the Bounding Box of the Image and Cropping Unnecessary Parts (Edges) of the Image**

Additional part other than signature content is removed. The bounding box of the image was found out, thereby eliminating blank area from the side of the images. Thus now each image consists only of the signature part. In the signature image, construct a rectangle encompassing the signature. This reduces the area of signature to be used for further processing and saves time.

• **Segmentation**

In this process signature contents are extracted for further process.

• **Thinning**

Thinning is used to eliminate the thickness differences of pen by making the image one pixel thick as shown in figure below.

![Thinned Signature](image)

**Figure 3: Thinned Signature**
Feature Extraction

In this paper for signature verification and recognition feature extraction is used. Features are of two types [1]:

- Function features
- Parameter features.

Function features consist of velocity, pressure, position etc. and these are used in online signature verification and recognition techniques. Parameter features are subdivided into global parameters and local parameters.

Global parameters consist of wavelet transform, Fourier transform etc. Local parameters are again divided into component-oriented and pixel-oriented. Component-oriented features consist of contour based, geometric based, slant based etc. Pixel-oriented features consist of grid based, intensity based etc. Here we are going to use grid based feature extraction.

Algorithm [1]

- Get the preprocessed signature image (Thinned image) of size 100x200(pixels).
- Then form a grid of size m x n.
  
  Where m is less than n, m<<100 and n<<200. The signature image is divided into 200 square cells where each cell consist of 100 pixels.
  
  Then find out the cells of a row of a grid that consist of the content of signature. The content of signature is calculated in terms of black pixels. Therefore consider the cells which consist of 3 or more black pixels. Same process is repeated for all the rows a grid. Thus we get all those cell positions which are part of the signature image.
  
  Create a matrix of size m x n corresponding to the grid of size m x 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

Figure 4: Preprocessed Signature

Figure 5: Grid over Pre-Processed Signature Image
Calculate the number of black pixels in cells of a row containing signature content. Repeat the process for all rows. Then the values of m rows are put in an array. Then same process is applied to columns. We get another array having n elements corresponding to each column.

- Matrix m x n corresponding to a m x n grid.
- An array of size m in which 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,
- An array of size n in which 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 extracted features are further used in verification process. Then compare these extracted features of the test and reference signature images stored in the data base and then verify signature as a original or forge.

Signature Verification/Classification

The verification/classification phase is used to compare the test image with stored image in the data base images using extracted features and to decide whether the test image is original signature of the writer or forgery.

Verification Algorithm

Consider Test Image and Reference Image. Consider Counter C0 and Counter C1

Calculate Column Matching Score (CMS)

- Consider M0 and M1 as the matrices of reference image and test image respectively. Compare the columns of the matrix M1 with M0. Each column is having m elements. If at least 7, elements are same then that column is said to be matched and increase the column count C0 by one.
- Consider A0 and A1 be the arrays of reference image and test image respectively containing number of black pixels in each column. Compare the corresponding elements of array A1 with A0. If these are matched then increase the counter C1 by one.
- If C0 and C1 are equal then CMS is 100%.

Calculate Row Matching Score (RMS)

Then calculate the RMS. If CMS ≥ 60% then only calculate Row Matching Score (RMS). If at least 14 elements are matched then Calculate C0 and C1. Calculation of RMS is same as CMS use rows in place of column.

Figure 6: Matrix Corresponding to the above Grid
Calculate the Average of CMS and RMS

Threshold

Threshold is decided by user as per requirement. If it is security level it can be 100% and for this average of CMS and RMS should be 100% for the acceptance of signature. Threshold range is from 100 to 65.

CONCLUSIONS

In this paper, we have discussed an offline signature verification technique using grid based feature. The signature image is first converted in to gray image then into binary, segmentation and then thinned. The preprocessed signature i.e. gray image, black and white, segmented, thinned and signature is divided into the grid of size m x n. and matrix is formed. Then CMS is calculated and if CMS is greater than or equal to 60 then RMS is calculated. Threshold is in between 65 to 100. Finally the signature is detected as original or duplicate.

REFERENCES

1. Offline Signature Verification using Grid based Feature Extraction, Swati Srivastava Department of Computer science & Engineering Motilal Nehru National Institute of Technology Allahabad, India cs0905@mnnit.ac.in, Suneeta Agarwal department of Computer Science & Engineering Motilal Nehru National Institute of Technology Allahabad, India suneeta@mnnit.ac.in

2. Signature Verification Using Morphological Features Based on Artificial Neural Network Ms. Vibha Pandey Ms. Sanjivani Shantaiya M.Tech Scholar Assistant Professor DIMAT, India DIMAT, India vibha.pnd@gmail.com sanjivaninice@gmail.com

3. Neural Network-based Offline Handwritten Signature Verification System using Hu’s Moment Invariant Analysis Sandeep Patil, Shailendra Dewangan


7. Offline signature verification and recognition by support vector machine Emre Özgündüz, Tülin Şentürk and M. Elif Karslıgil Computer Engineering Departm]


