Offline handwritten Signature Verification by using Pixel based Method

Anu Rathi, Divya Rathi, Parmanand Astya

Computer Science and Engg. Department, Mahamaya University
MIET, Meerut

Abstract

Many systems or software are available to verify the signatures in bank cheques. In this paper, we verify the offline/handwritten signatures by taking a boundary of the entire signature and do the pixel wise comparison. Detection process is done after data acquisition and preprocessing. Experimental result shows that 80% of accurate matching with the existing one from the database. Signature is acquired using a scanner.

Keywords: **Pre-processing, Data acquisition, Off-line signature, Edge detection, Noise removal, Gray-scale manipulation.**

1. Introduction

Signature verification is natural and intuitive. The technology is easy to explain and trust. Takagi Sugeno (TS) model is used to detect the forgery detection of off-line signatures using fuzzy logic [1,2]. The primary advantage that signature verification systems have over other types of biometric technologies is that signatures are already accepted as the common method of identity verification. This history of trust means that people are very willing to accept a signature based verification system. Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer user. Another survey article [5] has been summarized the approaches used for off-line signature verification from 1993-2000. Unlike the older technologies of passwords and keycards – Which are often shared or easily forgotten, lost and stolen–dynamic signature verification provides a simple and natural method for increased computer security and trusted document authorization Signature verification is the process used to recognize and individual's hand–written signature. This is due to the fact that signature is a behavioral biometric. It differs from fingerprint, face, iris recognition, because these are based on the physical properties of the human beings. Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer user. Ammar et al. [3] who were one of the earliest researchers to analyzing the speed, shape, stroke, and pen pressure and timing information during the act of signing. As a replacement for a password or a PIN number, dynamic signature verification is a biometric technology that is used to positively identify a person from their handwritten signature.

There is an important distinction between simple signature comparisons and dynamic signature verification. Both can be computerized, but a simple comparison only takes into account what the signature looks like. Dynamic signature verification takes into account how the signature was made. Only the original signer can recreate the changes in timing and X, Y and Z (pressure). A pasted bitmap, a copy machine or and expert forger may be able to duplicate what a signature looks like, but it is virtually impossible to duplicate the timing changes in X, Y and Z (pressure).There will always be slight variations in a person's handwritten signature, but the consistency created by natural motion and practice over time creates a recognizable pattern of biometric identification steps in order to get a good quality image. A scanner digitized the signature in 256 gray levels with 400 dpi resolution and the images are stored in tagged image file format. A specimen copy of 20 signatures is acquired from each individual customers and it is stored in the database.

2. Proposed Approach

This paper deals with verifying the off-line signature in cheques. In this approach, this makes a pattern comparison of pixels captured within a specified boundary of signature.

Figure1shows the steps involved in our system.

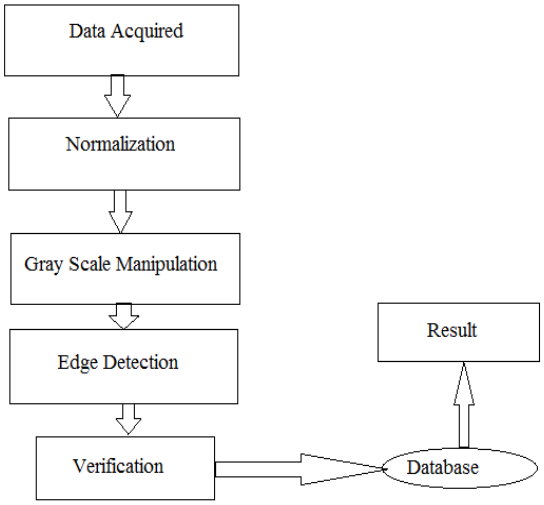

Figure 1. Steps involved in the system

3. Methodology

The methodology of this study involves data acquisition, preprocessing, feature extraction, signature comparison process, and performance evaluation which are discussed below.

A. Data Acquisition

A signature database of 2492 signatures is collected from 65 different signers which are scanned using a resolution of 300 dpi and stored as a BMP file type (no compression used). All signature sheets are manually cropped using a photo editor to separate them as individual images. The data acquisition process involved:

1) Acquisition of a total of 40 signatures from each author; 25 on blank sheets and 15 in provided random sized rectangles

2) Acquiring the signatures on 5 different days (when possible); 5 on blank sheets and 3 in provided rectangles on each day

3) Using 8 different pens which vary in colour (black, blue, red and green) and type (ball point, normal pen and fountain pen)

4) Signers asked to use as much as intra personal variations as possible

The group of 65 persons contributing to this exercise comprises mainly of family members friends and work colleagues having different background; education level, language, age and region. They represent a wide variety of signature

B. Pre-Processing

The pre-processing stage follows the four steps proposed in [3]: data area cropping, width normalization, binarization and skeletonization. Noise reduction is not required since the signatures are acquired on white sheets.

1. Data Area Cropping. Initially**,** the original 24-bit colour image is segmented from the background to remove the white space surrounding the signature using the segmentation method of vertical and horizontal projections [4].

2. Width Normalization. The cropped image is scaled using bicubic interpolation to a constant width, keeping the aspect ratio fixed.

3. Binarization. The 24-bit color signature is converted to grayscale and then finalized using a histogram-based binarization.

4. Skeletonization. The algorithm proposed by [5] is used in order to reduce data storage without losing the structural information of the image as well as to facilitate the extraction of morphological features from digitized patterns.

C. Feature Extraction and Selection

The choice of features is essential in optical recognition systems. The selected features must be suitable for application of the applied classifier. Feature extraction is divided into 2 sets of features including global and grid feature.

1. Global Features. Global features provide information about the entire structure of the signature. The proposed set of global features by [6] is extracted from the skeletonized signature in this study.

i) Signature Height - The height of the signature (in pixels), after width normalization, is considered as a global characteristic.

ii) Height-to-Width Ratio - The proportionality rate of the skeleton signature image. This is calculated by dividing the height with the width of the signature.

iii) Pure Width - The width of the skeleton signature with horizontal blank spaces removed.

iv) Pure Height - The height of the skeleton signature with vertical blank spaces removed.

v) Image Area - The number of black pixels in the skeleton signature.

vi) Maximum Horizontal Projection - The skeleton signature image is scanned vertically and each time calculating the horizontal projection. The horizontal projection represents the number of black pixels in the current row. Then, the row containing the maximum number of black pixels is taken to represent the maximum horizontal projection.

vii) Maximum Vertical Projection - Similarly to above, the maximum vertical projection represents the maximum number of black pixels in a column when scanning the skeleton signature image horizontally.

2. Grid Features

As explained in [7] grid segmentation is a technique used for signature detail analysis. A virtual grid of 12 x 8 segments are superimposed on the skeleton image and the following features are calculated for each segment.

1) Pixels Density. This is the number of black pixels within each segment

2) Pixels Distribution. It represents the pixel geometric distribution in a cell. The black pixels are projected in four side-line cell sensors from the central axis of the cell. Each sensor provides a numerical value corresponding to the total of the projected pixels.

3) Predominant Axial Slant. The predominant axial slant is a value representing the predominant inclination in each cell. For each cell the number of three pixels connections is calculated against the following templates.

D. Verification

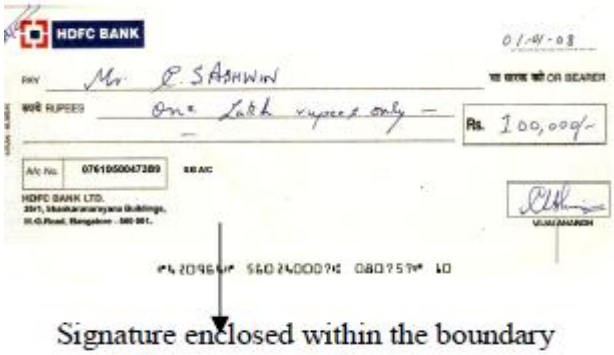

Figure 2. Shows a sample cheque

Algorithm to implement our approach:
Step 1: Get the processed signature image
Step 2: Assign count = 0; matched image = 0
Step 3: Compare the processed signature images with the corresponding customer's image in the database.
Step 4: Comparing pixels of both the images. If both corresponding pixels matched, then increment the
count value.
Step 5: Consider the next pixel and go to step 4.
Step 6: Repeat steps 4 and 5 until all the corresponding pixels are matched.
Step 7: If the pixel comparison is greater than 50 percentage, then increment counter value of matched image.
Step 8: If the matched image is greater than or equal to 10 then accept signature is correct.
Step 9: If the matched image is less than 10, then accept signature is incorrect.

4. Implementation and Result

Each customer shall have their sample signatures recorded and stored in the database. The images are stored in JPG format. The extraction of a signature from a bank cheque is a difficult task [7] at the cheque backgrounds are complex in nature. The cheques are scanned and compares with the signature of his/her database and comes out with a result. Signature in the cheques is compared with that of the existing database signature of that particular. Since we have 20 specimen signatures of the same person, we have wider area of comparison. We have limited that, if 10 of them matches, then we accept else reject it. We have implemented in MATLAB.

5. Conclusions

Signature scan has several strengths. Because of the large amount of data present in a signature scan template, as well as the difficulty in mimicking the behavior of signing, signature scan-technology is highly resistant to imposter attempts. As a result of the low false Acceptance Rate(FAR), a measure of the likelihood that a user claiming a false identity will be accepted, deploys can have a high confidence level that successfully matched users are who they claim to be. Signature-scan also benefits from its ability to leverage exiting processes and hardware, such as signature capture tablets and systems based on Public Key Infrastructure (PKI), a popular
method for data encryption. Since most people are accustomed to providing their signature during customer interactions, the technology is considered less invasive than some other biometrics.

However, signature-scan has several weaknesses. A pseudo-outer product-based fuzzy neural network drives the signature verification system [6]. Signature-scan is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner series of signatures those are similar enough that the system can locate a large percentage of the common characteristics between the enrollment signatures. For the purpose of signature detection and verification of forgeries TS model I used in the existing methods [8, 9]. During verification enough characteristics must remain constant to determine with confidence that the authorized person signed. As a result, individuals with muscular illnesses and people who sometimes sign with only their initials might result in a higher False Rejection Rate (FRR), which measures the likelihood that a system will incorrectly reject an authorized user. Since many users are unaccustomed to signing on a tablet, some subjects' signatures may differ to their signatures on paper, increasing the potential for false rejection.

6. References

[1] Hanmandlu, K.R. Murali Mohan, S. Chakraborty G.Garg, *Fuzzy modeling based signature verification system*, in: Proceedings of the sixth International Conference on Document Analysis and Recognition, USA, 2001, pp.110-114

[2] M. Hanmandlu, K.R. Murali Mohan S. Chakraborty, S. Goel, D. Roy Choudhury, *Unconstrained handwritten character recognition based on Fuzzy logic*, *Pattern Recognition* 36 (3) (2003) 603-623

[3] M. Ammar, Y. Yochida, T. Fukumura, *A new effective approach for offline verification of signature by using pressure features in*: Proceedings of the International Conference on Pattern Recognition, 1986, pp 566-599

[4] Sabourin, R. Plamondon, G. Lorette, *Offline identification with handwritten signature images: survey and perspectives*, *Structured Image Analysis*, Springer, New York, 1992, pp 219-234.

[5] R. Plamondon, S.N SriHari, *Online and Offline handwriting recognition: a comprehensive survey*, IEEE Trans. Pattern Anal. Mach. Intell.22 (1) (2000)63-84.

[6] C. Quek, R.W. Zhou. Antiforgery: *a novel pseudo-outer product based fuzzy neutral network driven. Signature verification system*, *Pattern Recognition* Lett.23 (2002) 1795-1816.

[7] S. Djeziri, F. Nouboud, R. Plamondon, *Extraction of signatures from check background based on filiformity criterion*, IEEE Trans. Images Process.7 (10) (1998) 1425-1438.

[8] M. Hanmandlu, K.R. Murali Mohan. Vivek Gupta, *Fuzzy Logic based character recognition*. Proceeding of the International Conference on Image Processing, Santa Barbara, USA, pp.714-717.

[9] Madasu Hanmandlu, Mohd. Hafizuddin, Mohd. Yusuf, Vamsi Krishna Madasu, *Offline signature verification and forgery detection using Fuzzy Modeling*, *Pattern Recognition* 38(2005)341-356.

[10] A.J. Elms, *The representation and recognition of text using hidden markov models*," in Ph.D., 1996.

[11] E. J. R. Justino, F. Bortolozzi, and R. Sabourin, "*offline signature verification using hmm for random, simple and skilled forgeries,"* in Proceedings of 6th International Conference On Document Analysis and Recognition, 2001, pp. 1031-1034.