A Simple Signature Recognition System

Suvarnsing G. Bhable

Research Student Dept. of CS & IT Dr. B.A.M.University, Aurangabad

Abstract: The signature of a person is an important biometric characteristic of a human being which can be used to verify human identity. Signature verification is an important research area in the field of authentication of a person as well as documents in e-commerce and banking. Signatures are verified based on features extracted from the signature using Invariant Central Moment and Modified Zernike moment for its invariant feature extraction because the signatures are Hampered by the large amount of variation in size, translation and rotation and shearing parameter. This signature recognition system is designed using MATLAB. This work has been tested and found suitable for its purpose.

Keywords: Biometrics, Hidden Markov models (HMM), Normalized area of signature, Off-line Signature Recognition, OCR

I. Introduction

Biometrics is technologies used for measuring and analysing a person's unique characteristics. There are two types of biometrics: behavioral and physical. Behavioral biometrics are generally used for verification while physical biometrics can be used for either identification or verification. Among the different forms of biometric recognition systems such as fingerprint, iris, DNA, face, voice, vein structure palm etc.,In our society, traditional and accepted means for a person to identify and authenticate himself either to another human being or to a computer system is based on one or more of these three (3) general principles:

- What the person knows
- What he possesses
- ➤ What he is

The signature recognition & verification system shown in Fig. 1 is broadly divided into three subparts

- a) Preprocessing,
- b) Feature extraction,
- c) Recognition & Verification.

The input signature is captured from the scanner or digital high pixel camera which provides the output image in term of BMP Color image. The preprocessing algorithm provides the required data suitable for the final processing. In the feature extraction phase the invariant central moment and Zernike moment are used to extract the feature for the classification purpose. In classification the Back propagation Neural Network is used to provide high accuracy and less computational complexity in training and testing phase of the system.



Fig.1: Flow Diagram of SRS (Signature Recognition System)

II. Classification

Major techniques used for offline signature verification system are based on Template Matching, Statistical Approach, Structural Analysis Approach, Spectrum Analysis Approach, Neural Network Approach [1]

• **Template Matching Approach** – The template matching is the simplest and earliest but rigid approach to pattern recognition in which instances of pre-stored patterns are sought in an image. It is performed at the pixel level and also on higher level. This approach has a number of disadvantages due to its rigidity. It may fail if the patterns are distorted due to the imaging process, viewpoint change etc as in the case of signatures. It can detect casual forgeries from genuine signatures But cant verify between the genuine signature and skilled ones. The template matching method can be categorized into several forms such as graphics matching, stroke analysis and geometric feature extraction, depending on different features.

• Statistical Approach – In this approach, each pattern is represented in terms of features and is viewed as a point in a d-dimensional space. Each pattern vector belonging to different categories occupy compact and disjoint regions in a d-dimensional feature space. Decision boundaries are set in feature space to separate different classes. The effectiveness of the feature set is determined by how well patterns from different classes can be separated. Hidden Markov Model (HMM), Bayesian these are some statistical approach commonly used in pattern recognition. They can detect causal forgeries as well as skilled and traced forgeries from the genuine ones.

- **Structural Approach** It is related to graph, string and tree matching techniques and is used in combination with other techniques. It shows good performance detecting genuine signatures and forgeries. Its major disadvantage is that it uses large dataset for greater accuracy.
- **Spectrum Analysis Approach** In this method the first stage of the procedure is the transformation of the data into another matrix which is a version of the trajectory matrix in Spectrum Analysis. Than a square window is placed in all possible places of image.[2] It basically decomposes a curvature-based signature into a multi-resolution format. This approach is used for long scripted signatures
- Neural Network Approach- The main characteristics of neural networks are that they have the ability to learn complex nonlinear input-output relationships, use sequential training procedures, and adapt themselves to the data. The most commonly used family of neural networks for pattern classification tasks is the feed-forward network, which includes multilayer perceptron, Radial-Basis Function (RBF) networks Self-Organizing Map (SOM), or Kohonen- Network.

III. Database

For training and testing of the signature recognition and verification system 500 signatures are used. The signatures were taken from 50 persons. The templates of the signature as shown in Fig.2 for training the system 50 person's signatures are used. Each of these persons signed 8 original signature and The input signature is captured from the scanner or digital high pixel camera which provides the output image in term of BMP Colour image. The preprocessing algorithm provides the required data suitable for the final processing. In the feature extraction phase the invariant central moment and Zernike moment are used to extract the feature for the classification purpose. In classification the Back propagation Neural Network is used to provide high accuracy and less computational complexity in training and testing phase of the system.

Signed 4 forgery signatures in the training set the total number of signatures is 500 (10 x 50) are used. In order to make the system robust, signers were asked to use as much as variation in their signature size and shape and the signatures are collected at different times without seeing other signatures they signed before. For testing the system, another 100 genuine signatures and 100 forgery signatures are taken from the same 50 persons in the training set.

IV. Preprocessing

Signature verification system is pre-processing. The need of pre-processing is explained through system. It can be clearly seen that while scanning a signature on white paper, residues are also scanned. This increases in fuzziness of the pattern. Thus, in the first step such scanning noise must be eliminated. We perform this by first converting the image to gray scale image. We then convert the image to binary image with a threshold. This results in particularly clear signature pattern as seen in system. Considering that the signature is scanned against a white background, it can be present at any side of the paper or it can be centralized. Considering this whole image as a sample will lead to improper statistics. Hence ROI of the signature must be

extracted first. Many literatures have proposed signature ROI detection using simple bounding box which is demonstrated in system. This involves two steps: First inverting the signature so that background becomes black and foreground is white and then obtaining a bounding box. However this traditional solution is many limitations when it comes to detecting discontinues signature as shown in that system.

This problem is overcome by first dilating input signature with a structuring element of size 16x16 and then applying the bounding box over it. The bounding box region is then annotated over non dilated image to extract the exact region. Results are shown in system.

Process of binary conversion also results in disconnected lines due to conversion error. This is overcome by first dilating and then eroding the binary image.

V. Feature Extraction

Emphasis of the proposed work is in detecting shape or boundary features. Features can be applied on binary image or thin image or edges. We performed a test to analyse the dominance of features in all three scenarios.

Figure 6 reveals that radon features are natural to shapes. Thus descriptors are dominant in same dimension for both normal as well as edge detected images. However number of dominant features is low in both cases. In order to obtain better descriptors we applied thinning with a structuring of kernel 2x2. Results are presented in Figure 7.

Place Tables/Figures/Images in text as close to the reference as possible. It may extend across both columns to a maximum width of 17.78 cm (7").

Captions should be Times New Roman 9-point bold. They should be numbered, please note that the word for Table and Figure are spelled out. Figure's captions should be centered beneath the image or picture, and Table captions should be centered above the table body.

Therefore it is proved that region of interest extraction must be followed by thinning process to extract good descriptor in signature verification system. Size is another important aspect of signatures. Local feature extraction techniques like Grid/Zone based features extractors demand that all the images be of same size. To study the effect of resizing, we performed feature extraction from resized ROI and without resizing. It can be clearly seen from that resizing induces interpolation losses. Hence feature descriptor changes. This leads to misclassification and results in low accuracy. To avoid this problem descriptor must be used on the actual image rather than resized image. However actual image size will vary from one signature to the other. Thus number of descriptors will also vary. One of the prerequisite for any classification is that feature dimensions must be same. Therefore it is wise to extract projection on different angles and extract statistics from them. It can be clearly seen that the transform descriptors varies as angle of projection varies. It is quite difficult to claim the actual projections that would result in optimized feature set. Hence we obtain Radon descriptors for 0' to 360' in steps of 15' and extract mean and standard deviation for each projection as our Radon feature set. Once Radon transform is extracted, we obtain Zernike moments before classifying or adding the features to database. Zernike like Radon is a shift invariant moments obtained from polar projection of image. Zernike moments are complex. Therefore real components from the moments are extracted as feature descriptor. Another major limitation of using Zernike moment is that the exponent of the dimension increases as number of moments is increased. But for modelling with HMM, dimensions must be normalized to single value domain. Hence after obtaining Zernike moments we normalize each dimension by dividing it with the highest exponent of that dimension. Thus all the feature values are brought in same value domain. Overall methodology is explained with a block diagram

VI. Conclusion

Signature verification and analysis are part of larger domain of work which finds application in graphology and forensic science. In this work we have presented a Novel technique of Signature Verification by combining Zernike moments with Radon transform values at different angle of projection from the user's Signature pattern and then forming a statistical state machine with HMM and PLSR. Further the technique was improved by the aid of kernel based techniques with the Help of SVM. It gives the poor performance for signature that is not in the training phase. Generally the failure to recognize/verify a signature was due to poor image quality and high similarity between 2 signatures. Recognition and verification ability of the system can be increased by using additional features in the input data set.

References

- M. J. Alhaddad, D. Mohamad and A. M. Ahsan, "Online Signature Verification Using Probablistic Modeling and Neural Network", IEEE, (2012)
- [2]. S. Srivastava and S. Agarwal, "Offline signature verification using grid based feature extraction", IEEE, (2011)
- [3]. J. Coetzer, B. M. Herbst and J. A. du Preez, "Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model", EURASIP Journal on Applied Signal Processing, (2004)

^{[4].} Sangramsing Kayte, Suvarnsing G.Bhable and Jaypalsing Kayte, —A Review Paper on Multimodal Biometrics System using Fingerprint and Signaturel. IJCA Volume 128 – No.15, October 2015.

- [5]. Ashwini Pansare, Shalini Bhatia, Handwritten Signature Verification using Neural Network, International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 1– No.2, January 2012
- [6]. O.C Abikoye, M.A MabayojeR. Ajibade "Offline Signature Recognition & Verification using Neural Network" International Journal of Computer Applications (0975 – 8887) Volume 35– No.2, December 2011
- [7]. Ozgunduz, E., Karsligil, E., and Senturk, T. 2005.Off-line Signature Verification and Recognition by Support Vector Machine. Paper presented at the European Signal processing Conference.
- [8]. Jain, A., Griess, F., and Connell, S. "Online Signature Recognition", Pattern Recognition, vol.35,2002, pp 2963-2972.
- [9]. Shashi Kumar D R, K B Raja, R. K Chhotaray, Sabyasachi Pattanaik, Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks, International Journal of Engineering Science and Technology Vol. 2(12), 2010, 7035-7044
- [10]. Julio Martínez-R.,Rogelio Alcántara-S.,On-line signature verification based on optimal feature representation and neural networkdriven fuzzy reasoning
- [11]. ICAO, Development of a Logical Data Structure LDS for Optional Capacity Expansion Technologies, International Civil Aviation Organisation, Tech. Rep., Machine Readable Travel Documents, Revision 1.7, 2004.