A Fusion of Statistical Distance and Signature Length Based Approach for Offline Signature Verification

Yashpal jitarwal[1], Pawan mangal[2], Tabrej ahamad khan[3]

[1]*Govt. polytechnic college , sheopur*
[2,3] *DR. B.R. Ambedkar NIT Jalandhar*

---***---

Abstract - *In today's society signatures are the most accepted form of identity verification. However, they have the unfortunate side-effect of being easily abused by those who would feign the identification or intent of an individual. A great deal of work has been done in the area of off-line signature verification over the past two decades. Off-line systems are of interest in scenarios where only hard copies of signatures are available, especially where a large number of documents need to be authenticated*

***Key Words*: Thining,Smoothing, Binarization , Gravity, Statistical distance.**

1.INTRODUCTION

Humans usually recognize each other based on their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. These characteristics are their identity. To achieve more reliable verification or identification we should use something that really recognizes the given person.

1.1 BIOMETRICS

The term "Biometrics" is gotten from the Greek words bio (life) and metric (to measure). Biometrics implies the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of verification is preferred over traditional methods involving passwords and PIN numbers for its accuracy and case sensitiveness. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user

1.2 SIGNATURE VERIFICATION

Signature verification is a common behavioral biometric to identify human beings for purposes of verifying their identity. Signatures are particularly useful for identification of a particular person because each person's signature is highly unique, especially if the dynamic properties of the signature are considered in addition to the static features of the signature. Even if skilled forgers can accurately reproduce the shape of signatures, but it is unlikely that they can simultaneously reproduce the dynamic properties as well.

2. Literature survey

Literature survey regarding the previous work and related approach about offline signature verification is presented. Signature from a special class of handwriting in which legible letters or words may not be exhibited. They provide secure means for authentication attestation and authorization in legal, banking or other high security environments. Signature verification problem pertains to determining where a particular signature is verily written by a person so that forgeries can be detected. Based on the hardware front-end, a signature verification can be classified as either offline or online.

2 FEATURE EXTRACTIONS AND SELECTION

Feature extraction is the process of extracting the characteristics of a preprocessed signature image. This process must be supported by feature selection that will highly influence the results in the evaluation of the comparison method. It is paramount to choose and extract feature that are

- computationally feasible.
- Lead to good classification rate sample system with low false rejection rate and low false acceptance rate.
- Reduce the problem data into a manageable amount of information without affecting the signature structure
-

2.1 Global Feature Extraction

kai et al. [1] also proposed a method with the help NN architecture. Here various static features e.g. slant or height etc. and dynamic features e.g. pressure or velocity etc. are extracted and then used for training the Neural Network. Many Network topologies are also tested and then accuracy of all of them is compared. This system performed very well and has an error rate of 3.3% (Best case).

2.2.2 Grid Based Feature

Peter et al. [6] proposed Feature point extraction method in which Vertical and horizontal splitting of the signature image was done to extract a total of 60 feature points (30 each). The features are based upon the 2 sets of points in two dimensional plane. The vertical splitting of the signature image produces 30 feature points (v1, v2, v3, v30) and horizontal splitting produces 30 feature points (h1, h2, h3 ,, h30). Central geometric point of the signature image is used to obtain these 60 feature points

3. WORK RELATED TO VERIFICATION STRATGIES

This section categorizes some research in offline signature verification according to the technique used to perform verification, that is, Distance Classifiers, Artificial Neural Networks, Hidden Markov Models, Dynamic Time Warping, Support Vector Machines, Structural Techniques and Bayesian Networks.

2.3.1 Template Matching Approach

It is a process of pattern comparison so it is called “template matching”. A test signature is matched with templates of genuine signatures stored in a knowledge base; the most common approaches use Dynamic Time Wrapping (DTW) for signature matching.

2.3.2 Neural Networks Approach

The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power (the sophisticated techniques used in NNs allow a capability of modeling quite complex functions) and ease of use (as NNs learn by example it is only necessary for a user to gather a highly representative data set and then invoke training algorithms to learn the underlying structure of the data).The signature verification process parallels this learning mechanism. There are many ways to structure the NN training, but a very simple approach is to firstly extract a feature set representing the signature

2.3.2 Neural Networks Approach

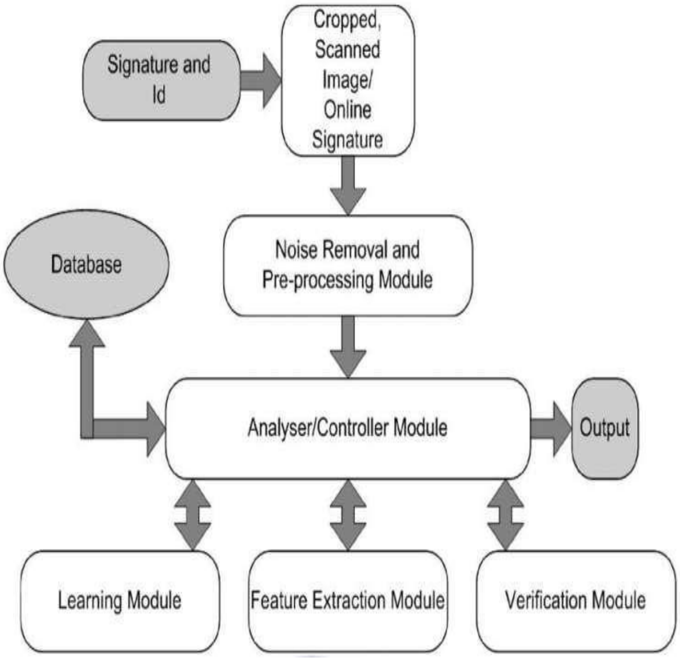
The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power (the sophisticated techniques used in NNs allow a capability of modeling quite complex functions) and ease of use (as NNs learn by example it is only necessary for a user to gather a highly representative data set and then invoke training algorithms to learn the underlying structure of the data).The signature Verification process parallels this learning mechanism. There are many ways to structure the NN training, but a very simple approach is to firstly extract a feature set representing the signature

3. PROPOSED SYSTEM.

We proposed a scheme for signature verification using signature length features and Statistical based features. The proposed system is organized into following sections. Section 3.1 describes database management, Section 3.2 describes preprocessing steps used in the system, Section 3.3 introduces feature extraction technique, Section 3.4 explains training and Section 3.5 describes signature verification.

3.1 DATABASE MANAGEMENT

This modules handles the various aspect of database management like creation, modification, deletion and training for signature instance. Data acquisition of static features is carried out using high resolution scanners. Figure 3.1 shows modular structure of an integrated signature verification system.


Signature and Id
Cropped, Scanned Image/ Online Signature
Database
Noise Removal and Pre-processing Module
Analyser/Controller Module
Output
Learning Module
Feature Extraction Module
Verification Module

3.2 PREPROCESSING

The signature image cannot be directly used for any feature extraction method. The image might contain certain noise or might be subjected to damage because it’s an old signature or the signature or signature under consideration may vary in size and thickness. Here some kind of enhancement operation need to be performed and they are carried out in this phase. The pre-processing step is applied both in training and testing phases. The pre-processing phases normally includes many techniques applied for binarization, noise removal, skew detection, slant correction, normalization, contour making and skeleton like processes to make character image easy to extract relevant features. The purpose of this phase is to make signature standard and ready for feature extraction. The pre-processing stage improves quality of the image and makes it suitable for feature extraction.

3.3 FEATURE EXTRACTION

Feature extraction stage is one of the crucial stages of an off-line signature verification system. Features cans be classified as global or local, where global features represents signature's properties a whole and local ones correspond to properties specific to a sampling point. Two types of features are used in the proposed work:
1.Signature length
2.Statistical Distance

3.4 TRAINING

Recent research in the field of machine learning focuses on the design of efficient classifier. The main characteristics of any classifier to correctly classify unseen data which were not present in the train set. Support vector machine (SVM) is used as the classifier for this research. The goal of SVM is to produce a model based on training set which predicts the target class of test data

3.4.1 Support Vector Machines

In general there are two approaches to develop classifiers: a parametric approach where a priori knowledge of data distributions is assumed, and a non-parametric approach where no a priori knowledge is assumed. Support Vector Machine (SVM) is a non-parametric binary linear classifier and supervised learning model used for classification and regression analysis

3.4.2 SIGNATURE VERIFICATION

In signature verification stage a signature to be tested is preprocessed and feature are extracted from the image as explained in the preprocessing and feature extraction section. Then it is fed into the trained support vector machine (SVM) which will classify it as genuine or forged signature

4. Experimental setup and results

4.1 LIBSVM

LIBSVM is an open source machine learning library developed at National Taiwan University. LIBSVM implements the SMO algorithm for kernelized support vector machines (SVMs), supporting classification and regression [42]. It is an integrated software for support vectorclassification, (C-SVC,nu-SVC),regression(epsilon-SVR, nu-SVR)anddistribution estimation (one-class SVM). It supports multi-class classification. LIBSVM provides a simple interface where users can easily link it with their own programs.

4.2 EXPERIMENTATION ON CEDAR DATASET

The experimental setups are performed four times on entire data set. In the first experimental set up, say ES1, The experiment process is carried out on each CEDAR signature set by randomly choosing 4 genuine and 4 forgery signature for training, while the remaining 20 genuine and 20 forgery signatures will be used for testing from each writer's signature. After the SVM is trained with signature length and statistical distance. The SVM is trained with labels '1' and '2', respectively denoting forgery and genuine signature. The trained network is tested against with remaining 20 genuine samples along with 20 forgery samples of the respective class. After intra class testing signatures some class of the signatures giving 60, 62.5, 65, 72.5, 75, 77.5, 80, 82.5, 90, 92.5, and 97.5

5. CONCLUSIONS

we proposed a novel approach for offline signature verification, in this we presented an automatic offline signature verification based on statistical distance and signature length. Statistical distance (mean and standard deviation) and signature length feature are used in different combination to construct feature vector. If statistical distance and signature length is used separately the performance of proposed system reduces significantly individually, statistical distance feature give better result than signature length this is a multi-algorithm system, and such system combines the advantage of individual feature sets and improve the accuracy rate. The algorithm can distinguish both random and skilled forgery with less error. SVM is a powerful classifier which outflanks numerous other existing classifier. The purpose of the SVM is to correctly classify test data using model trained from the reference data. The SVM is trained with the genuine and forged reference signatures.

REFERENCES

[1] Kai Huang, Hong Yan," Off-Line Signature Verification Based On Geometric Feature Extraction and Neural Network Classification", Proceedings of International Conference on Pattern Recognition (ICPR), Vol.30, Elsevier, pp. 9-17, 1997.

[2]M. C. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", in Electronics & Communication Engineering journal,273-280 ,1997.

[3]Peter Shao, Hua Deng, "Wavelet-based off-line handwritten signature verification", Proceedings of Computer Vision and Image Understanding (CVIU), Vol.76, Issue 3,173-190, 1999.

[4]Edson J. R. Justino, Abdenaimel Yacoubi, Flaviob Ortolozzi and Roberts Abourin, "An Off-Line Signature Verification System Using Hidden Markov Model and Cross-Validation" , Proceedings of International Conference on Neural Networks for Signal Processing (ICNNSP), IEEE, pp. 859–868, 2000.

[5]Katsuhiko Ueda, "Investigation of Off-Line Japanese Signature Verification Using a Pattern Matching", Proceedings of International Conference on document analysis and recognition (ICDAR), IEEE, pp. 951-955, 2003.

[6]Z. Lin. W. Liang. And R. C. Zhao, "Offline signature verification Incorporating prior model," Proceedings of International Conference on Machine Learning and Cybernetics (ICMLC), IEEE, vol. 3, pp. 1602–1606, 2003.

[7]J. Coetzer, B. M. Herbst, J. A. du Preez, "Offline Signature Verification Using DiscreteRadon Transform and a Hidden Markov Model", in EURASIP Journal on Applied Signal Processing, vol. 4, pp. 559–571, 2004.

[8]Hou Weiping, Xiufen Ye, and Keiun Wang, "A survey of off-line signature verification," Proceedings of International Conference on Intelligent Mechatronics and Automation (ICIMA), pp. 536-541, 2004.