A Survey On Signature Recognition

Emamul Haque Manna(160204)
Fatimatuj Jhora(160213)

April 16,2018

Abstract

The most used biometric identification and authentication for detecting a person is signature. It is widely used in bank, intelligence agencies and also used by many high-profile institutions to identify an individuals. In most of the cases the identification are done by visual inspection[1]. But it is very difficult and time consuming to verify every individuals signature. Thats why many initiatives were taken to automate the system. There are many techniques for signature verification, both online and offline. The purpose of this paper is to provide detailed overview on different signature verification techniques.

1 INTRODUCTION

Biometric technology is used for analyzing and measuring a person's unique characteristics.It can be either a physiological biometric system using face, fingerprint, iris, finger knuckle etc. or behavioral biometric system using voice or signature[1]. Among all of these signature is the most common and widely used techniques. Even with the emerging new technologies,signature is still continuously used as a means of communication in day to day life as, in a formal agreements, financial systems, government use, marketing documents. The inevitable side-effect of signatures is that they can be exploited for the purpose of feigning a documents authenticity[2]. Hence the need for research in efficient automated solutions for signature recognition and verification has increased in recent years to avoid being vulnerable to fraud[2].

Signature is used as a strong authentication feature of an individual. Manual verification of signature is very cumbersome and time consuming, to verify signature easily and within a short time without any error an automated system is essential. The objective of signature verification is to differentiate between original and forgery signature. Signature recognition can be identified by comparing test signatures with original signatures which is saved in database.

But it is not so easy process because every individuals signatures is not consistent. Individuals signature varies due to signing position, pen width, weight, stress, mood, time etc. Signature recognition can be classified into online and offline verification.

A. ON-LINE SIGNATURE

Online signature verification makes use of special equipment to acquire signature and extract dynamic features from signatures like pressure, speed, coordinates etc[1]. The accuracy of on-line signature recognition is high due to its dynamic characterstics.

B. OFF-LINE SIGNATURE

Offline signature verification uses scanned signature image or capture the image of the signature by camera from the written paper. It conatians lot of noise as compared to on-line signature and need complex processing to remove the noise.

2 BASIC CONCEPTS OF SIGNATURE VERIFICATION

(a) Preprocessing
(b) Feature Extraction
(c) Data Training
(d) Signature verification

2.1 Preprocessing[2]

The signature is first captured and transformed into a format that can be processed by a computer. Now its ready for preprocessing. In preprocessing stage, the RGB image of the signature is converted into grayscale and then to binary image. The purpose of this phase is to make signatures ready for feature extraction. The preprocessing stage includes two steps: Color inversion, Filtering and Binarization.

2.2 Feature Extraction

Feature means similar characteristics and Extraction refers to accurately retrieving those features. Proper feature extraction can increase the ratio of recognition a signature. There are three types of feature: Local features, Global features and Transition feature.

2.3 Data Training

Signature of individuals are collected and stored in database. In this collection both genuine and forgery are included. From these signatures, feature vectors are generated which can act as template for the verification stage.

2.4 Signature Verification

In this stage the signature of the individuals are authenticated by comparing their signatures with the genuine signature which is stored in database.

3 SURVEY

Pallavi Patil; Bryan Almeida; Niketa Chettiar; Joyal Babu [1] stated that the technique is used for offline signature recognition. In banks where thousands of cheques and scanned documents are to be processed every day, process of visually verifying the signatures become cumbersome and time consuming. In this paper the genuine user and forgery user is discriminated by using Histogram of Oriented Gradients. The proposed system comprises of three main modules; preprocessing module, feature extraction module and neural network based classifier module. Generally, scanning of signatures gives rise noise but after angle normalization all the signatures are resized into 256 X 512 pixels. After preprocessing the image of the signature goes through feature extraction process where gradient computation,gradient vote and normalization compution are included. In this paper signatures of 20 individuals were collected where 4 signatures were used for training and 8 signatures used for testing and the average accuracy is 96.875%. When they used 2 signatures for training the avergae accuracy decreased to 90.5% but when 6 signatures were used for training the average accuracy increased to 97.5%. In this system the False Reject Rate(FRR) is 3.152% and the False Acceptance Rate(FAR) is 0%.

A Karouni, B Daya, S Bahlak[2] presented the automatic signature verification,they made a sysytem for offline signature recognition where they used Artificial Neural Network(ANN). In their system they preprocessed the image first of all the RGB image of the signature is converted into grayscale and then to binary image.Preprocessing of image is occured by two steps
1.Color Inversion.
2.Image Filtering and Binarization.
After preprocessing the image of the signature it goes through feature extraction process which focused on Area, Centroid, Eccentricity, Kurtosis, Skewness. Artificial Neural Network or ANN resembles the human brain in learning through training and data storage. The ANN is created and trained through a given input/ target data training pattern. During the learning process, the neural network output is compared with the target value and a network weight correction via a learning algorithm is performed in such a way to minimize an error function between the two values. In this paper The system has been tested for its accuracy and effectiveness on a database of about 100 signatures from 3 users which Their database consists of signatures done with different pens with different colors. All the samples of their database were pre-processed and the global features were extracted out. After features extraction, testing is done and the result is displayed, and the threshold was taken 90% in the study that is below the percentage of 90% the signature is considered forged. The accuracy of the system is 93% under the 90% threshold.

D.S. Guru and H.N. Prakash[3] proposed a new method of representing online signatures by interval-valued symbolic features. Methods for signature verification and recognition based on the symbolic representation are also proposed. They investigate the feasibility of the proposed representation scheme for signature verification and also signature recognition using all 16,500 signatures from 330 individuals of the MCYT bimodal biometric database. They had made two option of threshold selection, Common Threshold Selection and Writer-Dependent Threshold Selection for calculating error. When Writer-Dependent Threshold is selected the error rate is less compared to Common Threshold Selection.

F.A. Afsar,M. Arif, U. Farrukh [4], focused on an efficient algorithm for an online signature verification system that is based on the extraction of global features from the spatial coordinates obtained during the online acquisition of a signature using one dimensional wavelet transform.The proposed method is based on the use of wavelet based global features for signature verification.VQ and feed forward neural network classifiers are used for classification purposes. The various steps involved in the operation of an online signature verification system include:
a. Acquisition
b. Preprocessing
c. Feature Extraction
d. Template Generation
e. Feature Matching
Minimum reported error rate for a dataset comprising of 982 genuine and 401 forged signatures is 2% after the system had been trained on 6 signatures of each individual.

Amruta B. Jagtap, Ravindra S. Hegadi [5] proposed and implemented an innovative approach based on upper and lower envelope and Eigen values techniques. Envelope represents the shape of the signature. Upper envelope is a curve connecting uppermost pixels of the signature. And the lower envelope is a curve connecting lower most pixels of the signature. Eigen value is a scalar associated with a given linear transformation of a vector space and having the property that there is some nonzero vector which when multiplied by the scalar is equal to the vector obtained by letting the transformation operate on the vector. The feature set consists of features such as large and small Eigen values computed from upper envelope and lower envelope and its union values. Both the envelopes are fused by performing union operation and their covariance is computed. The difference and ratios of high and low points of both the envelopes are computed. Lastly average values of both the envelopes are obtained. These features set are coupled with support vector machine classifier. The accuracy of proposed work obtained by linear SVM is 98.5%.

Emanuele Maiorana; Patrizio Campisi; Julian Fierrez [6] proposed an approach, which they refer to as BioConvolving, that is able to guarantee security and renewability to biometric templates. Specifically, they introduce a set of noninvertible transformations, which can be applied to any biometrics whose template can be represented by a set of sequences , in order to generate multiple transformed versions of the template. Once the transformation is performed, retrieving the original data from the transformed template is computationally as hard as random guessing. The proposed approach is applied to an on-line signature recognition system, where a hidden Markov model-based matching strategy is employed. The performance of a protected on-line signature recognition system employing the proposed BioConvolving approach is evaluated, both in terms of authentication rates and renewability capacity, using the MCYT signature database. The reported extensive set of experiments shows that protected and renewable biometric templates can be properly generated and used for recognition, at the expense of a slight degradation in authentication performance.

4 CONCLUSION

This paper presents a brief survey of the works done on various signature verification techniques. Different existing methods and approaches are also discussed. Each method has its own uniqueness. Lots of work has been already done, still there are many challenges in this research field. So, Future work should be extended by fusion of different classifier for better verification results.

References

[1] Pallavi Patil; Bryan Almeida; Niketa Chettiar; Joyal Babu *"Offline signature recognition system using histogram of oriented gradients"*, 2017 International Conference on Advances in Computing, Communication and Control (ICAC3).

[2] A Karouni, B Daya, S Bahlak *"Offline signature recognition using neural networks approach"*, Procedia Computer Science, 2011 - Elsevier.

[3] D. S. Guru; H. N. Prakash *" Online Signature Verification and Recognition: An Approach Based on Symbolic Representation"*, IEEE Transactions on Pattern Analysis and Machine Intelligence.

[4] F.A. Afsar,M. Arif, U. Farrukh *"Wavelet Transform Based Global Features for Online Signature Recognition"* ,9th International Multitopic Conference, IEEE INMIC 2005.

[5] Amruta B. Jagtap, Ravindra S. Hegadi *"Offline Handwritten Signature Recognition Based on Upper and Lower Envelope Using Eigen Values"*, World Congress on Computing and Communication Technologies (WCCCT).

[6] Emanuele Maiorana; Patrizio Campisi; Julian Fierrez; Javier Ortega-Garcia; Alessandro Neri *"Cancelable Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition"*, IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans.