Signature Recognition and Verification: The Most Acceptable Biometrics for Security

Deepali H. Shah¹, Dr. Tejas V. Shah²

¹Associate Professor, Instrumentation & control Engg. Department, L. D. college of Engineering, Ahmedabad, Gujarat, India
²Associate Professor, Instrumentation & control Engg. Department, S. S. Engineering College, Bhavnagar, Gujarat, India

Abstract

As every person carries distinct signature with its specific behavioral feature, signatures are widely accepted biometric for authentication and identification. Hence, it is quite necessary to prove the authenticity of signature itself. The extraordinary diffusion of the internet in our daily life as well as growing need of personal verification in many daily applications, signature verification systems for authorization and authentication have become enormously important in every sector due to increasing concerns for security. Signature verification finds its application in the field of net banking, passport verification system, credit cards, bank cheques, which may be the target of duplicity. This leads to rising demand for processing of individual identification faster and more correctly such as an automatic signature verification system. The offline and online signature verification system are enumerated in this paper. On-line approach uses an electronic tablet and a stylus connected to a computer which extracts information about a signature. The dynamic information like; pressure, velocity are used for online approach. Offline systems are more applicable and easy to use in comparison with on-line systems but it is more difficult due to the lack of order of strokes, the velocity and other dynamic information. Feature extraction stage is the most important stage in both signature verification systems.

Keywords: Biometrics, HMM, wavelet, OCR.

1. INTRODUCTION

Biometric verification is defined as a method of uniquely identifying a person by analyzing one or more of biological traits. Biometrics has two basic categories, physical and behavioral [1]. The physical biometrics uses the characteristics of the human body like the eye retina scans, facial features, fingerprints, hand geometry, earlobe geometry and DNA. The behavioral characteristics use features like voice, handwriting, typing and gait. Historians have found thumbprint samples that were used ages before in China for authenticating the genuine person. These systems are basically a pattern recognition system which includes all the hardware and associated software and interconnecting infrastructure, enabling identification by matching a live sample to a stored pattern in a database.

Major analysis issue with biometrics systems is the change of state of biometric information over time as per the physical conditions or emotional situations of human beings. Signature is found to be the foremost authentic parameter within the field of authentication. Signature is that special pattern provided by human to authenticate himself/herself at secured and private zones [1]. Signature is the most common authentic entity that has been used earlier in numerous confidential purposes from the user aspect. For security, the signature is enrolled and verified for authentication system. The proposed authentication system is the replacement for password based authentication [1]. Signatures acts as a strong authentication feature of the signer. But, the manual verification of signatures by humans is tedious job. Signatures are composed of special characters and flourishes. The intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together [2]. Therefore, automated signature verification is user demand in recent time.

Signatures biometrics can be classified in to online and offline depending upon the approach. Online signatures verification is more unique and difficult to forge than offline signature verification. Offline signature verification uses shape information while its counterpart uses dynamic features like speed, pressure and capture time of each point on the signature trajectory. In short, online signatures have an extra dimension, which is not available for the offline signatures which make online signature verification more reliable than the other one.
Figure 1 summarizes the task to be performed by a signature verification system. The test signature and a claimed ID are given, either accept a user as the identity owner or deny him based on a dissimilarity degree between the test and reference set signatures. In either of the two signature verification systems, the users are first enrolled by providing reference signature samples. When a user presents a test signature and claims to be a particular individual, the test signature is compared with reference set signatures of the claimed identity [3]. If the dissimilarity between the test and reference set signatures is above a certain threshold, the user is rejected [4], [3].

The dissimilarity between two signatures can be established in two ways. For first distance approach, if each time a signature is presented to the system, equal number of features is being extracted from that signature. Euclidian distance can be used to compare these two signatures. Global features which describe the signature as a whole are used in this type of comparison. These systems are generally fast but have low performance. The second alternative is to make a point by point comparison, where the so called local features, pertaining to particular points on the signature trajectory, are used. As signatures signed by the same person may vary in length which lead to implying feature vectors of different length, methods that are able to non linearly associate vectors of different lengths, such as Dynamic Time Warping (DTW) or Hidden Markov Models (HMM) are used [3].

Figure 2 shows the different forgery cases. In skilled forgery, it is signed by a person who has had access to a genuine signature for practice [5]. In simple forgery, it is signed by a person who has not access to a genuine signature [5]. In random or zero effort forgery, it is signed without having any information about the signature or even the name of the person whose signature is forged [5]. State of the art performance of the available online signature verification algorithms lies between 1% and 10% equal error rate, while off-line verification performance is still between 70% and 80% equal error rate. Unfortunately no public signature database of either type is available, which makes it difficult to compare existing signature verification systems [3].
2. SIGNATURE RECOGNITION STEPS

Data are preprocessed in signature recognition system. The steps are as follows

2.1 Data Acquisition

The signature is scanned through optical scanner from the document for the verification purpose and it should be improper digital image format.

2.2 Preprocessing

Input image of signature is normalized as it is captured from image capturing devices, this is called preprocessing. This stage is further subdivided into Normalization, Image Binarization, Data Area Cropping, Thinning [6].

![Original Image, Binarized Image, Normalized Image, Eroded and Dilated Image](image)

**Figure 3** Signature Recognition Steps

2.2.1 Normalization

Before any further processing takes place, a noise reduction filter is applied to the binary scanned image. The aim is to eradicate single white pixels on black background and single black pixels on white background. In order to accomplish this, we apply a 3 X 3 mask to the image with a simple decision, basic principle is that if the number of the 8 neighbours of a pixel that have the same colour with the central pixel is less than two, then reverse the colour of the central pixel [7]. Figure 3 shows normalized image of the original one.

2.2.2 Image Binarization

It allows us to reduce the amount of image information by removing colour and background so the output image is black & white. The black & white type of the image is much easier for further processing [7]. Image binarization is shown in Figure 3.

2.2.3 Data Area Cropping

The signature area is alienated from the background by using the well known segmentation methods of vertical and horizontal projection. Thus, the white space surrounding the signature is discarded. Morphological operation Erosion and Dilation applied to perform this step [7]. Eroded and dilated image is shown in Figure 3.

2.2.4 Thinning

Size of the image is abridged. In this procedure unnecessary signature areas are removed. First of all, mark all the points of the signatures that are candidates for removing (black pixels that have at least one white 8-neighbor and at least two black 8 neighbors’ pixels). Then after, examine one by one all of them, following the contour lines of the signature image, and remove these as their removal will not cause a break in the resulting pattern. At last, if at least one point was deleted, go again to initial step and repeat the process once more [7]. Edge detected image is shown in Figure 3.

3. FEATURE EXTRACTION FOR OFFLINE SIGNATURE

The characteristic data are gathered and output result is a set of the unique information of the signature. The choice of a powerful set of features is crucial in optical recognition systems. The features used must be suitable for the application as well as for the applied classifier [7].

Global features provide information concerning the structure of the signature. Signature density in terms of pixels is identified. Signature’s height to width ratio is obtained by dividing signature height to signature width which can change. Obviously, this ratio of one person’s signatures is always approximately equal. The horizontal histograms are calculated for each row and the row which has the highest value is taken as maximum horizontal histogram. The
vertical histograms are calculated for each column and the column which has the highest value is taken as maximum vertical histogram. Aspect Ratio is the ratio of signature pure height to signature pure width [8]. Grid information and texture features are intended to provide overall signature appearance information in two different levels of detail. The skeletonized image is divided into 120 rectangular segments (15x8), and for each segment, the area (the sum of foreground pixels) is calculated. The results are normalized so that the lowest value i.e., the rectangle with the smallest number of black pixels would be zero and the highest value i.e., the rectangle with the highest number of black pixels would be one. The resulting 96 values form the grid feature vector. It is very encouraging to recognize diagonally so that more points may be diagnosed for generating the vector matrix to get results more accurate than the simple grid. This feature is shown in Figure 4.

Figure 4: Grid for Signature Image

4. APPROACHES TO OFFLINE SIGNATURE VERIFICATION

4.1 Template Matching
Fang et al. [9] has proposed two methods for the detection of skilled forgeries using template matching. In one method, optimizing matching of the one dimensional projection profiles of the signature patterns is carried out. In second method, the elastic matching of the strokes in the two dimensional signature patterns is carried out. For verification of test signature, the positional variations are compared with the statistics of the training set and a decision based on a distance measure. In this method, both binary and grey level signature images are tested. The average verification error rate of 18.1% was reported when the local peaks of the vertical projection profiles of grey level signature images were used for matching and for full estimated covariance matrix incorporated [10]. The performance of verification is affected by the variation of signature stroke widths and a registered signature image selected from a collection of samples in offline signature verification using a pattern matching scheme.

4.2 Statistical approach
The rule of Correlation Coefficients between two or more data items can easily be implemented. The relation between some collected data items can be find out using statistical approach based on departure of two variables from independence. To verify an entered signature with the help of an average signature, which is obtained from the set of previously collected signatures, follows the concept of correlation to find out the amount of divergence in between them [9].

A Bayesian model is used for off-line signature verification including the representation of a signature throughout its curvature. It is generative for specifying the knots in a rough calculation limited to a buffer region close to a template curvature, beside independent time warping scheme [9]. In this case, prior shape information about the signature can be built into the analysis. The observation model is related to additive white noise superimposed on the underlying curvature. This approach is implemented using Markov chain Monte Carlo (MCMC) algorithm and used as set of standards instances of Shakespeare’s signature [9].

4.3 Hidden Markov Model Approach
Markov model is a mathematical model depending on stochastic processes which produce random outcomes as per associated possibilities. A hidden Markov model presents only sequence of outputs or emissions, but hides the sequence of the states the model underwent to produce the emission [11]. Hidden Markov Model (HMM) is a probabilistic pattern matching technique which absorbs variability and the similarity between signature samples. Hidden Markov Models (HMM) represent a signature as a sequence of states. In each state an observation vector can be generated, according to the associated probability distribution. Transitions among the states are governed by a set of probabilities called transition probabilities [11]. The parameters of an HMM are trained using observation vector extracted from a representative sample of given signature. Recognition of an unknown signature is based on the probability that a signature was generated by the HMM. A well chosen set of feature vectors for HMM could lead to design of an efficient signature verification system. Justino et al. [12] proposed basic and robust system for offline verification using simple features in which simple and random forgery error rates have shown to be low and close to each other. A false rejection rate (FFR) of 2.83% and a false acceptance rate (FAR) of 1.44%, 2.50 % and 22.67% are reported for random, causal, and skilled forgeries, respectively [11].
4.4 Structural or Syntactic Approach

In structural approaches, patterns are represented by symbolic data structures such as string, graph, and tree. The unknown pattern is recognized by comparing its symbolic representation with a number of prototypes stored in a database. Structural features use modified direction and transition distance feature (MDF) which extracts the transition locations and are based on the relational organization of low level features into higher level structures [5]. The Modified Direction Feature (MDF) [13] utilizes the location of transitions from background to foreground pixels in the vertical and horizontal directions of the boundary representation of an object.

Nguyen et al [14] presents a new method in which structural features are extracted from the signature's contour using the (MDF). In its extended version, the Enhanced MDF (EMDF) and further two neural network-based techniques and Support Vector Machines (SVMs) are investigated and compared for the process of signature verification [5]. A distinguishing error rate (DER) of 17.78% was obtained with the SVM whilst keeping the false acceptance rate for random forgeries (FARR) below 0.16%.

4.5 Neural Networks

In this approach, signature is divided into two halves and for each half a position of the centre of gravity is calculated with reference to the horizontal axis. The structure features from modified direction feature and other features as surface area, length skew and centroid feature are considered. For classification, two approaches are compared: the Resilient Backpropagation (RBP) neural network and Radial Basic Function (RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries [9]. These two classifiers register 91.21% and 88 % true verification respectively.

In one approach, signature is captured and presented to the user in an image format [15]. The Signatures are verified by using parameters extracted from the signature based on various image processing techniques. It helps in detecting the exact person and it provides more accuracy of verifying signatures as compared to prior works [9]. Feed Forward Neural Network (FFNN) is used for recognition and verification of signatures.

4.6 Wavelet Approach

The decomposed lowpass and highpass information of signal is obtained by multi resolution wavelet transform. The sharper variations in time domain are represented in highpass information. Wavelet theory [5] is used to decompose a curvature based signature into a multi resolution signal. If the whole signature curves are matched, it is very hard to distinguish the genuine signatures and the forged ones effectively, because the signature curves are very complex and changeful, even the genuine signatures of the same person have very large differences [5].

In one novel approach to offline signature verification, static and pseudo dynamic features are extracted as original signals. These features are processed by Discrete Wavelet Transform (DWT) and converted into stable features in each sub band which can enhance the difference between a genuine signature and its forgery. During the training phase, the proposed fuzzy net is trained with genuine signatures only [5]. The signatures with the maximal ratio of the mean value of the similarity to the standard deviation are selected as the training samples from a set of genuine signatures. The verification scheme is achieved by combining the proposed fuzzy net output in each sub band level. The entire system was tested by using two databases of English and Chinese signatures, and the average error rates of 12.57% and 13.96% were obtained, respectively [5].

5. Online Signature Verification Approach

The algorithm developed for online verification give a high performance of signature recognition. Figure 5 shows the process of recognition. The OCR feature is combined with algorithm which improves the process of pattern recognition. The input is taken from either scanner or a camera. This software recognizes each signature individually with less error. All the inputs are stored in the database for each client and is recalled for verification as per requirement with optimization [16].

Classifier is built with several steps. The features of the new input signature, new hand writing or even just a character are leaned by it. The features from each individual character are extracted with edge detection. Extraction of features from the data base is also carried out. The pixels numbers in each input character segmented and center of mass (most pixels at a point) is obtained. The oval factors such as Conventionality, Position, Kurtosis and skewness, Moments of high demand, A series of code conversion, Series and Fourier conversion are considered [16].

Once, the classification process is completed, the output of classification process is fed to the recognition process in order to test the data and check the performance of the testing process of recognition of the real time data [16].
6. Conclusion

For offline signature verification, different techniques can be used to get optimum results depending on feature set selected. The offline signature verification and recognition technique are based on global, mask, grid features of signatures. Recognition and verification ability of the system can be increased by using additional features in the input data set. This technique can be combined with speech and face recognition for better outcome which can lead to minimizing the cases of forgery in business transactions.

For online signature recognition, feature extraction process of OCR is a highly efficient and robust recognition technique. Furthermore, segmentation plus feature extraction approach makes the developed system more practical. The classifier gets trained for the individual’s handwriting as well as lower case, upper case and the signature of an individual’s data which helps the classifier achieve more accurate results. The said system achieves accurate recognition results even for poor handwritten which is a major achievement.

References


