Offline Signature Recognition Using Fourier Descriptor and Histogram

Jin Wu

Department of Electrical and Computer Engineering
University of Toronto

ABSTRACT

This paper describes a new implementation method of offline signature recognition using Fourier Descriptors and Histograms. As signature recognition is one of the oldest and arguably safest biometric methods to date, our intention is to implement an accurate recognition system that can be used for security purposes. A database of 300 signatures was collected from 30 individuals. 150 of which were forged attempts. A FAR rate of 1.3% was achieved.

1. INTRODUCTION

There is an increasing demand for improved security for services such as banking and credit cards. In a study conducted by the Identity Theft Resource Center, it was stated that only 15% of identity theft victims find out about the theft through proactive action taken by businesses. Identity theft is a billion dollar problem, and the current counteractive measures in place are clearly not doing a good enough job of averting the problem.

Biometrics is the study of methods for uniquely recognizing humans based upon one or more of their characteristics. This includes methods such as face recognition, iris recognition, fingerprint recognition, and signature recognition. Signature recognition is arguably the safest of all these techniques, as forgeries usually do not impose risks to human lives. News of human fingers being cut off in biometric crimes is not uncommon. [1]

The biometric concerning the topic of identity theft is signature recognition. This consists of identifying the signature, and more importantly verifying the signature. A signature will be captured and then compared with what is stored in a database for verification. The issue with accurately recognizing a signature input is that individuals bear unique signatures, but samples of that individual’s signatures are not identical. The key of the problem is to identify and fine-tune the recognition of the same individual’s signature as the sample size increases.

Signature recognition methods can be divided into two categories: online signature recognition, and offline signature recognition. Online methods vary and may take things such as speed, direction, pressure, and shapes/sizes of signatures into consideration. Common methods include the Wavelet Transform. Offline signature recognition is by far much more limited as it can only take shapes and pressure into consideration. **Section 2** will talk further about four of these methods. Due to technical constraints, our method is an offline recognition method; it uses Fourier descriptors and histograms to classify the signature. The implementation and results will be described in details in **Section 3**, and a comprehensive comparison with other methods will be done in **Section 4**.

2. BACKGROUND

As signature recognition is one of the oldest biometrics around, many implementation methods have been developed over time.

This section will briefly summarize several of these methods:

Offline Signature Recognition

- General Offline Signature Recognition
- Neural Network Classification
- Hidden Markov Method (HMM)

Online Signature Recognition

- General Online Signature Recognition
- Wavelet Transform Based Global Features

2.1. General Offline Signature Recognition

In general offline signature recognition systems, the shape and/or pressure information is generally obtained and analyzed. Decisions are made purely on these.

This method is quite limited, and results of several papers that use this method are shown in **Table 1** below.

Method	**Recognized**	**Not Recognized (FAR)**
[8]	96.06%	3.94%
[9]	60%	40%

Table 1: Signature Recognition through General Offline Signature Recognition

2.2. Neural Network Classification

The Neural Network Classification method is an offline algorithm done in the following way: First, basic image processing such as noise reduction, scaling and normalization are done on the signature. After that, features are extracted in two ways: through global features and local features. Global features include image area, width, height, centroid(s), baseline shift, slant angle, number of edge points, number of cross points, and number of closed loops amongst others. Local features are unique to each signature. Data is then stored in vectors and neural network based decisions are made.

This method obviously does not perform as well as some of the other methods as it depends solely on the geometry of the data. Speed, and direction, among other factors are not taken into consideration. However, if done well, the basic shape of the signature is well recognized, and any forgery attempt would have to be fairly accurate in shape in order to be mistaken as a real signature.

The results of several papers [2] that implemented this method are shown in **Table 2** below.

Method	**Recognized**	**Not Recognized (FAR)**
[2]	80%	20%
[10]	100%	0%

Table 2: Signature Recognition through Neural Network Classification

2.3 Hidden Markov Method (HMM)

The Hidden Markov Method (HMM) is an online signature recognition method that uses temporal information to process the signature. First, basic pre-processing was done on the signature. This includes noise reduction, binarization, normalization, and outline detection via a skeletonization/thinning algorithm. Then, length and direction of strokes are analyzed and predicted by assigning a HMM model to each of the signatures and analyzing the states.

This is a more accurate method that takes shape, time, and directional information into consideration, but does not consider the effects of pressure, which may be of importance when it comes to forgery.

The results of several papers [3] that used this method are shown in **Table 3** below.

Method	Recognized	Not Recognized (FAR)
[3]	92%	8%
[6]	92.5%	7.5%
[7]	99.1%	0.9%

Table 3: Signature Recognition through Hidden Markov Method (HMM)

2.4 General Online Signature Recognition Technique

Online signature recognition is generally done in the following way: data such as the shape, speed, pressure, and direction of strokes are captured when the signatures are obtained; then the data is analyzed on each set of data. Information such as x versus time, y versus time, pressure versus time, altitude versus time, and azimuth versus time are plotted, decision was then made based on each of these plots.

This method is possibly one of the best methods for signature recognition. It uses both the shape and temporal information to analyze the signatures. Unfortunately, due to limited resources available to us (i.e. lack of a time capturing tablet), we were unable to use this method.

The results of several papers [4] that implemented this method are shown in **Table 4** below.

Method	Recognized	Not Recognized (FAR)
[4]	99.6%	0.04%
[11]	86.67%	13.33%

Table 4: Signature Recognition with Generic Online Signature recognition Technique

2.5 Wavelet Transform Based Global Features

Since wavelets provide better results than Fourier transforms (as deviations of results are localized), the wavelet transform is a popular strategy for online signature recognition. First, data such as the x position, y position, speed in x direction, and speed in y direction are extracted and calculated. Then, these information are transformed by the wavelet transform and further analysis is done on the data to determine whether a signature is valid.

This is a great signature recognition technique as it incorporates shape and velocity information into part of the decision making, and wavelets give more accurate results than most other techniques.

The results of several papers [5] that used this method are shown below in **Table 5**.

Method	**Recognized**	**Not Recognized (FAR)**
[5]	96.69	3.21

Table 5: Signature Recognition through Hidden Markov Method (HMM)

3. IMPLEMENTATION

Due to technical constraints (i.e. the lack of a tablet capable of capturing speed and time information), our implementation had to be an offline recognition method. The method used is a new technique that uses Fourier descriptor as well as histograms to classify the signature. This method gives higher accuracy in determining the shape and pressure of the signature compared to other offline methods that used geometric properties such as the centroid.

Similar to many literatures we've come across, the general steps for signature recognition can be shown in a diagram form in **Figure 1**:

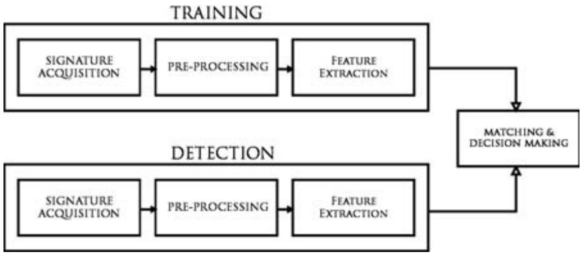


Figure 1: Steps of implementation

3.1. Signature Acquisition

This was done via an HP TX2524 convertible tablet PC. This eliminates any potential noise that may result from paper signatures. 30 individual's signatures were obtained. Each individual provided five real signatures and five forged signatures, for a total of 300 signatures. Signatures were captured in Adobe Photoshop on 500x500 pixel screens.

3.2. Pre-processing

Generic normalizations and scaling were done on the signatures. Binarized versions of signatures were also obtained for the Fourier descriptor module of the feature extraction.

3.3 Feature Extractions

Feature extractions were based on two methods: Fourier descriptors and histograms.

3.3.1 Fourier Descriptor

As geometric properties of the same person's signatures can fluctuate quite inconsistently, Fourier transforms of these signatures seem to produce much more reliable classifications compared to other methods.

Table 5 shows several different signatures and their corresponding Fourier transform.

It is quite obvious that the shapes of the Fourier transformed versions of different signatures are quite different. However, it is still challenging finding correlations between signatures simply by calculating the Mean Square

Error (MSE) of signatures as the images are quite noisy after the Fourier transform. To solve this problem, two things were done to the images:

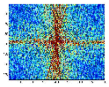
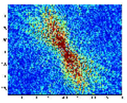
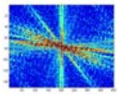
Original Signature	Fourier transform of Signature
	
	
	

Table 5: Sample signatures and their corresponding Fourier transforms after normalization

1. Values of the Fourier descriptor were sorted from highest to lowest, the 4000 largest coefficients were kept and the rest were discarded. This preserves the basic shape without too much noise.
2. All non-zero values were set to a value of 50 to further standardize the shape of the graphs.

Table 6 shows comparisons between an original Fourier transform and the corresponding "cleaned up" version.

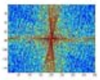
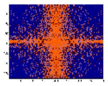
Fourier Transformed Signature	Cleaned-Up Fourier Transform
	

Table 6: Comparison between the original Fourier transform and a less noisy version

After the signatures have been cleaned up, MSE values are calculated in the following way:

1. The MSE was taken between each of the five authentic signatures (per person). The max MSE (*max_mse_real*) and min MSE (*min_mse_authentic*) were recorded.
2. A testing (possibly forged) signature is then tested by taking the MSE between the testing signature and each of the five authentic signatures. Then the average of these 5 MSEs is taken (*mse_testing_with_authentic)*
3. If *mse_testing_with_authentic* is 20% less than *min_mse_authentic* or 20% greater than *max_mse_authentic*, it is rejected. Otherwise it is accepted as a real signature.

3.3.2 Histogram

Histograms were calculated using the `imhist` function in Matlab. Images were taken as inputs, and calculations were performed on the intensity of the images. The general idea of this method is that if we have the histogram of one signature, and compare it to the histogram of a fake signature, the histograms will differ due to the differences in pressure of the two samples. The pressure differences produce different colour intensity levels in each signature's histogram. If the signature we are testing is from the same person who made the signature we are comparing to, the pressure differences will be minimal.

We can now calculate the Mean Squared Errors (MSE) between the authentic signatures and the test signature (more specifically, the matrix representations of their histograms). If the MSEs between the sample signatures and the signature being tested are insignificant, we can be reasonably confident that the tested signature comes from the same person that created the signature samples. After numerous trials between different sets of authentic signatures were performed, the threshold MSE value was determined. If a tested signature produces an MSE above the threshold MSE, it would be regarded as a fake signature attempt.

MSE values are calculated in the following way:

1. The MSE was taken between each of the five authentic signatures (per person). The max MSE (*max_mse_real*) and min MSE (*min_mse_authentic*) were recorded.
2. A testing (possibly forged) signature is then tested by taking the MSE between the testing signature and each of the five authentic signatures. Then the average of these 5 MSEs is taken (*mse_testing_with_authentic)*
3. If *mse_testing_with_authentic* is 20% less than *min_mse_authentic* or 20% greater than *max_mse_authentic*, it is rejected. Otherwise it is accepted as a real signature.

3.4 Matching and Decision Making

A signature is determined to be authentic if and only if it is accepted by both the Fourier Descriptor and the Histogram tests. Otherwise it will be rejected. Although this may potentially increase the FRR (False Rejection Rate), it significantly decreases the FAR (False Acceptance Rate), which we believe to be of more importance.

3.5 Results

Implementing the Fourier Descriptor alone, the following results are achieved (**Table 7**).

	FAR	FRR
Percentages	8%	6.66%

Table 7: Percentages of FAR and FRR with Fourier Descriptor signature recognition technique.

Using the Histogram alone produces the following results (**Table 8**).

	FAR	FRR
Percentages	12%	8.66%

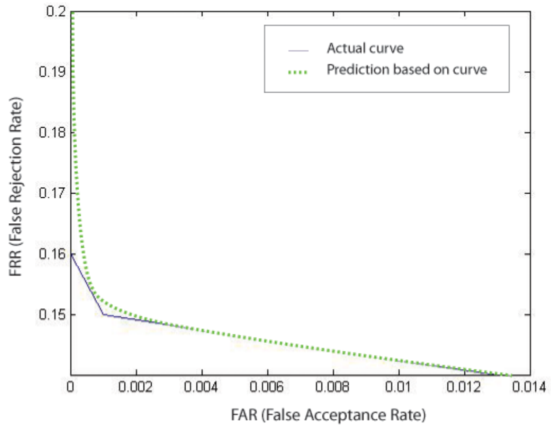
Table 8: Percentages of FAR and FRR with Histogram signature recognition technique.

With a combination of the Histogram and the Fourier Descriptor techniques, the following results are achieved (**Table 9**).

	FAR	FRR
Percentages	1.3%	14%

Table 9: Percentages of FAR and FRR with combined signature recognition techniques.

The results can be shown in a Receiver Operating Characteristic (ROC) graph as follows:



Graph 1: Operating Characteristic (ROC) Graph

4. COMPARISON

Table 10 below shows a comprehensive comparison between different methods. Our method is highlighted in yellow. Most of the offline methods were done on paper whereas the online techniques were primarily done on digital media systems such as tablets. Although our method was done on a tablet as well, it can also be done on paper; however, with the rapid change of technology, having paper signatures, scanning them, and making comparisons defeats the purpose of an efficient biometric system.

Method	**Recognized**	**Not Recognized (FAR)**	**Number of Samples**	**Method of Capture**
OFFLINE METHOD				
Neural Network[2]	80%	20%	300	Paper
Hidden Markov Method[3]	92%	8%	240	Paper
Fourier Descriptor/ Histogram	98.7%	1.3%	300	Digital Tablet
ONLINE METHOD				
General Online Method[4]	99.6%	0.04%	Unknown	Tablet
Wavelet Transform Method[5]	96.69%	3.21%	3460	Camera-based Interface

Table 10: Comparison of performance of Fourier Descriptor/Histogram method with other method.

Thus, having done the signatures on a noise-free tablet, we do not see this as a disadvantage, but rather an advancement of technology over the years. Although our dataset was limited due to time and resources constraints, it was sufficient enough to produce good results. More sample sets would definitely give a more accurate picture of how well our method performed, but we do not have time to collect hundreds of signatures.

5. CONCLUSION

We've introduced a more accurate form of offline signature recognition using Fourier Descriptors and Histograms. A FAR rate of as low as 1.3% was achieved as a result of this. The results prove to out-perform most other offline recognition techniques.

REFERENCES:

[1] “Malaysia car thieves steal finger“; Mar. 2005; BBC News [http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm]

[2] Karki, M.; Indira, K.; Dr. Selvi, S.; “Off-Line Signature Recognition and Verification using Neural Network”; Volume 1, 13-15 Dec. 2007 Page(s):307 – 312.

[3] Camino, J.; Travieso, C.; Morales, C.; and Ferrer, M.; “Signature Classification by Hidden Markov Model”; 5-7 Oct. 1999 Pages:481 – 484.

[4] Adamski, M.; Saeed, K.; “Online Signature Classification and its Verification System”; 26-28 June 2008 Pages: 189-194.

[5] Afsar, F.A.; Arif, M.; and Farrukh, U.; “Wavelet Transform Based Global Features for Online Signature Recognition”; 24-25 Dec. 2005 Page(s):1 – 6.

[6] Fard, M.M.; Mozayani, N.; “A new on-line signature verification by Spatio-Temporal neural network”; 17-20 June 2008 Page(s):233 – 235.

[7] Zois, E.N.; Nassiopoulos, A.A.; Anastassopoulos, V.; “Signature verification based on line directionality”; 2-4 Nov. 2005 Page(s):343 – 346.

[8] Porwik, P.; Para, T.; Some Handwritten Signature Parameters in Biometric Recognition Process; 25-28 June 2007 Page(s):185 – 190.

[9] Cavalcanti, G.D.D.C.; Doria, R.C.; Filho, E.Cde.B.C.; “Feature selection for off-line recognition of different size signatures”; 4-6 Sept. 2002 Page(s):355 - 364

[10] Papamarkos, N.; Baltzakis, H.; “Off-line signature verification using multiple neural network classification structures”; Volume 2, 2-4 July 1997 Page(s):727 - 730 vol.2

[11] Tong Qu; El Saddik, A.; Adler, A.; “A stroke based algorithm for dynamic signature verification”; Volume 1, 2-5 May 2004 Page(s):461 - 464 Vol.1.