Biometric Handwritten Signature Recognition

Syed Faraz Ali Zaidi Shahzaan Mohammed
Email: {syeza930, shamo291}@student.liu.se
Supervisor: Viiveke Fåk, viiveke@isy.liu.se
TDDD17: Information Security Course
Linköpings universitet, Sweden

Abstract:

This report is a theoretical study of dynamic handwritten signature parameters that can be considered to improve the biometric lab system at ISY department. In the previous lab we used x, y coordinates and pressure. Previous work was based on frequency distribution of signatures with simple hardware devices like a signing pen and tablet. We are considering some simple parameters like speed, acceleration, pen down time, distance, etc. Based on the literature studies we will discuss how these parameters can be used in the lab environment to improve the performance of biometric handwritten signature.

Keywords: *handwritten signature, dynamic features, signature verification methods.*

Background:

The word biometrics comes from the Greek word bios (life) and metrikos (measure). In general, there are three levels of computer security schemes. The first one relies on something a person carries, such as an ID badge with a photograph or a computer card key. The second relies on something a person knows, such as a password or a code number. The last one relies on something a part of a person's biological makeup or behaviour, such as fingerprint, facial image, or a signature. Biometric verification is defined as a method of uniquely identifying a person by analysing one or more of his/her biological traits. Biometrics is basically of two categories, physical and behavioural.
The physical biometrics makes use of the characteristics of the human body like the eye retina scans, facial features, fingerprints, hand geometry, earlobe geometry and DNA, while the behavioural characteristics include 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, including all the hardware and associated software and interconnecting infrastructure, enabling identification by matching a live sample to a stored pattern in a database. Multi-modal biometrics refers to the combination of two or more biometric modalities into a single system. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when features of different biometrics are statistically independent.

Handwritten signatures Overview:

The basic goal of the handwritten signatures is to provide an accurate method in order to verify a person's identity based on the way in which he/she signs his/her name. Hence for this reason, the handwritten signatures are widely accepted, socially and legally throughout the world. There are basically two types of systems – online and offline. The hand-written signature verification uses the features conveyed by every signatory such that the features considered have a unique understanding and the way of signing presents the behavioural biostatistics. Some researchers considered common issues with the extraction of identification data from different biometric types, and protection of such data against conceivable attacks. Handwritten signatures are very much dependant on the user's psychology and has great difference in different surroundings and time.

Applications:

This technology has reached far enough and is being implemented in several organizations and sectors such as in banking, insurance, government, education, retail and in the automotive industry. A specific Signature LCD tablet named Sign Pad was exhibited in the US at BAI Retail Delivery Show 2007. The tablet has the capability to capture all distinct behavioural characteristics of an individual's signature including shape, speed, stroke, pen pressure, and timing information. Their current products include a suite to secure electronic documents (Sign Doc) in different formats and a software development kit (Sign Ware) for the integration of the software application into third-party applications [8]

Dynamic features of biometrics can be used in the following applications:

Finance: IT-Processing centres of German savings banks are offering their customers solutions to embed dynamic signatures securely into electronic documents in an Adobe Live Cycle environment.

Insurance: Signing an insurance contract and documenting the consulting process that is required by EU legislation from July 1st 2007 onwards are triggers for several insurance companies to go paperless with either signature capturing tablets connected to a notebook or a tablet PC.

Real Estate: Increasingly popular among real estate agents in USA, there are options of paperless contracting through signing on Tablet PCs.

Health: The hospital of Ingolstadt is capturing and verifying the signatures of their doctors that fill electronic patient records on tablet PCs. The "National Health Service" organization in the United Kingdom has started such an implementation.

Telecom: Signing phone and DSL contracts in the telecom shops is another emerging market.

Forgeries and its types:

There are three types of forgeries:

1. Random Forgery - In random forgery, the person doesn't have the shape of the original signature. The signer uses the name of the victim in his own style to create a forgery known as the simple forgery or random forgery.
2. Unskilled Forgery - The signer initiates the signature in his own style without any knowledge of the spelling and does not have any prior experience.
3. Skilled Forgery - undoubtedly professional impostors or persons who have experience in copying the signature create the most difficult of all forgeries.

Stages of verification: [3]

Most HSV (Handwritten signature verification) techniques use the following six-step procedure for performance evaluation:

1. Registration: This involves capturing of a few signatures for each individual at enrolment or registration time (these signatures are called sample signatures).

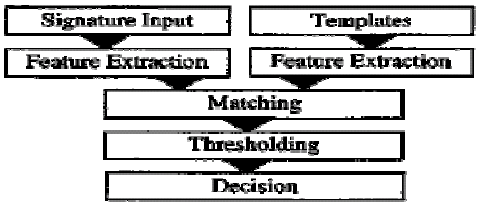
2. Pre-processing and building reference signature(s): This involves the deletion of virtual pen-up strokes from the raw signatures. The main reason of virtual pen-up is not keeping enough pressure of the pen all through the signing process. When the pressure of the pen point is less than minimum pressure which the tablet can detect, it causes virtual pen-up. Usually the pressure is high when there is straight virtual pen up or turning virtual pen up. The required features are computed and one or more reference signatures are produced. Then the parameters are decided on which the threshold is calculated.

3. Test signature: When a user wishes to be authenticated, he/she presents a signature (we call this signature the test signature). The features of this test signature are computed as usual.

4. Comparison processing: The test signature is then compared with the reference signature(s) based on feature or feature set values and the difference between the two is then computed using one of the distance or time measurements.

5. Performance evaluation: For each signature that claims to be a genuine one, we compare the distance or time computed with the threshold decided in Step 2 above. If the difference between the two is smaller, accept the signature otherwise reject it.

6. Steps 3–5 are then repeated for the given set of genuine signatures and forged ones; false rejection and false acceptance rates are then computed.



Verification methods:

There are several verification methods for the online and offline signature verification which most of the companies use nowadays. Online and offline signature verification methods are denoted by ONSV and OFSV respectively. Online systems use the dynamic features of a handwritten signature considering the time and frequency factors which involves signal processing techniques like the normalization, Fourier transforms and correlation functions for the proper analysis of the handwritten signatures. However on the other hand the offline signatures use the static features of the system which involves image processing techniques to analyse the accuracy of the signatures. These include the initial identification of a person through the password. There are other multimodal systems that use the two different biometric features in order to strictly authenticate a person's identity.

Offline Signature Verification Methods:

Template Matching methods and Hidden Markov model techniques are based on structure and features.

- A-template matching using warping:

The warping method warps one curve onto an other curve in such a way that the original shape is maintained. In this method the coordinates of the exterior curves that lie in the template signature and the test signature, are matched. The method is also known as elastic matching.

- Hidden Markov model:

In HMM stochastic matching (model and the signature) is involved. This matching is done by steps of probability distribution of features involved in the signatures or the probability of how the original signature is calculated. If the results show a higher probability than the test signatures probability, then the signatures are by the original person, otherwise the signatures are rejected.

- Structural techniques:

Features regarding the direction and the transition distance come under the account of the structural features. Boundary representation of an object transition can be shown for pixels from background to foreground in both the vertical and horizontal directions. In the object boundary, stroke direction, where transition occurs, can be defined as direction of transition. [2]

Online Signature Verification Methods:

Online methods of verification are divided into four approaches. [11]

- Global parametric feature based approach - All the available values are not used. Instead, a number of global values, called statistical features or parameters like time, distance, pen up and pen down times, are computed and compared.

- Function based approach - all the collected position (or velocity or acceleration) values of the test and reference signatures are compared point-to-point, perhaps by computing a set of correlation coefficients between the two signatures. Such comparison may require signature segmentation and comparison of corresponding segments may require alignment.

- Hybrid method for both feature based and function based approaches and

- Trajectory Construction metods.

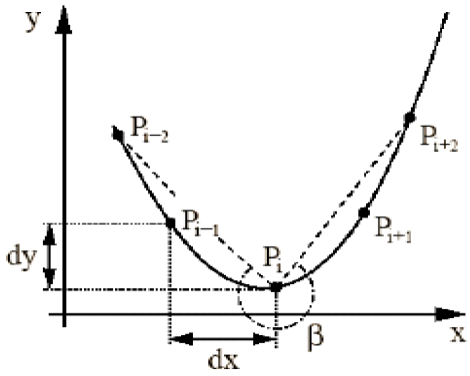
Feature Extraction:

The feature extraction is the key step in the recognizing of the on-line hand-written signatures. According to the coordinates, curvatures and the recorded time information, a series of biological features of the signatures are usually obtained for such systems. The systems extract the features like time, length of strokes and speed and then obtain a resultant function using the Gauss function to calculate the probability density through other density functions also. During the estimation, the system obtains the corresponding averages, variances and standard deviations which will be the unique features for the signatures. There are other methods of feature extraction in offline systems in which the pre-processed image is divided into portions using the equal horizontal density method in which the image is scanned horizontally from left to right and then from right to left and the total number of dark pixels is obtained over the entire image.

Simple features selected as an improvement over previous features.

- D : Total distance of the pen travelled on the hand-written signature the Euclid distance of all the points:

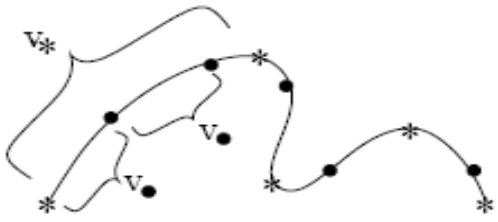
$$D = \sum \{(x_i - x_{i+1})^2 + (y_i - y_{i+1})^2\}^{1/2}, i=0, 1, \cdots, N-1$$



xi is the coordinate in direction x and yi is the coordinate in direction y;

Speed vx and vy express the functions of time, which can be calculated with the following formulae：

$$\begin{cases} v_{x_m} = (x_{m+1} - x_m)/(t_{m+1} - t_m) \\ v_{y_m} = (y_{m+1} - y_m)/(t_{m+1} - t_m) \end{cases}$$



where m is the serial number, m=0, 1, …, N−1; xm is the coordinate in direction x; ym is the coordinate in direction y; tm is the time of movement; vx is the speed at point tm in direction x; vy is the speed at point tm in direction y.
Acceleration ax and ay can be calculated with different speeds, the acceleration at point tm in directions x and y can be expressed in the following formulae:

$$\begin{cases} a_{x_m} = (v_{x_{m+1}} - v_{x_m})/(t_{m+1} - t_m) \\ a_{y_m} = (v_{y_{m+1}} - v_{y_m})/(t_{m+1} - t_m) \end{cases}$$

Most signatures take between 2 and 10 seconds with an average time of *5* seconds (slightly longer times for forgeries). Previous studies say that the average amount of time for a genuine signature is usually 3 to *6* seconds and for a forged was 10 to 11 seconds.

- T_k , total time of the hand-written signature;

The total time, the length of the strokes, the time for lifting the pen can be different for the same user's different signatures. These features oscillate about the average and variance which can symbolize one person's biometric features.

There are two time-related features: the first is the total signature time *T*. The second is the time down ratio *Tdr*, which is the ratio of pen-down time to total time.

Total Signature time $T = t_K - t_1$
Pen-down time ratio $T_{dr} = t_d / T$

k = 1,2..., K data points for a given signature.

- Length-to-width ratio $L_w = V_m\ T_d / X_w$

V_m, X_m, $Y_{m,\ are}$ the means of v; x; and y respectively
$X_w = \max(x) - \min(x)$

The other features that can be implemented are:

- *Nvx and Nvy* , amount of zero speed in direction *x and y directions*;
- *Nax* and *Nay* amount of zero acceleration in direction *x and y directions.*

Different Approaches with different parameters:

I. "Cornell - Reliable On-line Human Signature Verification Systems" researches experiment with 49 features of the handwritten signature: [4]
15 static off-line features (considering the x and y coordinates):

- Maximum distance between the highest and lowest points.
- Signature length.
- standard deviation of x / change in x, y/change in y
- ((x|y)(min|max)-(x|y)(0|end))/change in (x|y)
- initial direction

35 dynamic features (considering the velocity and time):

- Maximum Forward Velocity
- Signature Maximum Velocity occurrence coordinates with respect to time.
- First Time Instance of v = 0
- Average Velocity over x and over y
- Average Writing speed
- Number of pen ups and downs
- Time of second pen down
- Direction at first pen down, first pen up
- Total cordinates recorded
- Duration of negative x and y velocities
- Duration of positive x and y velocities.

With 1% false rejection, there is a 20% false acceptance error. This error is when using the best 15 features out of the 49 feature set.

II. "Hidden Markov Model approach to online handwritten signature verification" research considered 21 features of online handwritten signatures. In this there was an equal error rate (EER) of 2.5%, at 1% false rejection, error rate is 5%.

- Total Signing Time.
- Pen down time.
- Root Mean Square speed.
- Average Horizontal speed.
- Integrated Absolute Centripetal. Acceleration.
- Length to Width ratio.
- Horizontal Span ratio.
- 8 directional histograms.
- 4 directional change histograms.
- x, y Speed Correlation.
- First Moment.

False Acceptance / False Rejection Rates and Equal Error Rates:

By considering the adhoc parameters like speed, acceleration and pen downs, a simple system can be improved. The improvement that we are referring in the biometric handwritten system is to minimize the rate of false acceptance and false rejection. The Equal Error Rate (EER) corresponds to the error value for which FAR is equal to FRR. These rates determine the quality of an authentication system, but the acceptable values depend on the level of security desired for a specific application.
Many algorithms can be applied to parameters and be calculated in mathematical way. The first step is to obtain the sample signature from the users through the signing pad or tablet. We can extract many features from the signing tablet such as the pressure, time, distances, pen ups, pen downs, velocity etc.

Figure 2 above shows that the signature consist of sample points. The length of the signature is directly proportional to the time of signature. The pen up symbols is shown in black.

Result:

Our study shows that the biometric handwritten signature verification methods can be improved by simple methods. This improvement is possible by adding some adhoc and simple parameters that we have discussed earlier in our report. Experiments are performed by taking a set of global and local parameters altogether. Many algorithms are also applied to the parameters and can be calculated in a mathematical way. In dynamic processing, run time feature extraction is involved and the features are extracted as discussed above. After comparing and analysing the related work in our report, we conclude that global parameters like total distance, total time, total speed in x direction and y direction are more easily calculated than the local parameters. This is because feature extraction is more complex and time consuming in local parameters.

References:

1. Ma Mingming,W.Sardha Wijesoma,Eric Sung, "An Automatic On-line Signature Verification System Based on Three Models", in Proc. Canadian Conf on Electrical and Computer Engineering, vol 2,pp 890-894,May2000

2. Vu Nguyen, Michael Blumenstein, Vallipuram Muthukkumarasamy ,Graham Leedham, "Off-line signature verification using enhanced modified direction features in conjunction with neural classifiers and support vector machines", in Proc. Int Conf of Pattern Recognition , vol 4 , pp. 509 – 512 , 2006.

3.Hand written signature verification methods K R Radhika, M K Venkatesha and G N Sekhar rkr.ise@bmsce.ac.in, principal_rnsit@yahoo.com, hod.maths@bmsce.ac.in.

4. A brief survey of Approaches to Signature Verification. David Feil-Seifer and Benjamin B. Kimia

5. Online Handwritten Signature Verification Using Hidden Markov Models
Juan J. Igarza, Iñaki Goirizelaia, Koldo Espinosa, Inmaculada Hernáez, Raúl Méndez, and Jon Sánchez Department of Electronics and Telecommunications. University of the Basque Country, Alameda Urquijo, s/n 48013 Bilbao, Spain {jtpigugj, jtpgoori, jtpesacj}@bi.ehu.es {inma, raul, ion}@bips00.bi.ehu.es

6. Improved Offline Signature Verification Scheme Using Feature Point Extraction Method
Debasish Jena1, Banshidhar Majhi2, Saroj Kumar Panigrahy3, Sanjay Kumar Jena4 1Centre for IT Education, Bhubaneswar, 751010, Orissa, India 2, 4National Institute of Technology Rourkela, 769008, Orissa, India 3Roland Institute of Technology, Berhampur, 761008, Orissa, India

7. Authentication based on feature of hand-written signature ZHU Shu-ren
(1. School of Information Science, Guangdong University of Business Studies, Guangzhou 510320，China; 2. School of Computer, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

8. The usage of handwritten dynamic (biometric) signatures in the digital world - and its implications
Signature Verification and Fraud Detection Detection Solution Specialist Softpro outlines the status of Dynamic Signature Verification at BAI Retail Delivery Conference in Las Vegas http://www.findbiometrics.com/article/468.

9. Signature Verification and Forgery Detection System
Mohd Hafizuddin Mohd Yusof' and Vamsi Krishna Madasu' 'Faculty of Information Technology, Multimedia University, *63* 100 Cyberjaya, Selangor, Malaysia 'School of Infosation TechnoIogy and Electrical Eng., University of Queensland, Brisbane, QLD 4072, Australia.

10. Chinese Handwriting Signature Authentication using the Data mining techniques.CHENG-JIANG WANG, DI DAI ,China Three Gorges Univ., Yichang 443002, China.

11. Using position extrema points to capture shape in on-line handwritten signature verification
G.K. Guptaa,∗, R.C. Joyceb, aFaculty of Information Technology, Monash University, Clayton, Victoria 3800, Australia, bOutsource Laboratories, Eatontown, NJ 07724-1878, USA.