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

Abstract. Most people are used to signing documents and because of this, it is a trusted and natural method for user identity verification, reducing the cost of password maintenance and decreasing the risk of eBusiness fraud. In the proposed system, identity is securely verified and an authentic electronic signature is created using biometric dynamic signature verification. Shape, speed, stroke order, off-tablet motion, pen pressure and timing information are captured and analyzed during the real-time act of signing the handwritten signature. The captured values are unique to an individual and virtually impossible to duplicate. This paper presents a research of various HMM based techniques for signature verification. Different topologies are compared in order to obtain an optimized high performance signature verification system and signal normalization preprocessing makes the system robust with respect to writer variability.

1 Introduction

Day by day, natural and secure access to interconnected systems is becoming more and more important. It is also necessary verifying people identity in a fast, easy to use and user-friendly way.

Traditionally, during the process of identification and controlling the access to systems or applications, we used objects, e.g. keys or smart cards, or we used knowledge based systems like PINs, or passwords. However, objects may be lost and knowledge may be forgotten and both may be stolen or copied.

Biometrics [1] relies on several personal and unique body features (e.g. fingerprints, iris or the retina) and individual behavior features (e.g. the way of speaking, writing, signing or walking). Those individual features, either physical or behavioral, allow identifying each individual univocally offering a solution for the conventional security problem. Because of this, biometric solutions are considered one of the most

A. Sanfeliu and J. Ruiz-Shulcloper (Eds.): CIARP 2003, LNCS 2905, pp. 391–399, 2003.

trusted and natural ways of identifying a person and controlling access to systems and applications.

Normally, most citizens are not confident on biometric identification systems based on body features like fingerprints, iris o retina, because they feel these systems to be related to criminals and police issues. However, those features related to our behavior are accepted even though they are much less precise.

Research groups of four Spanish universities joined in the research project [2] called *"Aplicación de la Identificación de Personas mediante Multimodalidad Biométrica en Entornos de Seguridad y Acceso Natural a Servicios de Información"*. The first result from this project was the creation of a Multimodal Biometric Database [3] (fingerprints, signatures and voice) which is the starting point for the rest of the research of each participating group. This paper is a result of the subsequent research on handwritten signature using that database.

Section 2 is an introduction to signature verification, section 3 is dedicated to the description of the system, section 4 to the produced results and finally, in section 5 the conclusions are explained.

2 Signature Verification

Handwritten signature is commonly used and accepted as a way to verify people's identity; we usually sign documents to verify their contents or to authenticate financial transactions. Signature verification usually consists just of an "eye inspection" as if we compared two photographs, but this is not an efficient method against impostors and many times there is no verification process at all.

The automation of the verification process tries to improve the current situation and eliminate the eBusiness fraud. Automatic signature verification is divided into two main areas, depending on the way the data are acquired: In *off-line* signature verification, the signature is available in a handwritten document which is scanned to obtain the digital representation of the image. On the other hand, in *on-line* signature verification specific hardware is used (digitizing tablets) to register pen movements on the paper during the act of signing.

Off-line verification is used with signatures from past documents, not acquired in a digital format, and only the shape of the signature remains important. However, in on-line verification, we also use dynamic information of the signature, such as pen pressure or inclination, apart from the 2D spatial representation. The presence of the individual at the time of the digital capture is also required.

3 System Description

3.1 Online Signature Acquisition Module

Our system uses a graphics tablet from Wacom as capturing device. More precisely it is the Intuos A6 model with USB interface. This tablet provides 100 samples per second containing values for pressure and the four degrees of freedom: X and Y coordinates, pen azimuth and inclination for every sample.

Strokes with no pressure, also known as *pen-ups,* are also sampled, and because of this the system is able to know the trajectory with ink and inkless, which means that we have extra information, making the system more robust.

The signature information, once digitized, is stored in a file as a matrix, and afterwards it may be used to create a new input in the database or as a test signature for the verification process.

Fig. 1. The digitized signature consists of a sequence of sample points along the signature, captured with a frequency fixed by the acquisition device. Its length is directly proportional to the time of signing, in this example 9.4s. *Pen-up* symbols occur during the time in black.

3.2 Online Signature Database

The system uses a database, in which each individual has 25 true signatures. At the same time, each individual makes 5 forgeries of every of his/her 5 immediately previous entries in the database. This means that for every individual we have 25 true signatures and 25 forgeries made by 5 different people.

Data from 150 individuals were used in the research presented in this paper, i.e. 3.750 files of true signatures and the same number of forgeries.

The forgeries in the database are *skilled forgeries*, as the impostor tries several times to imitate the true user's signature before the forgery is acquired and finally stored in the database. Trying to improve the quality of the forgeries we encouraged the participants to do their best offering them a prize.

3.3 Signature Preprocessing

Every time we sign, we do it in a different way. Because of this, some factors like speed variation, different sizes or rotations or different places within the tablet have to be taken into account in order to get a representation of the signature independent from these factors.

The preprocessing module makes a time normalization so that the resulting signatures have the same length or number of samples. To do this, a process of interpolation or extrapolation is done depending on the number of samples of the original signature. This normalization is user-defined as the user can decide to keep the original size.

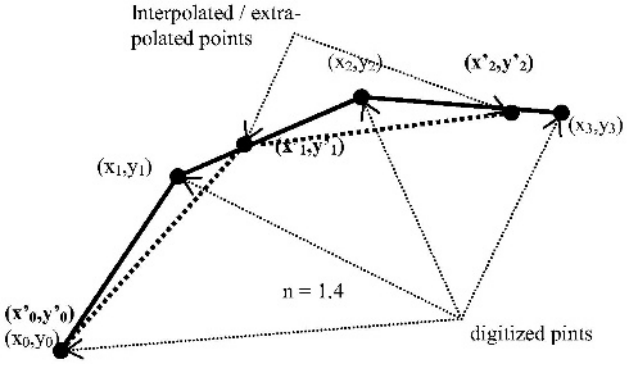

Fig. 2. Time normalization algorithm. In the example, n = 1.4 represents the ratio between the original size of the signature (420 samples) and the normalized one (300 points). The acquired points are represented as (x_j,y_j), with j from 0 to 420, and the normalized points are (x'_i,y'_i), with i from 0 to 300.

Coordinates after normalization are calculated following this algorithm:

$$(x'_i, y'_i) = (a * x_j + b * x_{j+1}, a * y_j + b * y_{j+1}) \quad (1)$$

$$\text{with:} \begin{vmatrix} j = \text{floor}\,(i * n) \\ b = (i * n) - j \\ a = 1 - b \end{vmatrix}$$

Yang, Widjaja and Pradsad's method [4] consists of an algorithm that eliminates size variability (X-Y coordinates) and rotations with respect to the tablet. These authors use the absolute value of the angle corresponding to the segment that ties two consecutive normalized points, using the formula below:

$$\phi(k) = \arctan\left[\frac{\sum_{l=i+1}^{i+n} s_l^{(k)} \sin \theta'^{(k)}_l}{\sum_{l=i+1}^{i+n} s_l^{(k)} \cos \theta'^{(k)}_l}\right] \tag{2}$$

with $\theta'^{(k)}_l = \theta_l^{(k)} - \theta_1$, where θ_1 is the absolute angle of the first segment and $s_l^{(k)}$ is the length of the segment between two consecutive points. This formula normalizes the signature and subtracts the absolute value of the first segment at the same time.

To improve the computational efficiency of this algorithm we propose some modifications to the Yang's original formula, adapting it to the algorithm represented in the figure 2. Developing $\sin(\theta_l^{(k)} - \theta_1)$ and $\cos(\theta_l^{(k)} - \theta_1)$ trigonometric expressions and as $\Delta y_l^{(k)} = s_l^{(k)} \sin\theta_l^{(k)}$ and $\Delta x_l^{(k)} = s_l^{(k)} \cos\theta_l^{(k)}$, Yang, Widjaja and Prasad's formula (2) takes this new appearance:

$$\phi(k) = \arctan\left[\frac{\left(y_{i+n}^{(k)} - y_i^{(k)}\right)\cos\theta_1 - \left(x_{i+n}^{(k)} - x_i^{(k)}\right)\sin\theta_1}{\left(x_{i+n}^{(k)} - x_i^{(k)}\right)\cos\theta_1 + \left(y_{i+n}^{(k)} - y_i^{(k)}\right)\sin\theta_1}\right] \tag{3}$$

Although this formula seems much more complex, it is more efficient, as $\cos\theta_1$ and $\sin\theta_1$ are only computed once, because they are constant values for all the samples along the signature. Besides, if we apply this algorithm to the normalized length the final result is as follows:

$$\phi(i) = \arctan\left[\frac{\left(y'_{i+1} - y'_i\right)\cos\theta_1 - \left(x'_{i+1} - x'_i\right)\sin\theta_1}{\left(x'_{i+1} - x'_i\right)\cos\theta_1 + \left(y'_{i+1} - y'_i\right)\sin\theta_1}\right] \tag{4}$$

3.4 Model Training

Training a verification system consists of generating a model of the item that we want to verify using a set of observations of it. Models are initialized using the first 5 original signatures of each signer and reestimated using 4 more signatures. Afterwards they are stored in a database.

The set of observations used to generate the model must show the natural variation of the user's signature and the efficiency of these systems depends strongly on how representative these observations are of the user's signature during the creation of the database.

3.5 Verification and Threshold Selection

To verify whether the signer is a true user or an impostor we calculate the similarity between its signature and the trained model. Then we compare this value to the threshold selected to determine if we accept the signature or we reject it.

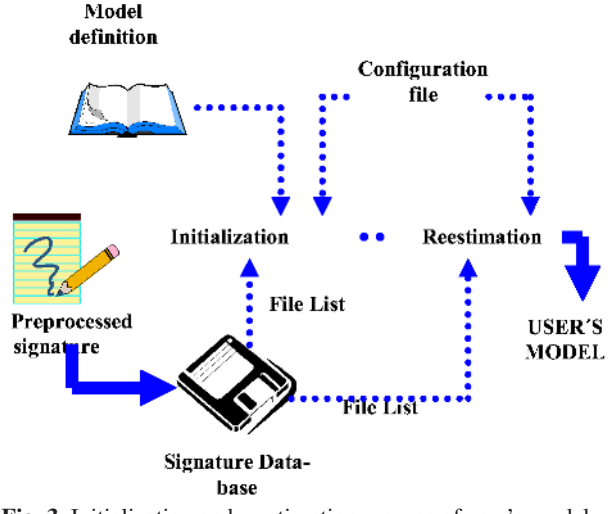

Fig. 3. Initialization and reestimation process of user's model.

Defining this threshold, we have to take into account the security level we need for our application, this is, if we need a low FAR (*False Acceptance Rate*) or a low FRR (*False Reject Rate*) as reducing one of this values means increasing the other. Normally, a security system should guarantee a FAR close to zero, but this means a higher FRR, because they are inversely proportional.

To check how accurate this algorithm is, we studied the DET plots (*Detection Error Tradeoff*) for all the users, defining the minimum cost point as follows:

$$DCF = Cmiss * Pmiss \mid True * Ptrue + Cfa * Pfa \mid False * Pfalse \quad (5)$$

where Cmiss and Pmiss are respectively the cost and probability of a false reject, Cfa and Pfa the cost and probability of a false acceptance, Ptrue is the a priori probability of the target and Pfalse is 1-Ptrue. This function will be evaluated for every point along the DET plot, finding the point where the function takes the minimum value. This point defines the threshold for which the accuracy of the algorithm is optimum. Another reference point is the EER point (*Equal Error Rate*) where FAR and FRR are the same.

These plots have been calculated using the free software of NIST [5]. These programs dynamically change the reject threshold and calculate the FAR and the FRR for different situations. The more collaborative the user is the lower FRR we'll get. His/her DET plot will be closer to the axis and the EER will be lower too.

4 Developed Models

In our first models, signatures were described using the directional normalized angle along the trajectory of the signature (equation (4)). An important part of this study was the definition of the number of states, the number of symbols, the transition matrix, and the initial probability of the distribution of the states, i.e. the topology of the models.

We made some tests to determine which topology of the HMMs [6] showed the best efficiency, these tests were made with signatures normalized to 300 samples and quantified with 32 symbols. We verified that 6-state L-R (*left-right*) models were more efficient than other L-R models. The worst results were obtained using ergodic or generalized models, those in which transitions between all the states are allowed.

Having defined the architecture of our models, we tested the application's accuracy for different normalized lengths. We normalized all the signatures to 100, 200, 300, 400, 500, 600 samples and also we used non-normalized signatures (keeping their original size) and found that the algorithm was more accurate using values between 300 and 500. These values are clearly related to the average signatures duration of about 3 seconds.

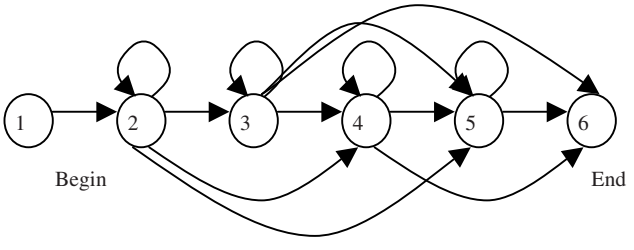

Fig. 4. 6-state HMM L-R topology

4.1 Verification Results

We studied the performance of the system working in verification mode, i.e. validating a person's identity comparing the captured signature with the individual's template, which is stored in the system database. Table 1 shows the initial results.

Table 1. Initial results using Yang, Widjaja and Prasad's preprocessing, which only includes angles. Although the FAR is close to 0, the false reject rate is nearly 50%, which means that an average user should sign twice to gain access to the system.

	FAR	FRR	EER
Mean value	0,295%	48,21%	17,565%

To set the optimum working point, we calculated the minimum cost point with NIST functions, favoring a very low FAR weighted 10 to 1, at expense of a high FRR.

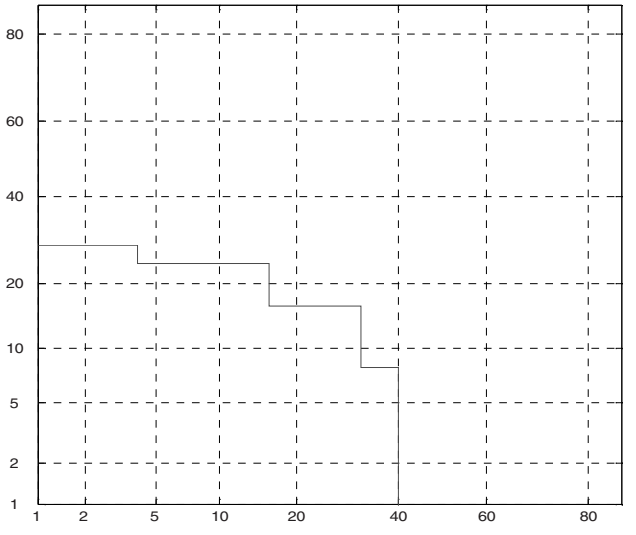

Fig. 5. DET (Detection Error Tradeoff) plot for user No.208, with FAR and FRR as X and Y axis. EER is quite similar to the mean value shown in table 1 and FRR is slightly better.

In the next tests we eliminated the first angle subtraction proposed by Yang, Widjaja and Prasad because we believe that the database creation methodology (users signed inside a grid) made it unnecessary. The new results showed that the ERR was halved by eliminating this subtraction, implying that it introduced a noise harmful to the verification process. Finally, our system was trained including pressure, azimuth and inclination.

Table 2. Results with the new preprocessing method including angles, pressure, azimuth and inclination

	FAR	FRR	EER
Mean value	0,00%	31,52%	9,253%

Introducing these additional parameters results in a remarkable improvement of the algorithm efficiency.

5 Conclusions

The first angle subtraction proposed by Yang, Widjaja and Prasad is unnecessary in our system because users sign all inside a grid and it introduces a noise harmful to the verification process. For a system in which users are not asked to sign inside a grid, we propose to subtract the angle of the principal axis of inertia of the signature, as it is a more stable value than the first angle.

Adding additional parameters such as speed, acceleration, mass center, inertia axis, linear and circular segments length [7], curvature radii, etc. would result in a large EER improvement of the system, satisfying commercial requirements.

Multimodal fusion of several biometric methods (fingerprints, voice, signature, etc.) is another way to improve the efficiency of the verification. In the same way, we could talk about intramodal fusion, combining several verification methods based on the same biometric feature. Fusion of on-line and off-line signature methods can make the system more robust and efficient.

References

1. S. Prabhakar, S. Pankanti, A. Jain “Biometric Recognition: Security and Privacy concerns” IEEE Security and Privacy. March/April 2003. pp. 33–42
2. Site of the Project TIC2000-1669-C04-03 [Online] http://www.infor.uva.es/biometria
3. J. Ortega, D. Simón, M. Faúndez, V. Espinosa, I. Hernáez, J.J. Igarza, C. Vivaracho, Q.I. Moro. “MCYT: A Multimodal Biometric Database” COST275-The Advent of Biometrics on the Internet. Rome, 2002. pp. 123–126
4. L.Yang, B.K.Widjaja, R. Prasad. ”Application of Hidden Markov Models for Signature Verification”. Pattern Recognition, 28(2). 1995. pp. 161–170
5. National Institute of Standards and Technology. [Online] Available http://www.nist.gov
6. L.R. Rabiner, B.H. Juang “An Introduction to Hidden Markov Models”, IEEE ASSP Magazine, January 1986. pp. 4–16
7. I. Goiricelaya, J.J. Igarza, J.J. Uncilla, F. Pérez, J. Romo, K. Espinosa “Modelización de Contornos Mediante la Búsqueda de Segmentos Lineales y Circulares en Imágenes de Nivel de Gris” XII Simposium Nacional de la Unión Científica Internacional de Radio, Bilbao September 97. pp 1203–1206