Biometric Authentication using Online Signatures

Alisher Kholmatov and Berrin Yanikoglu
alisher@su.sabanciuniv.edu, berrin@sabanciuniv.edu
http://fens.sabanciuniv.edu

Sabanci University, Tuzla, Istanbul, Turkey 34956

Abstract. We overview biometric authentication and present a system for on-line signature verification, approaching the problem as a two-class pattern recognition problem. During enrollment, reference signatures are collected from each registered user and cross aligned to extract statistics about that user's signature. A test signature's authenticity is established by first aligning it with each reference signature for the claimed user. The signature is then classified as genuine or forgery, according to the alignment scores which are normalized by reference statistics, using standard pattern classification techniques. We experimented with the Bayes classifier on the original data, as well as a linear classifier used in conjunction with Principal Component Analysis (PCA). The classifier using PCA resulted in a 1.4% error rate for a data set of 94 people and 495 signatures (genuine signatures and skilled forgeries).

1 Introduction

Biometrics is the general term to refer to the utilization of physiological characteristics (e.g. face, iris, fingerprint) or behavioral traits (e.g. signature, keystroke dynamics) for verifying the identity of an individual. Authentication actually refers to two separate problems: identification and verification. In identification, Biometric authentication is gaining increasing popularity as a more trustable alternative to password or key based security systems. Signature is a behavioral biometric: it is not based on the physical properties, such as fingerprint or face, of the individual, but behavioral ones.

Signature verification is split into two according to the available data in the input. Offline (static) signature verification takes as input the image of a signature and is useful in automatic verification of signatures found on bank checks and documents. Online (dynamic) signature verification uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number and order of the strokes, the overall speed of the signature, the pen pressure at each point etc. and make the signature more unique and more difficult to forge. As a result, online signature verification is more reliable than offline signature verification. Application areas of online signature verification include protection of small personal devices (e.g. PDA, laptop); authorization of computer users for accessing sensitive data or programs; and authentication of individuals for access to physical devices or buildings.

As a behavioral biometric, signature is not as unique or difficult to forge as iris patterns or fingerprints, however signature's widespread acceptance by the public, make it more suitable for certain lower-security authentication applications, as well as certain applications where online signatures can be the most suitable biometric (e.g. online banking and in credit card purchases). Furhermore, one's signature may change over time; yet, a person signs his/her signature rather uniquely at any given time period and forgeries can be identified by human experts quite well.

In an online or offline signature verification system, users are first enrolled by providing signature samples (reference signatures). Then, when a user presents a signature (test signature) claiming to be a particular individual, this test signature is compared with the reference signatures for that individual. If the dissimilarity is above a certain threshold, the user is rejected, otherwise authenticated.

In evaluating the performance of a signature verification system, there are two important factors: the false rejection rate (FRR) and the false acceptance rate (FAR). As these are inversely related, decreasing the FRR results in an increase in the FAR. When a single figure is needed, the Equal Error Rate (EER), where FAR equals FRR, is often reported.

Since obtaining actual forgeries is difficult, two forgery types have been defined in signature verification papers: A *skilled* forgery is signed by a person who has had access to a genuine signature for practice. A *random* or *zero-effort forgery* is signed without having any information about the signature, or even the name, of the person whose signature is forged.

In the verification process, the test signature is compared to all the signatures in the reference set, resulting in several dissimilarity/distance values. One then has to choose a method to combine these distance values so as to represent the dissimilarity of the test signature to the reference set in a single number, and compare it to a threshold to make a decision. The single dissimilarity value can be obtained from the minimum, maximum or the average of all the distance values. Typically, a verification system chooses one of these approaches and discards the other ones. For instance, Jain et al. report the lowest error rates with the minimum distance criterion, among the other three [1]. We use all three in deciding whether the signature is genuine or not, instead of choosing which distance is most useful for the task.

These distance values, normalized by the corresponding average values of the reference set, are used as the features of a signature in its classification as genuine or forgery, as explained in Section 3.

2 Previous Work

A comprehensive survey of signature verification can be found in [2, 3]. Most commonly used on-line signature acquisition devices are pressure sensitive tablets with or without LCD screens, together with smart pens capable of measuring forces at the pen-tip exerted in three directions. More than 40 different feature types have been used for signature verification [1, 4, 5]. Features can be classified in two types: global and local. Global features are features related to the signature as a whole, for instance the signing speed, signature bounding box, and Fourier descriptors of the signature's trajectory. Local features correspond to a specific sample point along the trajectory of the signature. Examples of local features include distance and curvature change between successive points on the signature trajectory. In Jain et al. [1], some of these features are compared in order to find the more robust ones for signature verification purposes. Other systems have used Genetic Algorithms to find the most useful features [6].

Due to the variability in signing speed, two signatures belonging to the same person may have different trajectory lengths (hence feature vectors of differing lengths). Therefore, the dynamic time warping algorithm with some variant of the Euclidian distance [7, 5, 1, 8] and Hidden Markov models [9] are commonly used in aligning two signatures.

Number of signatures taken during the user enrollment also varies: between 3 and 20 samples are used in previous signature verification systems. The distance of the test signature to the closest reference signature has been found as most useful (giving the lowest error rates) in [1], however other criteria, such as the average distance to the reference signatures or the distance to a template signature are also used. Template generation is generally accomplished by simply selecting one or more of the sample signatures as templates [5, 10].

Various thresholds can be used in deciding whether the distance between the test signature and the reference and/or template signatures are acceptable. Two types of threshold selections are reported: writer dependent and writer independent thresholds [1]. In writer dependent scenario, thresholds are calculated for each user individually, whereas in writer independent one, a global threshold for all the writers is set empirically during the training phase of the system.

State of the art performance of the available on-line signature verification algorithms lies between 1% and 10% equal error rate.

3 Proposed Method

During the enrollment phase, the user supplies a set of reference signatures which are used to determine user dependent parameters characterizing the variance within the reference signatures. The reference set of signatures, together with these parameters, are stored with a unique user identifier in the system's database.

When a test signature is input to the system for verification, it is compared to each of the reference signatures of the claimed person. The person is authenticated if the resulting dissimilarity measure is low, rejected otherwise. The details of the system is described in the following sections.

3.1 Data Acquisition

We have used Wacom's Graphire2 pressure sensitive tablet and pen. The tablet is capable of sampling data at 100 samples per second: at each sample point, the x,y coordinates of the signature's trajectory and the time stamp are recorded. Unlike some other tablets, Wacom's pen capture samples only during the interaction of the pen tip with the tablet.

3.2 Feature Extraction

It is important to find features that are invariant with respect to small changes in genuine signatures, yet can be used to discriminate forgeries. We have experimented with the following local features of the points on the signature trajectory: x-y coordinates relative to the first point of signature trajectory, the x and y coordinate differences between two consecutive points(Δ_x, Δ_y), and the curvature differences between consecutive points. The results shown in Section 4 are for the Δ_x, Δ_y features which gave the lowest error rates.

A signature is considered a ballistic movement, and as such, the timing of someone's signature carries important information. For that reason, we have chosen not to do any preprocessing steps (e.g. resampling) in order to preserve the timing information of the signer. During the alignment of the two signatures, a significant difference in the speed and timing of two signatures, even if they have the same shape, results in a high dissimilarity score. This is desired, because the shape information can be easily copied if the forger gets a sample, whereas the timing information is more difficult to imitate (and to observe).

3.3 Signature Alignment

In order to compare two signatures of differing lengths, we use the dynamic time warping algorithm which is a well-known and widely used method for aligning vectors of different lengths. Dynamic time warping algorithm finds the best non-linear alignment of two vectors such that the overall distance between them are minimized.

There are three parameters that needs to be set in the dynamic time warping algorithm. The missing point and spurious point costs, penalizing a missing or extraneous point in one of the signatures, are taken to be equal in our system. The actual value of this parameter is set so that small extra strokes do not cause a large dissimilarity score. When two points are aligned, we use the Euclidian distance between the features of the two points as the alignment cost. However, a threshold is added to this metric to allow for insignificant variation between two signatures, without adding to the cost.

Note that even though the dynamic time warping aligns signatures in differing lengths, the timing information that we intended to keep by not resampling is not lost: the speed difference between two signatures causes spurious points, adding to the total matching cost.

3.4 Enrollment

During enrollment to the system, the user supplies a number of signatures (eight in our system). Supplied signatures are pairwise aligned to find the distance between each pair, as described in section 3.3.

From these alignment scores, the following reference set statistics are calculated: (i) average distance to nearest neighbor, $\overline{d}_{min}$ (ii) average distance to farthest signature, $\overline{d}_{max}$ (iv) average distance to the *template signature*, X_T, which is the signature with minimum average distance to all other supplied signatures, $\overline{d}_{tmp}$. These are illustrated in Fig. 1.

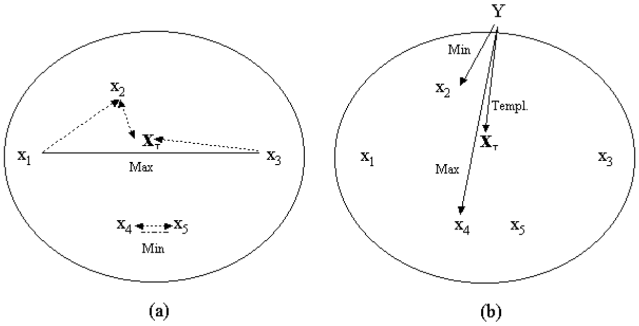

Fig. 1. a)Calculation of the reference set statistics b) Calculation of the test signature Y's distances to the reference set

3.5 Training

A training data set consisting of 76 genuine signatures and 54 forgery signatures is collected in order to learn the threshold parameter separating the forgery and genuine classes. These signatures are separate from the signatures collected as reference signatures.

First, each training signature is compared to the reference set of signatures it claimed to belong, using the Dynamic Time Warping algorithm described in Section 3.3, giving a 3-dimensional feature vector (d_{min}, d_{max}, d_{tmp}). The feature values are then normalized by the corresponding averages of the reference set ($\overline{d}_{min}$, $\overline{d}_{max}$, $\overline{d}_{tmp}$) to give the distribution of the feature set shown in Fig. 2. The distribution of this normalized data supports that genuine and forgery samples in the training set are well separated with these normalized features. Note that by normalizing the measured distance vectors by the corresponding reference set averages, we eliminate the need for user-dependent thresholds commonly used in deciding whether a signature is similar enough to the reference set.

Finally, we train a classifier to separate the genuine and forgery samples in this normalized feature space. For this work, we trained two classifiers: the Bayes classifier using the 3-dimensional feature vectors assuming independent covariance matrices and a linear classifier used in conjunction with the Principal Component Analysis (PCA). As the three features are highly correlated, we could reduce the dimensionality from three to one while keeping most of the variance, using Principal Component Analysis (PCA). Then, a linear classification is made by picking a threshold value separating the two classes within the training set. This threshold is fixed and later used in the verification process. The results are summarized in Section 4.

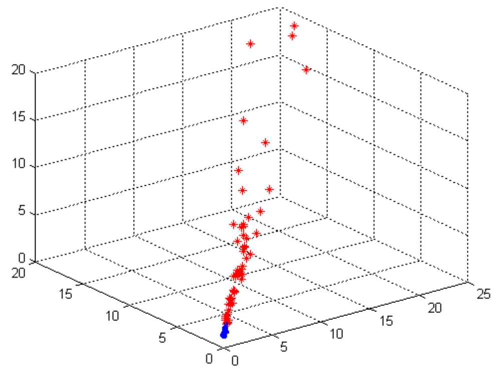

Fig. 2. Plot of genuine (dots) and forgery signatures (stars) with respect to the 3-dimensional normalized distance vector.

3.6 Verification

In order to verify a test signature Y, we first proceed as in the training stage: the signature is compared to all the reference signatures belonging to the claimed ID using the Dynamic Time Warping algorithm described in Section 3.3. Then, the resulting distance values $((d_{min}, d_{max}, d_{tmp})$, normalized by the averages of the claimed reference set $(\overline{d}_{min}, \overline{d}_{max}, \overline{d}_{tmp})$, are used in classifying the signature as genuine or forgery, by the trained recognizer.

4 Performance Evaluation

The system performance was evaluated using the sample signatures supplied by 94 subjects enrolled to our system. Each subject supplied 10 to 15 genuine signatures in total. Eight of the signatures were used for profile creation (reference set) for that user and the rest was used in the evaluation of the system(DS1 of 182 genuine signatures). There were no constraints on how to sign, nor was any information given about the working of the system, so that the subjects signed in their most natural way.

To collect skilled forgeries we added a signing simulation module to our system. Simulation module animates the signing process of a given signature so that the forger could see not only the signature trajectory's points sequence but also the signing dynamics (speed and acceleration). Forgers had a chance of watching the signature's animation several times and practice tracing over the signature image a few times before forging it. Our forgery data set (DS2) consists of 313 skilled forgeries obtained in this way. Note that training data is separate from both the reference set of genuine signatures and the test data used to in performance evaluation.

The results shown in Table 1 and 2 are with the $\Delta_x$and Δ_y features, using the Bayes classifier and the PCA approach, respectively. Best results were obtained using PCA, with approximately a 1.4% total error rate (which is also roughly the equal error rate). The results of the experiments with the Bayes classifier using the 3-dimensional feature vector were inferior; this may be due to a poor fit to the assumed Gaussian distribution or the relatively small number of training data used to estimate the model parameters.

Data Set	*Type*	*Size*	*FRR*	*FAR*
DS1	Genuine	182	2.19%	-
DS2	Skilled	313	-	3.51%

Table 1. Verification results obtained using the Bayes' classifier using the 3-dimensional data.

Data Set	*Type*	*Size*	*FRR*	*FAR*
DS1	Genuine	182	1.65%	-
DS2	Skilled	313	-	1.28%

Table 2. Verification results obtained using the linear classifier used with PCA, with a 1.4% total error rate.

5 Summary and Conclusion

We have presented an online signature verification system that approaches the problem as a two-class pattern recognition problem. The distance values of a test signature to the reference set, normalized by the respective averages of the reference set, are used as features.

We experimented with two different classifiers and obtained a 1.4% overall error rate for a data set of 94 people and 495 signatures (genuine signatures and skilled forgeries). These results are quite good, given the fact that the forgeries used on the experiments were not random forgeries, as it is typically done, but relatively skilled forgeries. Even though these results are on our relatively small database, the proposed system received first place at the First International Signature Verification Competition [11], with the lowest average equal error rate ($< 2.9\%$) when tested with skilled forgeries with or without pressure information.

References

1. Jain, A., Griess, F., Connell, S.: On-line signature verification. Pattern Recognition **35** (2002) 2963–2972
2. Plamondon, R., Lorette, G.: Automatic signature verification and writer identification - state of the art. Pattern Recognition **22** (1989) 107–131
3. Leclerc, F., Plamondon, R.: Automatic signature verification: The state of the art. International Journal of Pattern Recognition and Artificial Intelligence **8** (1994) 643–660
4. Vielhauer, C., Steinmetz, R., Mayerhofer, A.: Biometric hash based on statistical features of on-line signatures. 16'th International Conference on Pattern Recognition (2002)
5. Ohishi, T., Komiya, Y., Matsumoto, T.: On-line signature verification using pen-position, pen-pressure and pen-inclination trajectories. In: ICPR. (2000) Vol IV: 547–550
6. Yang, X., Furuhashi, T., Obata, K., Uchikawa, Y.: Constructing a high performance signature verification system using a ga method. In: 2nd New Zealand Two-Stream International Conference on Artificial Neural Networks and Expert Systems (ANNES '95). (1995)
7. Martens, R., Claesen, L.: Dynamic programming optimisation for on-line signature verification. In: ICDAR97. (1997) Poste
8. Parizeau, M., Plamondon, R.: A comparative analysis of regional correlation, dynamic time warping and skeletal tree matching for signatures. IEEE Trans. Pattern Analysis and Machine Intelligence **12** (1990) 710–717
9. Van Oosterhout, J.J., Dolfing, H., Aarts, E.: On-line signature verification with hidden markov models. In: ICPR. (1998)
10. Connell, S., Jain, A.: Template-based online character recognition. Pattern Recognition **34** (2001) 1–14
11. Yeung, D., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G.: SVC2004: First international signature verification competition. In: Proceedings of the Int. Conf. on Biometric Authentication. (2004) Also available at `http://www4.comp.polyu.edu.hk/~icba/`.