Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2009, Article ID 260516, 13 pages
doi:10.1155/2009/260516

Research Article

Online Signature Verification Using Fourier Descriptors

Berrin Yanikoglu[1] and Alisher Kholmatov[2]

[1] *Faculty of Engineering and Natural Sciences, Sabanci University, Istanbul 34956, Turkey*
[2] *National Research Institute of Electronics and Cryptology (UEKAE), Scientific and Technological Research Council of Turkey (TUBITAK), Gebze, Kocaeli 41470, Turkey*

Correspondence should be addressed to Berrin Yanikoglu, berrin@sabanciuniv.edu

Received 27 October 2008; Revised 25 March 2009; Accepted 25 July 2009

Recommended by Natalia A. Schmid

We present a novel online signature verification system based on the Fast Fourier Transform. The advantage of using the Fourier domain is the ability to compactly represent an online signature using a fixed number of coefficients. The fixed-length representation leads to fast matching algorithms and is essential in certain applications. The challenge on the other hand is to find the right preprocessing steps and matching algorithm for this representation. We report on the effectiveness of the proposed method, along with the effects of individual preprocessing and normalization steps, based on comprehensive tests over two public signature databases. We also propose to use the pen-up duration information in identifying forgeries. The best results obtained on the SUSIG-Visual subcorpus and the MCYT-100 database are 6.2% and 12.1% error rate on skilled forgeries, respectively. The fusion of the proposed system with our state-of-the-art Dynamic Time Warping (DTW) system lowers the error rate of the DTW system by up to about 25%. While the current error rates are higher than state-of-the-art results for these databases, as an approach using global features, the system possesses many advantages. Considering also the suggested improvements, the FFT system shows promise both as a stand-alone system and especially in combination with approaches that are based on local features.

1. Introduction

Signature verification is the task of authenticating a person based on his/her signature. Online (dynamic) signatures are signed on pressure sensitive tablets that capture dynamic properties of a signature in addition to its shape, while offline (static) signatures consist of only the shape information. Dynamic features, such as the coordinates and the pen pressure at each point along the signature's trajectory, make online signatures more unique and more difficult to forge compared to offline signatures.

In online signature verification systems, like in any other biometric verification system, users are first enrolled to the system by providing reference samples. Later, when a user presents a signature claiming to be a particular individual, the query signature is compared with the reference signatures of the claimed individual. If the dissimilarity is above a certain fixed threshold, the user is rejected.

As a behavioral biometric, online signatures typically show more intrapersonal variations compared to physical biometrics (e.g., iris, fingerprint). Furthermore, forging a signature may be relatively easy if the signature is simple and its timing can be guessed from its static image (e.g., short signature showing a strictly left to right progression). Despite these shortcomings, signature is a well-accepted biometric and has potential niche applications such as identity verification during credit card purchases. Also, forging the shape and timing at the same time proves to be difficult in reality, as evidenced by the success of automatic verification algorithms [1].

In this work, we present an online signature verification system based on the spectral analysis of the signature using the Fast Fourier Transform (FFT). The advantage of using the Fourier domain is the ability to compactly represent an online signature using a fixed number of coefficients, which leads to fast matching algorithms. More importantly, the fixed-length is better suited or even necessary in certain applications related to information theory and biometric cryptosystems. For instance, the template protection scheme by Tuyls et al. [2] requires a fixed-length feature representation of the biometric signal. Similarly, an earlier version of the proposed system was used for assessing the individuality of online signatures, where the fixed-length representation was important for simplifying the analysis [3]. Approaches using global and local features are called feature-based and function-based in literature, respectively. In this work, we also refer to them shortly as global and local approaches.

The challenge of using the Fourier domain representation, on the other hand, is to find the right preprocessing steps and matching algorithm for this representation. We report on the effectiveness of the proposed method, along with the effects of individual preprocessing and normalization steps, on the overall system performance, based on comprehensive tests over two public signature databases. While the current error rates are higher than state-of-the-art results for the used databases, this is to be expected since approaches based on global features of the signature normally underperform those using local information. On the other hand, in addition to the aforementioned advantages, global approaches are good complements to local approaches such as Dynamic Time Warping (DTW) or Hidden Markov Models (HMMs). In fact, we show that the fusion of the proposed system improves the performance of our DTW system by up to about 25%. With regard to the preprocessing, we show that the proposed incorporation of the pen-up durations significantly improves verification performance, while subsampling which is commonly used to obtain equal-length signatures, has the opposite effect. Finally, we discuss potential improvements and conclude that the proposed system has potential both as a stand-alone system and especially in combination with approaches that are based on local features.

This paper is organized as follows. Section 2 describes the previous work in the general area of online signature verification problem, along with some specific work that are more closely related to ours. Section 3 describes the proposed method, including preprocessing, feature extraction, and matching steps. Sections 4 and 5 present and discuss the experimental results using the SUSIG and MCYT databases. Finally Section 6 mentions future work to improve the current performance.

2. Previous Work

Signature verification systems differ both in their feature selection and in their decision methodologies. In fact, more than 70 different feature types have been used for signature verification [4–7]. These features can be classified in two types: global and local. Global features are those related to the signature as a whole, including the signature bounding box dimensions, average signing speed, and signing duration. Fourier Descriptors studied in this work are also examples of global features. Genuine signatures of a person often differ in length due to the natural variations in signing speed. The advantage of global features is that there are a fixed number of measurements (features) per signature, regardless of the signature length; this makes the comparison of two signatures a relatively straightforward task. The fixed-length representation is also better suited or even necessary in certain applications. Xu et al. use the Fourier transform to obtain a fixed-length representation of fingerprint minutiae [8]. Similarly, Yi et al. use the phase information of the Gabor filter to align online signatures and use the temporal shift and the shape dissimilarity measures to represent online signatures using a fixed-length feature vector [9].

In contrast to global features, local features are measured or extracted at each point along the trajectory of the signature and thus vary in number even among genuine signatures. Examples of local features include position, speed, curvature, and pressure at each point on the signature trajectory. In [5, 10], some of these features are compared in order to find the more robust ones for signature verification purposes. When local features are used, one needs to use methods which are suitable to compare feature vectors of different lengths: for instance, the Dynamic Time Warping algorithm [4, 5, 11–13] or Hidden Markov Models [14–19]. These methods are more complicated compared to the relatively simple metrics used with global features but they are generally more successful as well. Methods using global and local features are called feature-based and function-based approaches in literature [7]. Comprehensive surveys of the research on signature verification, including a recent one, can be found in [20–22].

The performance of biometric verification systems are evaluated in terms of false reject rate (FRR) of genuine samples, false accept rate (FAR) of impostors, and equal error rate (EER), where the two types of errors are equal. Due to the differences in databases and forgery qualities, comparing reported performance results is difficult. The First International Signature Verification Competition (SVC2004), organized in 2004, provided a common test set and tested more than 15 online signature verification systems from industry and academia. The results of this competition indicate state-of-the-art results of 2.6% equal error rate in skilled forgery detection and 1.85% equal error rate in random forgery detection tasks, using only position sequence (x, y) of a signature [1]. Our DTW-based system using only positional information, later described in [13], was declared as the winning system (Team 6) for its performance in the skilled forgery tests. We will refer to this system as our DTW system from now on.

Many different features and matching algorithms have been used to compare two signatures but the use of the Fourier Transform has not been widely explored [23–25]. In the work by Lam et al. [23], the signature is first resampled to a fixed-length vector of 1024 complex numbers consisting of the x- and y-coordinates of the points on the signature trajectory. This complex signal then undergoes various preprocessing steps, some of which are suggested by Sato and Kogure [24], including normalization for duration, drift, rotation, and translation, prior to the application of the Fast Fourier Transform (FFT). Feature extraction involves calculating the Fourier Descriptors of the normalized signature and selecting the 15 Fourier Descriptors with the highest magnitudes, normalized by sample variances. Discriminant analysis is then used with the real and imaginary parts of the 15 selected harmonics, to find the most useful features and their weights. The proposed system was tested using a very small signature dataset (8 genuine signatures of the same user and 152 forgeries provided by 19 forgers), achieving a 0% FRR and 2.5% FAR. In a similar work, Quan et al. [25] use windowed FFT to avoid the discontinuities in the signal, also using discriminant analysis to pick the important FFT coefficients. The authors show that windowing improves performance, resulting in an EER of 7% EER on the MCYT-100 database, using 15 reference signatures.

Similar to the Fourier transform, the Discrete Wavelet Transform (DWT) is recently used for online signature verification by Nanni and Lumini [26]. The results of this system on the MCYT-100 database are 11.5% equal error rate on skilled forgeries, when using only the coordinate information (x- and y-coordinates as a function of time) of the signature. The DWT is also used by Nakanishi et al. [27], with about 4% EER on a small private database.

Recent research on signature verification has concentrated on the fusion of multiple experts [7, 26, 28]. These systems typically combine new methods with proven ones such as DTW and HMMs (e.g., [13, 19] which received the first and second place in the SVC2004 competition). Fusion systems have some of the best results obtained for their respective databases; this is not very surprising because online signature is a complex signal of several dimensions and one method may concentrate on one aspect of the signal (e.g., shape), while another method may focus on another (e.g., timing).

In this paper, we present a novel online signature verification system based on the Fast Fourier Transform. Our work differs from previous work using Fourier analysis [23–25] in preprocessing and normalization steps as well as the matching algorithm. Furthermore, the results of the proposed algorithm and the individual preprocessing steps are comprehensively tested on two large, public databases. The results show the potential of the proposed system and also highlight the importance of the timing information for online signatures, in contrast to previous work where the timing information was discarded to a large extent [23–25].

3. Proposed Method

3.1. Input Signal. An online signature S, collected using a pressure-sensitive tablet, can be represented as a time sequence:

$$S(n) = \left[x(n) \quad y(n) \quad p(n) \quad t(n)\right]^{\mathrm{T}} \tag{1}$$

for $n = 1, 2, \ldots, N$, where N is the number of points sampled along the signature's trajectory; $x(n)$ and $y(n)$ denote the coordinates of the points on the signature trajectory, while $p(n)$ and $t(n)$ indicate the pen pressure and timestamp, at sample point n. A pressure-sensitive tablet typically samples 100 points in a second (100 HZ) and captures samples only during the interaction of the pen tip with the tablet. Depending on the tablet capabilities, pen azimuth ($az(n)$) and pen altitude ($al(n)$), indicating the angle of the pen with respect to the writing surface, can also be collected. Other features such as local velocity and acceleration may be calculated using the above features, as done by many signature verification systems [5–7, 12, 14].

The positional information consisting of $x(n)$ and $y(n)$ is important because it describes the shape of the signature and it is common to all tablets. The pressure information, on the other hand, had not seem very useful in some previous studies [10, 13, 26], while others have found it useful [29]. In particular, our DTW system [13] using just the positional information achieved the lowest error rates in the skilled forgery tasks of SVC2004, including the task where pressure, azimuth, and altitude were available to participating systems [1]. On the other hand, Muramatsu and Matsumoto [29] tested the discriminative power of the component signals of an online signature both alone and in groups and achieved 10.4% EER when they included the pressure and azimuth information, compared to 12.7% without them, using the SVC2004 database. In the current work, we have also observed that the pressure, azimuth, and altitude information improves the performance, although not drastically. In addition, we propose to use the timestamp information to identify and use the pen-up periods in identifying forgeries.

In the remainder of the paper, we use the sequence index n as if it refers to time (see Section 3.2.1) and describe the methodology concentrating on the positional information, denoted as $s(t)$, while the other input components are used as available.

3.2. Preprocessing. Preprocessing of online signatures is commonly done to remove variations that are thought to be irrelevant to the verification performance. Resampling, size, and rotation normalization are among the common preprocessing steps. While useful in object recognition, our previous research [13] had suggested that preprocessing may decrease biometric authentication performance by removing individual characteristics of the user. Therefore, we keep the amount of preprocessing done to a minimum, preserving as much of the discriminatory biometric information as possible.

In the previous work on online signature verification using FFT [23–25], the signature undergoes various preprocessing steps, consisting of spike and minor element removal to remove noise and extraneous segments; adding ligatures to connect consecutive strokes to reduce discontinuities that would affect FFT results; equi-time subsampling to obtain a fixed-length signature; drift removal; and rotation, translation, and scale normalization. In [23], the effects of drift removal and ligature processing are analyzed and authors report that drift removal significantly improves verification performance, while ligature processing only brings a marginal improvement. They guess that ligature processing that is done to reduce discontinuities is not very helpful because the high-frequency components affected by the discontinuities are discarded in the matching process.

We tested the individual effects of the preprocessing steps found to be important in [23], using two large databases. The results described in Section 4.4 show that subsampling which is commonly done to normalize the length of a signature significantly reduces verification performance by removing most of the timing information. This was also confirmed in our previous research. On the other hand, mean and drift removal are found to be useful, while scale removal is not needed since our features (Fourier Descriptors) are normalized to be invariant to translation, rotation, and scale changes.

In addition to the steps described above, we propose to use the timestamp information to identify and use the pen-up periods in identifying forgeries. The next sections describe the preprocessing steps used in this work.

3.2.1. Pen-up Durations. Pen-up periods indicate the times when the pen is not in contact with the tablet. These periods may be detected using discontinuities between the timestamps of consecutive points ($t(n)$ and $t(n+1)$) and actual pen-up durations can be calculated using the sampling rate of the tablet and the difference between timestamps.

Forgery signatures often have longer pauses between strokes, compared to genuine signatures, which may help in identifying forgeries. Thus, while the pen-up durations can be useful for verification, such as in detecting a forger's hesitation or recomposition, it is often discarded, keeping just the order of the sampled points. In fact, the timing information is discarded to a large extent by many systems that use resampling to obtain a fixed-length signature, including the previous work using FFT [23–25]. Note that resampling results in keeping only the relative order of the points on the trajectory, while other timing information is discarded.

We propose to fill the pen-up durations with imaginary points, which has a twofold benefit: (i) it incorporates pen-up durations directly into the signature trajectory; (ii) it reduces trajectory discontinuities, which enhances the FFT analysis. For example, if there is a 50 ms wait between two consecutive points of the trajectory using a 100 Hz tablet (corresponding to 10 ms between consecutive samples), we add 4 imaginary points. Imaginary points can be generated through (a) interpolation between the last and first points of the two strokes corresponding to the pen-up event or (b) as if the pen was actually left on the tablet after the stroke prior to the pen-up event. In order for the pen-up events not to dominate the signal, we place imaginary points sparingly (every 30 ms for the 100 Hz tablet). Both methods of adding imaginary points improve the system performance, though the more sophisticated method of interpolation obtains better results, as expected.

Note that after this process, the timestamp information ($t(n)$) itself is basically redundant and discarded. We use the sequence index n and time t interchangeably in the rest of the paper.

3.2.2. Drift and Mean Removal. In signatures that go from left to right, $x(t)$ has a significant drift as time increases and the same can be said for signatures being signed top to bottom and $y(t)$. Drift removal step aims to remove the baseline drift component of a signal, so as to keep only the important information in the signal. We use a linear regression using least squares fit to estimate the drift. Given a discrete time signal y of length n, the drift removed version y' can be computed as

$$y' = y - \beta \times (t - \bar{t}), \tag{2}$$

where

$$\beta = \frac{\Sigma yt - n\bar{y}\bar{t}}{\Sigma t^2 - n\bar{t}^2}. \tag{3}$$

Mean removal on the other hand is simply achieved by subtracting the mean of the signal from itself: $y' = y - \bar{y}$.

3.3. Feature Extraction. We use the Fourier Transform to analyze the spectral content of an online signature. The details of the Fourier transform are out of the scope of this paper but can be found in many references (e.g., [30]). Below we give the basic idea and necessary definitions.

3.3.1. Fourier Transform. Any periodic function can be expressed as a series of sinusoids of varying amplitudes, called the *Fourier Series*. If the signal is periodic with fundamental frequency ω, the frequencies of the sinusoids that compose the signal are integer multiples of ω and are called the *harmonics*. The Fourier Transform is used to find the amplitude of each of the harmonic component, which is called the *frequency spectrum* of the signal. It thus converts a signal from the time domain into the frequency domain.

The Discrete Fourier Transform discrete time signal $f(t)$ is defined as follows:

$$C_k = \frac{1}{N}\sum_{t=0}^{N-1} f(t)e^{-i2\pi kt/N} \quad k = 0, 1, \ldots, N-1, \tag{4}$$

where $f(t)$ is the input signal; N is the number of points in the signature; k indicates the frequency of the particular harmonic; $e^{ix} = \cos(x) + i\sin(x)$.

The amplitude of the kth harmonic found by the Fourier transform is referred to as the kth *Fourier Coefficient*. Given a complex Fourier coefficient $C_k = a_k + ib_k$, the magnitude and phase corresponding to the kth harmonic are given by $|C_k| = \sqrt{a_k^2 + b_k^2}$ and $\tan^{-1}(b_k/a_k)$, respectively.

The Fourier coefficients are normalized to obtain the *Fourier Descriptors* which are the features used in this study, as described in Section 3.3.3.

The Inverse Fourier Transform is similarly defined as

$$f(t) = \sum_{k=0}^{N-1} C_k e^{i2\pi kt/N} \quad t = 0, 1, \ldots, N-1. \tag{5}$$

The Fourier transform has many uses in signal processing. For instance, reconstructing a time signal using the inverse Fourier transform by discarding the high-frequency components of a signal can be done for noise removal.

3.3.2. Input Signal Components. An online signature consisting of x- and y-coordinates can be represented as a complex

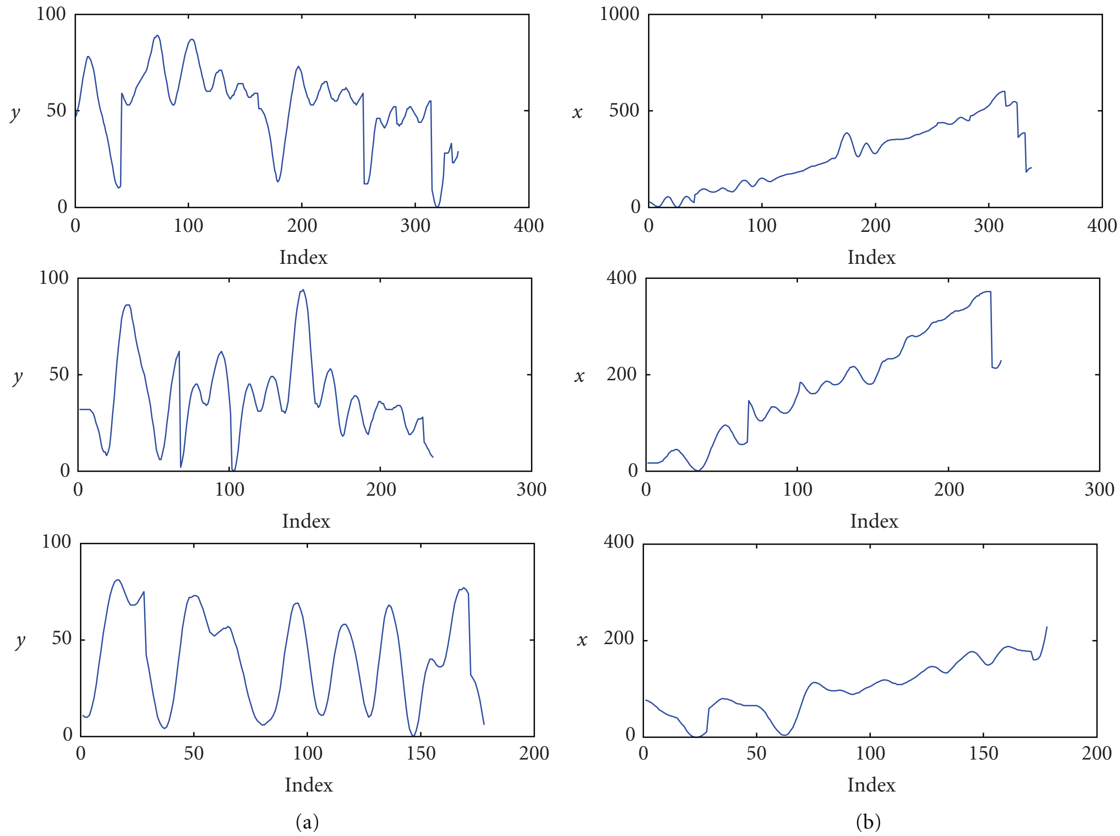

Figure 1: The y-coordinate (a) and x-coordinate (b) profiles belonging to genuine signatures of 3 different subjects from the SUSIG database.

signal $s(t) = x(t)+iy(t)$ where $x(t)$ and $y(t)$ are the x- and y-coordinates of the sampled points. The Fourier transform of the signature trajectory can then be directly computed using the complex signal $s(t)$ as the input, as described in (4).

In signatures which are signed from left to right or right to left, $x(t)$ is a monotonic function for the most part and carries little information, as shown in Figure 1. Based on this observation, we first evaluated the discriminative power of $y(t)$ alone, discarding $x(t)$ for simplicity. Later, we also did the reverse and used only $x(t)$ for completeness. Similarly, we assessed the contribution of other input signal components to the verification performance, by concatenating features extracted from individual component signals (e.g., $x(t)$, $y(t)$, $p(t)$), to obtain the final feature vector. We denote these feature vectors by indicating the individual source signals used in feature extraction: for instance, $x \mid y \mid p$ denotes a feature vector obtained from the x-, y-coordinates and pressure component, respectively. The input signal $f(t)$ in (4) can be any one of these signals ($s(t)$, $y(t)$, $x(t)$, $p(t)$, etc.).

3.3.3. Fourier Descriptors. The extracted Fourier coefficients are normalized to obtain the Fourier Descriptors, using normalization steps similar to the ones used in 2D shape recognition. In particular, the Fourier coefficients obtained by applying the Fourier Transform to the object contour $(x(t), y(t))$ can be normalized to achieve invariance against translation, rotation, and scaling of the original shape [30]. Specifically, translation of a shape corresponds to adding a constant term to each point of the original shape and affects (only) the first Fourier coefficient. By discarding C_0, defined in (4), one obtains translation invariance in the remaining coefficients. Rotation of a shape results in a phase change in each of the Fourier coefficients; rotation invariance is automatically obtained when one uses only the magnitude information of the Fourier Transform. Alternatively, each coefficient can be normalized such that the phase of one of the coefficients (e.g., C_1) is zero; this is equivalent to assuming a canonical rotation that gives a zero phase to C_1. Finally, scaling of a shape corresponds to multiplying all coordinate values of the shape by a constant factor and results in each of the Fourier coefficients being multiplied by the same factor. Therefore, scale normalization is achieved by dividing each coefficient by the magnitude of one of the components, typically $|C_1|$.

An online signature must show adequate match to the reference signatures of the claimed identity in *both* shape and dynamic properties, in order to be accepted. As with the above normalization steps, it is easy to see that by discarding C_0 and using the magnitudes of the remaining coefficients as features, we obtain invariance to translation (position of the signature on the tablet) and rotation (orientation relative to the tablet). Scale invariance is more complicated, due to the additional dimension of time. If a signature is only

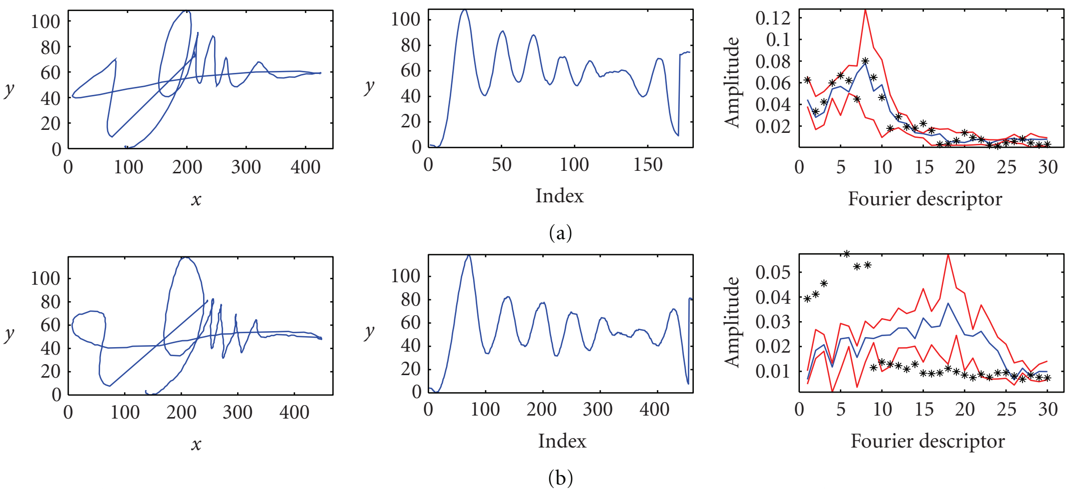

Figure 2: A verification case is shown for illustration, using only the y-profile. From left to right: (a) Genuine signature, its y-profile and its Fourier Descriptors. (b) Forgery signature, its y-profile and its Fourier Descriptors. The Fourier Descriptors of genuine and forgery signatures (shown as dots) are overlaid on top of the envelope showing the min and max values of the reference signatures' descriptors, while the line in the middle denotes the mean reference feature.

scaled in space, while keeping the signing duration the same, dividing each coefficient's magnitude by $|C_1|$ achieves scale normalization. However for the more general case involving both scale and time variations, we have found that a more robust approach is to divide each coefficient by the total magnitude of the Fourier spectrum:

$$m = \sum_{k=0}^{N-1} |C_k| = \sum_{k=0}^{N-1} \sqrt{C_k * C_k^*}, \tag{6}$$

where N is the length of the signature; $|C_k|$ is the magnitude of the complex coefficient C_k; C_k^* is the complex conjugate of C_k.

The total energy of the Fourier spectrum is also commonly used for normalization of the Fourier coefficients:

$$e = \sum_{k=0}^{N-1} |C_k|^2. \tag{7}$$

In our experiments, we have found that the normalization by the total amplitude has outperformed normalization done either by dividing each component by $|C_1|$ or by the total energy of the Fourier Transform (about 3% and 1% percent points less error, resp.).

Using (7), our final features or the Fourier Descriptors F_k are thus obtained as

$$F_k = \frac{|C_k|}{m} \quad k = 1, \ldots, \frac{N}{2}. \tag{8}$$

Notice here that k goes from 1 to $N/2$ since we discard half of the coefficients due to the symmetry of the Fourier transform spectrum.

3.3.4. Zero-Padding. Due to the natural variation in the signing process, genuine signatures of the same user almost never have equal lengths. The length variation results in Fourier domain representation with varying number of components, hence feature vectors of varying lengths. While one can cut out the high-frequency components, leaving only the first k Fourier coefficients, when the signatures are of different lengths, these components do not correspond to the same frequencies.

In order to obtain an equal number of Fourier Descriptors which correspond to the same frequencies, we pad each signature to be compared (reference set + query) with zeros, to match the length of the longest signature in the set, prior to the application of the Fourier Transform. This process is called *zero-padding* and does not affect the amplitudes of the Fourier coefficients but changes the frequency resolution.

3.3.5. Smoothing. We smooth the computed Fourier descriptors F_k by averaging two consecutive descriptors, to account for the normal timing variations between genuine signatures that would result in energy seeping into the neighboring harmonics. The smoothing is found to have a significant effect (roughly 2% point) in overall system performance in both tested databases.

Sample signatures and their forgeries, along with the resultant Fourier descriptors, are shown in Figure 2, using only the y-dimension for simplicity. The figure shows the envelope of the reference set descriptors to indicate the difference between query and reference signature descriptors, while in matching we only use the distance to the mean. The difference in the Fourier descriptors of the reference signatures for the genuine and forgery queries is due to zero-padding used in this example. As explained before, zero-padding does not change the frequency content of a signal but increases the frequency resolution (here note that the forgery signature that is used in determining the padding amount is much longer than the references).

Table 1: The summarizing characteristics of the public databases used in this study. In both of them, the genuine signatures are collected in multiple sessions and there are 5 reference signatures per user.

Dataset	Subjects	Genuine	Skilled forgeries	Input
SUSIG-Visual	100	2000	1000	x, y, p, timestamp
MCYT-100	100	2500	2500	x, y, p, az, al

Table 2: Equal error rates obtained using different components of the input signal. The timestamp is discarded after incorporating the pen-up durations into the trajectory, for the SUSIG database.

Dataset	$x + iy$	y	x	$x \mid y$	$x \mid y \mid p$	$x \mid y \mid p \mid az$	$x \mid y \mid p \mid az \mid al$
SUSIG-Visual	8.37%	9.90%	8.42%	**6.20**%	—	—	—
MCYT-100	17.62%	17.38%	17.42%	14.53%	12.99%	12.61%	**12.11**%

3.4. Matching. When a query signature is input to the system along with a claimed ID, the dissimilarity of its Fourier Descriptors from those of the reference signatures of the claimed person is calculated. Then, this distance is normalized using the reference set statistics of the user, and the query signature is accepted as genuine if this normalized distance is not too large. These steps are explained in detail in the following subsections.

3.4.1. Distance Between Query and Reference Set. During enrollment to the system, the user supplies a number of reference signatures that are used in accepting or rejecting a query signature. To find the dissimilarity between a query signature q and the reference set R_i of the claimed user i, we compute the Euclidian distance between the query features F_q obtained from q and the vector $\overline{F}_{R_i}$ which is the mean of the feature vectors of the reference signatures in R_i:

$$d(q, R_i) = \left\| F_q - \overline{F}_{R_i} \right\|. \tag{9}$$

We have also evaluated different matching algorithms, such as the number of matching Fourier Descriptors between the compared signatures but the presented matching algorithm gave the best results. Ideally, one can apply machine learning algorithms to find the most important descriptors or to decide whether the query is genuine or forgery given the Fourier descriptors of the query and reference set.

3.4.2. User-Dependent Distance Normalization. In order to decide whether the query is genuine or forgery, the distance computed in (9) should be normalized, in order to take into account the variability within the user's signatures. We use a normalization factor computed only from the reference signatures of the user. The normalization factor D_i which is separately calculated for each user i, is the average dissimilarity of a reference signature r to the rest of the reference signatures:

$$D_i = \text{mean}_{r \in R_i} d(r, R_i/r), \tag{10}$$

where R_i/r indicate the set R_i without the element r. The normalization factor D_i is calculated by putting a reference signature aside as query and calculating its dissimilarity d to the *remaining* reference signatures (R_i/r). The resulting normalized distance $d(x, R_i)/D_i$ is compared to a fixed, user-*independent* threshold.

We have previously found that this normalization is quite robust in the absence of training data [13]. Results of similar methods of normalization using slightly different statistics of the reference signatures are shown in Table 5. More conventional normalization techniques using client and impostor score distributions can be used when training data is available [31] and are expected to perform better.

3.4.3. Removing Outliers. Often, there are some important differences (in timing or shape) among the reference signatures of a user. In this work, we experimented with the removal of outliers from the reference set. While the template selection is a research area by itself, we found that eliminating up to one of the outlier from the reference set in a conservative fashion brings some improvement. For this, we sort the reference set distances of a user, as calculated using (9), and discard the last one (the one with the highest distance to the remaining references) if there is a big difference between the last two.

4. Experimental Results

4.1. Databases. The system performance is evaluated using the base protocols of the SUSIG [32] and MCYT [33] databases. The SUSIG database is a new, public database consisting of real-life signatures of the subjects and including "highly skilled" forgeries that were signed by the authors attempting to break the system. It consists of two parts: the Visual subcorpus obtained using a tablet with a built-in LCD display providing visual feedback and the Blind Subcorpus collected using a tablet without visual feedback. The Visual subcorpus used in this study contains a total of 2000 genuine signatures and 1000 skilled (half are highly skilled) forgeries collected in two sessions from 100 people. The data in SUSIG consists of x, y, and *timestamp*, collected at 100 Hz.

The MCYT database is a 330-people database of which a 100-user subcorpus is made public and is widely used for evaluation purposes. The database contains 25 genuine signatures and 25 skilled forgeries signed by 5 different forgers, for each user. The data in MCYT database consists of consists of x, y, pressure, azimuth, and altitude, collected at 100 Hz. Table 1 summarizes these datasets, while the details can be found in their respective references.

4.2. Results of the Proposed System. We evaluated the usefulness of various preprocessing steps and the different components of the input signal, on the overall verification performance. The results obtained using the best set of preprocessing steps, while varying the input signal, are summarized in Table 2. As can be seen in this table, using only the coordinate information of the signature, we obtained minimum equal error rates of 6.20% and 14.53% for SUSIG and MCYT databases, respectively. These results are obtained using the concatenation of the Fourier descriptors obtained from $y(t)$ and $x(t)$. The pressure, azimuth, and altitude information available in the MCYT-100 database further reduced the EER to 12.11% EER. In addition to the EER results, the DET curves showing how FAR and FRR values change according to changing acceptance thresholds are given for the databases used in the evaluation, in Figure 3.

These results are obtained using 30 normalized Fourier descriptors per signal component (i.e., 30 for $y(t)$, 60 for $y(t) \mid x(t)$, etc.) and the preprocessing steps described in Section 4.4. However, very similar results were obtained with 20 and 25 descriptors. As described in Section 4.4, up to one reference signature was removed from the reference set, if deemed as an outlier. Timestamp information was not available for the MCYT database, and subsequently the pen-up durations were not used for this database.

Considering the effects of the different input signal components, we see that each information source brings the error rate down, from 14.53% using $x \mid y$ to 12.11% using $x \mid y \mid p \mid az \mid al$, for the MCYT database. Notice that the diminishing improvement is not necessarily and indication of the value of an input signal by itself. As for the positional information, we observe that the signature encoded as a complex signal (i.e., $s(t) = x(t) + iy(t)$) which was used in [23] gave significantly worse results compared to the concatenation of the features obtained from the x- and y-components separately (i.e., $x \mid y$). Another interesting observation is that our initial assumption about the x-component being mostly useless was not reflected in the results. While the x-component indeed contains little information in signatures signed strictly from left to right, the results show that it contains enough discriminative information to separate genuine and forgery signatures to a large extent, for the particular databases used.

In order to see the variation of the overall performance with respect to different sets of reference signatures, we ran 25 tests using the proposed method with different sets of 5 reference signatures, on the MCYT database. The mean EER for these tests was 10.89%, while standard deviation was 0.59. In fact, the worst performance was with the original set of references (genuine signatures [0–4]). The better performance with other reference sets can be explained by the fact that reference signatures collected over a wider time span better represent the time variation in the data.

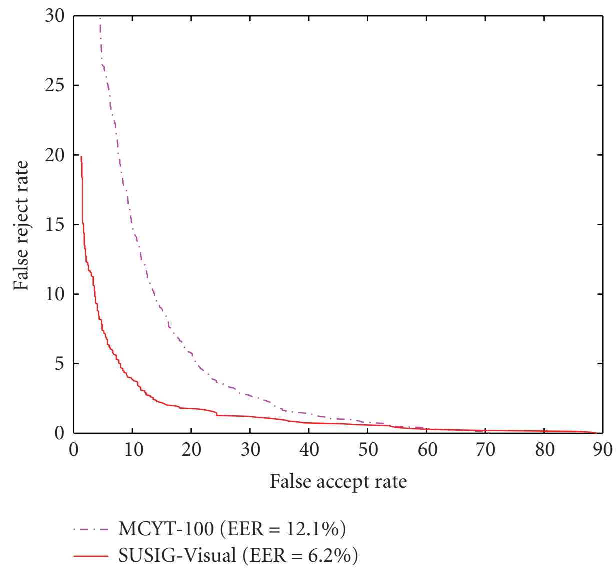

Figure 3: DET curves show how FAR (x-axis) and FRR (y-axis) values change according to changing acceptance threshold, for the tested databases.

The proposed FFT system is very fast: it can process 4500 queries in the MCYT-100 database in 69 seconds of CPU time.

4.3. Effects of Preprocessing Steps. The best results reported in Table 2 were obtained using few preprocessing steps, namely, pen-up duration encoding and drift and mean removal. Some of the other preprocessing steps used in previous work based on FFT [23, 25] were just not useful due to our normalized features (e.g., rotation and scale normalization), while resampling worsened results by removing discriminative information (30.02% versus 6.20% EER for the SUSIG database and 17.82% versus 12.11% EER for the MCYT database). On the other hand, removal of the drift (especially significant in the x-component) was found to improve performance in both our work and in previous work [23], by a few percent points. The effects of drift and mean removal are most apparent when they are used together. Note that mean removal is normally not necessary, since translation invariance is provided when the first Fourier coefficient is discarded; however mean removal affects the outcome due to zero padding.

The proposed incorporation of the pen-up duration is also found to help increase performance (9.09% EER versus 6.20% EER for the SUSIG database).

4.4. Effects of Distance Normalization. Normalization of the query distance, prior to using a *fixed* threshold across all users, has been found to make a significant difference on verification performance, as shown in Table 4. Here, AvgN refers to dividing the distance between the query and the mean descriptor vector by the average distance of the reference signatures. This average is obtained by using a leave-1-out method whereby one of the reference signature

Table 3: Effects of various preprocessing steps on the best configuration. The bold face shows the results of the proposed system, while the last column shows the results if resampling was added to the proposed preprocessing steps (drift and mean removal and pen-up duration incorporation when available).

Dataset	Feature	Raw	Drift	Mean	Drift + Mean	Proposed = Drift + Mean + PenUp	Proposed if resampled
SUSIG-Visual	$y \mid x$	8.18%	7.34%	11.52%	9.09%	**6.20**%	30.02%
MCYT-100	$y \mid x \mid p \mid az \mid al$	20.31%	20.38%	13.51%	**12.11**%	—	17.82%

Table 4: Different methods for user-dependent distance normalization using *only* the reference data.

Dataset	Feature	AvgN	MinN	MaxN	None
MCYT-100	$y \mid x \mid p \mid az \mid al$	**12.11**%	13.2%	14.3%	21.5%
SUSIG-Visual	$y \mid x$	**6.20**%	8.1%	5.8%	14.1%

is treated as query, while the others are used as reference, as described in Section 3.4.2. Similarly, MinN and MaxN refer to dividing the distance between the query and the mean descriptor vector by the minimum and maximum of the reference signature distances (again using the leave-one-out method), respectively. All three of these normalization methods are better than not doing any normalization at all.

Notice that while AvgN gives the best results for the MCYT-100 dataset, MaxN has given the best results for the SUSIG database. This difference highlights an important aspect of the current work, which is the fact that the exact same system is used in testing both databases, without any adjustment. In all of the presented results, we use the AvgN normalization method.

4.5. Results of the Fusion with the DTW System. It has been shown in the last couple of years that the combination of several experts improves verification performance in biometrics [7, 28, 34, 35]. Some of the results, especially as related to the work described here, are summarized in Section 4.6.

In order to show that the proposed FFT system may complement an approach based on local features, we combined the FFT system with a slightly modified implementation of the DTW system described in [13]. The distribution of the DTW and FFT scores in Figure 4 shows that the two systems' scores show a loose correlation, which is an important factor in classifier combination systems. The combination is done using the sum rule, after normalizing the scores of the two systems. The score normalization factor is selected separately for each database, so as to equalize the mean scores of the two systems, as computed over the *reference* signatures in that database. A better selection of the normalization factor can be made when training data is available. Note that using the sum rule with score normalization is equivalent to separating the genuine and forgery classes using a straight line with a fixed slope, where the y-intercept is adjusted to find the equal error rate.

The results given in Table 5 show that the FFT system improves the performance of the DTW system significantly, by 8% or 26% depending on the database. Furthermore, the

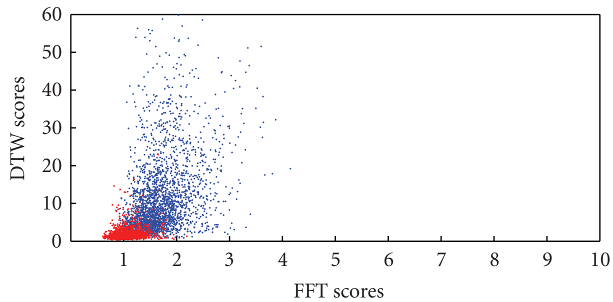

Figure 4: The distribution of the DTW and FFT scores for the MCYT-100 database.

improvement brings the EER rates to state-of-the-art levels given in Table 6 for both databases (3.03% for SUSIG and 7.22% for MCYT-100).

The proposed FFT system is very fast: it can process 4500 queries in the MCYT-100 database in 69 seconds of CPU time. In comparison, the DTW system takes 36 800 seconds for the same task, which corresponds to a factor of more than 500. Theoretically, the time complexity of the DTW system is $O(N \times M)$, where N and M are the lengths of the two signatures being compared, while that of the FFT is $O(N \log N)$ for a signature of length N. Hence, even though using the FFT system in addition to the DTW system results in negligeable time overhead, Figure 4 shows that the systems can also be called in a serial fashion to eliminate the more obvious forgeries using the FFT system and calling the DTW system only for the less certain cases. Using this test with a threshold of 4, the same reported results were obtained while gaining around 10% speed overall.

The DTW approach is probably the most commonly used technique in online signature verification, while quite successful overall and in particular in aligning two signatures, the basic DTW approach has some shortcomings, such as assigning low distance scores to short dissimilar signatures. One such example is shown in Figure 5, along with all of the genuine signatures of the claimed user. As an approach using global features, the FFT-based system is expected to be useful in eliminating some of these errors, when used in fusion with DTW or other local approaches.

4.6. Comparison with Previous Work. Results of previous work tested on the MCYT database are given in Table 6 for comparison. Since SUSIG is a new database, we concentrated on previous work reporting results on the MCYT database. Even with this database, comparing different results is

Table 5: Results of the fusion of the FFT system with our Dynamic Time Warping system.

Dataset	$y \mid x$	$y \mid x \mid p \mid az \mid al$	DTW	DTW + $y \mid x$	$DTW + y \mid x \mid p \mid az \mid al$	Improvement
SUSIG-Visual	6.20%	—	**3.30**%	**3.03**%	—	8%
MCYT-100	14.53%	12.11%	**9.81**%	7.8%	**7.22**%	26%

Table 6: State-of-the-art results on the MCYT database using a priori normalization techniques. Unless otherwise indicated, all dimensions of the input signal are used.

Reference	Dataset	Method	Features	Performance
Garcia-Salicetti et al. [35]	MCYT-280	HMM [18]		5.73%
		HMM [31]		8.39%
		String Matching [36]		15.89%
		Fusion of [18, 31]		3.40%
Faundez-Zanuy [28]	MCYT-280	VQ		11.8%
		DTW		8.9%
		VQ-DTW		5.4% (DCF)
Vivaracho-Pascual et al. [37]	MCYT-280	Length normaliz./p-norm		6.8% (DCF)
Nanni and Lumini [34]	MCYT-100*	SVM	100 global features	17.0%
		SVM-DTW [13]		7.6%
Nanni and Lumini [26]	MCYT-100	Wavelet-DCT	x, y	11.4%
		Wavelet-DCT	x, y, az	9.8%
		Wavelet-DCT fused w/DTW, HMM, GM		5.2%
Quan et al. [25]	MCYT-100*	STFT		7%
This work	MCYT-100	Proposed FFT	x, y	12.11%
		DTW [13]		9.81%
		FFT-DTW		7.22%

difficult due to varying experimental setups. In particular, we have (i) the subset of the MCYT database used: MCYT-280 is the test subset of the full database of 330 people where a 50-people portion is used for training, while MCYT-100 is the publicly available part consisting of 100 people and no allocated training subset; (ii) the number of reference signatures used (most systems use the first 5 genuine signatures as suggested, while others use more, as necessitated by their verification algorithm); (iii) number of available component signals used, such as coordinate sequence, pressure, and azimuth (not counting derived features); and (iv) whether *a priori* or *a posteriori* normalization is used for score normalization, as defined in [31].

In general, the higher the number of references, the better one would expect the results to be, due to having more information about the genuine signatures of a user. Similarly, higher number of signal components normally give better results. Finally, score normalization affects the performance significantly, since the *a posteriori* normalization results are intended to give the best possible results, if all genuine and/or forger statistics in the database were known ahead of time. For this comparison, we tried to included recent results on the MCYT database, using 5 reference signatures as suggested and *a priori* score normalization methods, to the best of our knowledge.

Given the various factors affecting performance and the difficulty in assessing the exact experimental setups of others' work, an exact comparison of different systems is not very easy. Nonetheless, we give the following as indicative results. The best results obtained with the MCYT-100 database is reported by Nanni and Lumini, with 5.2% EER using 3 measured signals (x, y, azimuth) using four experts including Wavelet, DTW and HMM approaches [26]. In that work, the Wavelet based system itself achieves 9.8% EER. The other system developed by the same authors which uses Support Vector Machines (SVMs) with 100 global features obtains 17.0% on the MCYT-100 database (using a 20-people subset for training), while the combination of SVM and DTW (based on our DTW system used in the fusion part of this work [13]) achieves 7.6% [34]. Quan et al. report 7% EER of using windowed FFT on the MCYT-100 but using 15 genuine signatures as reference (instead of 5 which is the suggested number).

On the MCYT-280 database, Garcia-Salicetti et al. evaluates 3 individual systems in a study of complementarity; the individual systems' performance are given as 5.73%, 8.39%, and 15.89%, while the best fusion system obtains 3.40% EER on skilled forgeries [35]. Faundez-Zanuy reports 11.8% and 5.4% using Vector Quantization (VQ) and VQ combined with DTW respectively [28]. However, instead of EER, they

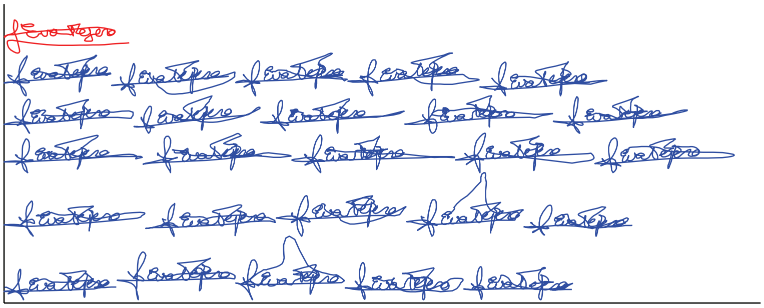

Figure 5: A forgery signature (shown on top) that was misclassified using the DTW system while it was correctly classified using the combined system.

report the main results using the Detection Cost Function (DCF) with 5 genuine and 25 forgery signatures per person. Similarly, Vivaracho-Pascual et al. report a DCF of 6.8%, using the same experimental setup.

The most apparent factor in these results is the effect of classifier combination. Classifier combination or fusion systems are found to be useful in many pattern recognition problems, so the improvement of the results is not surprising and is parallelled in our current results as well. The other important factor affecting performance is the dimensionality of the input signal. In some databases, x- and y-coordinates are the only available dimensions, while pressure, azimuth, and altitude are also available in others. Increasing the number of dimensions generally increases the verification performance, as more relevant information is available to the classifier. One interesting note is that the DTW appears as a component in each of the listed fusion systems.

The performance of the proposed FFT system is lower than the state-of-the-art fusion systems, while it seems to be in par with single engine systems on the same database (12.11% versus 9.8% [26], 17.0% [34], and 9.81% with our DTW approach, on the MCYT database). Approaches using global features typically underperform compared to those using local features. On the other hand, global approaches are necessary in certain applications. Furthermore, due to their speed and complementarity, they are expected to be useful in fusion systems to increase the performance and/or the speed.

We also have to underline the fact that when reporting results on a database, researchers typically report the results of the optimal set of features and algorithm steps, which introduces bias to the results. In fact, often a particular step of an algorithm improves the results on one database, while degrading it on another (e.g., different distance normalization methods gave the best results in SUSIG and MCYT databases, as shown in Table 5). Therefore, the fact that our results are obtained by testing the same exact system on two different databases with different characteristics (e.g., signature types, sensors, measured signals, forgery skills) is important.

As for comparison with previous work using FFT, the system developed by Lam et al. [23] is reported to have 2.5% error rate, however the dataset in their work is very small (8 genuine signatures of the same user and 152 forgeries provided by 19 forgers) and old, making a direct comparison impossible. Similarly, while the improvement of using windowed FFT, suggested by Quan et al. [25] is reasonable, their results are not readily comparable to ours: they report an EER of 7% on the MCYT-100, using 15 genuine signatures as reference instead of 5, presumably necessitated by their use of the Mahalanobis distance. As mentioned before, increased number of reference signatures are expected to increase performance and the resulting test set in their case is significantly different than ours. Furthermore, we have also shown that resampling step used in both of these works significantly degrades verification performance for the proposed method by removing some of the timing information which is useful in discriminating forgery and genuine signatures.

5. Future Work

In the current system, we use only the magnitude of the Fourier coefficients, discarding the phase information for simplicity, while phase information is actually a fundamental part of the signal. We expect that the use of the phase information can improve the system performance. Similarly, other extracted features, such as local velocity, can easily be used and would be expected to improve the system performance based on others' work [35].

Another improvement may be the use of windowed or Short Term Fourier Transform. The STFT aims to give more information about the timing as well as the frequency component of the signal, by breaking the input signal into a number of small segments by a windowing signal prior to the application of the Fourier transform. The size of the window used for this operation is an issue in general but for online signature verification, separate strokes or high curvature points can be used for this purpose.

An analysis of the errors shows that large portion of the errors is due to simple signatures, composed of simple or easily reproducible trajectories. While not much may be done to reduce errors on these types of signatures, one could at least envision a system alerting users when they use simple signatures at enrollment time.

6. Summary and Discussions

We presented a novel approach for online signature verification using global features consisting of Fourier Descriptors that provide a compact and fixed-length representation of an online signature. Our approach is significantly different in preprocessing, feature extraction, normalization and matching steps, compared to previous online signature verification systems that are based on FFT. These steps are carefully designed to retain the full discriminatory information available in the signature; in particular the incorporation of the timestamp information for representing pen-up durations is novel and had significant effects on performance.

The proposed system is extensively tested using two large public databases, both in terms of overall performance and the effects of individual preprocessing steps. The results are inferior to the best results obtained by fusion systems but the system shows potential as a stand-alone system to be used wherever fixed-length representation is needed, and in complementing an approach based on local features. The latter is supported experimentally by the fact the combination of the proposed FFT system improved the results of our state-of-the-art DTW system, resulting in EER of 3.03% for the SUSIG database and 7.22% for the MCYT-100 database. Furthermore, given the previously mentioned factors affecting performance and the difficulty in assessing the exact experimental setups of others' work, an exact comparison of EER results is not always meaningful. This is especially true since the proposed system is tested with *exactly* the same parameters on two different databases with different characteristics (e.g., signature types, sensors, measured signals, forgery skills).

As for overall speed, the proposed system is very fast, about 500 times faster than a dynamic programming approach on the same database. The speed is thus one of the advantages of the proposed system and is especially important in fusion systems and identification problems as well as quickly testing new algorithms or preprocessing steps.

The main aspects of the developed FFT system can thus be summarized as follows:

(i) it is very fast in training, feature extraction, and matching (about 2-3 orders of magnitude faster than the DTW system);

(ii) it uses a fixed-length feature vector comprised of global features of the signature, which is required in certain applications;

(iii) its performance is lower than state-of-the-art results obtained by fusion systems; however its advantages and potential improvements make it a useful alternative in online signature verification, especially in complementing more complex but slower methods based on local features, such as the DTW or HMM approaches.

Given its merits as a global approach and the suggested improvements, we believe that the proposed FFT-based system has potential as a stand-alone system but especially in complementing an approach based on local features. Furthermore, we would expect to have a lower EER by adding more features that are found useful in other studies, such as local velocity or acceleration; this would be done by simply concatenating the new features to the ones used in this work.

Acknowledgments

The authors would like to thank Professor Anil Jain for hosting B. Yankoglu during her sabbatical, Dr. Özgür Gürbüz for valuable help with the Fourier transform, and J. Fierrez-Aguilar and J. Ortega-Garcia for sharing the MCYT-100 database. This work was partially supported by TÜBİTAK (The Scientific and Technical Research Council of Turkey), under project no. 105E165.

References

[1] D. Yeung, H. Chang, Y. Xiong, et al., "SVC2004: first intional signature verification competition," in *Proceedings of the 1st International Conference on Biometric Authentication (ICBA '04)*, pp. 16–22, 2004.

[2] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical biometric authentication with template protection," in *Proceedings of the International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA '05)*, vol. 3546 of *Lecture Notes in Computer Science*, pp. 436–446, 2005.

[3] A. Kholmatov and B. Yanikoglu, "An individuality model for online signatures," in *Defense and Security: Biometric Technology For Human Identification V*, Proceedings of SPIE, Orlando, Fla, USA, March 2008.

[4] T. Ohishi, Y. Komiya, and T. Matsumoto, "On-line signature verification using pen-position, pen-pressure and pen-inclination trajectories," in *Proceedings of the 15th International Conference on Pattern Recognition (ICPR '00)*, vol. 4, pp. 45–47, 2000.

[5] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognition*, vol. 35, no. 12, pp. 2963–2972, 2002.

[6] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, "Biometric hash based on statistical features of online signatures," in *Proceedings of the 16th International Conference on Pattern Recognition (ICPR '02)*, vol. 1, p. 10123, 2002.

[7] J. Fieriez-Aguilar, L. Nanni, J. Lopez-Peñalba, J. Ortega-Garcia, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," in *Proceedings of the 5th International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA '05)*, pp. 523–532, 2005.

[8] H. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar, A. H. M. Akkermans, and A. M. Bazen, "Spectral minutiae: a fixed-length representation of a minutiae set," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPR '08)*, pp. 1–6, 2008.

[9] J. Yi, C. Lee, and J. Kim, "Online signature verification using temporal shift estimated by the phase of gabor filter," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 776–783, 2005.

[10] H. Lei and V. Govindaraju, "A comparative study on the consistency of features in on-line signature verification," *Pattern Recognition Letters*, vol. 26, no. 15, pp. 2483–2489, 2005.

[11] M. Parizeau and R. Plamondon, "Comparative analysis of regional correlation, dynamic time warping, and skeletal tree matching for signature verification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 7, pp. 710–717, 1990.

[12] R. Martens and L. Claesen, "Dynamic programming optimisation for on-line signature verification," in *Proceedings of the 4th International Conference on Document Analysis and Recognition (ICDAR '97)*, vol. 2, pp. 653–656, Ulm, Germany, 1997.

[13] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognition Letters*, vol. 26, no. 15, pp. 2400–2408, 2005.

[14] J. J. van Oosterhout, H. Dolfing, and E. Aarts, "On-line signature verification with hidden markov models," in *Proceedings of the 14th International Conference on Pattern Recognition (ICPR '98)*, vol. 2, p. 1309, 1998.

[15] R. Kashi, J. Hu, W. L. Nelson, and W. Turin, "A hidden markov model approach to online handwritten signature verification," *International Journal on Document Analysis and Recognition*, vol. 1, pp. 102–109, 1998.

[16] G. Rigoll and A. Kosmala, "A systematic comparison of on-line and off-line methods for signature verification with hidden markov models," in *Proceedings of the 14th International Conference on Pattern Recognition (ICPR '98)*, pp. 1755–1757, 1998.

[17] D. Muramatsu and T. Matsumoto, "An hmm on-line signature verifier incorporating signature trajectories," in *Proceedings of the 7th International Conference on Document Analysis and Recognition (ICDAR '03)*, 2003.

[18] B. Ly Van, S. Garcia-Salicetti, and B. Dorizzi, "On using the viterbi path along with hmm likelihood information for on-line signature verification," *IEEE Transactions on Systems, Man and Cybernetics, Part B*, vol. 37, no. 5, pp. 1237–1247, 2007.

[19] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: feature extraction and signature modeling," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2325–2334, 2007.

[20] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification-the state of the art," *Pattern Recognition*, vol. 22, no. 2, pp. 107–131, 1989.

[21] F. Leclerc and R. Plamondon, "Automatic signature verification: the state of the art," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 8, no. 3, pp. 643–660, 1994.

[22] D. Impedovo and G. Pirlo, "Automatic signature verification: the state of the art," *IEEE Transactions on Systems, Man and Cybernetics, Part C*, vol. 38, no. 5, pp. 609–635, 2008.

[23] C. F. Lam, D. Kamins, and K. Zimmermann, "Signature recognition through spectral analysis," *Pattern Recognition*, vol. 22, no. 1, pp. 39–44, 1989.

[24] Y. Sato and K. Kogure, "Online signature verification based on shape, motion and writing pressure," in *Proceedings of the International Conference on Pattern Recognition (ICPR '82)*, pp. 823–826, 1982.

[25] Z.-H. Quan, D.-S. Huang, X.-L. Xia, M. R. Lyu, and T.-M. Lok, "Spectrum analysis based on windows with variable widths for online signature verification," in *Proceedings of the International Conference on Pattern Recognition (ICPR '06)*, vol. 2, pp. 1122–1125, 2006.

[26] L. Nanni and A. Lumini, "A novel local on-line signature verification system," *Pattern Recognition Letters*, vol. 29, no. 5, pp. 559–568, 2008.

[27] I. Nakanishi, N. Nishiguchi, Y. Itoh, and Y. Fukui, "Multi-matcher on-line signature verification system in dwt domain," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E89-A, no. 1, pp. 178–185, 2006.

[28] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," *Pattern Recognition*, vol. 40, no. 3, pp. 981–992, 2007.

[29] D. Muramatsu and T. Matsumoto, "Effectiveness of pen pressure, azimuth, and altitude features for online signature verification," in *Proceedings of the International Conference on Biometrics*, pp. 503–512, 2007.

[30] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Addison-Wesley, Reading, Mass, USA, 1992.

[31] J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Target dependent score normalization techniques and their application to signature verification," *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 35, no. 3, pp. 418–425, 2005.

[32] A. Kholmatov and B. Yanikoglu, "SUSIG: an on-line signature database, associated protocols and benchmark results," *Pattern Analysis and Applications*, pp. 1–10, 2008.

[33] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, et al., "MCYT baseline corpus: a bimodal biometric database," *IEE Proceedings: Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 395–401, 2003.

[34] L. Nanni and A. Lumini, "Advanced methods for two-class problem formulation for on-line signature verification," *Neurocomputing*, vol. 69, no. 7–9, pp. 854–857, 2006.

[35] S. Garcia-Salicetti, J. Fierrez-Aguilar, F. Alonso-Fernandez, et al., "Biosecure reference systems for on-line signature verification: a study of complementarity," *Annals of Telecommunications*, vol. 62, no. 1-2, pp. 36–61, 2007.

[36] S. Schimke, C. Vielhauer, and J. Dittmann, "Using adapted levenshtein distance for on-line signature authentication," in *Proceedings of the International Conference on Pattern Recognition (ICPR '04)*, vol. 2, pp. 931–934, 2004.

[37] C. Vivaracho-Pascual, M. Faundez-Zanuy, and J. M. Pascual, "An efficient low cost approach for on-line signature recognition based on length normalization and fractional distances," *Pattern Recognition*, vol. 42, no. 1, pp. 183–193, 2009.