Handwritten Text Verification on Mobile Devices

Nilson Donizete Guerin Júnior, Flávio de Barros Vidal and Bruno Macchiavello
Department of Computer Science, University of Brasilia, Brasilia, DF, Brazil

Keywords: Handwriting Recognition, Biometrics, Mobile Device Authentication.

Abstract: In this work we propose an online verification system for both signature and isolated cursive words. The proposed system is designed to be used in a mobile device with limited computational capability. In the proposed scenario it is assumed that the user will use either his fingertip or a passive pen, therefore no azimuth or inclination information is available. Isolated words have certain desirable traits that can be more useful on a mobile device. Different isolated words can be used to verify the user in different applications, combining a knowledge-based security systems (i.e. passwords) with a behavioral biometric verification system. The proposed technique can achieve 4.39% of equal error rate for signatures and 6.5% for isolated words.

1 INTRODUCTION

The use of biometric systems has significantly increased in recent years. Applications of these systems can vary from identity authentication during secure transactions to granting physical access to certain location. The goal of a biometric system is to recognize an individual based on a set of unique attributes. These attributes are inherent characteristics of the individual, which gives biometric systems an advantage against systems based on knowledge (e.g. passwords) that can be forgotten, or tokens (e.g. badges, IDs) that can be lost (Impedovo and Pirlo, 2008). Biometric recognition based on physical attributes, like fingerprints, normally presents a higher performance than recognition based on behavioral characteristics. Nonetheless, behavioral attributes are less invasive, and some of them, like a person signature, are widely accepted as a legal mean to verify a person's identity.

A handwritten text biometric system can be classified into two categories: offline and online. Offline systems consist basically on the analysis of the shape information contained in the input image (Bulacu and Schomaker, 2007; Tang et al., 2013), while online systems can access features like trajectory, pressure and velocity which are more unique, making harder to forge an identity (Fierrez-Aguilar et al., 2005; Nanni and Lumini, 2008; Yanikoglu and Kholmatov, 2009; Sae-Bae and Memon, 2014; Zalasiński and Cpałka, 2013; Cpałka and Zalasiński, 2014). In both cases, as in most biometric systems, the users will be normally asked to be enrolled by providing one or more samples. Recognition is then performed by comparing the new sample to the previously stored. The recognition can be performed either to verify or identify certain individual. In verification mode the subject claims its identity, which is then authenticated. In identification task the subject's identity is established among those enrolled.

Feature extraction is an important part of a handwritten text verification system. Global features are related to the text as a whole, while local features, also referred as function-based, are measured at each point along the trajectory of the text. Systems based on global features have higher error rates than the function-based ones, on the other hand they have a much lower computational load and can be used as a first step in a hybrid (local-global) system (Yanikoglu and Kholmatov, 2009).

Handwritten signature has a long history as an identity authentication method, mostly due to the fact that signatures exhibit considerable inter-writer variability. Nowadays there is a growing need for security application in mobile devices (like touch screen laptops), where signature verification can substitute or complement other authentication methods. However, if the signature is compromised it is not easy for a person to create a new and different signature. Therefore, the use of isolated words for writer authentication in mobile devices can be more appropriate. Isolated words are easy to modify once the previous one has been compromised. The user can be requested to use a specific word or sentence, combining behavioral biometrics with knowledge-based systems. Furthermore, different words can be used for authentication during different actions. Nevertheless, isolated words

Guerin Júnior N., de Barros Vidal F. and Macchiavello B..
Handwritten Text Verification on Mobile Devices.
DOI: 10.5220/0005355200260033
In *Proceedings of the 10th International Conference on Computer Vision Theory and Applications* (VISAPP-2015), pages 26-33
ISBN: 978-989-758-091-8

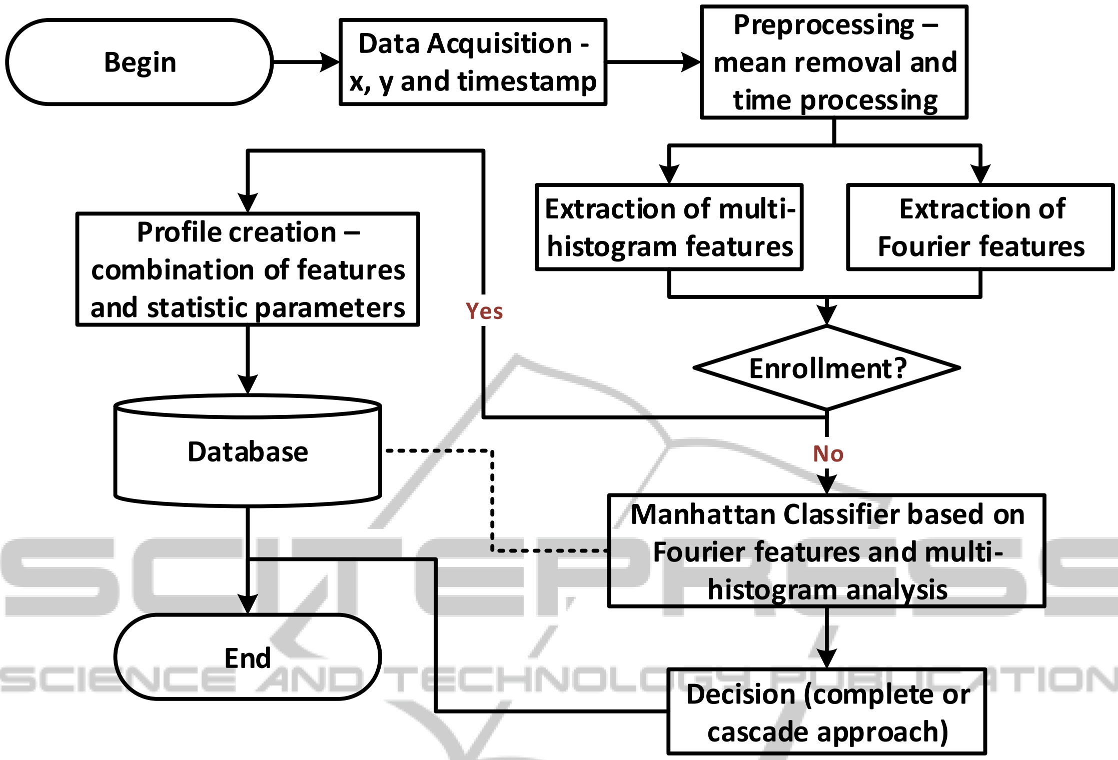


Figure 1: Architecture of the proposed system.

have fewer discrimination capacity than signatures, therefore low error rates are harder to achieve. Online handwritten recognition based on isolated words have received little attention in the literature. A previous work (Sesa-Nogueras and Faundez-Zanuy, 2012) focused on block uppercase letters, identifying the writer based on pen-down and pen-up strokes using information from an active pen found in traditional digitizers, that provides information like azimuth, and inclination. However, in a regular mobile device an active pen is not always available. A user will normally use a finger or a passive pen to write in his mobile device. Histograms of angles combined with pressure information has been used recently for signature verification on mobile devices (Sae-Bae and Memon, 2014).

In this work, we propose a global feature system, that works for both handwritten signature and isolated words. It is assumed that the user will use cursive handwritten, which is more natural than uppercase letters, and that the system will work on a mobile device without the use of an active pen. The proposed technique combines histogram of angles, velocity and a Fourier Transform analysis. Different from (Sae-Bae and Memon, 2014), we use one-dimensional $(1-D)$ histograms of angles to create several levels of discrimination. Moreover, pressure is not required as a feature, since it can change depending on the use of a passive pen or fingertip. An spectral analysis of the online text using Fast Fourier Transform (FFT) has been already proposed (Yanikoglu and Kholmatov, 2009). The main advantages of this technique is its capacity to compactly represent an online text, which leads to fast matching algorithms. However, the error-rates of FFT descriptors are not as good as other global methods. Here, a variation of the previously proposed FFT analysis is used along with histograms of angles. Finally, the proposed technique does not require any online training or elaborated matching algorithm which can limit its use in a power-constrained mobile device.

2 SYSTEM ARCHITECTURE

The general system architecture is composed of two main tasks: the enrollment and verification. In the first one, a person is registered in the system by donating M reference samples to create his profile. In the second, the person will be authenticated in the system by providing a sample and the user identification which is claiming to be. The architecture is described in Figure 1.

2.1 Data Acquisition

In this study, our main focus is handwritten text, signatures or cursive isolated words, captured by a mobile touch sensitive device without using any active pen. In the case of isolated words, the user can provide samples of several words, which later can be used to verify different actions.

To the best of our knowledge there's no available database for isolated cursive handwritten words in the proposed scenario, therefore we created one. Our database will be referred as LISA-01 [1] (from the Laboratory of Image and Audio Signals of the University of Brasilia). The device used to collect the cursive words was a Samsung tablet, model Galaxy Tab 7.0 Plus, with Operational System Android 4.1.2. The database is composed of 50 writers, each one donating 10 samples of 4 different words: “love", “December", “intelligence" and “pattern". Words could have few discontinuities, even though they should be predominantly cursive (see Figure 2). They were all written by fingertip.

Figure 2: Sample of word "pattern".

2.2 Preprocessing

Previous works reported loss of discrimination during recognition due to preprocessing tasks (Kholmatov and Yanikoglu, 2005). Therefore, we avoided any filtering during preprocessing.

The collected data can be seen as a vector of the form $V_j = [timeStamp_j, \hat{x}_j, \hat{y}_j]$, where $1 \leq j \leq N$, N is the number of points acquired for a certain word/signature, $timeStamp_j$ is the time in milliseconds (since the application started) when the point j was acquired and the pair $(\hat{x}_j, \hat{y}_j)$ represents the spatial coordinates.

Initially, we obtain the difference time vector by subtracting the first timestamp from all others: $[t_j] = [timeStamp_j - timeStamp_0]$. Then, we performed the mean removal from the spatial coordinates: $[x_j, y_j] = [\hat{x}_j - Mean(\hat{x}), \hat{y}_j - Mean(\hat{y})]$. This mean removal do not interfere with the histogram computation and it is necessary in order to obtain translation invariance on the Fourier descriptors.

[1]The vectors of the dynamic features and images are available at http://www.cic.unb.br/~fbvidal/htdb.

2.3 Feature Extraction

Histograms are widely used as feature sets in order to capture attribute statistics in several recognition tasks, for example, object recognition (Chaudhry et al., 2009), human action recognition (da Rocha et al., 2012) and off-line signature verification (Pirlo and Impedovo, 2013). Works applying histograms of features to on-line signature recognition can also be found elsewhere (Sae-Bae and Memon, 2014; Fierrez-Aguilar et al., 2005), however here we propose a novel use of histogram of angles along with Fourier analysis for on-line verification.

Given the feature vector $V_j = [t_j, x_j, y_j]$, $1 \leq j \leq N$, it is possible to derive other important information, by instance the angle/direction $\theta_j = \tan^{-1}\left(\frac{y_{j+1}-y_j}{x_{j+1}-x_j}\right)$, the magnitude $mag_j = \sqrt{x_{j+1} - x_j{}^2 + (y_{j+1} - y_j)^2}$, the velocity in both directions, $(v_x)_j = \frac{x_j - x_{j-1}}{t_j - t_{j-1}}$, $(v_y)_j = \frac{y_j - y_{j-1}}{t_j - t_{j-1}}$, and so on.

In our approach an on-line word or signature is represented by a set of histograms of θ_j, with values limited to $[-\pi, \pi]$, a velocity feature and Fourier descriptors. The set of histograms is defined as $H = \{h^1, h^2, \ldots h^K\}$, where each histogram h^i consists of angle counts divided into b^i bins, with $b^1 < b^2 < \ldots < b^i < \ldots < b^K$. For the remaining of the paper we will refer h^i as a histogram of level i. Since, the system will work with different words/signatures from different users, the optimal number of bins can vary. Therefore, the use of several levels can improve the system's performance in the presence of intra-user variability.

The Fourier descriptors were obtained using a technique inspired on a previous work (Yanikoglu and Kholmatov, 2009). We apply FFT and obtain a coefficient vector $\mathcal{F}(V_j) = [\mathcal{F}(x_j), \mathcal{F}(y_j)]$. These coefficients are normalize by their respective total magnitude, i.e. $\sum_{j=1}^{N} |\mathcal{F}(y_j)|$ for the vertical component and $\sum_{j=1}^{N} |\mathcal{F}(x_j)|$ for the horizontal component. We discard half of the spectrum, due to symmetry, and the DC component. The final step is to average two consecutive descriptors, to account for variations in the neighboring harmonics.

In order to obtain an equal number of Fourier descriptors, prior to FFT computation, we pad each sample with zeros. The size of the padded sample varies for each user and word/signature. It is set to

1.5 times the longest word/signature in the enrolled samples. Differently from (Yanikoglu and Kholmatov, 2009), this padding process will prevent for constant cropping of future samples during verification, thus avoiding loss of data. Also, we found no need for drift estimation as done in (Yanikoglu and Kholmatov, 2009). Since, the Fourier descriptors are used along with histogram information, no significant gain is obtained by performing drift correction. The first p coefficients of each sample generates the descriptor vector $F = [f_x, f_y]$.

As mentioned earlier, a velocity feature is also used. It has already been showed that velocity is a discriminative and helpful feature regarding signature verification (Rashidi et al., 2012). Our feature is computed as follows:

1. Compute the root mean square velocity of all points in a sample:

$$RMS\_Vel = \sqrt{\left(\frac{\sum_{j=1}^{N}(v_x)_j}{N}\right)^2 + \left(\frac{\sum_{j=1}^{N}(v_y)_j}{N}\right)^2}; \quad (1)$$

2. Evaluate the difference in velocity of two consecutive points, referred as $diff\_Vel$ (this feature will be related to acceleration);
3. Compute the root mean square of $diff\_Vel$, similar to (1), referred as RMS_Dif
4. Combine these two metrics into one value: $velFeature = 0.6 \times RMS\_Dif + 0.4 \times RMS\_Vel$.

2.4 Profile Creation

A profile is created when a new user registers M samples of a particular word/signature following the steps described below:

1. Compute the mean between all of the M provided samples of the velocity feature, $meanVelFeature$;
2. For each set $H^i = \{h_1^i, h_2^i, ..., h_M^i\}$ with b^i bins:
   (a) Calculate a matrix, $dMatrix$ of size $M \times M$, whose elements are given by $d_{m,n} = ||h_m^i - h_n^i||$, where $|| \bullet ||$ indicates the Manhattan distance between two vectors. Each line of this matrix represents a comparison between the jth sample with all other samples;
   (b) Calculate the column vector, $minVector$ of size M, where each element is the mean of the respective line in $dMatrix$, disregarding the self-comparisons;
   (c) Evaluate the following metrics: (i) the mean of the minimum value in each line of $dMatrix$, defined as $minVal^i$, which indicates the average distance between all nearest pairs of samples, (ii) $tempVal^i = minimum(minVector)$, which reflects the average distance of the sample that is closest to all others, and (iii) $maxVal^i$, the mean of the maximum value in each line of $dMatrix$, that measures the average distance between all farthest pairs of samples;
   (d) The sample that corresponds to $tempVal^i$ is also identified. This template sample will be the closest in average to all other samples and will be denoted by $tempSample^i$;
   (e) The statistics vector P_H^i, for level i, is defined as $P_H^i = \{minVal^i, tempVal^i, maxVal^i, tempSample^i, H\}$;
3. For the set of Fourier descriptors $F = \{F_1, F_2, ..., F_M\}$, a similar approach is performed and the statistics vector $P_F = \{minVal, tempVal, maxVal, tempSample, F\}$ is obtained.

The profile is then represented by the set $P = \{meanVelFeature, P_H, P_F\}$, where $P_H = \{P_H^1, P_H^2, ..., P_H^K\}$

2.5 Classifier

This stage is performed during verification and is inspired on a previous work (Kholmatov and Yanikoglu, 2005). Considering the query sample, denoted by S, and a profile P, for each set of histograms H^i in the profile and the corresponding query histogram H_S^i, a comparison is performed as follows:

1. Compute the column vector $diffQuery$, of length M, whose elements are given by $q_j = ||h_S^i - h_j^i||$, where $|| \bullet ||$ indicates the Manhattan distance between two vectors;
2. Select three values from $diffQuery$: the minimum (min_S), the maximum (max_S) and the difference to the corresponding $tempSample$ ($temp_S$);
3. Normalize those values by the respective components of profile P at level i: $min_S' = min_S/minVal^i$, $tempS' = temp_S/tempVal^i$ and $max_S' = max_S/maxVal^i$;

Note that min_S', $temp_S'$ and max_S' are highly correlated. Therefore, the three-dimensional vector can be reduced to one dimension using PCA (Principal component analysis). This will generate the resulting distance value:

$$histDistance^i = k_1 \times min_S' + k_2 \times temp_S' + k_3 \times max_S'.$$

For the set of Fourier descriptors F, a similar approach is performed and a unique $fourierScore$ is obtained. However, after several tests it was verified that the we could use fixed values $k_1 = 0.3870$, $k_2 = 0.3705$ and $k_3 = 0.2425$ without any significant loss in performance. Hence, differently from many proposals (Rashidi et al., 2012; Sesa-Nogueras, 2011; Sesa-Nogueras and Faundez-Zanuy, 2012; Zalasiński and Cpałka, 2013; Maiorana et al., 2012; Kholmatov and Yanikoglu, 2005), we do not require a training phase during user enrollment.

In previous works several techniques for features combination were presented (Damer et al., 2013; Gudavalli et al., 2012; Scheidat et al., 2011; Shekhar et al., 2014). Here, we use a score value based on a linear combination of the acquired features. Moreover, the proposed technique can be used in two ways: (i) the "complete approach", where the information obtained from all the different histograms levels, $histDistance$, is computed as the mean of all $histDistance^i$ and (ii) using the $histDistance^i$ values at each level in a "cascade approach". In the first case, we calculate the score $finalDistance = k_4 \times histDistance + k_5 \times fourierScore + k_6 \times velScore$, where $velScore = |meanVelFeature - velFeature_S|$. This method will yield better performance, the intra-user variability is minimized due to the average of the statistics, while the inter-user variability is maximized. After several empirical tests, we verified that the constants can be set as $k_4 = 0.29$, $k_5 = 0.57$ and $k_6 = 0.14$. This final score is compared to certain threshold, and the sample is considered to belong to the user if it is below that threshold.

The cascade approach can be used when the mobile device has limited computational capabilities or when it is operating in low-battery mode. A final score is computed at each level ($levelDistance^i = k_4 \times histDistance^i + k_5 \times fourierScore + k_6 \times velScore$), starting with the level with fewer number of bins. Once again, this value is compare to a threshold, if the sample is above that threshold we continue to the next level, otherwise the sample is considered to belong to that profile. As it can be noticed, in this approach the computational effort during authentication is reduced however it happens at the expense of error rate increment.

2.6 Decision

The decision stage is basically the comparison between the metric obtained in the classifying stage with a given threshold. Since we adopted a user-dependent normalization, it's possible to define a global threshold instead of finding optimal thresholds for each profile. In the cascade approach, there is a threshold for each group of histograms at level i. Again, in order to avoid specific optimization at each level, the same threshold used in the complete approach can be adapted to be used in the cascade approach. The set of thresholds T^i can be defined as $T^i = a^i \times T$, where $0 < a^1 < a^2 < ... < a^i < ... < a^K = 1$ and T indicates the global threshold.

3 EXPERIMENTS AND RESULTS

As mentioned in previous works, comparison between methods for signature verification is not easy (Yanikoglu and Kholmatov, 2009; Cpalka et al., 2014) mainly due to the difference in databases and proposed scenarios. Nevertheless, in this section we present the results of the proposed technique and compare them to previously reported results. For signature verification we used a widely adopted signature database, the MCYT-100 (Ortega-Garcia et al., 2003).

3.1 Experiments Setup

We use the following setup for our simulations:

- The number of reference samples, M, was set to 5 . This number of enrollment samples was also used in (Yanikoglu and Kholmatov, 2009; Cpałka and Zalasiński, 2014; Zalasiński and Cpałka, 2013);
- We used the set of bins numbers $B = \{6, 8, 10, 12, 14, 16\}$;
- We adopted $p = 30$ for the number of Fourier descriptors;
- Simulations were repeated 5 times on each database, raffling the samples used for composing the profiles and leaving the remaining ones for testing. This is a common practice (Yanikoglu and Kholmatov, 2009; Rashidi et al., 2012) in order to better evaluate the system;
- Results were measured using EER (Equal Error Rate), a widely used measure (Cpałka and Zalasiński, 2014; Kholmatov and Yanikoglu, 2005; Maiorana et al., 2012; Rashidi et al., 2012; Sesa-Nogueras, 2011; Sesa-Nogueras and Faundez-Zanuy, 2012; Yanikoglu and Kholmatov, 2009; Zalasiński and Cpałka, 2013);
- When using the LISA-01 database, we also raffled samples of other users to compose the forgeries ones;
- In MCYT-100 database, skilled forgeries for each user are available. Therefore, we evaluated the system considering that the forger has access to

the reference signature. Note, that in this scenario the expected ERR's are higher than using random forgeries.

3.2 Histograms Analysis

First, we analyze the performance of the proposed "complete" and "cascade" approaches. We ran several tests and selected a fixed the number of bins that yields the better overall results (referred as the "Best Histogram" mode). Then, we performed verification for all users, using only the histogram information. Table 1 shows the results.

Table 1: Scenarios of histogram analysis.

Kind of analysis	EER
Best histogram - 16 bins	14.17%
Complete approach	12.49%
Cascade approach	13.56%

From the results, it can be observed that both proposed techniques present an improvement over the use of a single histogram of angles.

3.3 Signature Evaluation

In Table 2 the results for signature verification using the MCYT-100 database of the proposed techniques and previous works are presented.

Even though the proposed techniques do not yield the best EER's, our results are adequate when compared to previous studies. However, it is important to notice that our technique does not require any complex training phase (Maiorana et al., 2012), complex $2-D$ histograms analysis (Sae-Bae and Memon, 2014), local features (Van et al., 2007) or the use of features from active devices (Maiorana et al., 2012).

3.4 Cursive Isolated Words Evaluation

In Table 3 we present the results from isolated cursive words using the LISA-01 database. In order to provide a comparison, we implemented a previous proposal for signature verification (Yanikoglu and Kholmatov, 2009) and applied to our isolated words database. The implemented proposal is based only on Fourier descriptors. Therefore, this comparison can show how the use of histograms of angles can adequately complement the use of Fourier descriptors.

As expected the ERR for isolated words is higher. This is due to the fact that isolated words have less discriminative power than signatures. Nevertheless, as mentioned earlier, isolated words possess desirable traits for use in mobile devices. The observed values of EER for each word separately in the complete approach were 7.2%, 5.78%, 8.6% and 4.42% for the words "December", "intelligence", "love" and "pattern", respectively, when considering forgeries from the same words. It means that the forger has already acquired the knowledge of the correct word. These rates become 4.8%, 3.86%, 6%, 3.86%, respectively, if the forgeries are raffled from random words (which can include the same word). This case leads to an EER of 4.63%. Note that the results suggest that shorter words have fewer discriminative power, as already noticed elsewhere (Sesa-Nogueras and Faundez-Zanuy, 2012; Sesa-Nogueras, 2011). In Fig. 3 the curves relating the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are depicted. The point of intersection represents the Equal Error Rate (EER) of the approaches. It's related to the word "pattern" in LISA-01 database, and it can be observed that the proposed techniques have better performance than the simple use of Fourier Descriptors.

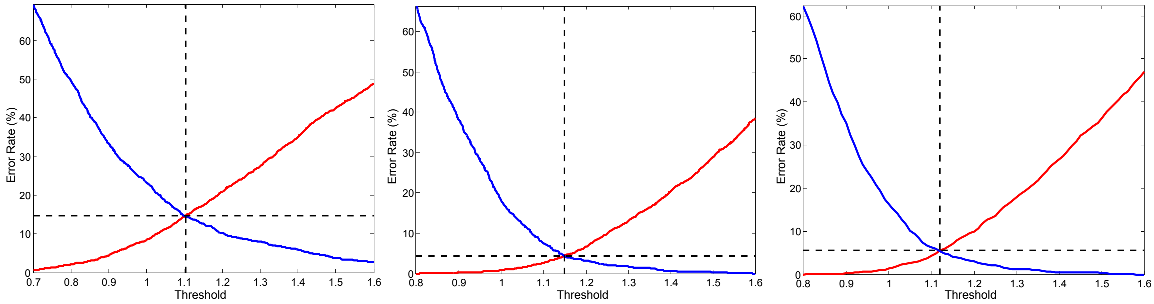
3.5 Computational Complexity

The system proposed here is based on extraction of global features. We performed an analysis on the frequency domain in order to compose Fourier descriptors vectors and a spatial analysis to create histograms of angles. A velocity feature is also computed. The asymptotic complexity for calculating the velocity feature is $O(N)$, since we pass over the feature vector a constant number of times.

In the case of histograms, we also perform $O(N)$, considering that we pass a constant number of times over the vector to create a fixed number of histograms with constant number of bins. The creation of the Fourier descriptor involves the computation of the FFT. The algorithm for this has asymptotic complexity $O(N \log N)$, also performed a constant number of times. The overall asymptotic system computational complexity is $O(N \log N)$.

4 CONCLUSIONS

We presented a method for both handwritten signatures and isolated cursive words to be used on mobile devices. The technique does not require any complex training or computation calculations, therefore it is adequate for the limited capabilities of a mobile device. The results show a good performance for both signatures and isolated words, without the use of features like azimuth, inclination or pressure that are dependent on the input device (active pen, passive pen or



(a) Fourier(Yanikoglu and Kholmatov, 2009) (b) Complete approach (c) Cascade approach

Figure 3: The relation of False Acceptance Rate (FAR, in red) and False Rejection Rate (FRR, in blue) related to a given threshold. The point of intersection, given by the dashed lines represents the Equal Error Rate (EER). Each plot relates to each of the approaches tested with respect to the word "pattern".

Table 2: Signature verification on MCYT-100 database.

Proposal	Features used	EER for skilled forgeries
Histogram + Quantizer (Sae-Bae and Memon, 2014)	x, y, time, pressure	4.02%
HMM + Likelihood (Van et al., 2007)	All available	3.37%
Polynomial (Maiorana et al., 2012)	All available	4.22%
Fourier (Yanikoglu and Kholmatov, 2009)	All available	10.89%
DCT + WT (Nanni and Lumini, 2008)	x, y, azimuth	9.80%
Our proposal (complete)	**x, y, time**	**4.39%**
Our proposal (cascade)	**x, y, time**	**4.64%**

Table 3: Results obtained in the LISA-01.

Proposal	Features used	EER for skilled forgeries
Fourier (Yanikoglu and Kholmatov, 2009)	x, y	17.19%
Our proposal (complete)	**x, y, time**	**6.5%**
Our proposal (cascade)	**x, y, time**	**7.18%**

fingertip). Future work will focus on adopting a better and systematic fusion method for combining the different scores (histogram, Fourier descriptors, etc.). Also it can be possible to analyze parts of the provided samples, instead of the complete word or signature, that may have more discriminative information between different users. Moreover, an analysis of the robustness of the system to external factors, such as word inclination, or user movement while writing, can be made. Finally, we can expand the LISA-01 database in order to include skilled forgeries.

REFERENCES

Bulacu, M. and Schomaker, L. (2007). Text-independent writer identification and verification using textural and allographic features. In *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pages 701–717.

Chaudhry, R., Ravichandran, A., Hager, G., and Vidal, R. (2009). Histograms of oriented optical flow and binet-cauchy kernels on nonlinear dynamical systems for the recognition of human actions. In *Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on*, pages 1932–1939. IEEE.

Cpałka, K. and Zalasiński, M. (2014). On-line signature verification using vertical signature partitioning. *Expert Systems with Applications*, 41(9):4170–4180.

Cpalka, S., Zalasinski, M., and Rutkowski, L. (2014). New method for the on-line signature verification based on horizontal partitioning. *Pattern Recognition*, 47(8):2652–2661.

da Rocha, T., De Barros Vidal, F., and Romariz, A. R. S. (2012). A proposal for human action classification based on motion analysis and artificial neural networks. In *Neural Networks (IJCNN), The 2012 International Joint Conference on*, pages 1–6.

Damer, N., Fuhrer, B., and Kuijper, A. (2013). Missing data estimation in multi-biometric identification and verification. In *Biometric Measurements and Systems* *for Security and Medical Applications (BIOMS), 2013 IEEE Workshop on*, pages 41–45. IEEE.

Fierrez-Aguilar, J., Nanni, L., Lopez-Peñalba, J., Ortega-Garcia, J., and Maltoni, D. (2005). An on-line signature verification system based on fusion of local and global information. In *Audio-and video-based biometric person authentication*, pages 523–532. Springer.

Gudavalli, M., Babu, A., Raju, S., and Kumar, D. S. (2012). Multimodal biometrics–sources, architecture and fusion techniques: An overview. In *Biometrics and Security Technologies (ISBAST), 2012 International Symposium on*, pages 27–34. IEEE.

Impedovo, D. and Pirlo, G. (2008). Automatic signature verification: the state of the art. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 38(5):609–635.

Kholmatov, A. and Yanikoglu, B. (2005). Identity authentication using improved online signature verification method. *Pattern recognition letters*, 26(15):2400–2408.

Maiorana, E., Campisi, P., La Rocca, D., and Scarano, G. (2012). Use of polynomial classifiers for on-line signature recognition. In *Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on*, pages 265–270. IEEE.

Nanni, L. and Lumini, A. (2008). A novel local on-line signature verification system. *Pattern Recognition Letters*, 29(5):559–568.

Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J.-J., Vivaracho, C., et al. (2003). Mcyt baseline corpus: a bimodal biometric database. *IEE Proceedings-Vision, Image and Signal Processing*, 150(6):395–401.

Pirlo, G. and Impedovo, D. (2013). Verification of static signatures by optical flow analysis. *Human-Machine Systems, IEEE Transactions on*, 43(5):499–505.

Rashidi, S., Fallah, A., and Towhidkhah, F. (2012). Feature extraction based dct on dynamic signature verification. *Scientia Iranica*, 19(6):1810–1819.

Sae-Bae, N. and Memon, N. (2014). Online signature verification on mobile devices. *Information Forensics and Security, IEEE Transactions on*, 9(6):933–947.

Scheidat, T., Vielhauer, C., and Fischer, R. (2011). Comparative study on fusion strategies for biometric handwriting. In *Proceedings of the thirteenth ACM multimedia workshop on Multimedia and security*, pages 61–68. ACM.

Sesa-Nogueras, E. (2011). Discriminative power of online handwritten words for writer recognition. In *Security Technology (ICCST), 2011 IEEE International Carnahan Conference on*, pages 1–8. IEEE.

Sesa-Nogueras, E. and Faundez-Zanuy, M. (2012). Biometric recognition using online uppercase handwritten text. *Pattern Recognition*, 45(1):128–144.

Shekhar, S., Patel, V. M., Nasrabadi, N. M., and Chellappa, R. (2014). Joint sparse representation for robust multimodal biometrics recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 36(1):113–126.

Tang, Y., Wu, X., and Bu, W. (2013). Offline text-independent writer identification using stroke fragment and contour based features. In *Biometrics (ICB), 2013 International Conference on*, pages 1–6.

Van, B. L., Garcia-Salicetti, S., and Dorizzi, B. (2007). On using the viterbi path along with hmm likelihood information for online signature verification. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 37(5):1237–1247.

Yanikoglu, B. and Kholmatov, A. (2009). Online signature verification using fourier descriptors. *EURASIP Journal on Advances in Signal Processing*, 2009:12.

Zalasiński, M. and Cpałka, K. (2013). New approach for the on-line signature verification based on method of horizontal partitioning. In *Artificial Intelligence and Soft Computing*, pages 342–350. Springer.