FEATURE-BASED DYNAMIC SIGNATURE VERIFICATION UNDER FORENSIC SCENARIOS

Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez and Javier Ortega-Garcia

Biometric Recognition Group - ATVS, Escuela Politecnica Superior
Universidad Autonoma de Madrid
Avda. Francisco Tomas y Valiente, 11 - Campus de Cantoblanco - 28049 Madrid, Spain
{ruben.tolosana, ruben.vera, julian.fierrez, javier.ortega}@uam.es

ABSTRACT

Nowadays forensic document examiners (FDE) have to analyse more and more signatures captured by digital devices. While they can still use the static image of the signature, it has been proven that the dynamic information contains very discriminative information. This paper is focused on dynamic signature recognition applied to forensic scenarios. An automatic featured-based or global recognition system is considered as some of the features extracted by these systems could be used by FDE in their work. A system comprised of 117 global features is proposed and evaluated with BioSecure DS2 database. A subset of 40 features is selected by SFFS algorithm as the optimal feature vector in the development phase. Results of 10.6% EER are achieved for skilled forgeries which improve previous results using similar approaches. In addition, a set of selected features have been analysed statistically for genuine and forged signatures in order to obtain useful information that could be used by forensic experts in their reports.

Index Terms— Biometrics, dynamic signature, feature-based system, global features, SFFS, statistical analysis, BioSecure

1. INTRODUCTION

Signature is one of the most socially accepted biometrics traits. It is due to the fact that signature has been used in financial and legal transactions for centuries [1]. Nowadays, signatures can be captured easily with many devices (i.e. Pen tablets, PDAs, Grip Pen, Smartphones). For this reason the success of this biometric trait has increased a lot in the last years. However, one of the main challenges in signature verification is related to the signature variability. While the signatures from the same users show considerable differences between different captures (high intra-class variability), skilled forgers can perform signatures with high resemblance to the users signature (low inter-class variability).

There are two main classes of signature verification systems depending on the information extracted from the signature. Off-line systems only use the static signature image to extract features, while on-line systems employ digitized time functions of the captured signature and can achieve better recognition performance [2].

In the forensic field, traditionally only off-line systems have been considered [3, 4]. This is starting to change as nowadays digital signature devices are spreading in the commercial sector to facilitate payments and also in banking to facilitate the digital storage of all the signed paperwork. Therefore, forensic document examiners (FDEs) are being required to provide forensic evidence to determine the authenticity of handwritten signatures written on digitizing tablets [5], which can provide an static image of the signature but also, and most importantly, contain the dynamic information of at least the X and Y spatial coordinates.

Regarding on-line signature systems there are two main approaches for feature extraction: i) *feature-based* systems, which extract global information from the signature (e.g. signature duration, number of pen ups, etc.) in order to obtain a holistic feature vector [6]. On the other hand, *function-based* systems use the signature time functions (e.g. X and Y coordinates, pressure, etc.) for verification [7]. Traditionally, function-based systems have achieved better recognition performance than feature-based systems [6, 8].

This paper is focused on the analysis of a feature-based signature recognition system for forensic applications. Some of the global information extracted with these systems could be used by forensic examiners in their work as they can have a physical meaning, such as the duration, or the average velocity of the signatures (genuine and forgeries).

In this paper, we propose a novel feature-based system comprised of a total number of 117 global features. Seventeen new features are added to a system obtained from previous works [6]. Experiments are carried out using BioSecure DS2 database with 120 users. The low amount of available training data motivates the usage of feature selection techniques, being the Sequential Forward Feature Selection (SFFS) [9] one of the best performing methods reported [10]. A subset of 40 features is finally obtained which includes 6 of the new pro-

978-1-4799-8105-2/15/$31.00 © 2015 IEEE

posed features and automatic results are presented. Additionally, an statistical analysis of the most discriminative selected dynamic features is carried out for the populations of genuine and forged signatures in order to provide background information that can be used by forensic document examiners.

The remainder of the paper is organized as follows. Section 2 describes the databases used in the experimental work carried out. Section 3 describes the feature-based signature verification system proposed. Section 4 reports the experimental work, Section 5 describes an statistical analysis carried out on a set of selected global features. Finally, Section 6 draws the final conclusions.

2. SIGNATURE DATABASE

BioSecure Multimodal Database (BMDB) [11, 12] is used in the experiments. In particular, the subcorpus DS2 captured using a digitizing pen tablet WACOM Intuos 3 A6 digitizer at 100 Hz with a subset of 120 users is considered in the experimental work reported in this paper. Fig. 1 shows the capturing process of BioSecure DS2 and an example of a genuine and a forgery signatures contained in DS2 and considered in the experimental work reported in this paper.

The available information in Biosecure DS2 is the following: X and Y coordinates, pressure, pen orientation (azimuth and altitude angles) and timestamp information. Information of pen orientation was not considered in the experiments because this information is not available in most of the capture devices nowadays (e.g. smartphones, tablets).

Signatures of Biosecure DS2 were captured in two sessions with a gap of 2 months between them. A total of 30 genuine signatures and 20 skilled forgeries are available per user. The users had visual access to the dynamics of signing process of the signatures they had to forge.

Normalization based on mean subtraction of X and Y coordinate are applied due to the way that signatures were captured in the device. This provides a better performance in the system.

3. DYNAMIC SIGNATURE VERIFICATION SYSTEM

3.1. Global Signature Verification System

A feature-based or global signature verification system is considered. In this work, we analyze an extended set of 117 features, of which 100 were used in previous works [6], and here we propose 17 new features (see Table 1). Most of the new features are pressure-related, while some others have been extracted from related works [5]. The whole set of 117 features can be divided in five categories corresponding to the following magnitudes (the numbering of the first 100 features is the same as in [6]):

- **1. Time** (25 features), related to signature duration, or timing of events such as pen-ups or local maxima.

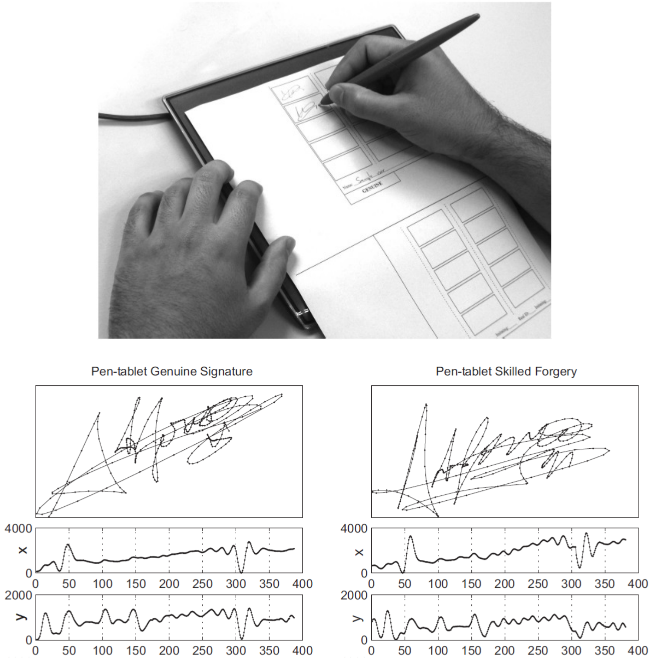

Fig. 1. Top shows the capturing process of BioSecure DS2 with WACOM Intuos 3, and bottom shows an example of a genuine and a forgery signatures contained in DS2 and considered in the experimental work reported in this paper.

- **2. Kinematic** (27 features), from the first and second order time derivates of position time functions, like average speed or maximum speed. In this category two news features have been added: 116-117.

- **3. Direction** (18 features), extracted from the path trajectory like the starting direction or mean direction between pen-ups.

- **4. Geometry** (32 features): associated to the strokes or signature aspect-ratio.

- **5. Pressure** (15 features): associated to pressure information like the mean pressure or number of pen-downs samples. This category was not considered in previous works. The numbering of these new features are: 101-115.

Mahalanobis distance is used to compare the similarity between a signature and a claimed user model. A user model is created from a training set of signatures. This model is defined as $C = (\mu,\Sigma)$, where μ is a feature vector with the mean of feature vectors extracted from each signature of this user and Σ is a diagonal covariance matrix. The matching score is obtained as the inverse of the Mahalanobis distance between the input signature feature vector x and the claimed user model C:

$$s(x,C) = \left((x-\mu)^T(\Sigma)^{-1}(x-\mu)\right)^{-1/2} \tag{1}$$

#	Feature Description	#	Feature Description
101	average pressure $\overline{p}$	102	median pressure
103	N (Pen Downs samples)	104	N (Pen Ups samples)
105	median N (Pen Ups samples) individually	106	average N (Pen Ups samples) individually
107	median N (Pen Downs samples) individually	108	average N (Pen Downs samples) individually
109	$\overline{p}$ / p_{max}	110	($\overline{p}$ - p_{min}) / $\overline{p}$
111	median pressure last pen-down	112	average pressure last pen-down
113	median pressure first pen-down	114	average pressure first pen-down
115	(p_{max} - p_{min}) / $\overline{p}$	116	average velocity $\overline{v}$
117	average acceleration $\overline{a}$		

Table 1. Set of 17 global features proposed in this work. N denotes number of events. Note that some symbols are defined in different features of the table (e.g. $\overline{p}$ in feature 109 is defined in feature 101). The first 15 features are pressure-related. The last two features are kinematic-related.

If the score $s(x, C)$ is above a specific threshold, the signature is considered genuine. On the contrary it is rejected by the system.

3.2. Feature extraction

The small available number of training signatures and the low amount of samples per signatures is the typical case in a signature verification system in practical applications. For this reason, due to the curse of dimensionality [13] a subset of the 117 global features has to be chosen in order to improve the performance of the system.

Sequential Forward Floating Search (SFFS) has been considered. This algorithm obtains a suboptimal solution since it does not account for all the possible feature combinations. This algorithm considered correlations between features. This is the main goal of this algorithm. The system EER has been chosen as the optimization criteria.

4. EXPERIMENTAL WORK

4.1. Experimental protocol

User models are trained with the 5 first genuine signatures of the first session, while the remaining 15 genuine signatures of the second session are left for testing.

Skilled forgery scores (the case when a forger tries to imitate the signature of another user of the system) are obtained comparing the user model against the 20 skilled forgeries available for the same user.

Random forgery scores (the case when a forger uses his own signature claiming to be another user of the system) are obtained comparing the user model to one genuine signature of the second session of the remaining users.

The first 50 users of the databases are used for development and training the system, while the remaining 70 users are left for evaluating the system.

4.2. Development Experimental Results

Feature selection is performed on the development set of 50 users. SFFS algorithm has been implemented in order to improve the EER of the system for both skilled and random forgeries cases. A subset of 40 features was obtained. Most of the features chosen in the optimal feature vector are kinematic-related (14 features) and geometry-related (11 features). Only 3 direction features are presented in the optimal vector. This may be due to the fact that no rotation normalization techniques have been performed in our experiments. Six of the features proposed in this paper, which have not been considered in previous works [6], have been selected by the SFFS algorithm (Table 2). This proves the importance of pressure-related features.

Features
101, 102, 103, 109, 116, 117

Table 2. New features considered in this work selected by SFFS algorithm.

4.3. Validation Experimental Results

To validate the implemented system, we compute the verification performance on the remaining 70 users of the database selecting the best feature vector obtained on the development phase. The system performance is represented using DET plots as shown in Fig. 2.

As can be seen, the performance of the system in the skilled forgeries case (EER = 10.66%) and random forgeries case (EER = 6.95%) is in the same range than previous works using a similar experimental protocol [14], achieving slightly better performance for the most critical case of skilled forgeries, as the random forgeries would be much easier to detect by a forensic expert. In this case 6 of the 17 proposed features are considered showing the benefits of using pressure information.

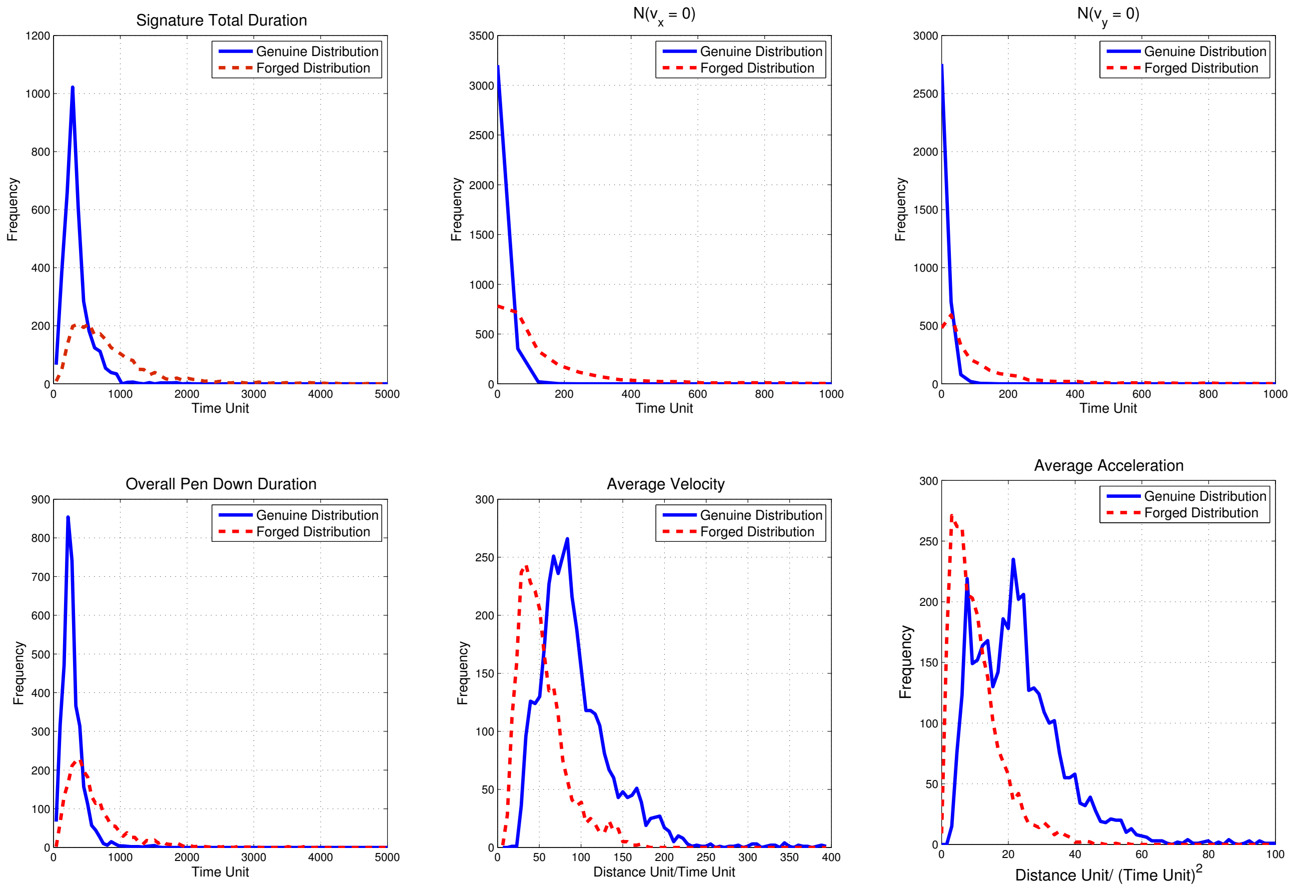

Fig. 3. Frecuency histograms of set of 6 selected features: duration, number of samples with V_x and V_y = 0, overall pen down duration, average velocity and average aceleration.

5. STATISTICAL ANALYSIS OF SELECTED FEATURES

In this section, a subset of 6 features of the 40 selected by SFFS algorithm have been statistically analysed. These features, which beside have provided the best individual EER, can be used by forensic experts when analysing dynamic signatures as they also have a physical meaning. The analysis of global features is carried out using frequency histograms using for that the whole dataset (120 users). The analysis is focused on genuine and skilled forgeries. Fig. 3 shows the frequency histograms for each global feature selected.

- **Signature total duration:** The frequency histogram (Fig. 3) indicates that a questioned signature is most likely to be a forged counterpart (with 96.9% probability) if the signature total duration is more than 1000 time units (i.e. more than 1000 × 10 ms = 10 seconds).
- **N (v_x = 0):** The frequency histogram (Fig. 3) indicates when the number of times that v_x = 0 of a questioned signature is above 120 times unit, is most likely to be a forged specimen with 99.4% probability.
- **N (v_y = 0):** The frequency histogram (Fig. 3) for this feature shows a shape similar to N (v_x = 0). From the frequency histogram, we can deduce that a questioned signature is most likely to be a forged counterpart (with 99.5% probability) if the number of N (v_y = 0) is more than 100 times units.
- **Overall Pen Down Duration:** The frequency histogram (Fig. 3) represents that overall pen down duration for genuine signatures are lower compared with forgers. This results agrees with previous works [5]. The graph indicates that a questioned signature is most likely to be a forged counterpart (with 94.7% probability) if the overall pen down duration is above 1000 time units (i.e. more than 1000 × 10 ms = 10 seconds).
- **Average Velocity:** The frequency histogram (Fig. 3) indicates that a questioned signature is most likely to be a genuine counterpart (with 99.2% probability) if the average velocity is more than 175 distance units/(time unit).
- **Average Acceleration:** The frequency histogram (Fig.

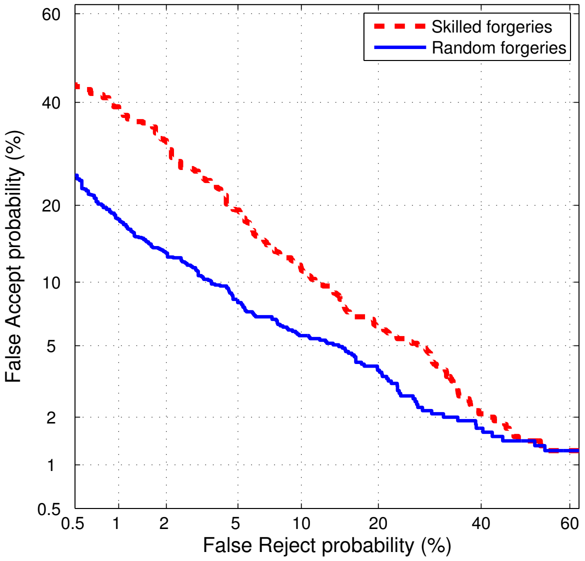

Fig. 2. DET curves for the proposed feature-based signature recognition system on the evaluation set of BioSecure DS2.

3) indicates when the average acceleration of a questioned signature is above 45 distance units/(time unit)^2, is most likely to be a genuine specimen with 98.0% probability.

A similar statistical analysis was carried out in [5] for a different set of features. Only the overall pen down duration is considered in both studies showing different time durations, but the main reason for that is that in [5] signatures belong to a Malaysian population, while in BioSecure an European population is considered.

6. CONCLUSIONS

Signatures captured from digital devices are started to being used by forensic document experts due to the deployment of these devices in many applications. This paper has proposed and analysed a feature-based signature verification system in order to extract useful information that could be used by FDE in their work when analysing dynamic signatures.

A novel feature-based signature system has been proposed containing a set of 117 global features, of which 17 are novel from previous works. Most of these features are related to pressure information not consider previously. Then a feature selection algorithm (SFFS) has been applied in order to extract an optimal set of features (40 in this case). Six of the 17 proposed features have been selected, which implies that pressure is a discriminative information to take into account in dynamic signature recognition. Recognition experiments have been performed on BioSecure DS2 database obtaining 10.66% EER for skilled forgeries and 6.95% EER for random forgeries.

The last part of the paper has reported an statistical analysis of a set of 6 selected features. Feature values have been calculated for 120 users of the database for genuine and forged signatures extracting some information that could be useful for forensic experts in their work when analysing signatures captured from digital devices. For example, some of the time patterns like the signature total duration can be very discriminative (regarding genuine or forgery). In the population examined, a questioned signature is most likely to be a forged counterpart (with 96.9% probability) if the signature total duration is more than 10 seconds.

7. ACKNOWLEDGMENT

This work has been partially supported by project Bio-Shield (TEC2012-34881), Cecabank and Catedra UAM-Telefonica.

8. REFERENCES

[1] 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.

[2] Vivian L. Blankers, C. Elisa van den Heuvel, Katrin Franke, and Louis Vuurpijl, “Icdar 2009 signature verification competition.,” in *Proc. ICDAR*. 2009, pp. 1403–1407, IEEE Computer Society.

[3] L. Alewijnse, “Forensic signature examination,” in *Tutorial at Int. Workshop on Automated Forensic Handwriting Analysis (AFHA)*, 2013.

[4] B. Found and D. Rogers, “Documentation of forensic handwriting comparison and identification method: A modular approach,” *Journal of Forensic Document Examination*, vol. 12, pp. 1–68, 1999.

[5] S.M. Ahmad, L.Y. Ling, R.M. Anward, M.A. Faudzi, and A. Shakil, “Analysis of the effects and relationship of perceived handwritten signatures size, graphical complexity, and legibility with dynamic parameters for forged and genuine samples,” *Journal of Forensic Sciences*, vol. 58, pp. 724–731, 2013.

[6] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Pealba, J. Ortega-Garcia, and D. Maltoni, “An on-line signature verification system based on fusion of local and global information,” in *Proc. 5th IAPR Intl. Conf. on Audio- and Video-based Biometric Person Authentication, AVBPA*. July 2005, vol. 3546 of *LNCS*, pp. 523–532, Springer.

[7] J. Fierrez, 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, December 2007.

[8] M. Martinez-Diaz, "Dynamic signature verification for portable devices," M.S. thesis, Universidad Autonoma de Madrid, November 2008.

[9] J. Novovicov P. Pudil and J. Kittler, "Floating search methods in feature selection.," *Pattern Recognition Letters*, vol. 15, no. 10, pp. 1119–1125, 1994.

[10] A. Jain and D. Zongker, "Feature selection: Evaluation, application, and small sample performance.," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 2, pp. 153–158, 1997.

[11] J. Ortega-Garcia et. al., "The multi-scenario multi-environment biosecure multimodal database (BMDB)," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 32, no. 6, pp. 1097–1111, June 2010.

[12] N. Houmani et. al., "Biosecure signature evaluation campaign (bsec'2009): Evaluating online signature algorithms depending on the quality of signatures," *Pattern Recognition*, vol. 45, no. 3, pp. 993 – 1003, 2012.

[13] S. Theodoridis and K. Koutroumbas, *Pattern recognition.*, Academic Press, 1999.

[14] M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally, "Mobile signature verification: Feature robustness and performance comparison," *IET Biometrics*, 2014.