Dynamic Signature Verification on Smart Phones

Ram P. Krish, Julian Fierrez, Javier Galbally, and Marcos Martinez-Diaz

Biometric Recognition Group - ATVS, EPS - Univ. Autonoma de Madrid
C/ Francisco Tomas y Valiente, 11 - Campus de Cantoblanco - 28049 Madrid, Spain
{ram.krish,julian.fierrez,javier.galbally,marcos.martinez}@uam.es

Abstract. This work is focused on dynamic signature verification for state-of-the-art smart phones, including performance evaluation. The analysis was performed on database consisting of 25 users and 500 signatures in total acquired with Samsung Galaxy Note. The verification algorithm tested combines two approaches: feature based (using Mahalanobis distance) and function based (using DTW), and the results are shown in terms of EER values. A number of experimental findings associated with signature verification in this scenario are obtained, e.g., the dominant challenge associated with the intra-class variability across time. As a result of the algorithm adaptation to the mobile scenario, the use of a state-of-the-art smart phone, and contrarily to what has been evidenced in previous works, we finally demonstrate that signature verification on smart phones can result in a similar verification performance compared to one obtained using more ergonomic stylus-based pen tablets. In particular, the best result achieved is an EER of 0.525%.

Keywords: Biometrics, dynamic signature verification, smart phones, Mahalanobis distance, Dynamic Time Warping (DTW).

1 Introduction

Dynamic (or on-line) handwritten signature is one of the modalities within biometrics that has vital importance in terms of establishing the identity of an individual, mainly because of the social and legal acceptance of handwritten signatures as a means for person identification in the day-to-day life [1]. The latest innovations in touch screen technologies have provided a feasible environment for dynamic signature verification in smart phones and mobile scenarios.

Despite the fact that the technology innovations have made it to a point where dynamic signature acquisitions is easy in smart phones, inherently signature verification faces some challenges which are in general applicable to either smart phones or more ergonomically designed signature pads. The latter scenario (i.e., pen-based digitizing tablets) is commonly studied in the signature verification literature [1]. The purpose here is to adapt established technology previously developed for digitizing tablets for smart phones, and then evaluate its performance and discuss some of its particularities.

J.M. Corchado et al. (Eds.): PAAMS 2013 Workshops, CCIS 365, pp. 213–222, 2013.

More specifically, two of the challenges faced in signature verification are *intra-class* variability where the individual has slight variations in their own signature writing styles over a period of time, and *inter-class* variability where some other person tries to mimic or simulate the signature of an individual to get an illicit access through a signature verification system. Traditionally, it has been thought that these sources of variability, specially the intra-class variability, is much higher in mobile scenarios compared to desktop digitizing tablets for signature verification, which results in degraded verification performance in mobile scenarios [2]. Nevertheless, this comparison has always been evidenced using limited mobile acquisition devices, far from the capabilities of state-of-the-art touch-based and stylus-based smart phones [3].

With regard to the inter-class variability, forgeries can be classified as two types, *random* forgeries and *skilled* forgeries. In *random* forgeries the forger has no information regarding the target signature, whereas in case of *skilled* forgeries the forger has knowledge about the target signature [1]. In the present work, only random signatures are considered.

With respect to the kind of information used in the recognition process, the signature verification can be classified into *feature* based systems and *function* based systems [4]. In feature based systems, a set of global features derived from the signature sample is used, whereas in function based systems, temporal sequences which encapsulate the local properties of the signature samples are used.

As introduced before, in this paper we present the results of the adaptation of an already existing dynamic signature verification algorithm for smart phones. As with any technology, there are some pros and cons associated with smart phones in the context of signature verification, though there is a growing interest in the use of portable devices for personal authentication. For signature verification, one advantage is related to the acquisition hardware, as with touch or stylus based smart phones there is no need for specialized external hardware for signature recognition. Most smart phones come with enough computing power, good quality touch screens and supports pen based input which makes them a feasible platform for dynamic signature verification.

Coming to the challenges, usually smart phones do not provide big display areas which affects user interaction and leads to large intra-class variability, the quality of the signature acquisitions can show high disparity based on the quality of the touch screens and the amount of information that can be captured is limited as pressure, pen-azimuth and other attributes which could lead to improved performance cannot be captured. Finally, in smart phones it is also important to consider the security of the templates [5].

As also introduced before, the public domain evaluations of dynamic signature verifications like BioSecure Multimodal Evaluation Campaign (BMEC-2007) [3], and BioSecure Signature Evaluation Campaign (BSEC'2009) [2] have shown that the performance of dynamic signature verification with databases captured on handheld devices are significantly lower compared with databases captured on ergonomically designed signature pads or tablet PCs. The main reasons for such

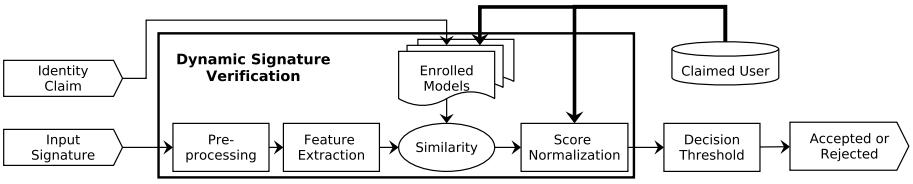

Fig. 1. General architecture of dynamic signature verification system

performance variations are the challenges discussed previously, such as small display area, quality of touch screen sample acquisitions and limited attributes of the samples acquired.

This paper is structured as follows. The general architecture of a dynamic signature verification system is described briefly in Section 2, and the hybrid system combining Mahalanobis distance and DTW used in the experimental work is described in Section 3. Next the database, experiment protocol and results are presented in Section 4, and conclusions drawn in Section 5.

2 Dynamic Signature Verification

The general architecture adopted by most dynamic signature verification systems is depicted in Fig. 1. The various stages and techniques involved are summarized as follows:

1. *Data Acquisition:* The dynamic signature data is in general acquired using devices like digitizing tablets or through the touch screen technologies provided on Tablet PCs, PDA or Smart Phones. The dominant attributes captured are x and y pen positions, and their timestamps. Depending on the functionality provided by the device, other attributes such as pressure, pen-azimuth, pen-up positions, etc can also be captured.
2. *Acquisition Rate:* Most of the devices used for dynamic signature acquisition operate between 100 to 200 samples per second. This sampling frequency is considered to be an accurate discrete time representation of the signature, which is justified by the fact that the bio-mechanical sequence related with such activity operates at a maximum frequency range of 20-30 Hz.
3. *Feature Extraction:* The performance of any biometric system depends largely on how well we can extract various types of discriminant features from the given sample. For dynamic signature data, the methods are traditionally classified into two : *feature-based* which use a set of global features, and *function-based* which use temporal sequences [1].
4. *Enrollment:* Depending on the methodology chosen for matching, and the number of training signatures available, the way signatures are enrolled can be classified into *reference-based* where features extracted from the signature are stored as templates, and *model-based* where a statistical model representing the signatures is generated [1].

5. *Similarity Computation:* In feature-based systems, the similarity score is calculated using Euclidean distance or Mahalanobis distance, whereas in a function-based system, the similarity score is calculated using Dynamic Time Warping (DTW) or Hidden Markov Models (HMM). Traditionally function-based systems have in general shown to perform better than feature-based systems.
6. *Score Normalization:* The similarity scores could be normalized to a given range of values. Score normalization helps when multiple algorithms are used in a system and eventually the scores need to be fused for a final decision.

2.1 Applications and Commercial Systems

A wide variety of applications with commercial importance can be designed over the concept of dynamic signature verification. In general, the main applications cover signature forensics, signature authentications, signature surveillance, digital rights management based on signatures and biometric cryptosystems based on signatures. More specifically, in a smart phone scenario which also serves as a computing platform, the possible applications could be payments in commercial environments, legal transactions, user logins, client validations and cryptobiometrics

There are also many commercial companies selling products designed based on dynamic signature verification. To mention a few of them, Sigma Technologies[1], Communication Intelligence Corporation, SOFTPRO and Cyber-SIGN [1].

3 Verification System Used in This Work

The verification system used in this work combines both feature-based and function-based approaches. The architecture of the hybrid system used in this work is shown in Fig. 2.

In the feature-based system, a set of global features are extracted from the given signature sample as presented in [6]. This feature set comprises 100 global features that include many of the features previously studied in the literature. These features can be divided into four categories based on their inherent properties, namely *time* based, *speed and acceleration* based, *direction* based and *geometry* based. More detailed explanation regarding these features can be found in [3].

To adapt the given feature set into the scenario of smart phones, a feature selection that minimizes the EER is performed using Sequential Forward Feature Selection (SFFS) on this 100 feature global set, which also reduces the dimensionality of the feature vector for the current scenario. This also helps optimizing the run time computational complexity of the system in general.

Normalization is performed on all the global features using *tanh* normalization [7], and the Mahalanobis distance is computed for the similarity score as explained in [8][9].

[1] `http://www.sigmatechnologies.es`

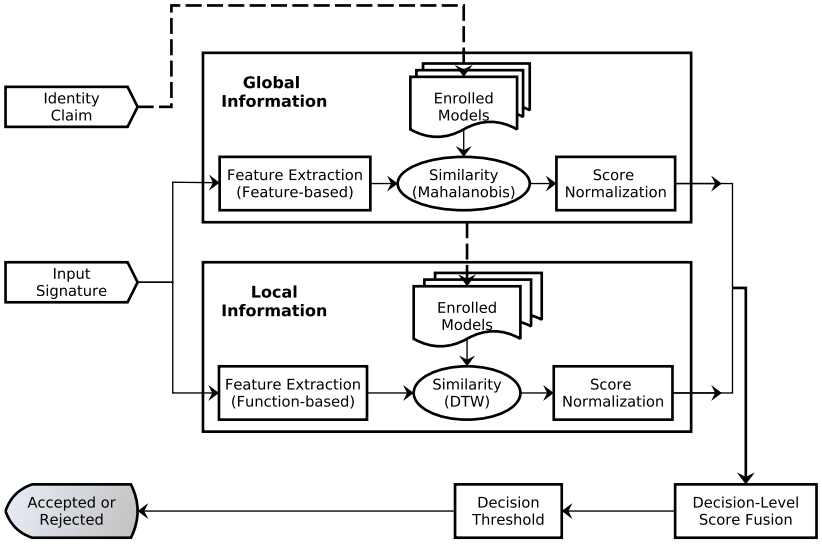

Fig. 2. The hybrid system combining features and functions used in this experiment

Function-based approaches are in general classified into *local* and *regional* based on the kind of matching strategy used. In *local* approach, time functions are directly matched using some elastic matching technique, whereas in *regional* approaches, the time functions of the signature are segmented into regions and their corresponding feature vectors are matched using Hidden Markov Models.

In this work, a *local* approach is employed and the matching is performed using Dynamic Time Warping. From the given signature sample, a set of time functions and their first and second derivatives are used as the feature set which is explained in [10]. It is also shown in this work that the contributions made by second derivatives in general are not so good, so an optimal subset of the second derivatives based on their discriminative power is used.

The score generated using DTW is normalized using *tanh* normalization, and the final match score is obtained as a weighted average of both Mahalanobis distance and DTW elastic distance.

4 Experiments

The signature samples for this experiment are acquired using Samsung Galaxy Note. The database is locally collected within our research lab and comprises 25 users and 20 signatures per user which totals to 500 signatures for the database. The acquisition device and some example signatures are shown in Fig. 3.

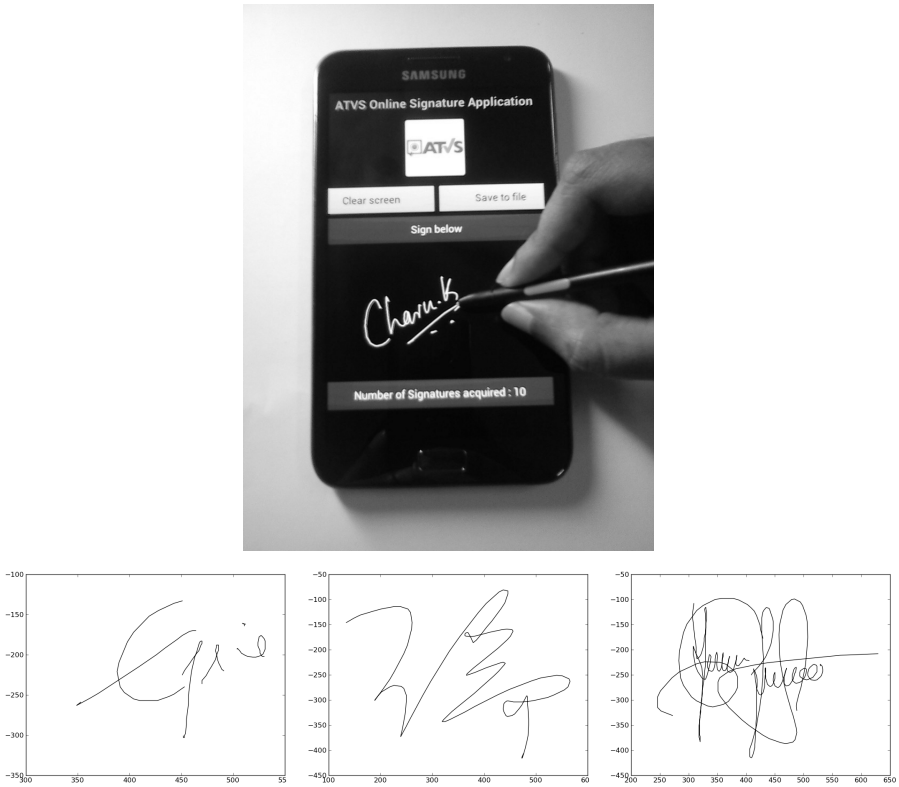

Fig. 3. Acquisition software running on Samsung Galaxy Note and example signatures

4.1 Acquisition Protocol

The signatures are captured in two different sessions with an average gap of 5 days between them, and each session involves two different phases.

In the first acquisition session, 5 signatures are first acquired on Samsung Galaxy Note (first phase) then the user is given a short time break, then again 5 signatures of that particular user are acquired (second phase). So, in the first session, 10 signatures of each user are acquired. The second acquisition session also repeats the same procedure.

The number of signature samples totals to 20 signatures per user. Total number of signatures in the database equals 500 signatures (25×20).

4.2 Evaluation Protocol

The signatures collected from the first acquisition session are used for enrollment in three different ways:

1. First three signatures of the first phase, named as Galaxy3.
2. First five signatures of the first phase, named as Galaxy5.
3. First three signatures of the first phase, and two signatures of second phase, named as Galaxy32.

As test signatures we used the signatures acquired from first session as for Experiment 1, and the signatures from the second session for Experiment 2 (in both cases all the signatures not used for enrollment). In our experiments, we considered only random forgeries, comparing the enrolled model at hand with all test signatures from all the other subjects for generating the impostor scores. Evaluation using skilled forgeries will be conducted in future research.

4.3 Experiment 1 : Intra-session Matching

In this experiment, only the signatures acquired in the first session of the database acquisitions are used. The enrolled models, as well as the signatures against which the system is tested come from the first session. Since all the signature samples come from the first session, the typical intra-class variations across time are not totally captured in this experiment. Fig. 4 shows the system performance of this experiment.

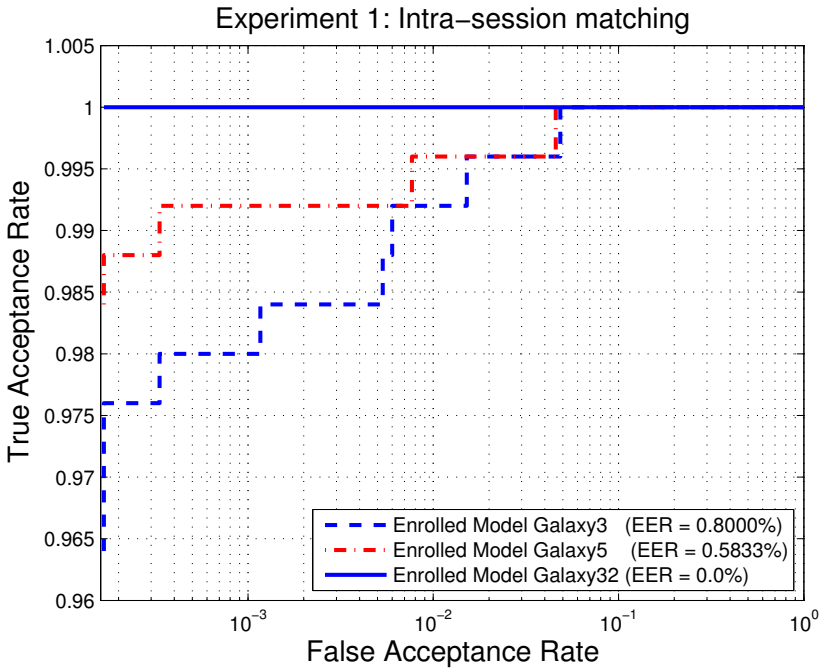

Fig. 4. ROC curve for Experiment 1, which considers enrollment and test signatures from the same session

4.4 Experiment 2 : Inter-session Matching

In this experiment, the enrolled model comes from the first session of database, and the test signatures come from the second session of database acquisition. This experiment helps us to understand better about the problem of intra-class variability of individual users with time variability because the signatures in the second session are collected with an average gap of 5 days with respect to first session. Fig. 5 shows the system performance of this experiment.

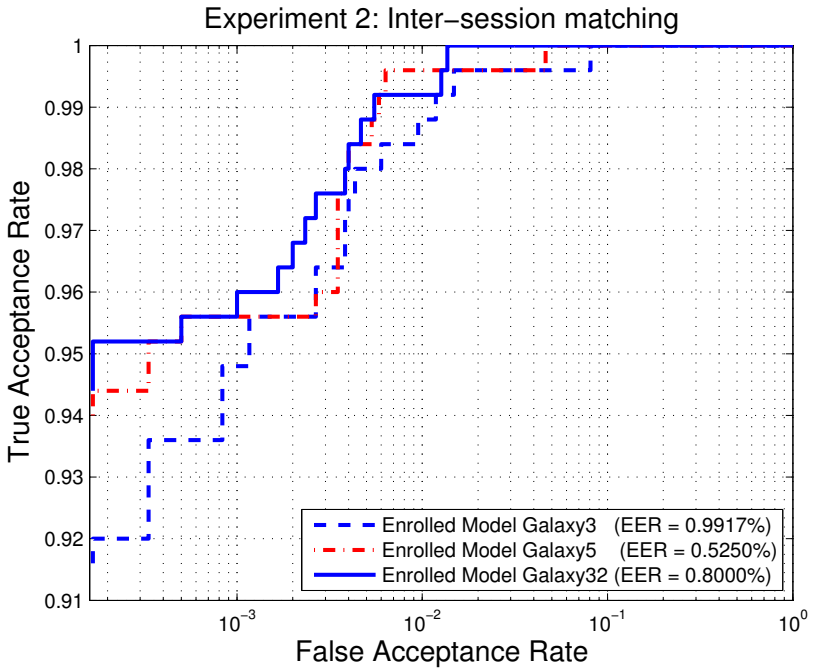

Fig. 5. ROC curve for Experiment 2, which considers enrollment and test signatures from different sessions (5 days gap on average)

4.5 Results and Discussion

An EER of 0% is obtained in the Experiment 1 (see Table 1), where the model signature is enrolled with information from the first session, 3 signatures from the first phase and 2 signatures from the second phase. This clearly shows that there was not much intra-class variability within the first session of acquisitions, but for the same set of models compared against the signatures acquired from the second session which was collected over a break of 5 days, the EER is found to be 0.8%, where we notice a higher intra-class variability. The best EER obtained in this scenario is 0.525%.

Table 1. Results in terms of EER values for both experiments

Enrolled Model	EER values in %	
	Experiment 1	**Experiment 2**
Galaxy3	0.8000	0.9917
Galaxy5	0.5833	0.5250
Galaxy32	0.0000	0.8000

In the BioSecure Signature Evaluation Campaign (BSEC'2009) [2], the *UAM-DTWr* system was ranked the first in the evaluation with an EER value of 0.51% which was a system specially tuned for random forgeries. The evaluation was performed on the BioSecure database. The protocol and various evaluation results are detailed in [2].

5 Conclusion

In this work, we adapted a hybrid version of an existing signature verification system for smart phones. The experiments were conducted on a dynamic signature database that was collected within our research lab on a state-of-the-art stylus-based smart phone (Samsung Galaxy Note). Different experiments were conducted to understand better the effect of intra-class variability with respect to time. The adapted hybrid system has shown promising results, and we obtained a best result with an EER of 0.525%, comparable to the one obtained by the top ranked systems in international evaluations using digitizing tablets [2]. We also discussed about the pros and cons associated with smart phones in the context of personal authentication and other applications built over signature verification concepts.

Acknowledgment. This work has been supported by Sigma Technologies, S.L., Madrid, Spain, and the following projects: Contexts (S2009/TIC-1485) from CAM, Bio-Challenge (TEC2009-11186) and Bio-Shield (TEC2012-34881) from Spanish MICINN, and Catedra UAM-Telefonica.

References

1. Fierrez, J., Ortega-Garcia, J.: On-line signature verification. In: Jain, A.K., Ross, A., Flynn, P. (eds.) Handbook of Biometrics, pp. 189–209. Springer (2008)
2. Houmani, N., Mayoue, A., Garcia-Salicetti, S., Dorizzi, B., Khalil, M., Moustafa, M., Abbas, H., Muramatsu, D., Yanikoglu, B., Kholmatov, A., Martinez-Diaz, M., Fierrez, J., Ortega-Garcia, J., Alcob, J.R., Fabregas, J., Faundez-Zanuy, M., Pascual-Gaspar, J., Cardeoso-Payo, V., Vivaracho-Pascual, C.: Biosecure signature evaluation campaign (bsec2009): Evaluating online signature algorithms depending on the quality of signatures. Pattern Recognition 45(3), 993–1003 (2012)

3. Martinez-Diaz, M., Fierrez, J., Galbally, J., Ortega-Garcia, J.: Towards mobile authentication using dynamic signature verification: useful features and performance evaluation. In: Proc. Intl. Conf. on Pattern Recognition, ICPR (December 2008)
4. Fierrez-Aguilar, J., Krawczyk, S., Ortega-Garcia, J., Jain, A.K.: Fusion of local and regional approaches for on-line signature verification. In: Li, S.Z., Sun, Z., Tan, T., Pankanti, S., Chollet, G., Zhang, D. (eds.) IWBRS 2005. LNCS, vol. 3781, pp. 188–196. Springer, Heidelberg (2005)
5. Freire, M.R., Fierrez, J., Galbally, J., Ortega-Garcia, J.: Biometric hashing based on genetic selection and its application to on-line signatures. In: Lee, S.-W., Li, S.Z. (eds.) ICB 2007. LNCS, vol. 4642, pp. 1134–1143. Springer, Heidelberg (2007)
6. Fierrez-Aguilar, J., Nanni, L., Lopez-Peñalba, J., Ortega-Garcia, J., Maltoni, D.: An on-line signature verification system based on fusion of local and global information. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 523–532. Springer, Heidelberg (2005)
7. Jain, A.K., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems. Pattern Recognition 38(12), 2270–2285 (2005)
8. Galbally, J., Fierrez, J., Freire, M.R., Ortega-Garcia, J.: Feature selection based on genetic algorithms for on-line signature verification. In: Proc. IEEE Workshop on Automatic Identification Advanced Technologies, AutoID, pp. 198–203 (June 2007)
9. Galbally, J., Fierrez, J., Ortega-Garcia, J.: Performance and robustness: a trade-off in dynamic signature verification. In: Proc. IEEE Intl. Conf. on Acoustics, Speech and Signal Processing, ICASSP, pp. 1697–1700 (March-April 2008)
10. Martinez-Diaz, M.: Dynamic signature verification for portable devices. Master's thesis, Universidad Autonoma de Madrid (November 2008)