FUSION OF STATIC IMAGE AND DYNAMIC INFORMATION FOR SIGNATURE VERIFICATION

F. Alonso-Fernandez, J. Fierrez, M. Martinez-Diaz, J. 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
{fernando.alonso, julian.fierrez, marcos.martinez, javier.ortega}@uam.es

ABSTRACT

This paper evaluates the combination of static image (off-line) and dynamic information (on-line) for signature verification. Two off-line and two on-line recognition approaches exploiting information at the global and local levels are used. Experimental results are given using the BiosecurID database (130 signers, 3,640 signatures). Fusion experiments are done using a trained fusion approach based on linear logistic regression. It is shown experimentally that the local systems outperform the global ones, both in the on-line and in the off-line case. We also observe a considerable improvement when combining the two on-line systems, which is not the case with the off-line systems. The best performance is obtained when fusing all the systems together, which is specially evident for skilled forgeries when enough training data is available. [1]

Index Terms— Biometrics, signature recognition, fusion.

1. INTRODUCTION

There is an increasing need for reliable automatic personal identification due to the expansion of the networked society. This has resulted in the popularity of *biometrics* [1], which refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics such as their fingerprint, face, iris, voice, hand, signature, and so on. A wide variety of applications require reliable personal recognition schemes to either confirm or to determine the identity of an individual requesting some kind of service.

In particular, automatic signature verification has been an intense research field because of the social and legal acceptance and the widespread use of the written signature as a personal authentication method [2, 3]. There are two main automatic signature recognition approaches [3]: off-line and on-line. Off-line methods consider uniquely the signature image, so only static information is available for the recognition task, which is commonly acquired by document scanning [4]. On the other hand, on-line systems use pen tablets or digitizers which capture dynamic information such as velocity and acceleration of the signing process, providing a richer source of information [5]. On-line signature verification systems have traditionally shown to be more reliable as dynamic features are more discriminative between users and are harder to imitate [6].

The increasing use of portable personal devices capable of capturing on-line signature signals (e.g, Tablet PCs, PDAs, mobile telephones, etc) is producing a growing demand of person authentication applications based on signature signals. But in spite of its advantages, there are cases in which on-line signature verification is not yet commonly used because signatures are collected off-line. This is the case of many government/legal/financial transactions that are performed daily. Also, off-line signature examination is the common type of criminal casework for forensic experts worldwide [7]. Furthermore, systems that combine both on- and off-line information are of interest in new scenarios where signatures are collected on a paper attached to a digitizing tablet (e.g. point-of-sale terminals). This is the scenario and problem considered in the present paper: fusion of static image and dynamic information for signature verification. In particular, this work evaluates the combination of two on-line [8, 9] and two off-line [10, 11] matchers exploiting global and local information,

2. SIGNATURE VERIFICATION SYSTEMS

This section describes the basics of the four machine experts used in this paper. In Figure 1, the overall system model of the fusion approach considered is depicted.

Global on-line system

In this system each signature is represented by means of a 100 dimensional vector based on the set of 100 features presented in [8]. These can be divided in four categories: i) Time (25 features), related to signature duration, or timing of events such as pen-ups or local maxima; ii) Speed and Acceleration (25 features), from the first and second order time

[1]This work has been supported by Spanish MCYT TEC2006-13141-C03-03 project. Author F. A.-F. is supported by a Juan de la Cierva Fellowship from the Spanish MICINN. Author J. F. is supported by a Marie Curie Fellowship from the European Commission. Authors want to thank Almudena Gilperez for valuable development work.

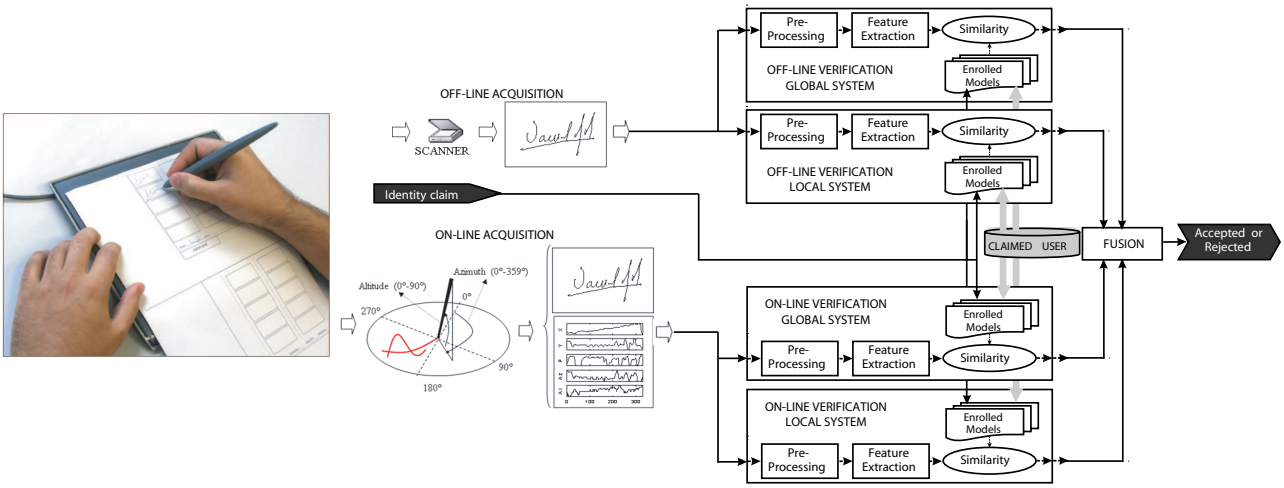

Fig. 1. System model for person authentication based on written signature.

derivatives of the position time functions, like average speed or maximum speed; iii) Direction (18 features), extracted from the path trajectory like the starting direction or mean direction between pen-ups; and iv) Geometry (32 features), associated to the strokes or signature aspect-ratio. Feature selection on this 100-feature set is performed using the SFFS algorithm [12], which is set to minimize the system EER using a classifier based on the Mahalanobis distance. Each client of the system is modeled by the mean and standard deviation vectors of an enrolment set of K signatures using the selected features.

Local on-line system

The on-line signature verification system [9] is based on the recognition algorithm from ATVS presented at the First International Signature Verification Competition (SVC 2004)[2]. Coordinate trajectories and the pressure signal are considered. Signature trajectories are first preprocessed by subtracting the center of mass followed by a rotation alignment based on the average path tangent angle. An extended set of 14 discrete-time functions are then derived from the preprocessed trajectories. Given an enrolment set of K signatures of a client, a left-to-right Hidden Markov Model (HMM) is estimated and used for characterizing the client identity (2 states, 32 Gaussian mixtures per state). This HMM is used to compute the similarity matching score between a given test signature and a claimed identity.

Global off-line system

This system is based on global image analysis and a minimum distance classifier [10]. In this matcher, slant directions of the signature strokes and those of the envelopes of various dilated signature images are extracted with mathematical morphology operators. Given a direction d, the number of

[2]www.cs.ust.hk/svc2004

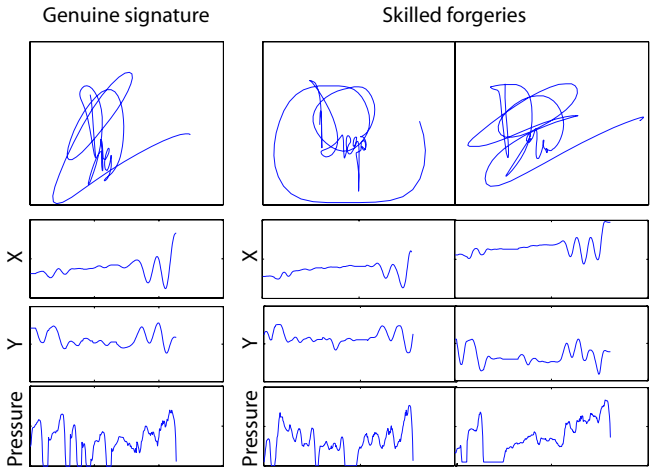

Fig. 2. Signature examples from the BiosecurID database [13]. The left sample is a genuine signature and the remaining ones are forgeries. Plots below each signature correspond to the on-line information stored in the database.

pixels of the whole signature image having direction d is computed. This is done for a number of different orientations regularly distributed between 0 and 360 degrees. Signatures are then represented by a 64-dimensional vector, 32 components corresponding to the slant direction analysis, and 32 to the envelope direction analysis. Each client of the system is modeled by the mean and standard deviation vectors of an enrolment set of K parameterized signatures. To compute the similarity between a claimed model and a parameterized test signature, the inverse of the Mahalanobis distance is used.

Local off-line system

This matcher uses contour level features [11]. Curvature of the signature contour is computed as follows. We consider

two contour fragments attached at a common end pixel and compute the joint probability distribution (PDF) of the directions ϕ_1 and ϕ_2 between that pixel and both fragments. Each client of the system is represented by a joint PDF computed using an enrolment set of K signatures. To compute the similarity between a claimed identity and a given signature, the χ^2 distance is used.

3. EXPERIMENTAL FRAMEWORK

3.1. Database and protocol

We have used for our experiments a sub-corpus of the BiosecurID multimodal database [13], containing signatures from 130 users acquired in 4 different sessions distributed in a 4 months time span. Each user has 4 genuine signatures and 3 forgery (skilled) signatures per session (from 3 different forgers, the same for the 4 sessions). Skilled signatures were done by showing an example of the target signature to the forger. The resulting sub-corpus has $130 \times 4 \times (4+3) = 3,640$ signatures. Signature information were acquired by using an inking pen and paper templates over a pen tablet (see Figure 1), so both signature images and digitized time functions were available. Paper templates were digitized with a scanner at 600 dpi. The dynamic information consists of horizontal and vertical trajectories, x and y respectively, and pressure over time (100 samples/second). Some signature examples are given in Figure 2.

Two enrolment strategies are considered in this paper using genuine signatures from sessions 1 to 3: **Scenario 1**, using K=4 genuine signatures from the first session (mono-session training), which models the situation where users are enrolled in the system by providing 4 signatures consecutively (i.e. in the same session); and **Scenario 2**, using K=12 signatures by taking all signatures from sessions 1 to 3 (multi-session training).

For both scenarios, the four genuine signatures of session 4 are used for testing. Real impostor test scores are computed by using all the available skilled forgeries. For a specific target user, casual impostor test scores are computed by using the four genuine signatures of session 4 from all the remaining targets. As a result, we have 130×4=520 genuine similarity scores, 130×3×4=1,560 scores from skilled forgeries, and 130×4×129=67,080 impostor scores from random forgeries for each scenario.

For the fusion experiments, we use linear logistic regression fusion. Given N matchers which output the scores $(s_{1j}, s_{2j}, ...s_{Nj})$ for an input trial j, a linear fusion of these scores is: $f_j = a_0 + a_1 \cdot s_{1j} + a_2 \cdot s_{2j} + ... + a_N \cdot s_{Nj}$. The weights $a_0, a_1, ...a_N$ are trained via logistic regression following the procedure described in [14]. We use this trained fusion approach because it has shown better performance than simple fusion rules (like the mean or the sum rule) in previous works [14].

	Skilled forgeries		**Random forgeries**	
	4 TR	**12 TR**	**4 TR**	**12 TR**
Global off-line	36.06	32.08	23.31	21.79
Local off-line	25.53	22.90	10.38	8.27
Combined off-line	25.99	21.34	9.23	6.94
Global on-line	12.56	6.22	11.43	5.85
Local on-line	9.94	3.76	6.14	0.90
Combined on-line	5.38	1.53	2.88	0.39
Combined all	3.43	0.00	1.73	0.38

Table 1. Verification performance of the experiments in terms of EER (%). TR denotes number of enrolment signatures.

3.2. Results

In Figure 3, verification performance results in four conditions (few/many training signatures and skilled/random forgeries) are given for i) the individual on-line and off-line machine experts, ii) the combination of the on-line and off-line experts, and iii) the combination of all the systems. Results in terms of EER are also given in Table 1.

We observe that, in general, the local systems work better that the global ones, both in the on-line and off-line cases. The only exception occurs in the on-line case and skilled forgeries, where comparable performance is observed at low FAR, as can be seen in Figure 3. It can also be observed a better performance as we increase the size of the training set, highlighting the importance of an adequate enrolment representative of the natural multi-session signer variability. This effect is specially evident in the two on-line systems. Since they exploit the dynamic information available in on-line signatures, they are more benefited by the incorporation of the increasing natural user variability of additional signatures for enrolment.

Concerning the separate combination of the on-line or the off-line experts, we observe that the fusion does not provide a remarkable improvement in the off-line case (only with 12 training signatures, an slight improvement is obtained). On the contrary, a considerable improvement is observed when combining the two on-line systems, both with 4 and with 12 training signatures. Similarly as above, since on-line systems use the dynamic information available, a higher benefit is obtained by fusing them.

An additional improvement is also observed when fusing all the systems (the thickest line of Figure 3). This is specially remarkable for skilled forgeries with 12 training signatures. In this particular case, we obtain perfect separation between the genuine and impostor classes (0% EER with our dataset).

4. CONCLUSIONS

The combination of on-line and off-line information for signature verification is evaluated in this work. We use two on-

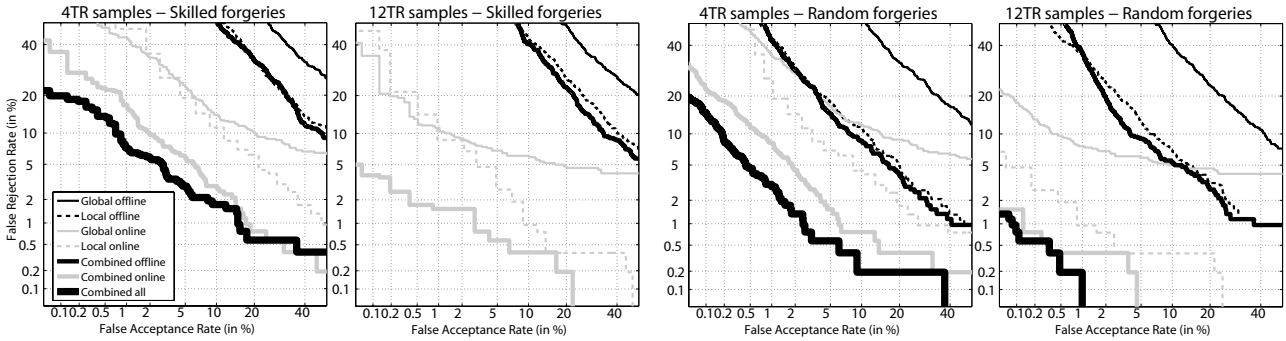

Fig. 3. Verification performance of the experiments. TR denotes number of enrolment signatures.

line and two off-line verification systems exploiting information at the global and local levels. We consider two enrolment strategies in our experiments: with few (4) training signatures acquired in a single session, and with many (12) training signatures acquired in 3 different sessions. For the fusion experiments, we consider a trained fusion approach based on linear logistic regression.

The best performance is obtained when fusing all the systems together, which is specially evident for skilled forgeries with 12 training signatures. The latter case produces an EER of 0% with the dataset used in this paper. Worth noting, it is not the aim of this work to obtain a perfect verification rate but to reveal the fundamentals for performance improvement using information fusion. This motivates us to extend the experiments of this work to other larger databases, or acquired in more adverse conditions, e.g. using mobile devices [15]. Future work also includes to evaluate the impact of quality measures [16] in the performance of the different matchers, to exploit differences in robustness of the various information sources against varying quality using quality-adaptive fusion rules [17].

5. REFERENCES

[1] A.K. Jain, A. Ross, S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. IFS*, vol. 1, pp. 125–143, 2006.

[2] M.C. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology," *Electronics and Communication Engineering Journal*, vol. 9, pp. 273–280, 1997.

[3] R. Plamondon and S.N. Srihari, "On-line and off-line handwriting recognition: A comprehensive survey," *IEEE Trans. PAMI*, vol. 22, no. 1, pp. 63–84, 2000.

[4] G. Dimauro, S. Impedovo, M.G. Lucchese, R. Modugno, and G. Pirlo, "Recent advancements in automatic signature verification," *Proc. IWFHR*, pp. 179–184, 2004.

[5] J. Fierrez, J. Ortega-Garcia, *Handbook of Biometrics*, ch. 10. On-line signature verification, pp. 189–210, Springer, 2008.

[6] G. Rigoll, A. Kosmala, "A systematic comparison between on-line and off-line methods for signature verification with Hidden Markov Models," *Proc. ICPR*, vol. 2, pp. 1755–1757, 1998.

[7] S. N. Srihari, C. Huang, H. Srinivasan, and V. A. Shah, *Digital Document Processing*, ch. 17. Biometric and Forensic Aspects of Digital Document Processing, pp. 379–406, Springer, 2007.

[8] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Penalba, J. Ortega-Garcia, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," *Proc. AVBPA*, Springer LNCS-3546, pp. 523–532, 2005.

[9] 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, pp. 2325–2334, 2007.

[10] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and J. Ortega-Garcia, "An off-line signature verification system based on fusion of local and global information," *Proc. BIOAW*, Springer LNCS-3087, pp. 295–306, 2004.

[11] A. Gilperez, F. Alonso-Fernandez, S. Pecharroman, J. Fierrez, and J. Ortega-Garcia, "Off-line signature verification using contour features," *Proc. ICFHR*, 2008.

[12] A. K. Jain and D. Zongker, "Feature selection: evaluation, application, and small sample performance," *IEEE Trans. PAMI*, vol. 19, no. 2, pp. 153–158, 1997.

[13] J. Fierrez, J. Galbally, J. Ortega-Garcia *et al.*, "BiosecurID: A multimodal biometric database," *Pattern Analysis and Applications (accepted)*, 2009.

[14] F. Alonso-Fernandez, J. Fierrez, D. Ramos, and J. Ortega-Garcia, "Dealing with sensor interoperability in multi-biometrics: The UPM experience at the Biosecure Multimodal Evaluation 2007," *Defense and Security Symposium, Proc. SPIE*, vol. 6944, pp. 69440J1–69440J12, 2008.

[15] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez *et al.*, "The multi-scenario multi-environment BioSecure Multimodal Database (BMDB)," *IEEE Trans. PAMI (to appear)*, 2009.

[16] F. Alonso-Fernandez, M. Fairhurst, J. Fierrez, J. Ortega-Garcia, "Automatic measures for predicting performance in off-line signature," *Proc. ICIP*, vol. 1, pp. 369–372, 2007.

[17] H. Fronthaler, K. Kollreider, J. Bigun *et al.*, "Fingerprint image quality estimation and its application to multi-algorithm verification," *IEEE Trans. IFS*, vol. 3, no. 2, pp. 331–338, 2008.