2009 10th International Conference on Document Analysis and Recognition

ROBUSTNESS OF SIGNATURE VERIFICATION SYSTEMS TO IMITATORS WITH INCREASING SKILLS

Fernando Alonso-Fernandez, Julian Fierrez, Almudena Gilperez, Javier Galbally, Javier Ortega-Garcia
Biometric Recognition Group - ATVS, Escuela Politecnica Superior, Universidad Autonoma de Madrid
C/ Francisco Tomas y Valiente 11, 28049 Madrid SPAIN
{fernando.alonso, julian.fierrez, almudena.gilperez, javier.galbally, javier.ortega}@uam.es

Abstract

In this paper, we study the impact of an incremental level of skill in the forgeries against signature verification systems. Experiments are carried out using both off-line systems, involving the discrimination of signatures written on a piece of paper, and on-line systems, in which dynamic information of the signing process (such as velocity and acceleration) is also available. We use for our experiments the BiosecurID database, which contains both on-line and off-line versions of signatures, acquired in four sessions across a 4 month time span with incremental level of skill in the forgeries for different sessions. We compare several scenarios with different size and variability of the enrolment set, showing that the problem of skilled forgeries can be alleviated as we consider more signatures for enrolment.

1. Introduction

Nowadays, due to the expansion of the networked society, an automatic correct assessment of identity is a crucial point. This has resulted in the establishment of a new research and technology area known as *biometrics* [1], which refers to automatic recognition of an individual based on behavioral and/or anatomical characteristics (e.g., fingerprints, face, iris, voice, signature, etc.).

The handwritten signature is one of the most widely used individual authentication methods due to its acceptance in government, legal and commercial transactions [2]. There are two main signature recognition approaches [3, 4]: off-line and on-line. Off-line methods consider only the signature image, so only static information is available for the recognition task. 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 and more reliability [3].

Despite the evident advantages of biometric systems, they are not free from external attacks which can decrease their level of security. Thus, it is of utmost importance to analyze the vulnerabilities of biometric systems, in order to find their limitations and to develop useful countermeasures for foreseeable attacks [5]. Like other biometric systems, signature verification systems are exposed to forgeries, which can be easily performed by direct observation and learning of the signature by the forger. Signature verification systems are usually evaluated by analyzing their ability to accept genuine signatures and to reject forgeries.

In this paper, we evaluate the robustness of signature verification systems to forgeries created with an increasing level of skill. For this purpose, we use the BiosecurID database [6], which contains both on-line and off-line versions of signatures acquired in several sessions with an incremental level of skill in the forgeries. For the verification experiments, three machine experts exploiting information at different levels have been used (one on-line [7] and two off-line [8, 9]). Several enrolment strategies with different size and variability of the enrolment set are studied.

The rest of this paper is organized as follows. The problem of forgeries with different level of skill is briefly addressed in Section 2. The three machine experts used are described in Section 3. The experimental framework used, including the database and protocol, is described in Section 4. The results obtained are presented in Section 5, and conclusions are finally drawn in Section 6.

2. Types of forgeries in signature recognition

When considering forgeries, five categories can be defined depending on the level of attack [10].

- **Random forgeries**, simulated by using signatures from other users as input, so no knowledge about the signature being attacked is exploited. This case does not represent intentional forgeries, but accidental accesses by impostors without information to help them in their attack to the system.

978-0-7695-3725-2/09 $25.00 © 2009 IEEE
DOI 10.1109/ICDAR.2009.261

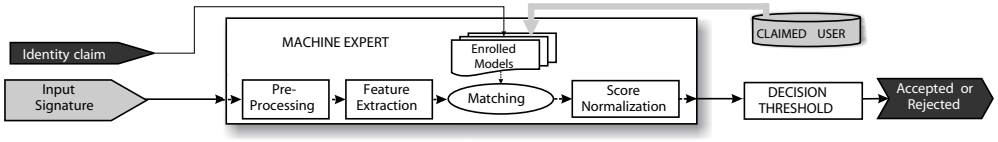

Figure 1. System model for person authentication based on handwritten signature.

- **Blind forgeries**, which are signature samples generated by intentional impostors that have access to a descriptive or textual knowledge of the original signatures (e.g. the name of the person).
- **Static forgeries** (low-force in [10]), where the forger has access to a visual static image of the signature. There are two ways to generate the forgeries. In the first one, the forger can use a blueprint to copy the signature, leading to static **blueprint** forgeries. In the second one, the forger can train to imitate the signature, with or without a blueprint, for a limited or unlimited amount of time. The forger then generate the imitated signature, without the help of the blueprint, leading to static **trained** forgeries.
- **Dynamic forgeries** (brute-force in [10]), where the forger has access to a visual static image and to the whole writing process (i.e. the dynamics). The dynamics can be obtained in the presence of the original writer, or through a video-recording, or also through the obtention of the on-line version of the signature. In a similar way as the previous category, the forger can then generate two types of forgeries. Dynamic **blueprint** forgeries are generated by projecting on the acquisition area a real-time pointer that the forger needs to follow. Dynamic **trained** forgeries are produced after a training period where the forger can use dedicated tools to analyze and train to reproduce the genuine signature.
- **Regained forgeries**, where the forger has only access to the static image of the signature and makes use of a dedicated software to regain its dynamics, which are later analyzed and used to create dynamic forgeries.

3. Signature verification systems

This section describes the basics of the three machine experts used in this paper. They exploit information at two different levels. The on-line signature system is based on local image analysis and left-to-right Hidden Markov Models [7]. For off-line analysis, we use an approach based on global analysis of the image [9] and a second approach based on local analysis [8]. In Figure 1, the overall system model of a signature machine expert is depicted.

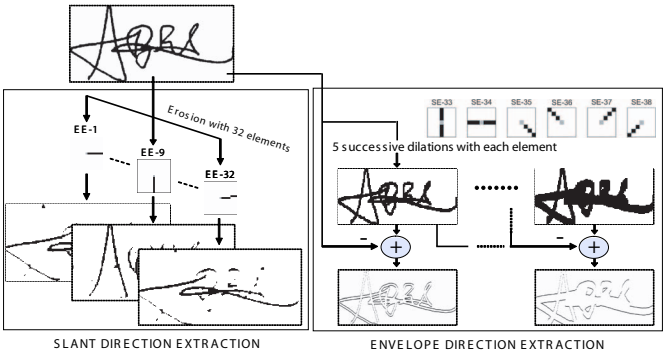

Figure 2. Feature extraction stage performed in the global off-line system.

3.1. On-line system based on HMM

The on-line signature verification system [7] is based on the recognition algorithm from ATVS presented at the First International Signature Verification Competition (SVC 2004)[1]. 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.

3.2. Global off-line system

This system is based on global image analysis and a minimum distance classifier [9]. In this matcher, slant directions of the signature strokes and those of the envelopes of the dilated signature images are extracted with mathematical morphology operators. For slant direction extraction, the preprocessed signature image is eroded with 32 structuring elements as those shown in Figure 2 (left). A slant direction feature sub-vector of 32 components is then generated, where each component is computed as the signature

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

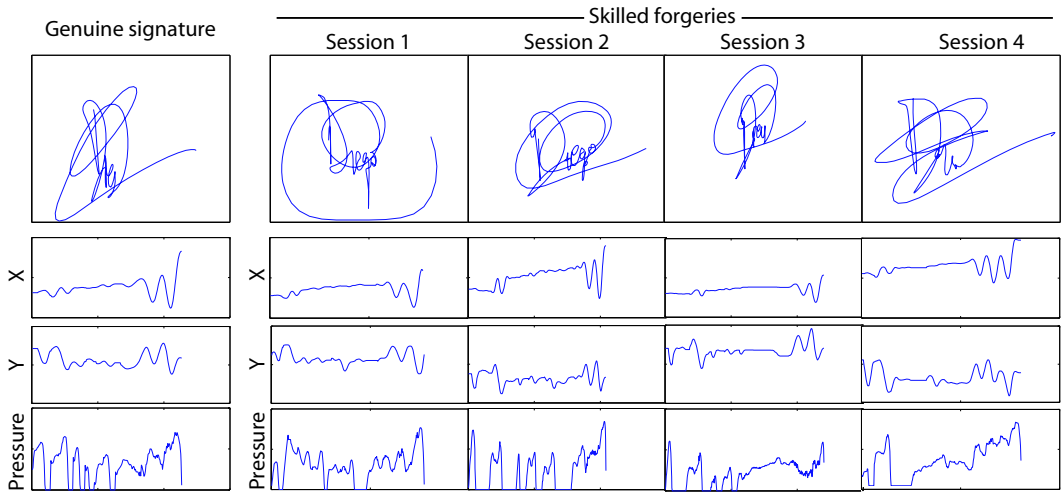

Figure 4. Signature examples from the BiosecurID Database. The left sample is a genuine signature and the remaining ones are forgeries with incremental level of skill. In each case, plots below each signature correspond to the on-line information stored in the database.

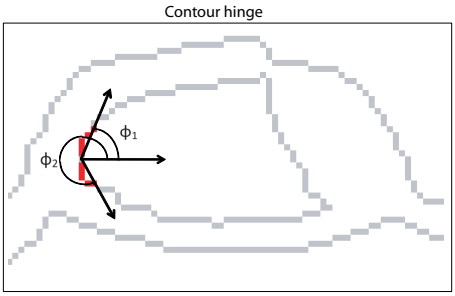

Figure 3. Graphical example of the contour curvature (local off-line system).

pixel count in each eroded image. For envelope direction extraction, the preprocessed signature image is successively dilated 5 times with the 6 structuring elements shown in Figure 2 (right). An envelope direction feature sub-vector of 5×6 components is then generated, where each component is computed as the signature pixel count in the difference image between successive dilations. The preprocessed signature is parameterized by concatenating the slant and envelope feature sub-vectors. Each client (enrolee) of the system is modeled by the mean and standard deviation vectors of an enrolment set of K parameterized signatures. To compute the similarity score between a claimed model and a parameterized test signature, the inverse of the Mahalanobis distance is used.

3.3. Local off-line system

This matcher uses contour level features [8]. Curvature of the contour is computed as follows. We consider two contour fragments attached at a common end pixel and compute the joint probability distribution of the orientations ϕ_1 and ϕ_2 of the two sides, see Figure 3. A joint density function (PDF) is obtained, which quantifies the chance of finding two "hinged" contour fragments with angles ϕ_1 and ϕ_2, respectively. Each client of the system (enrolee) is represented by a PDF that is 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.

4 Database and experimental protocol

4.1 Database

We have used for our experiments a sub-corpus of the BiosecurID multimodal database [6], containing signatures from 133 users acquired in 4 different sessions distributed in a 4 months time span. Each user has 4 genuine signatures and 3 forgery signatures per session (from 3 different forgers, the same for the 4 sessions). The resulting sub-corpus has $133 \times 4 \times (4+3) = 3,724$ signatures.

An incremental level of skill in the forgeries was considered during the acquisition of each session, resulting in four different scenarios (see Figure 4): **Skill level 1** in session 1, where the forger only sees the signature image once (off-line information) and tries to imitate it; **Skill level 2** in session 2, where the forger sees the signature image once (off-

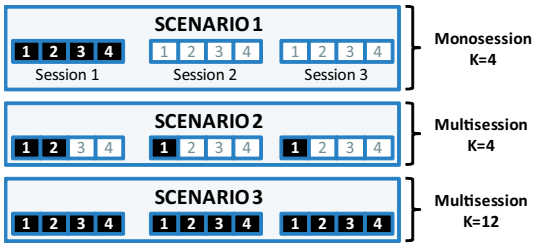

Figure 5. Enrolment strategies considered.

line information), trains for a minute in a piece of paper, and then imitates the signature; **Skill level 3** in session 3, where the forger sees the dynamic signature process 3 times using a dedicated software (on-line information), trains for a minute in a piece of paper, and then imitates the signature; and **Skill level 4** in session 4, where the forger sees the dynamic signature (on-line information) as many times as he/she requests, trains for a minute in a piece of paper and then imitates the signature. Following the nomenclature of Section 2, forgeries of sessions 1 and 2 are static forgeries, and those of sessions 3 and 4 are dynamic forgeries.

4.2 Experimental Protocol

Several enrolment strategies are considered in this paper using genuine signatures from sessions 1 to 3, see Figure 5: **Scenario 1**: using K=4 genuine signatures from the first session (mono-session). This scenario models the situation where users are enrolled in the system by providing 4 signatures consecutively (i.e. in the same session). **Scenario 2**: using K=4 genuine signatures, but considering also signatures from the second and third sessions (multi-session), capturing more user variability. **Scenario 3**: increasing the size of the enrolment set to K=12 signatures by taking all signatures from sessions 1 to 3 (multi-session).

For each scenario, the four genuine signatures of session 4 are used for testing. Real impostor test scores are computed by using the 3 skilled forgeries of each session. As a result, we have 133×4=532 genuine similarity scores for each scenario, and four sets of 133×3=399 scores from skilled forgeries for each scenario.

5 Results

Figure 6 shows the system performance based on the level of skill in the forgeries for the three machine experts used in this paper. We also report the results when fusing the two off-line systems available using the TANH normalization proposed in [11] and the SUM fusion rule.

Concerning the off-line systems, Figure 6 shows that a significant degradation in the verification performance is only observed for the maximum level of skill in the forgeries (level 4). For the other levels (1 to 3), there is no clear degradation in the performance. On the contrary, the on-line system exhibits a progressive degradation from level 1 to 4. These results suggest that the progressive level of skill in the forgeries that are introduced from level 1 to 4 mainly affects to the dynamic information of signatures, which are analyzed solely by the on-line system. Off-line systems, which analyze static information, are not as heavily affected (only in level 4).

Regarding the three enrolment scenarios considered, we observe that the performance is progressively improved from scenario 1 (K=4 genuine signatures from one session) to scenario 3 (K=12 signatures from three sessions). The only exception is the global off-line system, which does not show significant differences between scenario 1 and 2. Worth noting, the on-line system is quite robust to the level of skill in the forgeries in the scenario 3, resulting in similar performance in levels 2 to 4.

It is also worth noting that the on-line system results in the highest relative performance improvement in the multi-session enrolment scenarios. Since it exploits the dynamic information available in on-line signatures, it is more benefited by the incorporation of user variability and/or additional signatures in the enrolment set. In this sense, we also observe that the biggest improvement in the on-line system is from the enrolment scenario 1 to 2 (i.e., mono- vs multi-session training for the same number of enrolment signatures), which is much higher than from scenario 2 to 3 (i.e., from 4 to 16 multi-session training signatures). This result highlights the importance of an adequate enrolment representative of the natural multi-session signer variability, which can be obtained even with a reduced number of training signatures. The fusion of the two off-line systems also increases the relative improvement figures when considering better enrolment scenarios with respect to the two systems alone. In this case, the improvement from enrolment scenario 1 to 2 is similar to the one observed from scenario 2 to 3. This means that for different enrolment strategies in off-line recognition the performance improvement mainly comes from larger training sets, not from the multi-session aspect in the enrolment data, which was crucial in the online case.

6 Conclusions

The robustness of signature verification systems to forgeries with increasing level of skill has been studied. For this purpose, a database containing forgeries with incremental level of skill has been used. Three machine experts exploiting information at different levels have been used in the experiments: one off-line system based on local information that uses contour level features, one off-line system based

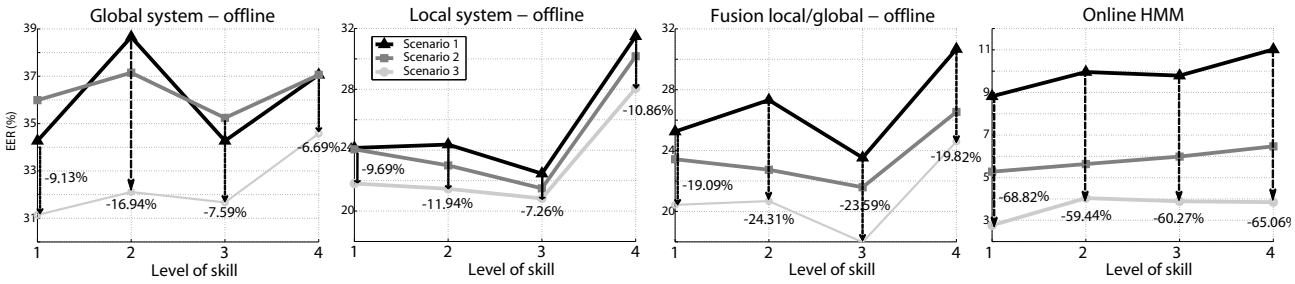

Figure 6. Verification performance based on the level of skill in the forgeries for the different scenarios presented in Section 4.2. Results are given in terms of Equal Error Rates (in %). For each level of skill, it is also given the relative gain of performance of the scenario 3 with respect to the scenario 1.

on global image analysis that computes slant directions of the signature strokes and those of the envelopes of the dilated signature images, and one on-line system based on HMM. Several enrolment strategies with different size and variability of the enrolment set have been also compared.

Our experiments show that the performance of the off-line systems is only degraded with the highest level of skill in the forgeries. On the contrary, the on-line system exhibits a progressive degradation with the level of skill, suggesting that the dynamic information of signatures is the one more affected by the considered increasing skills of the forgers.

Concerning the three enrolment scenarios proposed, it is observed that the performance of the three machine experts is improved as we increase the size and the variability of the enrolment set. It is worthy to remark that the on-line system becomes nearly insensitive to the level of skill in the forgeries for the third scenario (i.e. the one which has the maximum size and variability in the enrolment set). This results stresses the importance of having enrolment models generated with enough data, and acquired at different moments. The scarcity of available templates when a user is enrolled in a system is precisely one of the problems of signature systems. As can be observed from our results, several templates are needed and template signatures should be captured in different sessions in order to obtain a robust model that can deal with the natural user intra-variability, but this is not always possible due to application and user convenience constraints. One solution to this problem could be the generation of synthetic signatures from a user, in order to obtain more signatures for enrolment [12]. This will be a source of future work.

7 Acknowledgments

This work has been supported by the TEC2006-13141-C03-03 project of the Spanish Ministry of Science and Technology. Author F. A.-F. thanks Consejeria de Educacion de la Comunidad de Madrid and Fondo Social Europeo for supporting his PhD studies. 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. Author J. G. is supported by a FPU Fellowship from the Spanish MEC.

References

[1] A. Jain *et al*. Biometrics: A tool for information security. *IEEE Trans. Inf. Forensics and Sec.*, 1:125–143, 2006.

[2] M. Fairhurst. Signature verification revisited: promoting practical exploitation of biometric technology. *Electronics and Communication Engineering J.*, 9:273–280, Dec. 1997.

[3] R. Plamondon and S. Srihari. On-line and off-line handwriting recognition: A comprehensive survey. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 22(1):63–84, 2000.

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

[5] J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. *Proc. ICB*, Springer LNCS-4642:386–395, 2007.

[6] J. Fierrez *et al*. BiosecurID: A multimodal biometric database. *Pattern Analysis and Applications (accepted)*, 2009.

[7] J. Fierrez *et al*. HMM-based on-line signature verification: Feature extraction and signature modeling. *Pattern Recognition Letters*, 28:2325–2334, 2007.

[8] A. Gilperez *et al*. Off-line signature verification using contour features. *Proc. ICFHR*, 2008.

[9] J. Fierrez-Aguilar *et al*. An off-line signature verification system based on fusion of local and global information. *Proc. BIOAW*, Springer LNCS-3087:295–306, 2004.

[10] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold. A new forgery scenario based on regaining dynamics of signature. *Proc. ICB*, Springer LNCS-4642:366–375, 2007.

[11] A. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38(12):2270–2285, December 2005.

[12] J. Galbally *et al*. Synthetic generation of handwritten signatures based on spectral analysis. *Defense and Security Symposium, Proc. SPIE (to appear)*, 2009.