2012 10th IAPR International Workshop on Document Analysis Systems

A Signature Verification Framework for Digital Pen Applications

Muhammad Imran Malik*† , Sheraz Ahmed*†, Andreas Dengel*† Marcus Liwicki*
* *German Research Center for AI (DFKI GmbH)*
Knowledge Management Department, Kaiserslautern, Germany
{*firstname.lastname*}*@dfki.de*
† *Department of Computer Science, University of Kaiserslautern, Germany*

***Abstract*—In this paper we present a framework for real-time online signature verification scenarios. The proposed framework is based on state-of-the-art feature extraction and Gaussian Mixture Model (GMM) classification. While our signature verification library is generally applicable to any input device using digital pens, we have implemented verification scenarios using the Anoto digital pen. As such our automated signature verification framework becomes an interesting commodity for industry, because the Anoto SDK is easy to apply and the GMM-based classification can be seamlessly integrated. The novelty of this work is the application of our framework that takes real-time online signature verification to every scenario where digital pens may potentially be used. In this paper we describe several scenarios where our framework has been applied, including signatures in financial contracts or ordering processes. We also propose a general approach to integrate the GMM-descriptions into electronic ID-cards in order to also store behavioral biometrics on these cards. In experiments we have measured the performance of the signature verification system when skilled forgeries were present. The interest shown by our partner financial institutions and the results of our initial evaluations indicate that our signature verification framework suits exactly the demands of our clients.**

***Keywords*-Online signatures, Verification, Biometric authentication, Mixture models, Anoto, Digital pens, Forged signatures, Skilled forgeries, Handwriting analysis**

I. Introduction

Automated signature verification is in focus of research since decades. In many recent works automatic signature verification is described as a two-class pattern classification problem [1]. Here an automated system has to decide whether or not a given signature belongs to a referenced authentic author. If the system could not find enough evidence of a forgery from the questioned signature feature vector, it considers the signature as genuine belonging to the referenced authentic author; otherwise it declares the signature as forged.

Handwritten signatures are biometric attributes [2]. They suffer severely from intra-writer/within writer variations. Unlike some of the other biometric attributes, signatures are influenced by many factors from aging to psychological conditions of individuals. Despite of their difficult nature, signatures are considered as an important modality for person identification [2].

In general, automated signature verification is divided into two broad categories, online and offline, depending on the mode of the handwritten input. If both the spatial as well as temporal information regarding signatures are available to the systems, verification is performed on online data. In the case where temporal information is not available and the system can only utilize the spatial information gleaned through scanned or even camera captured documents, verification is performed on offline data [3], [4].

The main motivation of this paper is to take signature verification to the most commonly occurring real world scenarios, particularly in industry, where signature verification is required. Two of the most important areas where signature verification is highly demanded are, forensic signature analysis and signature verification in financial institutions. Until now online signature verification is not a common type of criminal casework for a forensic expert because the questioned signatures and the collected reference signatures (known) are commonly supplied offline [5]. However, in most of the today's modern financial institutions there is an increasing demand to perform signature verification in real-time right after signing contracts, etc. We focus explicitly on the online signature verification keeping in view its various applications in these institutions.

In this paper we apply our signature verification framework in different real world scenarios in connection with the Anoto digital pen. Note, however, that our framework can also be integrated with other hardware like digitizing tablets.

Figure 1 illustrates the hardware layout of the Anoto digital pen. This pen specializes in providing the look and feel of regular pens. It only demands to add Anoto dot pattern to any paper and data can be digitized seamlessly. The Anoto pattern makes it possible for the Anoto pen's built-in camera to detect strokes and record signatures that then can be stored in an internal memory or sent via communication unit using Bluetooth/USB. Due to this ease of use, Anoto pens are finding applications in fields from health care to finance. Our signature verification framework is an attempt to take signature verification to every area where the Anoto pen finds an application. In particular our system has already been applied in test scenarios for finance institutions and product manufacturing companies.

978-0-7695-4661-2/12 $26.00 © 2012 IEEE
DOI 10.1109/DAS.2012.10

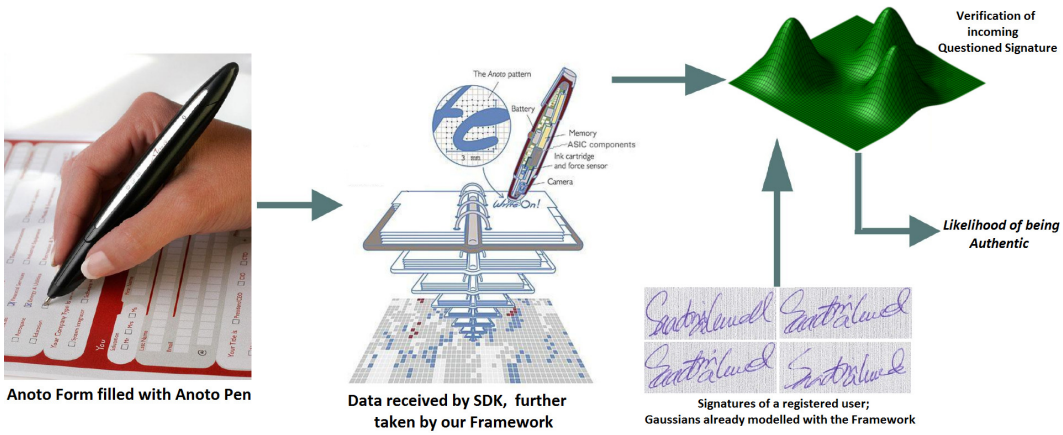

Figure 2. General overview of the proposed signature verification framework.

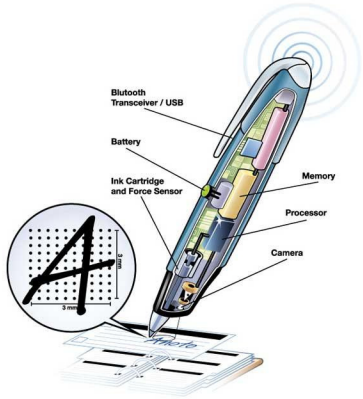

Figure 1. Anoto digital pen.

II. Signature Verification Framework Overview

The general overview of the signature verification framework proposed in this paper is illustrated in Figure 2. The online data is collected using the Anoto digital pen and saved in the pen's memory. The pen is then synchronized with some processing device like a computer or a mobile phone. Through this synchronization data is sent to the Anoto Software Development Kit (SDK). Once the data are received at the SDK, our framework picks the corresponding signatures data (questioned or referenced) and passes it to the signature verification module. The signature verification module then uses a Gaussian Mixture Model (GMM)-based approach to process the signature.

There can be two situations in our framework. In the first situation the user is interacting with our framework for the first time. In this case (s)he has to provide her/his genuine signatures as the reference signatures and prove the identity by any other traditional secure way. Now our framework generates reference GMMs for the user and stores them. In this way registration of a user with our system is completed.

In the second situation a user interacts with our framework by providing her/his signatures and claiming to be some specific person. Now our framework takes the claimed person's GMMs (assuming that this person is already registered with the framework) and fits the questioned person/signature model. Currently the system reports it's evaluation result in the form of probability values. Based on this value it can be decided whether the claiming person is the authentic writer or a forger.

III. Signature Verification Module

The system we are using for the framework is an optimized and adapted version of our previous system introduced in [6]. Given the online data as an input, the signatures are corrected with respect to their skew. We do not perform any more preprocessing steps as already proposed in [6].

The extracted features are the following (see Fig. 3 for an illustration): the pen-up/pen-down feature *(1)*; the pressure *(2)*; the speed *(3)*; the speed in x and y direction *(4,5)*; the acceleration *(6)*; the acceleration in x and y direction *(7,8)*; the log radius of curvature *(9)*; the normalized x- and y-coordinate *(10,11)*; the writing direction *(12,13)*; the curvature *(14,15)*; the vicinity aspect *(16)*; the vicinity slope *(17,18)*; the vicinity curliness *(19)*; the vicinity linearity *(20)*; the ascenders and descenders in the off-line vicinity of the considered point *(21,22)*; and the context map, where the two-dimensional vicinity of the point is transformed to a 3×3 map and the resulting nine values are taken as features *(23-31)*.

Gaussian Mixture Models [7] have been used to model the signatures of each person. More specifically, the distribution of feature vectors extracted from a persons handwriting is modeled by a Gaussian mixture density. For a D-dimensional feature vector denoted as x, the mixture density for a given

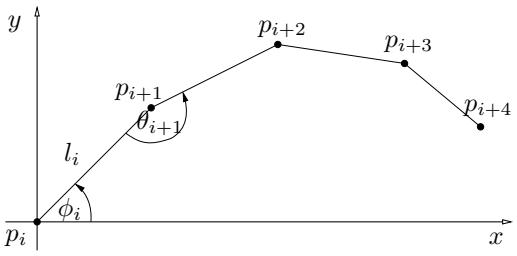

Figure 3. Illustration of point-based features.

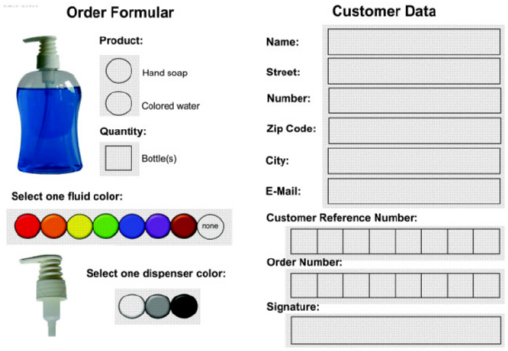

Figure 4. A pen based interaction order form.

writer (with the corresponding model A) is defined as:

$$p(x\|A) = \sum_{i=1}^{m} w_i p_i(x)$$

In other words, the density is a weighted linear combination of M uni-modal Gaussian densities, $p_i(x)$, each parameterized by a $D \times 1$ mean vector, and $D * D$ covariance matrix. For further details refer to [8].

IV. Application Scenarios

A. Automatic Order Processing

Highly customized products having shorter development life cycles is the demand of today's global market [9]. This makes efficient order processing an important area for any manufacturing company to improve. In traditional order processing a client fills an order form and then posts/faxes it to the company. On receiving the order the company follows its predefined procedure to establish authenticity of the order. One important modality in this process is using the signatures of the client and keeping them with the company as a seal of authenticity. This is a time consuming process. Alternatively, web based forms can be used. However, web based order processing suffer from a compendium of difficulties for customer as explained in [10].

To cope with this an intelligent approach for intelligent digital pen-based ordering has been recently introduced in [11]. Here, instead of traditional paper or Internet a digital pen is used to take customer specific orders that are afterwards used in production automation. The customer fills this form as a regular form and signs it. The pen is synchronized (attached to a computer via USB or Bluetooth) and the corresponding electronic form is mapped to the writing information. The final order is then sent to the *SmartFactory*^{KL} which allows for product automation (further details are provided in [11]).

A pen based interaction order form is shown in Figure 4. Here a user may select a product with different colors and enter her/his particulars using the Anoto pen. Note the signature field is also provided as it is on the traditional forms but now it is dealt with our proposed signature verification framework. The paper form used here is exactly the same as it was in the traditional approach except that now it also carries the Anoto dot pattern.

The final accept or reject of an order depends on the result of our signature verification framework. If sufficient likelihood for authenticity can be established the customized order is sent to the *SmartFactory*^{KL} and the customized production process is started. Otherwise, the order is rejected.

B. Signature Verification Framework in Banks

Financial institutions bear losses of billions of dollars on account of insufficient signature verification mechanisms. Often, only a rough visual comparison, if any, is performed by an untrained person to authenticate signatures.

In this paper we propose a novel idea to use our online signature verification framework that would help banks increase their immunity against fake credit or debit card users. Our idea is to integrate the GMM descriptions produced by our framework into electronic ID-cards.

Two example application scenarios for our framework are illustrated in Figures 5a and 5b respectively. Figure 5a illustrates a scenario where a customer registers at a bank for the first time. At first the customer applies for opening an account by providing her/his identity. This may be done by any card containing picture and particulars of the applicant like a passport or personal ID-card. For opening an account the bank takes a certain number of online signatures from the customer and provides them to our framework. Our framework is then applied to take GMM descriptions using various combinations of these genuine reference signatures. Note that already during this process a validation can be performed that all signatures are similar enough to produce a probability of being authentic. The obtained GMM descriptions are then stored on the electronic card of the customer. By doing this, the original signatures would not be available on the card (protecting the customer against fraud). Only the model used for comparison will be available. Furthermore, one cannot generate the genuine signatures from the stored model thereby removing the danger of any security attack of such kind.

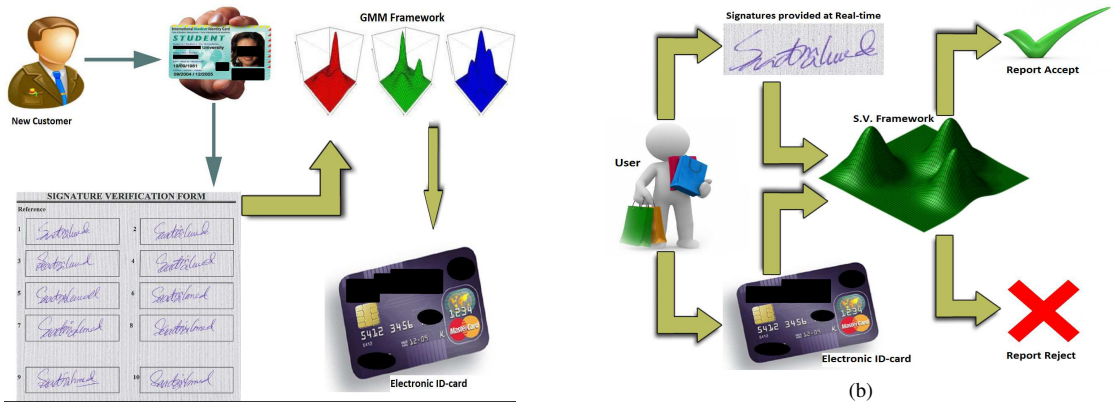

Figure 5. Application scenarios of the proposed framework: registering a customer and generating an electronic ID-card (a); establishing the authenticity of a customer (b).

Now the customer, whenever using the card for monetary transaction may use his/her signatures instead of or additionally to pin codes/logins. Figure 5b illustrates this scenario. Here a customer has an electronic card (developed in the previous scenario) after purchasing goods at a supermarket tries to pay with this card. At the counter (s)he provides her/his electronic card along with signatures written with a digital pen. These signatures are transferred to a local computer having an instance of our framework where the authenticity of these signatures is judged. If our framework then reports an accept it refers that the customer is authentic. Otherwise, the customer might be a forger/imposter trying to use some other person's card (in that case, another authentication method can be applied).

In most positive cases the scenario will lessen the memory burden the customers needs to have in remembering their pin codes/logins. Furthermore, it will enable only the authentic person to use his/her card alone. There can also be various other applications of these *behavioral information containing electronic cards* which are beyond the scope of this discussion.

V. Data sets and Ealuation

The evaluation of our framework was performed on two data sets. The first data set contained the data collected specifically using the Anoto digital pens on forms similar to the ones used by our clients. For this collection, ten authors (male and female) from different countries aging between 18 to 40 provided their genuine signatures. Ten forgers (students, researchers and a calligrapher) were asked to make skilled forgeries of each genuine author. Each genuine author contributed 9 of her/his signatures. Out of these nine, 7 signatures were used as reference signatures and remaining 2 were put in the test set for every genuine author. Each forger also produced 9 forgeries. As a whole, our test set for this data set contained 20 genuine signatures and 90 skilled forgeries.

Table I
Evaluation results of Anoto online data (data set 1)

Author-ID	FA	FR
1	0	0
2	0	0
3	2	1
4	0	1
5	0	1
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0

Note that we use the term skilled forgeries as the forgers were allowed to practice the given genuine signatures for as long as they wanted to perfect before making the first forgery attempt. This is in accordance with [12] and [13].

The second data set was the NISDCC signature collection of ICDAR 2009 online signature verification competition (Blankers et al.. 2009)[1]. This data set consists of 60 authentic signatures written by 12 authors. 31 forgers produced skilled forgeries at the rate of 5 forgeries per genuine author.

Since the number of signatures in the first data set is quite low we report our results in terms of number of Falsely Accepted signatures (FA) and number of Falsely Rejected signatures (FR). The results are given in Table I. However, we report False Accept Rate (FAR) and False Reject Rate (FRR) with the Equal Error Rate (EER) for the second data set. These results are shown in Table II.

An important observation is that on the second data set our system used only one reference signature per author. It is especially encouraging as it enables our system to be integrated in scenarios where only limited number of reference signatures is present, e.g., in forensic scenarios.

[1]publicly available for research purposes at http://sigcomp09.arsforensica.org

Table II
EVALUATION RESULTS OF ICDAR 2009 ONLINE DATA (DATA SET 2)

Overall (for all authors)	FAR	FRR	EER
GMM Framework	0.9	4.0	3.3

Results are computed at 4 Gaussians with variance flooring parameter of 0.08.

VI. CONCLUSION AND FUTURE WORK

In this paper we have presented a signature verification framework that is seamlessly integrable to scenarios where digital pens can be applied for data acquisition. We have reported the application scenarios in which our framework is applied. A novel idea of integrating GMM descriptions in electronic ID-cards using our framework is also proposed. The evaluation results indicate initial success that is also triggering the interest of our customers in this area.

In future we plan to apply the signature verification framework proposed in this paper for other application areas. An important area we are going to target is signature verification in forensic scenarios. We will make our framework produce decisions in terms of Log-Likelihood Ratios (LLRs) based on Bayesian approach [14], [15].

We also plan to develop a portable live application for industrial users to demonstrate the robustness of our framework. Note that the LLR analysis requires more data from more writers. Thus we plan to perform analyses on data that contain signatures from more reference writers and skilled forgers. Large and diverse test sets where signatures are produced by different authors under various different psychological and physical conditions may also yield interesting results.

REFERENCES

[1] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification – the state of the art," *Pattern Recognition*, vol. 22, pp. 107–131, 1989.

[2] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognition*, vol. 35, no. 12, pp. 2963 – 2972, 2002.

[3] R. Plamondon and S. N. Srihari, "On-line and off-line handwriting recognition: A comprehensive survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, pp. 63–84, 2000.

[4] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 609–635, Sep. 2008.

[5] V. L. Blankers, C. E. v. d. Heuvel, K. Y. Franke, and L. G. Vuurpijl, "Icdar 2009 signature verification competition," in *Proceedings of the 10th International Conference on Document Analysis and Recognition*, ser. ICDAR '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 1403–1407.

[6] M. Liwicki, "Evaluation of novel features and different models for online signature verification in a real-world scenario," in *Proc. 14th Conf. of the Int. Graphonomics Society*, 2009, pp. 22–25.

[7] J. Marithoz and S. Bengio, "A comparative study of adaptation methods for speaker verification," 2002.

[8] A. Schlapbach, M. Liwicki, and H. Bunke, "A writer identification system for on-line whiteboard data," *Pattern Recogn.*, vol. 41, pp. 2381–2397, July 2008.

[9] A. Piccini, M.and Carpignano and P. Cacciabue, "Supporting integrated design of control systems and interfaces: A human centred approach," in *Proceedings of the 8th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine-Systems*, Kassel, Germany, 2001, pp. 87–92.

[10] R. M. Julie Doyle, Zoran Skrba and B. Arent, "Designing a touch screen communication device to support social interaction amongst older adults," in *Proceedings of the 24th BCS International Conference on Human-Computer Interaction (HCI-2010)*, Dundee, Scotland, 2010.

[11] H. Koessling, D. G. Marcus Liwicki, M. W. Gerrit Meixner, and A. Dengel, "Pen-based interaction forms for smarter product customization," in *Proceedings of the 18th International Federation of Automatic Control World Congress. World Congress of the International Federation of Automatic Control (IFAC-2011), August 28 - September 2, Milano, Italy*. IFAC, 4 2011.

[12] M. Liwicki, M. Blumenstein, B. Found, C. E. van den Heuvel, C. Berger, and R. Stoel, Eds., *Proceedings of the 1st International Workshop on Automated Forensic Handwriting Analysis*, vol. 768. CEUR-WS, 2011. [Online]. Available: CEUR-WS.org/Vol-768/

[13] E. Mattijssen, C. E. van den Heuvel, and R. D. Stoel, "The relation between signature complexity and the perceived quality of signature simulations," in *Proceedings of the 15th Conference of the International Graphonomics Society*. IGS, 2011, 2011, pp. 185–189.

[14] J. Gonzalez-Rodriguez, J. Fierrez-Aguilar, D. Ramos-Castro, and J. Ortega-Garcia, "Bayesian analysis of fingerprint, face and signature evidences with automatic biometric systems," *Forensic science international*, vol. 155, no. 2-3, pp. 126–140, 2005.

[15] M. Liwicki, M. I. Malik, C. E. van den Heuvel, X. Chen, C. Berger, R. Stoel, M. Blumenstein, and B. Found, "Signature verification competition for online and offline skilled forgeries (sigcomp2011)," in *11th Int. Conf. on Document Analysis and Recognition*, Beijing, China, 2011, pp. 1480–1484.