SigSA: On-line Handwritten Signature Database

Alisher Kholmatov and Berrin Yanikoglu [*]

Sabanci University
Faculty of Engineering and Natural Sciences
Istanbul, 34956, Turkey

Abstract

Online signature verification is a challenging problem. It's difficulty comes from the problem of separation between genuine variation of an individual's signatures and that of forgery signatures. Different algorithms have been proposed by various researchers, however lack of the publically available signature databases hinders benchmarking their performances.

In this paper we introduce a signature database constructed from donations of 110 different signers. We describe acquisition process, hardware used for the acquisition as well as forgery collection. We also assess and report performance of the state of the art online signature verification algorithm using the database. The database will be made available for the academic purposes through `http://biometrics.sabanciuniv.edu/sigsa` .

Key words: On-Line Signature, Verification, Database, Handwriting, Biometrics

1 Introduction

Biometric authentication is gaining popularity as a more trustable alternative to password-based security systems. Signature is a behavioral biometric: it is not based on the physical properties, such as fingerprint or face, of the individual, but behavioral ones. As such, ones signature may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, however signature's widespread acceptance by the public, make it more suitable for certain lower-security authentication needs.

[*] Corresponding Author: Tel. +(90)-216-483-9528, Fax. +(90)-216-483-9550
E-mail addresses: alisher@su.sabanciuniv.edu, berrin@sabanciuniv.edu

Preprint submitted to Elsevier Science *11 October 2006*

Online (dynamic) signatures are captured by special hardware that extract dynamic properties of a signature in addition to its shape which is the only available information in offline (static) signatures. The signature acquisition hardware that is available in the market can be categorized into 2 major groups: i) smart pens and ii) pressure sensitive tablets. Smart pens generally have force sensors on the pen tip, which sense pen movement and acquire signature trajectory while pen is moving. On the other hand pressure sensitive tablets perceive pressure exerted by a pen tip on to their surfaces and record it's corresponding location. Depending on the hardware used following features are commonly measured at a particular sample point of a signature trajectory: i) time stamp, ii) pressure (force) exerted, iii) x & y coordinates, iv) azimuth of a pen, v) latitude of a pen, etc. Also, features such as velocity, acceleration, curvature, etc. are commonly calculated using hardware measured features and are used by corresponding verification algorithm.

Features themselves can be classified in two types: global and local. Global features are features related to the signature as a whole, for instance the average signing speed, the signature bounding box, and Fourier descriptors of the signatures trajectory. Local features correspond to a specific sample point along the trajectory of the signature. Examples of local features include pressure, distance and curvature change between successive points on the signature trajectory.

Due to more discriminative information, online signature verification is significantly more reliable than offline signature verification. While offline signature verification is used to verify signatures on bank checks and documents, application areas of online signature verification include verification in credit card purchases; authorization of computer users for accessing sensitive data or programs; authentication of individuals for access to physical devices or buildings; and protection of small personal devices (e.g. PDA, laptop).

In evaluating the performance of a signature verification system, there are two important factors: the false rejection rate (FRR) of genuine signatures and the false acceptance rate (FAR) of forgery signatures. As these two errors are inversely related, the equal error rate (EER) where FAR equals FRR is often reported. Measurement of realistic FRR & FAR is not straight forward as it is hard to obtain unbiased signature database that would contain comprehensive signature examples. For instance, genuine signatures are generally collected in single session. Then, a portion of these is used to train verification algorithm and the rest to measure FRR. However, FRR measured this way is misleading as performance could certainly change, if signatures used to train & test the system would be collected in different sessions. Obtaining forgeries is more difficult as it requires professional forgers, which would be really motivated to break the system. Instead, two forgery types have been defined: a skilled forgery is signed by a person who has had access to a genuine signature for practice. A random forgery is signed without having any information about the signature of the person whose signature is forged.

Lack of comprehensive and unbiased database hinders benchmarking performances of different verification methods. Generally, authors report performance assessment of their algorithms using their own databases, which are publically not available. In this work we aimed to collect close to realistic signature database and make it publically available free of charge.

There are two publically available signature databases up to our knowledge: MCYT **?** and the database collected for First International Signature Verification Competition (SVC 2004) **?**. MCYT contains signatures collected from 330 individuals, where there 25 genuine & 25 forgery signatures collected for each individual. Genuine signatures were collected in single session, where forgeries of an individual were provided by some other individual from the database. Although database is made publically available it is not free of charge.

SVC contains signatures collected from 100 individuals, where there 20 genuine & 20 forgery signatures collected for each individual. Signatures in this database are not real signatures, in contrary these were made up by signers just for the sake of contributing to the database. State-of-the-art results EER results for skilled forgeries reported by SVC 2004 are around 2.8% (Yeung et al., 2004).

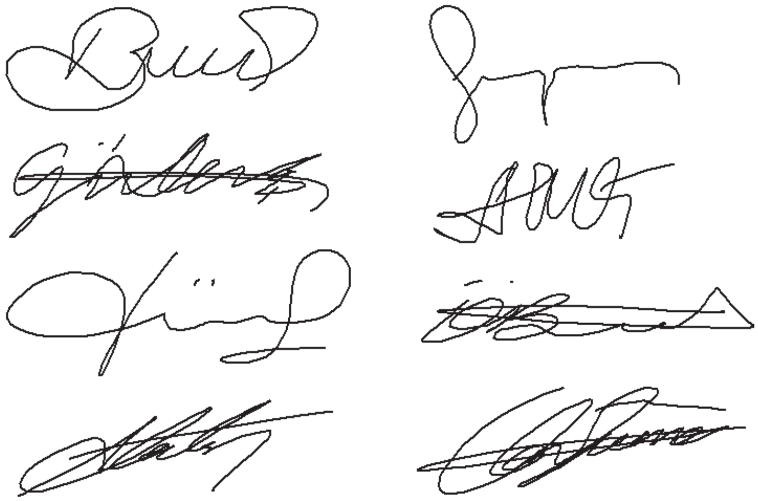

Fig. 1. Sample genuine signatures from the database.

2 SigSA Database

In this section we describe signature acquisition setup and methodology used to collect the database.

We have preferred to used Interlink Electronics's ePad-ink tablet, which has a pressure sensitive touchpad. The LCD screen of the touchpad gives visual feedback (i.e. user is able to see how he/she signs), that provides natural feeling of signing. The screen dimensions are 76 x 56mm (3" x 2.20") with 320 (H) x 240 (V) pixels and 3.8" diagonal screen display resolution. Besides, touchpad has 300 dpi resolution, 128 levels of pressure in z-axis and a sampling rate of 100 sample points per second (100Hz).

SigSA database was constructed using signatures donated by 110 unique signers (29 women & 81 men). Ages of signers vary between 21 and 52 years old. Most of the signers are students & faculty members of Sabanci University. Each signer was asked to supply samples of his/her signature which he/she was using in his/her daily life. There were no constraints on how to sign, nor was any information given about the working principles of any online signature verification system, so that the subjects signed in their most natural way. Each signer supplied 20 samples of his/her signature in two different sessions, supplying 10 signatures at each session. There was approximately 1 week time period in between two signing session.

To collect skilled forgeries, we added a signing simulation module to our system. Simulation module animates the signing process of a given signature so that the forger could see not only the signature trajectorys points sequence but also the signing dynamics (speed and acceleration). Forgers had a chance of watching the signatures animation several times and practice tracing over the signature image a few times before forging it. Doing this way 5 forgery signatures were obtained for each subject in SigSA database.

Each signature in SigSA database is stored as an ordered sequence of sample points and their features. Ordering is performed according to the time stamps of sample points. Besides, pressure exerted in z-axis as well as pen up or down events were also measured.

Table 1 summarizes SigSA database, where Figures 1 and 2 depict sample genuine and forgery signatures from the database, respectively.

Table 1
Database Summary

Data Set	*Type*	*Size*	*Samples/User*
SESSION 1	Genuine	1100	10
SESSION 2	Genuine	1100	10
FORGERY	Forgery	550	5

3 Experiments

In this section, we report & elaborate on the performance results of the state of the art signature verification algorithm using the SigSA database. We've tested the algorithm proposed by Kholmatov and Yanikoglu (2005). The algorithm received first place at the international signature verification contest Yeung et al. (2004).

We've used first five signatures from the SESSION 1 portion of the database as the reference set for each user. Next, to calculate FRR we used rest of the signatures of SESSION 1 and all signatures from SESSION 2 portion of the database. In other words, 15 genuine signatures per user (1650 in total) were used to test FRR of the algorithm. All signatures in FORGERY portion of the database (550 in total) were used to test FAR of the algorithm. Some one should notice that there was no intersection between reference set signatures and those used to test FRR, as well as non of the forgery signatures was used to train/tune the algorithm.

We have obtained 4.70% of FRR and 3.45% FAR. Closer look to the detailed results leads to the reason behind high false accept rate. The reason was that 4 users from the database had very inconsistent (Not: may be if we

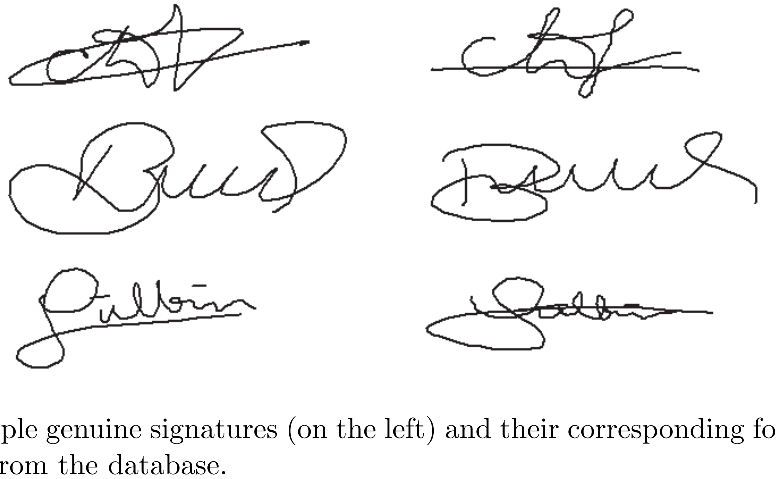

Fig. 2. Sample genuine signatures (on the left) and their corresponding forgeries (on the right) from the database.

could calculate complexity measure for these) signatures such that if we would eliminate those from the database we could achieve 0.54% of FAR, which is sufficient for many real life applications.

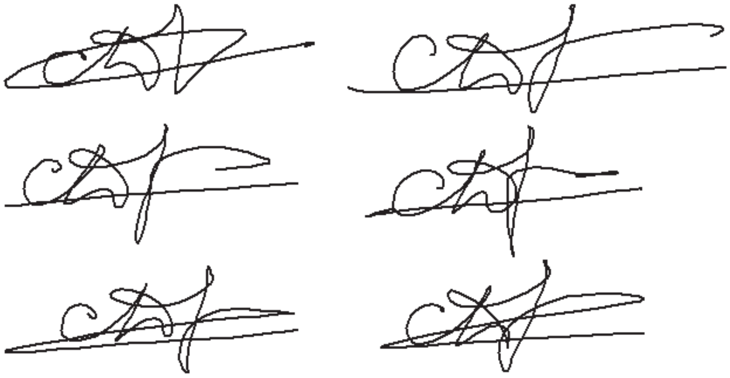

Fig. 3. Sample genuine signatures from the database which have high within class variation.

Figure 4 shows sample signatures from the database showing some very easy and very difficult signatures to forge, highlighting the fact that signature is a biometric the complexity of which can be adjusted; this is useful since one can use different signatures for different security applications.

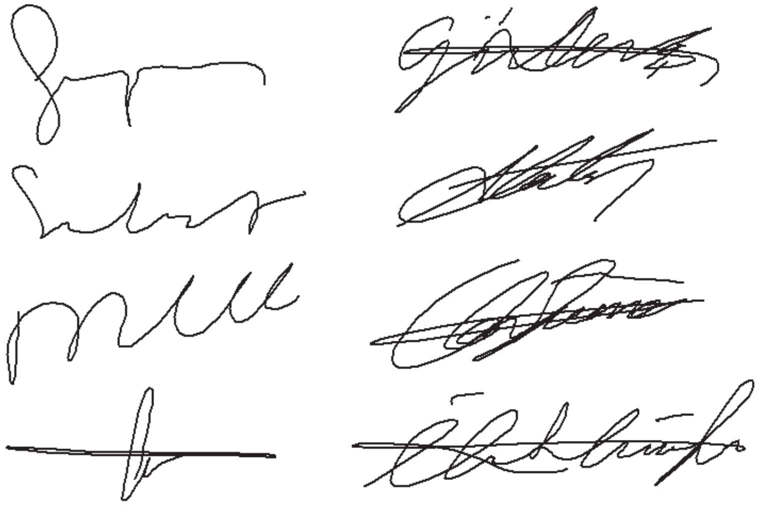

Fig. 4. Sample signatures on the left are relatively easier to forge than those on the right.

4 Database Distribution

The SigSA signature database is publically available (free of charge) to a research academia. Those interested in obtaining the database are kindly requested to drop by the web site `http:\\biometrics.sabaniuniv.edu\sigsa` and complete the database request process. References to the SigSA database are highly appreciated.

5 Summary and Conclusion

In this work, an online signature database is presented. We have explained details related to acquisition setup, features collected per signature and approaches used to collect genuine & forgery signatures, respectively.

Besides, we report the performance results of the state of the art verification algorithm using the database. Obtained results support the claim that the signature is the biometric the complexity of which is fully under the responsibility of its owner. To support the claim we've calculated complexity metric of signatures of each subject in the database. The metric indicated that 84 % of forged signatures have complexity metric greatly under the average of that of unforged signatures.

The SigSA signature database is publically available (free of charge) to a research academia. Please follow instructions described in Section 5 to obtain the database. We hope that the database will serve as the benchmark of verification algorithms.

Acknowledgments

We would like to thank Deniz Erdogan, who is an undergraduate student of Sabanci University, for her help in collection of signatures. Besides, we thank and express our respect to those who donated their signatures and their valuable time to this database.

References

Kholmatov, A., Yanikoglu, B., 2005. Identity authentication using improved online signature verification method. In: Pattern Recognition Letters. pp. 2400–2408.

Yeung, D., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G., 2004. SVC2004: First international signature verification competition. In: Proceedings of the Int. Conf. on Biometric Authentication. pp. 16–22, also available at `http://www4.comp.polyu.edu.hk/~icba/`.