

A behavioural biometric

Dr Claus Vielhauer, from the University of Magdeburg, discusses the signature as a biometric verification technique...

Biometric user recognition techniques are currently undergoing large-scale deployment, particularly due to political decisions to introduce biometric-enabled travel documents, for example, in the US and the countries of the EU. While, in the case of international passports, fingerprint and face images of the holder are to be stored digitally in the document, a number of alternative biometric modalities exist. These can be differentiated into two categories of methods: physiological and behavioural biometrics.

Physiological traits, such as hand and face geometry, or iris structure of the eye, are based on the measurement of biological properties of users by devices like digital cameras and scanners. In contrast to physiological systems, behavioural biometrics, such as recognition of subjects by voice or signatures, require an explicit action to be performed by individuals and thus imply awareness. Here, due to the traditional role of the handwritten signature, usage of signatures for automated user authentication appears to be particularly interesting in domains where combined document and user authentication is required. Signatures have been a legally and socially accepted means of authentication for centuries and are practised in the daily lives of most people, for example, for authentication in the case of credit card transactions or contract signatures. The biometric signature verification system aims to perform the authentication of persons automatically by characteristics of their signature.

Automatic user authentication based on the analysis of handwriting signals has been of interest to researchers since the 1960s. A great number of approaches based on signal and image processing have been published and, in general, recognition accuracy improved over time. From the technological point of view, a strong trend towards pen-enabled personal computers such as Personal Digital Assistants (PDA) and tablet-based personal computers (Tablet PCs) can be observed over the past 10 years. With the advances in handwriting recognition, the necessity for a keyboard as a dominant input device seems to be superfluous in many cases today. As a consequence of this

development, many personal computer systems exist today, which are already equipped with built-in digital sampling devices capable of recording handwriting dynamics, which can be used for biometric authentication purposes. This increasing availability of handwriting digitiser devices opens interesting new application areas for handwriting-based user authentication algorithms.

'Signatures have been a legally and socially accepted means of authentication for centuries and are practised in the daily lives of most people, for example, for authentication in the case of credit card transactions or contract signatures.'

Automated user authentication by signature verification has motivated a lot of work in the area of forensic image processing, for example, for automated verification of signatures on banking cheques. With the introduction of the first sampling devices for the recording of the temporal movement of the pen during writing processes, such as pen digitisers and PDAs, the new sub-discipline of online signature verification has emerged. These new online methods have shown a higher accuracy than the traditional, purely graphical approaches. Due to the additional

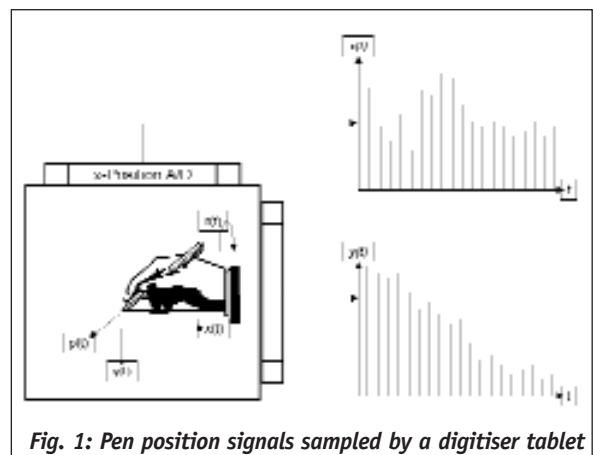


Fig. 1: Pen position signals sampled by a digitiser tablet

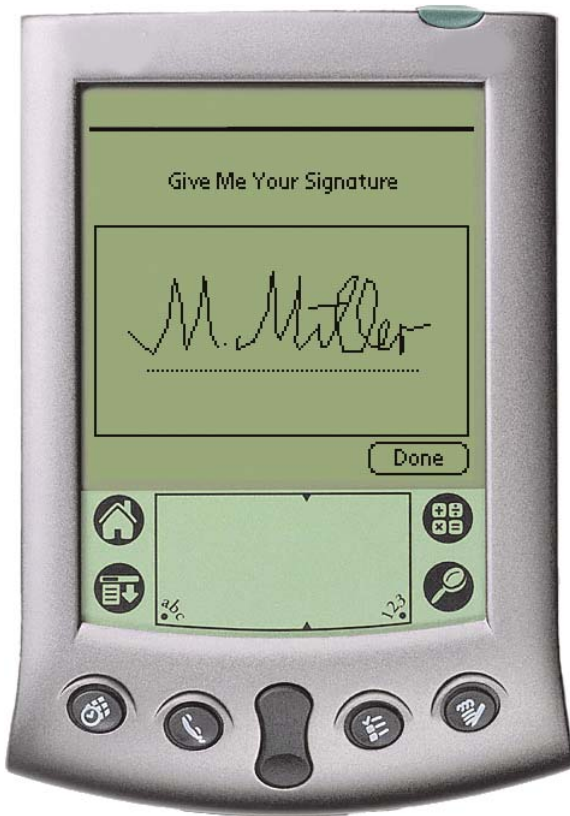


Fig. 2: Signature-based log-in screen for a PDA

information available from online digitisers, this new area has received an enormous degree of contributions from researchers and other people, mainly from the community of signal processing. However, almost all of these contributions aim to invent new algorithms and/or optimise these. Like for many other biometric modalities in this domain, which all have to deal with intrinsic fuzziness, the grand goal of accuracy improvements seems to be the predominant motivation of scientific work.

Application scenarios and commercial activities

A considerable number of commercial signature verification systems are available today, many of which represent the core of start-up companies, which have been established in recent years. Here, two main application areas can be identified: document management and access control to computer systems. In the first category, several systems are offered, which allow embedding of electronic signatures, taken from the undersigned on digitiser tablets, in various standard file formats, such as PDF and TIFF document files for authentication purposes. Most of such systems also provide a verification mode, where electronic signatures can be verified by comparison to a stored biometric reference of the original signer. Some systems additionally allow the inclusion of a unique identifier of the digitiser tablet for a later verification of the device used for signatures as well. Some of these electronic signature systems are bundles of a specific signature hardware device and software; others are solely software components to be used along with a variety of third party digitiser devices.

The other category of commercial signature verification systems address the known weaknesses in password-based access control to computer systems, as practised in most IT infrastructures today. Major problems here include the possibility that passwords are forgotten, or accidentally or purposely passed on to other, non-authorized users. Signature-based user verification may provide additional security and – compared to alternative biometric schemes like fingerprint recognition – has the benefit of requiring a specific action by the user, ie. implying an implicit declaration of intent and lifeless detection. Such signature-based access control systems are available from various providers today, for stand-alone computers, as well as for networked IT infrastructures.

‘Both error rates are intrinsic to all biometric modalities, they are correlated and dependent on system specific parameters, and therefore, they are usually presented in the form of receiver operating characteristics, also called ROC diagrams.’

Signature – a weak biometric?

Signature verification systems are often considered as weak or insecure biometrics, due to their tendency to recognition errors. As all other biometric modalities, signatures are subject to recognition errors because of two reasons. Firstly, all biometric measurements possess an intra-personal variability, that is, any two subsequent measurements of any biometrics of an identical person will never lead to exactly the same values. This effect leads to the error characteristics of false rejections, where users are rejected by a biometric system, despite the fact that they are authentic. A measurement for this effect is given by the False-Rejection-Rate (FRR) of biometric systems, ie. the occurrence probability of such kind of errors. On the other side, for any biometrics, there remains a probability of great similarity of biometric measurements of two different individuals (consider, for example, the facial images of identical twins), which leads to false acceptances of users and to the respective False Acceptance error Rate (FAR). Both error rates are intrinsic to all biometric modalities, they are correlated and dependent on system specific parameters, and therefore, they are usually presented in the form of receiver operating characteristics, also called ROC diagrams. For the sake of simplification, such error characteristics are quite often referred to at one specific operation point, the so-called Equal Error Rate (EER), denoting the point in the ROC where FAR and FRR yield the same values.

EER can be considered as a first level estimate for the accuracy of biometric systems and, consequently, they are

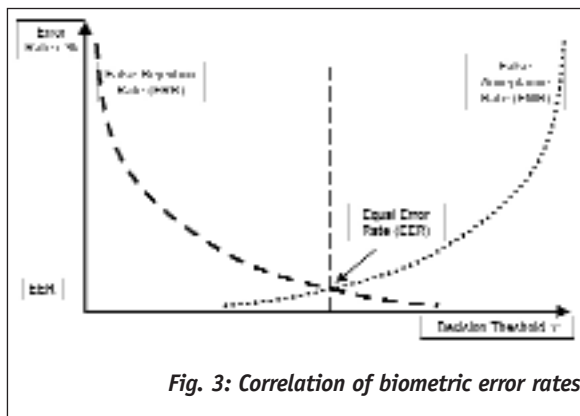


Fig. 3: Correlation of biometric error rates

often used to compare alternative biometric modalities. However, any error characteristics can only be determined empirically, that is, by observing the system's accuracy in field trials with a limited number of users and concluding from these tests to larger live populations. As, today, no standards for such evaluation tests exist, the vast majority of figures on accuracy provided for biometric systems have been determined on proprietary test sets of different type and origin, which makes between-system comparisons infeasible. To overcome this lack, scientific contests have been conducted for some biometric modalities in the recent years. Institutions were called to submit their algorithms for evaluation based on identical test sets by an independent organisation. Such contests have been performed for several modalities and results from those indicate that, for example, face recognition yields EER approximately between 5% and 10% (Face Recognition Vendor Test 2002, <http://www.frvt.org/FRVT2002/documents.htm>). The best algorithms submitted for fingerprint modalities reached an EER of approximately 2% (Third International Fingerprint Verification Competition, <http://bias.csr.unibo.it/fvc2004>) and for signatures, EER of 2-3% have also been reported for the best algorithms (SVC2004: First International Signature Verification Competition, <http://www.cs.ust.hk/svc2004/results.html>). Although these kind of comparisons have not been conducted exhaustively yet and are missing for some modalities, some of which are believed to be extraordinarily accurate (eg. iris recognition), the results can be interpreted as an indicator of the state-of-the-art in recognition accuracy.

'For large-scale international applications, the cross-cultural aspects of error rates and user acceptance of biometric writing data input become increasingly interesting.'

Given these indications, signature verification can be considered as not particularly less accurate than face or fingerprint techniques. However, it needs to be noted that the behavioural nature makes signatures vulnerable to

skilled forgeries, whereas the implicit expression of intention can make them more appropriate in document management scenarios, for example, more accurate, but passive, biometrics, such as iris recognition.

Future perspectives to signature verification

Due to the main problem intrinsic to all biometric techniques, classification errors, optimisation remains one of the most important areas of future activities for signature verification. This is reflected, for example, by activities within the Biosecure EU Network of Excellence (<http://www.biosecure.info/>), where selection and evaluation of signal enhancement and segmentation techniques, as well as feature extraction algorithms for online signatures, are being elaborated. Further, future work will address the combination of knowledge and biometrics for authentication of users, eg. by applying user specific passwords or personal identification numbers (PIN), which will be written by the users of the biometric system instead of, or in addition to, the signature. This will allow the achievement of higher accuracy of biometric authentication algorithms for handwriting. For large-scale international applications, the cross-cultural aspects of error rates and user acceptance of biometric writing data input become increasingly interesting. Recent results from the research project, CultureTech, funded by the EU-India Economic Cross Cultural Programme, show and analyse the fact that it is possible to estimate some meta-data like script language, origin, gender and age by statistically analysing human handwriting (see <http://amsl-smb.cs.uni-magdeburg.de/culturetech/>). By knowing this meta-data, it appears to be possible to adapt the recognition or authentication algorithms in order to improve their performance and/or accuracy. Further problems addressed in this project include privacy protection of personal data, both from legal and technical points of view. User authentication will also play an increasing role in some applications of Human-Computer-Interaction (HCI). Here, signatures and, more generally, natural handwriting may help to design seamless interfaces, which are similar to human-to-human interaction (see SIMILAR EU Network of Excellence: <http://www.similar.cc>).



Dr Claus Vielhauer
 Head of Biometrics Research Group
 University of Magdeburg
 Advanced Multimedia and Security
 Lab (AMSL)
 Department of Technical and
 Business Information Systems (ITI)
 Universitätsplatz 2, D-39016
 Magdeburg
 Germany
 Tel: +49 391 67 18046
 Fax +49 391 67 18110
 Claus.Vielhauer@
 iti.cs.uni-magdeburg.de
 www.iti.cs.uni-magdeburg.de/
 ~vielhaue/