

Activities in Biometrics

Henning Daum

An important aspect and a highly significant requirement for nearly all security mechanisms is the reliable authentication of users. During the authentication process the system verifies that the identity given by the user is actually associated to this person. In contrast to the identification token which is public, the information that is exchanged in the authentication process is either secret or only useful for this particular person.

Several attributes can be used to authenticate a person:

- Special knowledge like a password, a personal identification number (PIN) or other secret information,
- private property like a magnetic or smart card, or
- a characteristic attribute, i.e. a biometric feature of the person.

Biometric authentication systems use individual biometric features in order to authenticate the person's identity. A biometric feature can be static like a fingerprint, the geometry of the hand, the iris pattern of a person, or may be variable like the voice. Other biometric features vary with the behavior of a person, e.g. the written signature and the temporal characteristics of typing a sequence of keystrokes.

The use of biometric authentication has several advantages for the user as well as for the administrator. First of all, common authentication tokens like passwords and PINs can be obtained by observing its use or by social engineering. Widely used properties like keys, smart or magnetic cards can be copied more easily than a biometric feature. Therefore, the user is better protected against unwanted copying of his authorization token. On the administrator's side, the same arguments apply with the addition that a user cannot copy the feature easily even if he wants to.



Figure 1: The picture taken by an iris recognition system

German Abstract

Ein wichtiger Bestandteil vieler Sicherheitsmechanismen ist eine zuverlässige Authentisierung von Benutzern. Biometrische Authentisierungssysteme verwenden hierfür individuelle Körpermerkmale von Personen. Bekannte Verfahren sind die Fingerbildererkennung, Iriserkennung, Gesichtserkennung usw. Dabei ist neben einer guten Erkennungsleistung vor allem die Untersuchung der Überwindungssicherheit wichtig. Das Fraunhofer IGD evaluierte in 1999 in der Studie BioIS die Leistungsfähigkeit und Überwindungssicherheit von biometrischen Systemen. Die Erfahrungen daraus flossen u.a. in den Entwurf für die Technischen Evaluierungskriterien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein. Im Projekt ZAVIR werden seit 2001 weitere Systeme und biometrische Technologien auf deren Überwindungssicherheit untersucht. Im Bereich der Evaluierung führt das IGD derzeit zwei Studien für das BSI durch. In der Projektreihe BioFace wird die Leistungsfähigkeit verschiedener biometrischer Gesichtserkennungssysteme unter speziellen Umständen evaluiert, im Projekt BioFinger entsprechendes für Fingerbildererkennungssysteme.

A password, key etc. can be given to someone else, while a biometric feature will stay with the user. Another advantage is that it is nearly impossible to lose or forget the biometric feature. There are two main focuses on which biometric systems will need to concentrate: Firstly, the security of detecting forgeries and other attempts to overcome authentication, and secondly a reliable recognition of valid persons. In 1999/2000 the Fraunhofer Institute for Computer Graphics carried out BioIS. This study compared the performance and security of several biometric recognition systems and was commissioned by the German Federal Office for Information security (BSI) and the German Federal Office for Investigation (BKA).

The experiences of this first German biometrics test were introduced into the draft for the Technical Evaluation Criteria for the Assessment and Classification of Biometric Systems of the BSI and the Criteria Catalogue of the Teletrust. Since 2001 the project ZAVIR continues to research in security of biometric devices. The Fraunhofer IGD examines new biometric systems and technologies especially for resistance against fraud. The performance evaluation is also being continued.



Figure 2: The image of a handgeometry scanner



Figure 3: A fingerprint image taken by an fingerprint reader

Currently, two major studies are being carried out. In the project line BioFace, the Fraunhofer IGD examines the performance of biometric face recognition systems and algorithms. The study itself is divided into two parts: In the first part only algorithms are evaluated.

A large set of photographs was entered into a database and various face recognition systems had to pass a test program in which the images are enrolled and compared. The main focus is on the performance testing with a large number of photographs and the handling of degraded image material. The second part of BioFace consists of camera installations monitoring a site entrance. A set of test persons were enrolled into the biometric systems monitoring the entrance. The recognitions are compared to an external log to derive the recognition rate.

The performance of fingerprint systems and algorithms is being analyzed in the project BioFinger. This includes the investigation of different sensors on the differences in the resulting images of the fingerprint and the examination of technical performance such as the product life span or the deterioration during this period.

Another field of activity currently being investigated at Fraunhofer IGD is additional information extraction from iris photographs. As the iris can be used for biometric identification it is of interest how much more information can or cannot be extracted from an iris picture.

Points of contact

Dr. Christoph Busch
Dipl.-Inform. Henning Daum
Fraunhofer IGD, Darmstadt,
Germany
Email: busch@igd.fraunhofer.de
daum@igd.fraunhofer.de