Sesam öffne dich : biometrische Identifikation im Alltag

Sesam öffne dich

Armin Scharf Wird es bald keine Schlüssel mehr geben, sondern nur noch Türen, Tore und Schleusen, die sich per Fingerabdruck öffnen lassen? Die biometrische Identifikation bahnt sich langsam ihren Weg – auch in den Alltag.

Über 70 000 persönliche Jahreskarten brachte der Zoo in Hannover unter das tierliebende Volk – ein grosser Erfolg. Auf der einen Seite. Denn andererseits stieg damit auch die Zahl der «ausgeliehenen» Jahreskarten, die von Bekannten oder Verwandten der Karteninhaber genutzt werden. Daher installierte man in Hannover ein biometrisches System zur Gesichtserkennung. An den Eingängen erfassen nun Kameras die realen Gesichter der Dauerkarten-Inhaber; das System vergleicht zentrale Merkmale mit den Gesichtsdaten in der zentralen Datenbank, prüft die Eintrittsberechtigung und gibt dann die Schranke frei. Oder auch nicht. Die Anlage stammt von Bosch-Sicherheitssysteme und lässt sich laut dem Unternehmen weder von hinzugewachsenen Bärten oder Brillen beeinflussen. Dafür reduziert es die Schlangen an den Eingängen und hat den Jahreskartenverkauf sogar angekurbelt.

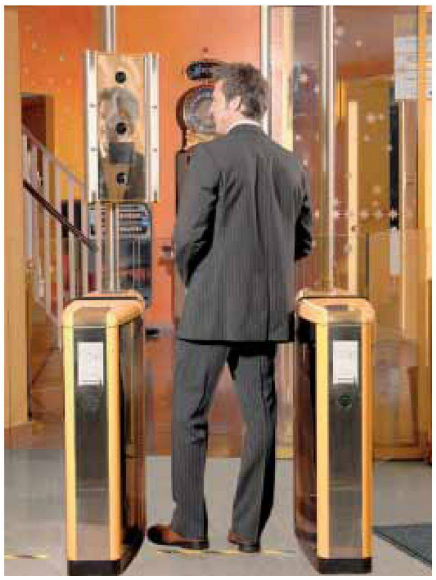
Das Prinzip, das da in Hannover offenbar sehr erfolgreich angewendet wird, nennt sich biometrische Verifikation – hier wird eine durch die Vorlage der Jahreskarte zunächst behauptete Identität bestätigt oder widerlegt. Das geschieht durch Abgleich des aktuell per Kamera ermittelten Datensatzes mit dem in der Datenbank hinterlegten Template.

Neben dem Prinzip der Verifikation steht noch das der biometrischen Identifikation, also der Ermittlung der Identität einer bestimmten Person.

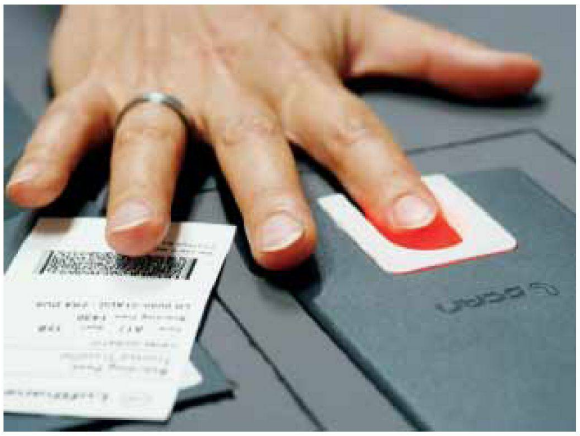
Beide Prinzipien verlangen ein abgestimmtes System aus Sensoren, Software und Datenspeicherung. Schliesslich geht es darum, körpereigene, unveränderliche und einzigartige Merkmale zu erfassen, auszuwerten und abzugleichen.

Einzigartig und eindeutig

Die biometrische Erkennung basiert auf der Tatsache, dass bestimmte Körper- und Verhaltensmerkmale ausschliesslich einem Menschen zuzuordnen sind. Diese Merkmale sind in der Regel dauerhaft an den Menschen gebunden, lassen sich nicht verändern oder von



1



2

3

ihm trennen. Zu den bekanntesten und auch schon am längsten genutzten physiologischen biometrischen Merkmalen gehört der Fingerabdruck. Er wurde schon in der Tang-Dynastie im 7. Jahrhundert genutzt, um Verträge zu authentifizieren. Ende des 19. Jahrhunderts zog der Fingerabdruck in die Kriminalistik ein, auch heute noch ist er neben der DNA-Analyse das wichtigste Ermittlungsverfahren zur Täteridentifikation.

In den 1960er Jahren begannen erste Versuche mit dem Ziel, die automatisierte Fingerabdruckerkennung als Sicherheitsverfahren zu nutzen. 1994–1996 schrieb das US-Verteidigungsministerium einen ersten Wettbewerb für Gesichtserkennungsverfahren aus – damit fiel der Startschuss für die Kommerzialisierung biometrischer Systeme. So gesehen, ist die Technologie also noch recht jung.

Dementsprechend befindet sich die Biometrie noch am Anfang ihrer Karriere – zwar sind Notebooks mit Fingerprint-Sensor zur Nutzerauthentifizierung keine Seltenheit mehr, aber die öffentliche Nutzung beginnt erst. So wird derzeit auf dem Mainzer Bahnhof die Gesichtserkennung getestet – freiwillige Probanden sollen hier aus der Menge an Reisenden zuverlässig herausgefiltert werden. Auch am Flughafen in Dubai probt man derzeit ähnliche Systeme, hat dort aber noch Probleme mit der landesüblichen Verschleierung. Denn: Um Personen zweifelsfrei identifizieren zu können, bedarf es einer Mindestzahl erfassbarer Merkmale. So werden bei der Gesichtserkennung zwar bis zu 8000 Einzelinformationen erfasst, doch muss das Gesicht mindestens zur Hälfte sichtbar sein. Abschattungen bereiten nach wie vor Probleme, weshalb in manchen britischen Kaufhäusern das Tragen von Hüten verboten ist. Hintergrund dieser in Grossbritannien weit verbreiteten Überwachung des öffentlichen und halböffentlichen Raumes ist vor allem die Terrorabwehr. Dafür eignet sich die Gesichtserkennung besonders, da sie für die betroffenen Personen unbemerkt stattfinden kann.

In der Schweiz kann man seit Ende 2006 den Pass 06 beantragen, der auf einem integrierten Chip die Gesichtsdaten des Eigentümers speichert. Bei der Kontrolle werden dann die berührungslos auslesbaren Daten mit dem Reisenden verglichen. Noch handelt es sich um ein Pilotprojekt, doch für USA-Reisende, die keinen Pass 03 besitzen, ist er unumgänglich.

Finger, Iris und Gesicht

Prinzipell stehen derzeit drei Verfahren zur Verfügung, die physiologische Merkmale nutzen: die Fingerprint-, Gesichtsfeld- und Iriserkennung. Daneben sind noch verhaltensbezogene Verfahren zu nennen, die Personen beispielsweise an ihrer Stimme, ihrem Tastaturanschlag oder ihrem Gang erkennen können. Die grösste Verbreitung bisher aber haben jene Verfahren, die mit Fingerabdrücken arbeiten.

Spezielle Sensoren nehmen den Fingerabdruck auf, setzen ihn in ein digitales Muster um, das softwaretechnisch bearbeitet und als Template mit den hinterlegten Vergleichsdaten abgeglichen wird. Dabei können das gesamte Bild, relevante Einzelbereiche oder die so genannten Minuzien als Vergleichsbasis dienen. Rund 44 Prozent der biometrischen Anwendungen basieren auf der als ausgereift geltenden Fingerprint-Erkennung. Sie lässt sich für viele Anwendungen nutzen, ist klein und wird von den Nutzern akzeptiert. Die Nutzerausfallrate bezogen auf die Gesamtbevölkerung soll bei rund fünf Prozent liegen, bei definierten Nutzerkreisen, beispielsweise Firmenangehörigen, sinkt die Fehlerrate unter ein Prozent.

Zeiterfassung und stiller Alarm

Beliebt ist der Finger als Ausweis im Zusammenhang mit der betrieblichen Zeiterfassung. So werden die Zeiterfassungsterminals mit entsprechenden Modulen nachgerüstet oder komplett ersetzt; die Mitarbeiter loggen sich dann nur noch mit dem eigenen, vorher festgelegten und hinterlegten Finger in das Zeitsystem

1 Am Eingang zur Spielbank in Bad Homburg prüft ein biometrisches Gesichtserkennungssystem die Besucher auf freiwillig gesperrte Personen, die dann dezent vom Spielen abgehalten werden. – Bild: Bosch

2 Am Frankfurter Flughafen testete die Lufthansa mit 400 Mitarbeitern, wie sich Passagiere per Fingerprint beim Boarding ausweisen können. Dazu wird der Fingerabdruck als zweidimensionaler Code auf die Bordkarte gedruckt, das System verifiziert dann beim Einstieg, ob es sich um den eingecheckten Passagier handelt. Bild: Siemens

3 Per Speedgate in die Bank: Die Mitarbeiter der Genfer Pictet & Cie Banquiers gelangen nach einer Gesichtserkennung zu ihrem Arbeitsplatz. Dabei wird automatisch auch die Zeiterfassung gestartet. Bild: Interflex

4 Sieht unspektakulär aus, ist aber höchst innovativ: Die Iriserkennung sichert bei Pictet & Cie Banquiers besonders sensible Bereiche innerhalb des Gebäudes extra ab. – Bild: Interflex

5 Zeiterfassung per Fingerabdruck: In vielen Unternehmen ersetzt diese Technik die Ausgabe und Verwaltung von Mitarbeiter-Ausweisen. – Bild: Interflex

ein. Das erspart die aufwändige Verwaltung von Ausweisen oder anderen Karten, die häufig verloren gehen. Die Verifizierung dauert in der Regel weniger als eine Sekunde, sollte der Mitarbeiter einen verletzten Finger haben, kann er sich meist noch über einen PIN-Code einbuchen.

Sind Zugänge per Fingerprint abgesichert, so lässt sich bei sensiblen Bereichen ein zusätzliches Feature einbauen, der so genannte stille Alarm. Wird zur Authentifizierung ein anderer Finger als der festgelegte benutzt, so kann dies für Dritte unbemerkt einen Alarm auslösen. Und auch das Mehraugen-Prinzip lässt sich in Hochsicherheitsbereichen umsetzen: Dann müssen sich mehrere Personen in genau festgelegter Abfolge mit definierten Fingern über das System ausweisen – erst dann öffnet sich der Zugang etwa zu Tresorräumen.

Im Privatbereich zählt eher das Komfortargument, ohne Schlüssel Zugang zur Wohnung oder bestimmten Bereichen zu haben – und zwar nicht nur im gehobenen Wohnbereich. Gerade für Familien mit Kindersegen bedeutet der biometrische Türöffner weniger Stress mit verlorenen oder vergessenen Schlüsseln – schliesslich trägt jedes Kind seinen Schlüssel stets mit sich.

Schau mir in die Augen

Mit der Iris, also der Regenbogenhaut, die die Pupille des Auges umschliesst, steht ein weiteres charakteristisches Merkmal zur Verfügung. Denn die Strukturen der Iris sind bei jedem Menschen unterschiedlich, selbst bei eineiigen Zwillingen. Daher gilt die Iriserkennung als eines der genauesten biometrischen Verfahren und wird daher in Hochsicherheitsbereichen genutzt. So kann es unter 30 Millionen Versuchen, das System zu überwinden, statistisch zu maximal einer Falschakzeptanz kommen.

Weil dunkle Augenfärbungen die Strukturen nur schwer erkennen lassen, wird bei der Aufnahme die Iris mit unsichtbarem Licht des nahen Infrarotbereichs beleuchtet, ohne das Gegenüber zu blenden. Aus den Aufnahmen extrahieren mathematische Methoden mehrere hundert Merkmale und bilden daraus einen kompakten Datensatz, der als Template für die Verifizierung dient.

Schlüssellose Bank

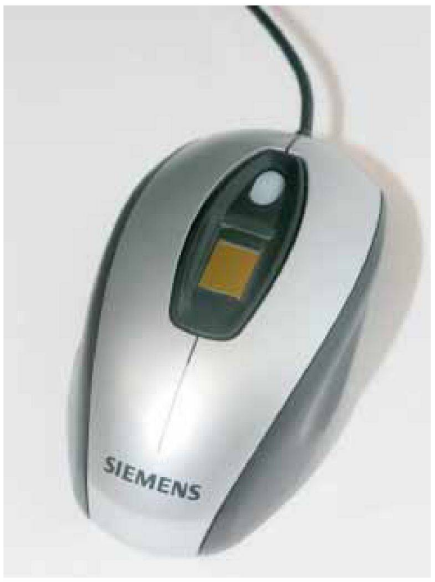
Wie die einzelnen biometrischen Verfahren in sehr sicherheitsrelevanten Bereichen zusammenwirken können, zeigt das Beispiel der Genfer Privatbank Pictet & Cie Banquiers.[1] Der Bankvorstand beschloss, seinen Neubau für rund 1500 Mitarbeiter ausschliesslich mit biometrischen Zugangstechniken auszurüsten, also komplett auf traditionelle Schlüssel oder Ausweise zu verzichten. Die Umsetzung dieses engagierten Vorhabens gilt in seiner Grössenordnung als weltweit einzigartig. Die Herausforderung auf technischer Seite lag vor allem darin, die für sich erprobten Technologien von ihrem Stand-Alone-Status in ein integriertes Gesamtsystem zu überführen.

So stammt die 3D-Gesichtserkennung für die Zutrittskontrolle und Zeiterfassung vom kanadischen Hersteller A4Vision. Aus dem Gesicht wird ein Raster von 40 000 messbaren Punkten generiert, diese in ein dreidimensionales Datenmodell überführt und mit den hinterlegten Modellen verglichen. Diese sehr genaue Identifikation läuft in weniger als einer Sekunde ab und sichert die Eingangsbereiche der Bank. Innere Hochsicherheitsbereiche wie Tresore oder Rechnerräume werden zusätzlich durch eine Iriserkennung der Byometrics AG abgesichert – insgesamt sind dafür rund 70 Kameras im Einsatz. Mit speziellen Zutrittsschleusen zur Personenvereinzelung wird garantiert, dass ausser der berechtigten Person keine weiteren Personen Zugang bekommen. Zu guter Letzt überwacht eine automatische Kennzeichenerkennung von Recognitec die Parkbereiche und Lieferzonen.

Die Gesamtkosten für die komplexe Technik sind laut Bank um etwa 20 Prozent höher als bei konven-

1 In Heft 9|2007 wird werk, bauen + wohnen ausführlich über den Bau berichten.

6 Ersetzt den Schlüssel: Das Fingerprint-System von Schüco ist dezent in den Türrahmen integriert und ist auch für den privaten Bereich interessant. – Bild: Schüco



7 Bequem einloggen: Mit der ID Mouse pro 3 von Siemens identifiziert sich der PC-Nutzer über seinen Fingerabdruck und wird von der Passwort-Eingabe befreit. Die Maus erleichtert zudem die Arbeit von mehreren Nutzern an einem Rechner. Bild: Siemens

8 Seit Ende 2006 gibt es in der Schweiz den Pass 06, der auf einem integrierten Chip die Gesichtsdaten des Eigentümers speichert. – Bild: Siemens

tionellen Ausweis-Anlagen. Dem stehen geringere laufende Kosten durch die obsolet gewordende Ausweisverwaltung und die bessere Zeiterfassung gegenüber.

Vom Auge zum Ohr

An der Universität Southampton macht man sich derweil über das Ohr her – dort hat man ermittelt, dass Ohren sehr individuelle Formen haben, und hat diese sogleich an 63 Personen überprüft. Die Ohrenform wird durch eine optische Analyse in einen Code umgewandelt, der Vergleiche mit anderen Ohren erlaubt. Die erste Versuchsreihe ergab eine Übereinstimmung von 99,2 Prozent, was die Forscher frohlocken liess. Nachfolgestudien sind in Planung, und vielleicht erkennt das Handy dereinst seinen Besitzer an der Ohrenform. Und das wäre doch auch ganz nett. ■

Armin Scharf arbeitet als freier Journalist und Texter in Tübingen. Er widmet sich insbesondere jenen Themen, bei denen durch neue Technologien neues Design bzw. neues Bauen entsteht. www.bueroscharf.de

Produkte: www.interflex.de, www.a4vision.com, www.kaba.de, www.bsi.bund.de/biometrie, www.bosch-sicherheitssysteme.de, www.biometrix.at, www.sagem.ds.comwww.iid.com, www.schueco.com, www.soton.ac.uk, www.siemens.de

Weiterführende Literatur: Michael Zinganel, Real Crime – Architektur Stadt & Verbrechen, Edition Selene, Wien 2003. Im Besonderen die Kapitel «Mikroarchitekturen der Sicherheitsindustrie» und «X-Large – Airport. Das Paradox von Offenheit und Überwachung moderner Transiträume».

résumé **Sésame ouvre-toi!** Procédés biométriques pour le contrôle des individus N'y aura t-il bientôt plus de clé, mais seulement des portes, des portails et des sas qui s'ouvrent grâce à une empreinte digitale? À l'entrée du zoo d'Hanovre, des cameras saisissent les visages réels et les données stockées dans les cartes d'abonnement des visiteurs. Cela devant empêcher l'utilisation de ces cartes personnelles par une tierce personne. Le principe se nomme «vérification biométrique».

Parallèlement il existe l'«identification biométrique»: la saisie de l'identité d'une personne donnée. Les deux principes requièrent un système coordonné de capteurs, logiciel et banque de données. Actuellement, il y a principalement trois procédés qui utilisent ainsi des caractéristiques physiologiques: l'empreinte digitale, la reconnaissance du visage et celle de l'iris. En outre, on peut aussi mentionner les procédés d'analyse comportementale qui identifient une personne à sa voix, sa dynamique de frappe au clavier, ou sa démarche.

Les procédés les plus répandus sont ceux qui utilisent les empreintes digitales. Celles-ci étaient déjà utilisées au 7e siècle sous la dynastie Tang pour authentifier les contrats. Elles firent leur entrée à la fin du 19e siècle dans la criminalistique, et restent encore aujourd'hui. Dans les années soixante, débutèrent les premiers essais ayant pour objectif d'utiliser la reconnaissance automatisée des empreintes digitales comme système de sécurité.

La biométrie se trouve encore au début de sa carrière. Son utilisation dans le domaine publique ne fait que commencer, avec – avant tout – la lutte contre le terrorisme comme toile de fond. La reconnaissance de visages s'y prête particulièrement bien puisqu'elle peut s'effectuer à l'insu des personnes concernées. En Suisse aussi, le projet pilote «Pass 06» enregistre des caractéristiques faciales et permet une comparaison sans contact direct.

L'exemple de la banque privée Pictet & Cie Banquiers à Genève, qui fonctionne uniquement avec des techniques d'accès biométriques, donc entièrement sans clé ni papier d'identité, montre comment les différents procédés biométriques peuvent agir ensemble. L'identification s'opère en moins d'une seconde et sécurise les zones d'accès de la banque. Les zones de haute sécurité, comme la salle des coffres, ou celle des ordinateurs, sont protégées de surcroît par une reconnaissance de l'iris, le plus précis de ces procédés. Et grâce à des sas d'accès spéciaux isolants les individus, on obtient la garantie qu'en dehors de la personne autorisée, personne d'autre n'y ait accès. ■

summary **Open, Sesame** Biometric methods of person control Will keys soon be obsolete, leaving doors, gates and access channels that can be opened only by fingerprint? At the entrance to the zoo in Hanover cameras compare real faces with data stored on the season tickets, the aim being to prevent these cards being used by persons other than those they were issued to. This principle is called biometric verification.

There is also the principle of biometric identification that establishes the identity of a specific person. Both principles require a coordinated system of sensors, software and data storage. Essentially at present there are three systems available that use physiological characteristics: recognition of the fingerprint, of the facial features and of the iris. There are also behaviour-related processes that can recognise people from their voice, the way they use a keyboard or the way they walk.

Most widespread are the processes that work with fingerprints. The fingerprint was used in the 7th century in the Tang dynasty to authenticate documents. At the end of the 19th century it entered the world of criminology. The first attempts at using automated fingerprint recognition as a security measure were made in the 1960s. Biometry is still at the start of its career – although notebooks with fingerprint sensors for user authentication are no longer rare, the public use of this technology is only starting. The background to this surveillance is, above all, the battle against terrorism. Face recognition is particularly useful here, as it can be carried out unbeknown to the persons concerned. Pass 06 that has been introduced as a pilot project in Switzerland stores facial characteristics and allows comparisons to be made without contact.

How individual biometric processes can work together is shown by the example of the private bank Pictet & Cie Banquiers in Geneva that operates entirely with biometric access technology, i.e. completely without keys or ID cards. Identification is carried out in less than a second and secures the entrance area of the bank. Internal high security areas such as safes or computer rooms are additionally protected by iris recognition, the most precise of these processes. With the use of special access gates to separate persons entering, it is possible to ensure that nobody, apart from those entitled to do so, can gain access. ■