Impressum

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich AGN
"Biometrik-Projekt"

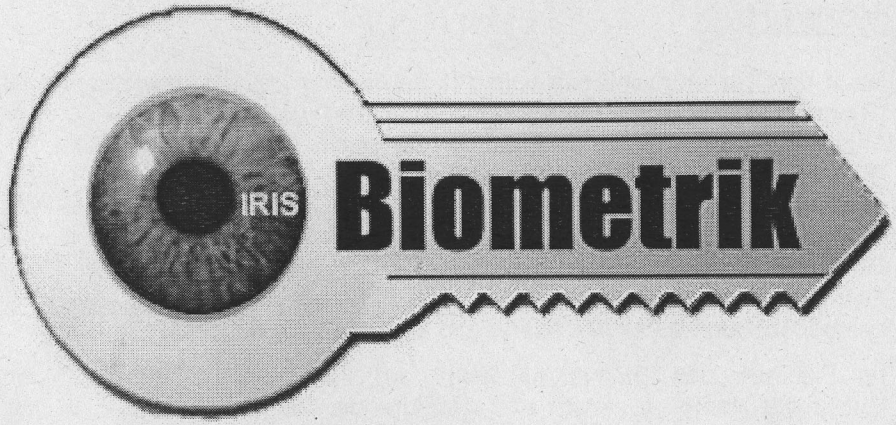
Vogt-Kölln-Straße 30
22527 Hamburg

Telefon: ☎040 / 42883 - 2405 (Sekretariat)

Fax: ☎040 / 42883 - 2226

eMail: biometrik@informatik.uni-hamburg.de

Web-Seite: http://agn-www.informatik.uni-hamburg.de



Biometrik in der Gesellschaft

Version 2.2

Projektgruppe:
Oliver Ellenbeck, Martin Johns, Marcel Kronberg, Willem Froehling, Aleksander Koleski, Christian Paulsen, Samer Abdalla und Timo Abschinski

Vorwort

Nach den Terroranschlägen vom 11. September 2001 ist der Begriff der "Biometrie" bzw. "Biometrik" zum Aufspüren von Terroristen in aller Munde. Eine Forschungsrichtung, die sich in der Informatik der Authentikation von Personen gegenüber IT-Systemen widmet, steht nunmehr vor der politisch-gewollten und eventuell gesellschaftlich gestützten Anforderung die Machbarkeit IT-basierender Identifikation von Personen anhand digitalisierter biologischer Merkmale einzuschätzen. Zahlreiche Faktoren der technischen Machbarkeit und datenschutzrechtlicher Anforderungen sind hierbei einzubeziehen.

Im Rahmen des Biometrik-Projekts am Fachbereich Informatik der Universität Hamburg setzen sich Studierende der Informatik bereits seit dem Wintersemester 1999/2000 im Hauptstudium mit Konzepten und Techniken biometrischer Algorithmen und Authentikationsystemen auseinander. Hierbei wurden von Anfang an nicht nur die technische Machbarkeit von biometrischen (Überwachungs-/Authentikations-) Systemen betrachtet, sondern auch kritisch die gesellschaftlichen Auswirkungen des Einsatzes biometrischer Systeme im Sinne des Datenschutzes und des generellen Schutzes der Privatsphäre diskutiert.

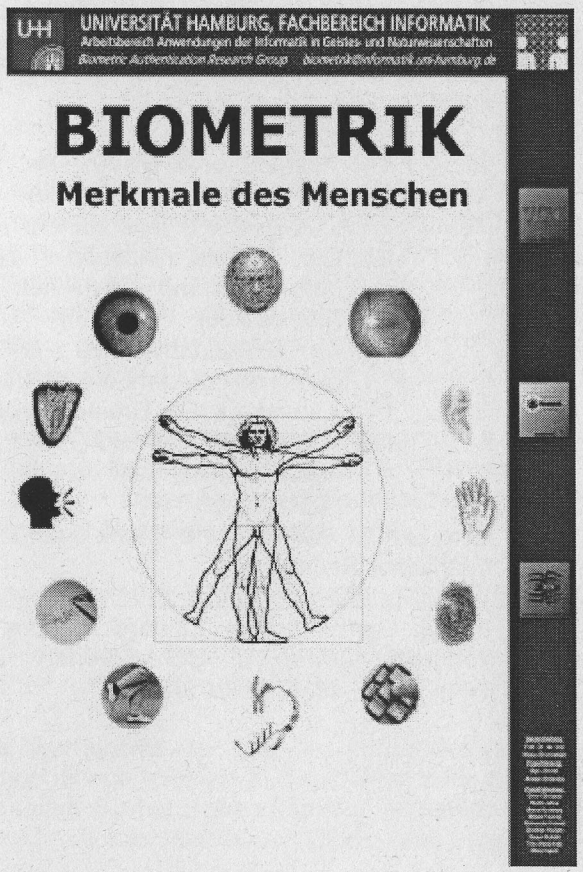
Im Rahmen des Biometrik-Projekts ergeben sich Möglichkeiten zur Anfertigung von Projektberichten, Baccalaureats-, Studien- und Diplomarbeiten sowie die Gelegenheit zur Mitwirkung an internationalen Fachpublikationen. Mit dieser Broschüre beabsichtigt das Biometrik-Projekt der Öffentlichkeit kostenfrei Informationen zum Thema Biometrik bereitzustellen.

Während der *Hamburger Computertage 2003* stehen die Mitglieder des Biometrik-Projekts für Fragen und Diskussionen der Öffentlichkeit zur Verfügung und stellen zusätzlich selbstentwickelte praktische Ergebnisse zur optischen Erfassung biometrischer Merkmale im Logon eines Betriebssystems und auf Applikationsebene vor.

Wir danken an dieser Stelle dem ehemaligen Projektleiter, Herrn Arslan Brömme, der dieses Projekt ins Leben gerufen hat. Ende 2002 verließ Herr Brömme die Biometrik-Gruppe aufgrund einer beruflichen Veränderung.

Biometrik Projektgruppe, Januar 2003

Inhalt:



Was ist "Biometrik" ?

Der Begriff Biometrik setzt sich aus den Bestandteilen "Biologie" und "Metrik" zusammen:

Biologie,die:

1. Wissenschaft von den Lebewesen und den Gesetzmäßigkeiten des Lebens
2. Beschaffenheit eines Lebewesens
3. der Natur entsprechende Beschaffenheit

(Aus: Langenscheidts Fremdwörterbuch
- Onlineausgabe
http://www.langenscheidt.aol.de/)

Metrik, die:

Der mathematische Begriff Metrik verallgemeinert das Verhältnismaß „Abstand“ auf beliebige Mengen:
Definiert eine Abbildung d aus dem betrachteten Raum bzw. der betrachten Menge (X) in die reellen Zahlen.
$d: X \times X \rightarrow IR$
$(x,y) \rightarrow d(x,y)$
d(x,y) heißt Abstand oder Distanz zwischen x,y. Die Abbildung hat für alle Elemente des Raums (hier x,y und z) folgende Eigenschaften:

- (M1) Der Abstand zwischen x und y ist gleich dem Abstand zwischen y und x (Symmetrie).
- (M2) Der Abstand zwischen x und z ist kleiner / gleich der Summe der Abstände zwischen x,y und y,z (Die Dreiecksungleichung).
- (M3) Wenn der Abstand zwischen x und y gleich null ist, folgt daraus, dass x und y gleich sind.

Eine Menge, auf der eine Metrik definiert wurde heißt metrischer Raum.

(Nach: Gerd Fischer, "Lineare Algebra", 8. Auflage, Friedrich Vieweg & Sohn Verlag, Braunschweig Wiesbaden, 1985, Seite 189)

Die Zusammenfassung der Begriffe zu **Biometrik** beschreibt u.a. eine Klasse von sogenannten biometrischen Algorithmen, die eine Computer-gestützte Vergleichbarkeit von verschiedenen digitalen Aufzeichnungen biologischer Personenmerkmale, wie z.B. den Fingerabdruck oder das Muster der Iris, herstellen. Biometrische Algorithmen spannen einen metrischen Raum auf, in dem die Abstände verschiedener biometrischer Merkmale mathematisch eindeutig definiert sind. Je kleiner der Abstand zweier biometrischer Merkmale ist, desto ähnlicher sind sich die Merkmale. Daraus resultiert die folgende Definition:

Biometrischer Algorithmus: Ein Verfahren, das aus einem biologischen Merkmal eine vergleichbare Kenngröße generiert. Diese Kenngröße heisst "biometrische Signatur".

In diesem Zusammenhang sei darauf hingewiesen, dass bei gängigen biometrischen Authentikationssystemen die Berechnungen des Algorithmus auf einer digitalisierten Aufzeichnung des biologischen Personenmerkmals durchgeführt werden.

Bei der Iriserkennung wird beispielsweise das digitalisierte Bild der zu analysierenden Iris verwendet. Aus diesen Gründen findet, bevor der eigentliche biometrische Algorithmus zu greifen beginnt, eine Abstraktion von dem eigentlichen biologischen Merkmal statt. Die Güte der Aufzeichnung der Iris ist von verschiedenen äußeren Einflüssen wie dem Beleuchtungszustand des Raumes, die Position der Person zur Kamera, der Winkel der Kopfneigung abhängig. Aus diesem Grund unterscheiden sich i.A. die generierten biometrischen Signaturen zweier unterschiedlicher Abbilder eines Merkmales des selben Menschen.

Die Eignung eines biometrischen Algorithmus wird u.a. daran gemessen, dass die Signaturen zweier unterschiedlicher Abbildungen des selben Merkmales nahe beieinander liegen, während der Abstand der Signaturen zweier verschiedener Merkmale groß sein sollte.

Anwendung der Biometrik – Authentikation und Identifikation

Biometrische Algorithmen finden in den beiden (verwandten) Bereichen der biometrischen *Authentikation* und *Identifikation* Anwendung.

Biometrische Authentikation: Bei der Authentikation geht es darum, eine vorher angegebene Identität zu verifizieren oder zu falsifizieren. Man weist anhand seiner biometrischen Signatur gegenüber einem IT-System nach, dass man tatsächlich die Person ist, die man vorgibt zu sein.

Fallbeispiel für eine biometrische Authentikation – der Bankautomat: Anstatt seine Identität einem Geldautomaten gegenüber durch die Kenntnis der PIN (persönliche Identifikationsnummer) nachzuweisen, wird sich eventuell der zukünftige Kontobevollmächtigte durch das Einscannen seines Fingerabdruckes ausweisen. Zuvor könnte dem Geldautomaten z. B. über das Einschieben einer Smartcard mitgeteilt werden, auf welches Konto zugegriffen werden soll. Neben der Kontonummer kann auf der Karte auch die biometrische Signatur des Fingerabdruckes des Kontobevollmächtigten als Vergleichswert abgelegt sein. Der Geldautomat berechnet nun aus dem eingescannten Fingerabdruck der Person, die Zugriff auf das Konto wünscht, eine biometrische Signatur und vergleicht diese mit der auf der Karte gespeicherten. Wenn der Vergleich positiv verläuft, wird der Zugriff auf das Konto gestattet.

Biometrische Identifikation: Bei der Identifikation wird anhand einer biometrischen Signatur die Identität der zugehörigen Person ermittelt. In diesem Fall muss die zu überprüfende biometrische Signatur gegen die gesamte Datenbank aller in Frage kommenden Signaturen getestet werden. Gesetzt den Fall, dass die Signatur einer der gespeicherten Signaturen hinreichend ähnlich ist, wird die Identität des Trägers der gespeicherten Identität als Antwort ausgegeben. Falls keine der gespeicherten Signaturen nahe an der untersuchten Signatur liegt, scheitert die Identifikation.

Fallbeispiel für eine biometrische Identifikation – das Fußballstadion: Eine mögliche Anwendung für einen biometrischen Algorithmus, der eine Identifikation erlaubt, ist die Ermittlung der Anwesenheit von bekannten Hooligans in einem Fußballstadion. Für diesen Zweck könnten mit ausreichend guter Kameratechnik die Sitzreihen des Stadion abgefilmt werden. Für die anwesenden Zuschauer werden die biometrischen Signaturen (z.B. der Gesichtsgeometrie) ermittelt. Nach diesem Schritt ist man in der Lage, diese Signaturen gegen eine Datenbank von bekannten Hooligans zu Testen, um so die Anwesenheit dieser Personen festzustellen.

Verallgemeinert lässt sich sagen, dass die Ansprüche an biometrische Algorithmen, die eine Identifikation von Personen ermöglichen sollen, höher sind als die an biometrische Algorithmen zur Authentikation.

Geeignete biologischer Merkmale

Um für eine biometrische Anwendung geeignet zu sein, muss das verwendete Merkmal bestimmte Eigenschaften ausweisen:

Eindeutigkeit für jede Person: Lediglich Merkmale, die zwischen einzelnen Personen deutlich variieren sind für biometrische Anwendungen geeignet, denn nur dieses sichert zu, dass für zwei verschiedene Merkmale (bzw. Personen) auch unterschiedliche biometrische Signaturen vorliegen.

Unveränderlichkeit durch Alterung: Ein Merkmal, dass sich im Laufe der Zeit deutlich ändert, ist nicht für alle Anwendungen geeignet, da eine Erkennung des Trägers nur in einem (nicht klar zu bestimmenden) Zeitfenster möglich ist.

Bei der Klassifizierung biologischer Merkmale unterscheidet man zwischen *phänotypischen* und *genotypischen* Merkmalen.

Genotypisch: Die Erscheinung genotypischer Merkmale ist vollständig durch die Erbanlagen des Trägers festgelegt. Dieses führt dazu, dass genotypische Merkmale bei eineiigen Zwillingen die gleiche Signatur erzeugen. Ein Beispiel für ein genotypisches Merkmal ist die DNA eines Menschen.

Phänotypisch: Die Ausprägungen phänotypischer Merkmale werden neben den Erbanlagen auch von den Umwelteinflüssen, denen der Träger zu einem frühen Zeitpunkt seiner Entwicklung ausgesetzt war, bestimmt. Dieses führt dazu, dass diese Merkmale sich auch bei Menschen mit den selben Erbanlagen unterscheiden. Ein Beispiel für phänotypische Merkmale sind die Strukturen der menschlichen Iris und der Fingerabdruck.

Für u.a. folgende biologische Merkmale sind biometrische Verfahren entwickelt worden: Fingerabdruck, Handgeometrie, Iris, Retina, Gesicht, Sprache, DNA, Bewegungsabläufe.

Bewertung eines biometrischen Algorithmus - FAR / FRR

Die Ergebnisse der Anwendung eines biometrischen Algorithmus auf unterschiedliche Aufnahmen des selben Merkmals (beispielsweise verschiedene Bilder der selben Iris) sind i.A. nicht 100% identisch, sondern nur nahe beieinander. Aus diesem Grund muss ein biometrischer Algorithmus innerhalb eines gewissen Toleranzrahmens Signaturen als zu dem selben Merkmal (bzw. zu dem selben Träger) gehörend erkennen. Ähnliche Signaturen werden als "gleich" und Signaturen, deren Abstand außerhalb des Toleranzrahmen ist, als "unterschiedlich" bewertet. Die Festlegung dieses Toleranzrahmens besitzt signifikanten Einfluss auf die Güte einer biometrischen Algorithmus. Legt man den Toleranzrahmen zu großzügig fest, kann es leichter zu Fehlurteilen kommen, ist er zu eng gewählt, kann es passieren, dass auch der Träger der Signatur nicht korrekt erkannt wird (z.B. bei zu schlechter Qualität der Bilddaten).

In diesem Zusammenhang spricht man von zwei Kenngrößen: der *FAR* und der *FRR*.

False Acception Rate (FAR): Bezeichnet die Rate der fehlerhaften Zuordnungen einer Signatur zu einen Träger. Je höher also die FAR, desto größer ist die Wahrscheinlichkeit, dass ein Betrüger erfolgreich eine falsche Identität vortäuschen kann.

False Rejection Rate (FRR). Bezeichnet die Rate der fehlerhaft fehlgeschlagenen Zuordnungen von Signaturen, also die Wahrscheinlichkeit, mit der einem Kontobevollmächtigten der Zugriff verweigert wird.

Die Kenngrößen FRR und FAR sind i.A. von einander abhängig. Eine Verbesserung der einen Größe hat im allgemeinen eine Verschlechterung der anderen zur Folge. Wenn der Toleranzrahmen für die Signaturen eingeengt wird, führt dieses z.B. zu einer niedrigeren FAR, da das Kriterium für die Erkennung einer Signatur verschärft wurde, resultiert aber ebenso in einer Erhöhung der FRR, da nun auch die Anforderungen an die Aufnahme des Merkmal erhöht wurden.

Beispiel: Fingerabdruckerkennung

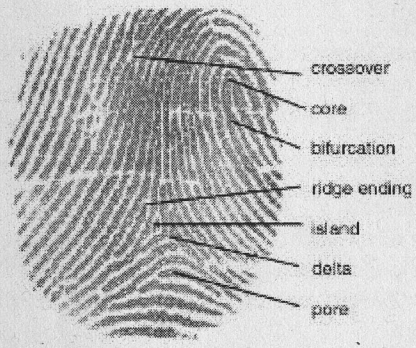
1. Merkmale von Fingerabdrücken

Der menschliche Fingerabdruck besteht aus verschiedenen Rillenmustern, die traditionell in fünf Basistypen unterteilt werden:

1. left loop (linke Schleife)
2. right loop (rechte Schleife)
3. arch (Bogen)
4. whorl (Wirbel)
5. tented arch (spitzer Bogen)

(Einteilung nach Henry)

Charakteristische Punkte eines Fingerabdrucks, beispielsweise Verzweigungs- und Endpunkte von Linien, nennt man Minutien. Sie bilden die Basis für die meisten Fingerscan-Verfahren. (siehe Abb.1)



Man unterscheidet verschiedene Arten von Minutien:

- Kreuzungen
- Punkte
- Striche
- Haken
- Verzweigungen
- Poren (nur bei hoher Auflösung erkennbar)

Abb.1

Ebenfalls essentielle Merkmale sind Cores und Deltas. Core nennt man den inneren Punkt, das Herzstück des Abdrucks. Er bildet das Zentrum der Schleifen und Linien und liegt häufig mittig. Deltas nennt man die Punkte, an der drei Linien von Rillen aneinander vorbeilaufen.

2. Fingerscan-Technologie

Die Fingerscan-Technologie beruht auf der Einzigartigkeit von Fingerabdruckmustern.
Es wird zunächst ein Bild eines Fingerabdrucks aufgenommen, bestimmte Merkmale extrahiert und in einer Fingerabdruckschablone (Template) gespeichert. Mit Hilfe dieser Daten können Personen identifiziert bzw. verifiziert werden.

Die Fingerabdruck-Technologie ist die am meisten verbreitete biometrische Technologie. (Siehe Abb.2)

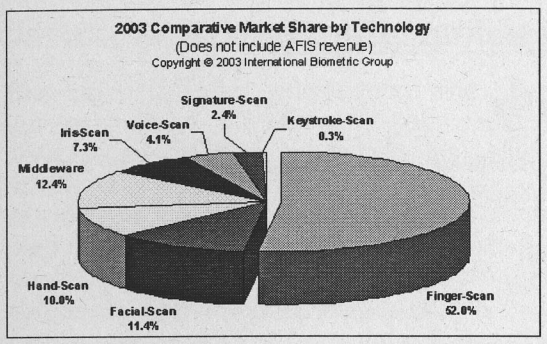


Abb.2 :
Marktanteile der biometrischen Technologien

3. Vorteile / Nachteile gegenüber herkömmlichen Authentikationsverfahren

Beispiele für andere Authentikationsverfahren:

- Wissen (PIN-Nummer, Passwort)
- Besitz (Schlüssel, Chip-Karte)

Vorteile:

- Man kann seinen Fingerabdruck nicht so leicht verlieren wie einen Schlüssel
- Man kann seinen Fingerabdruck nicht weitersagen oder vergessen

Nachteile:

- Höhere Komplexität
- Die Erkennung der Merkmale ist schwerer
- Die meist große Zahl der Eigenschaften muss auf ein leicht speicherbares codiertes Muster (Template) reduziert werden

4. Grundsätzlicher Unterschied zwischen klassischen Fingerabdrücken und Fingerscans

Die Forensik bedient sich seit ca. 100 Jahren der Fingerabdruckmethode. Die Abdrücke werden in großen Datenbanken gespeichert und werden weltweit zur Verbechensbekämpfung eingesetzt.
Mittlerweile haben sogenannte Live-Scans die veraltete Tinten-Abdruck-Methode als Standard abgelöst. Hochauflösende Bilder sind bis zu 250 K-Byte groß.

Die Fingerscan –Technologie bedient sich auch des Fingerabdrucks; sie speichert aber nicht das gesamte Bild, sondern nur das 250- 1000 Bytes große Template. Der Prozess der Datenextraktion ist nicht umkehrbar, d.h. der Fingerabdruck kann nicht aus dem Template rekonstruiert werden. Das ist auf den ersten Blick positiv, birgt aber trotz allem Missbrauchsgefahren.

5. Methoden zur Bilderzeugung

Das wichtigste Ziel bei der Fingerscan-Technik muß es sein, qualitativ hochwertige Aufnahmen des Rillenmusters zu bekommen. Dabei gibt es natürlich eine Reihe von störenden Faktoren:

- Schmutz
- Fett
- Narben
- Zu trockene/ zu fettige Haut
- alte Fingerabdrücke auf dem Sensor

Es gibt drei grundlegende Verfahren:

1. Optische Verfahren
2. Siliziumtechnik
3. Ultraschall

	Optische Methode	Chip-Methode	Ultraschall-Methode
Verfahren	- Finger wird auf beschichtete Oberfläche gelegt - CCD-Sensor erzeugt digitales Bild des Abdrucks	- misst Kapazitäten zwischen Siliziumsensor und Finger - Messung wird in digitales 8-bit Graustufenbild umgewandelt	- Ultraschallwellen werden ausgesendet und von der Umgebung unterschiedlich reflektiert - Reflektion wird gemessen und zu einem Bild verarbeitet
Vorteile	- am meisten erprobt - vergleichsweise günstig - temperaturunempfindlich	- gute Qualität - geringere Meßoberfläche	- die exakteste Methode - wird nicht von Schmutz, Narben und Kratzern beeinflußt
Nachteile	- Sensoren müssen ausreichend groß sein - alte Abdrücke können Ergebnis verfälschen	-eventuell zu kleine Sensorflächen	Methode befindet sich noch in der Entwicklung

Quellen:

International Biometric Group
www.biometricgroup.com
Artikel:
Biometric Technology Overview
Biometric Market Size

Association For Biometrics
www.afb.org.uk/pubs.htm
Artikel:
The Role of Biometrics within Document Security

GMD Forschungszentrum Informationstechnik GmbH
www.darmstadt.gmd.de

Intelligent Biometric Techniques in Fingerprint and Face Recognition
L.C. Jain/ U. Halici/ I. Hayashi/ S.B. Lee/ S. Tsutsui
Verlag: CRC Press / Springer

Politik-gewollte Anwendungen der Biometrik:
Fahndung, Ausweise, Terrorbekämpfung
Eine Diskussion unter Berücksichtigung des Datenschutzes
Arslan Brömme, Universität Hamburg

http://agn-www.informatik.uni-hamburg.de/papers/pub2001.htm

On the Individually of Fingerprints, S. Pankati, S. Prabhakar, and A. Jain
http://biometrics.cse.msu.edu/cvpr230.pdf