Handout zum Vortrag

Biometrische Authentifizierungsverfahren in der Mediensicherheit

im Rahmen des
Oberseminars „Mediensicherheit“

28.11.2006

Friedemann Schmuhl
Sebastian Schneemann
04IN

1. Einführung, Grundlagen

Was ist Biometrie?
Biometrie, auch Biometrik (griech./lat. Bio = Leben, Metron = Maß) = Vermessen von Lebewesen nach quantitativen Merkmalen.

Was sind biometrische Authentifizierungsverfahren?
Als biometrische Authentifizierungsverfahren bezeichnet man die Identifizierung und Verifizierung von Personen mit Hilfe charakteristischer und geeigneter Körpermerkmale, sogenannte biometrische Merkmale, durch Vergleich mit zuvor hinterlegten Referenzdaten.

Biometrie und Mediensicherheit!?
Die Definition von Mediensicherheit nach Prof. Frank: *„Das Oberseminar hat das Ziel, Aspekte der Sicherheit digitaler Medien in Vorträgen der Teilnehmer aufzuarbeiten.„*
Die hieraus entstehende Schwierigkeit ist, dass digitale Medien (per Definition *hier* Bild, Text, Film; nicht aber DVD, Festplatte, Datenübertragungskanal, etc.) z. Zt. nicht mit Hilfe von biometrischen Systemen geschützt werden. Diese Ausarbeitung bezieht sich deshalb auf biometrische Systeme im Allgemeinen sowie diese zur Sicherung *technischer Medien* im Besonderen.

Wie entstehen biometrische Merkmale?
Die Entstehung von Merkmalen wird in drei Kategorien eingeteilt. Man unterscheidet zwischen einer
- genotypischen,
- randotypischen und
- konditionierten Herkunft.

Dabei hängt zwar jedes Merkmal von allen Herkunftsmöglichkeiten ab, aber deren Einfluss unterscheidet sich zum Teil erheblich:

Biometrisches Merkmal	*genotypisch**	*randotypisch**	*konditioniert***
Fingerprint (nur Minuzien)	o	ooo	o
Unterschrift (dynamisch)	oo	o	ooo
Gesichtsgeometrie	ooo	o	o
Irismuster	o	ooo	o
Retina (Blutgefäßstruktur)	o	ooo	o
Handgeometrie	ooo	o	o
Fingergeometrie	ooo	o	o
Venenstruktur der Handrückseite	o	ooo	o
Ohrform	ooo	o	o
Stimme (Klang)	ooo	o	oo
DNA	ooo	o	o
Geruch	ooo	o	o
Tastenanschlag	o	o	ooo
Vergleich: Passwort			(ooo)

Quelle: [BROMBA]

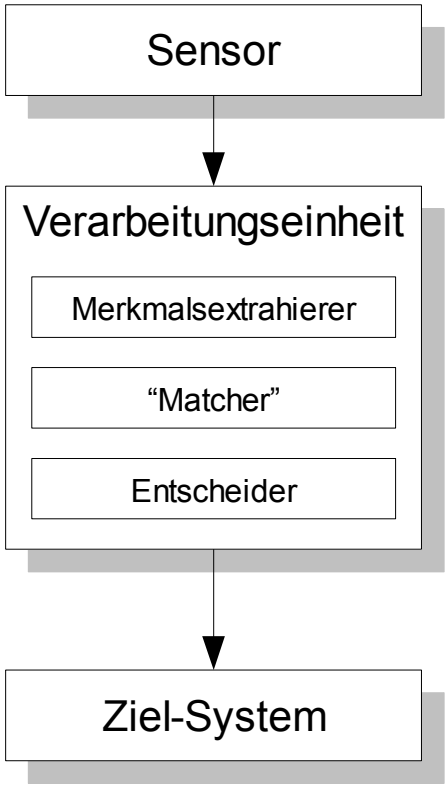
Zu beachten ist im Besonderen, dass biometrische Merkmale nicht dauerhaft beständig sein müssen. Die Klangfarbe zum Beispiel, ein hauptsächlich genotypisches Merkmal, unterliegt im Wachstums- und Alterungsprozess starken Schwankungen. Auch der Fingerabdruck nutzt sich im Laufe von Jahrzehnten ab. Ein über die Zeit sehr stabiles Merkmal ist hingegen das Irismuster.
Durch operative Eingriffe oder Unfälle können sich jedoch alle Merkmale teilweise oder vollständig, temporär oder auch dauerhaft verändern.

Biometrisches Merkmal	*Zeitliche Konstanz*
Fingerprint (Minuzien)	ooooo
Unterschrift (dynamisch)	oooo
Gesichtsgeometrie	ooooo
Irismuster	ooooooooo
Retina	oooooooo
Handgeometrie	ooooooo
Fingergeometrie	ooooooo
Venenstruktur der Handrückseite	oooooo
Ohrform	oooooo
Stimme (Klang)	ooo
DNA	ooooooooo
Geruch	oooooo?
Tastenanschlag	oooo
Vergleich: Passwort	ooooo

Quelle: [BROMBA]

Aus welchen Teilen besteht ein biometrisches Authentifizierungssystem und wie arbeiten diese zusammen?

Egal mit Hilfe welchen Merkmals die Authentifizierung stattfinden soll, besteht ein solches System oft aus den folgenden Komponenten:



Der Sensor, meisst der kostenintensivste Teil eines biometrischen Systems, erfasst das biometrische Merkmal des Nutzers, der sich gegenüber dem Zielsystem authentifizieren möchte. Die Schnittstelle zwischen beiden Systemteilen ist die Verarbeitungseinheit. Diese besteht aus dem Merkmalsextrahierer, dem sogenannten Matcher und dem Entscheider. Der Merkmalsextrahierer nimmt die vom Sensor gelieferten Rohdaten entgegen und erzeugt damit ein so genanntes Abfragetemplate. Die einfließenden Merkmale sind systemabhängig. Der Matcher erzeugt mit Hilfe des Abfragetemplates und den verfügbaren Referenzdaten (Referenztemplate) einen Scoring-Wert, mit Hilfe dessen der Entscheider dann ein Ergebnis fällt, also die merkmalsliefernde Person als ausreichend authentifiziert ansieht und zulässt oder aber abweist.

Welche biometrischen Merkmale lassen sich für Authentifizierungszwecke nutzen?

Beim praktischen Einsatz von biometrischen Verfahren zur Authentifizierung hängt die Akzeptanz des Nutzers (als Nutzer) und des Auftraggebers (als Finanziers) von den folgenden Kriterien ab:

- Komfort
- Genauigkeit
- Verfügbarkeit
- Kosten.

Der Komfort bezeichnet den Aufwand, den ein Nutzer über sich ergehen lassen muss, um authentifiziert zu werden. Hier spielt besonders die Dauer eine Rolle. Die Genauigkeit beschreibt die Rate, mit der ein Merkmal identisch bei zwei unterschiedlichen Nutzern auftriff. Mit kleiner Genauigkeit und steigender Menge der zu authentifizierenden Nutzer steigt die Nicht-Eindeutigkeit. Die Verfügbarkeit bezeichnet die Zahl der Nutzer, die über das geschwünschte Merkmal verfügen. Die Kosten zeigen an, welche Aufwendungen ein Systembetreiber für die Authentifizierung eines gewünschten Merkmals aufbringen muss.

Biometrisches Merkmal	*Komfort*	*Genauigkeit*	*Verfügbarkeit*	*Kosten*
Fingerprint	oooooooo	oooooooo	oooo	ooo
Unterschrift (dynamisch)	ooo	oooo	ooooo	oooo
Gesichtsgeometrie	ooooooooo	oooo	ooooooo	ooooo
Iris	oooooooo	ooooooooo	oooooooo	oooooooo
Retina	oooooo	oooooooo	ooooo	ooooooo
Handgeometrie	oooooo	ooooo	oooooo	ooooo
Fingergeometrie	ooooooo	ooo	ooooooo	oooo
Venenstruktur der Handrückseite	oooooo	oooooo	oooooo	ooooo
Ohrform	ooooo	oooo	ooooooo	ooooo
Stimme	oooo	oo	ooo	oo
DNA (= DNS)	o	ooooooo	ooooooooo	ooooooooo
Geruch	?	oo	ooooooo	?
Tastenanschlag	oooo	o	oo	o
Vergleich: Passwort	ooooo	oo	oooooooo	o

Quelle: [BROMBA]

Welche Vor- und Nachteile bietet biometrische gegenüber klassischer Authentifizierung?

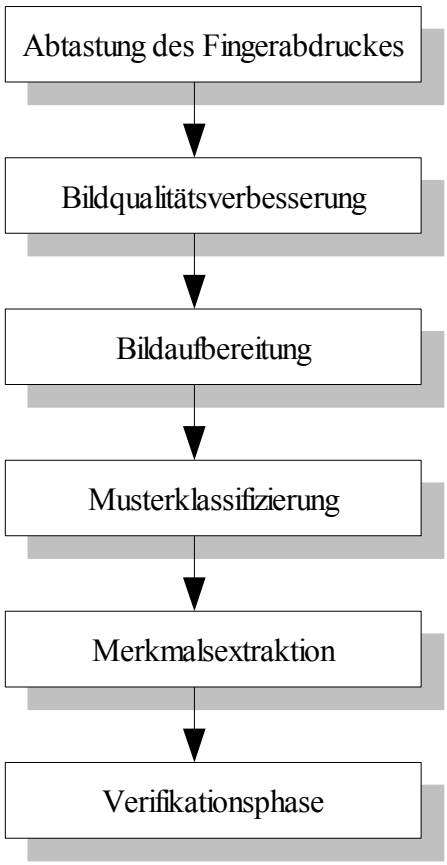
	Geheimes Wissen	Persönlicher Besitz	Biometrie
Beispiele	Passwort, PIN	Schlüssel, Ausweis/Karte	Fingerprint, Gesicht, DNS
Kopierbarkeit	"Software"	einfach bis sehr schwierig	einfach bis schwierig
Verlust	"vergessen"	einfach	sehr schwierig
Diebstahl	ausspionieren	möglich	schwierig
Weitergabe	einfach	einfach	einfach bis schwierig
Änderbarkeit	einfach	einfach	einfach bis sehr schwierig

Quelle: [BROMBA]

2. Technische Details und Produktbeispiele

Fingerabdruckscanner

Fingerabdrücke verwendet man schon seit dem 19. Jh. in der Kriminaltechnik, um Personen eindeutig identifizieren zu können, da man schon früh die biometrischen Eigenschaften des Fingerabdruckes erkannt hatte, dass also jeder Fingerabdruck durch die verschiedenen Muster einzigartig ist und somit jeder Fingerabdruck zu einer Person zuzuordnen ist.
Durch den technologischen Fortschritt gewann der Fingerabdruck im Bereich der Sicherheitstechnik mehr an Bedeutung, etwa im Gebiet der Zugriffskontrollen.
Den Prozess der Fingerabdruckanalyse kann man in 6 Schritten darstellen:



Prozess der Fingerabdruckanalyse (Quelle: [BSI01])

Erläuterungen zu den einzelnen Phasen

Abtastung des Fingerabdruckes
Für die Erfassung des Fingerabdrucks bei automatischer Fingerabdruckerkennung werden spezielle Sensoren optischer, kapazitiver (Halbleiter), thermischer oder direkt-optischer Technologie verwendet, damit die verschiedenen Hauttypen, Beschädigungen, Trockenheit oder Feuchtigkeit der Fingeroberfläche tolleriert werden können.

Bildqualitätsverbesserung
In diesem Schritt werden optische Verbesserungen an dem Bild vorgenommen, um die Strukturen der Papillarlinien besser sichtbar zu machen.

Bildaufbereitung
Das ist die Vorbereitung für die Musterklassifizierung und Merkmalsextraktion.

Musterklassifizierung
Der Fingerabdruck wird in dieser Phase in einer der drei Hauptfingerklassen eingeordnet, da die Fingerabdrücke eine globale Ähnlichkeit aufweisen. Dieses Phase kommt aber nur noch im daktyloskopischen Systemen wie z.B. beim BKA zum Einsatz.

Merkmalsextraktion
In diesem Schritt werden nach bestimmten Merkmalen wie Lage der Minuzien (Gabelung und Linienendung) gesucht.

Verifikationsphase
Es werden zwei Merkmalsvektoren verglichen. Der Vergleich ist stark abhängig von den extrahierten Merkmalen.

Erstellung der Fingerabdruckbilder

Bei der Abtastung des Fingerabdruckes gibt es zwei Methoden:

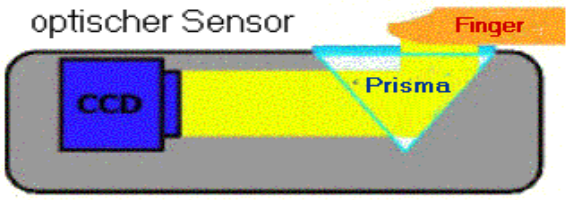
1. Erfassung vom Farbabdruck auf Papier
Der Fingerabdruck wird durch gleichmäßiges abrollen des Fingers mit Tinte gewonnen, dabei wird der Finger von einer Lageseite zur anderen abgerollt, damit die gesamte Linienform erfasst wird.

Farbabdruck, Quelle: [BSI01]

Danach wird der Fingerabdruck abfotografiert oder abgescannt.
Die Nachteile dieser Methode sind zum einen, dass das Bild verzerrt werden kann durch das Aufdrücken und Abrollen des Fingers, und zum anderen ist der Ablauf für den Benutzer unangenehm und langsam. Daraus ist zu schließen, dass sich diese Methode nicht für ein teilautomatisiertes Zutrittskontrollsystem eignet. Diese Methode zur Fingerabdruckerfassung wir auch als „offline-System“ bezeichnet.

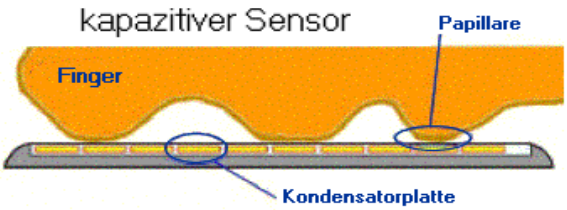
2. Erfassung vom Lebendabdruck des Fingers
Hierbei wird der Finger direkt durch leichtes Auflegen auf einen Sensor abgetastet. Der Ausschnitt des Fingerabdruckes ist demnach kleiner als bei dem obigen Verfahren. Es gibt dafür mehre Arten von Sensoren: optische Sensoren, E-Feld-Sensoren, polymere TFT- Sensoren, thermische Sensoren, kapazitive Sensoren, kontaktlose 3D-Sensoren und Ultraschall-Sensoren.

Optischer Sensor
Bei den optischen Sensoren besteht das Aufzeichnungsgerät prinzipiell aus einer Lichtquelle (LED) und einer CCD-Kamera, die sich beide im Gerät befinden.



Quelle: [BSI01]

Kapazitiver Sensor
Hierbei bildet die Sensoroberfläche zusammen mit der Fingeroberfläche einen Kondensator, dessen Kapazität sich aufgrund des Hautreliefs (Rücken und Täler) ändert.



Quelle: [BSI01]

Diese Art von Sensoren werden mit dem dazugehörigen datenverarbeitenden System als „online-System“ bezeichnet. Die Qualität ist stark abhängig von dem Kontrast zwischen Papillarlinien und den nebenliegenden Furchen.
Unabhängig von der Art der Erfassung des Fingerabdrucks steht dem Verfahren stets ein Graustufenbild des Fingers, der Fingerabdruck, zur Verfügung. Dieses Bild wird weiterbearbeitet und mit Hilfe von Software verbessert, um höhere Matching-Ergebnisse erzielen zu können. Schritte der Bildverarbeitung sind etwa die Verminderung des Bildrauschens oder die Detektion der Merkmale.

Ausgewählte Produktbeispiele

Flash-Speicher mit Fingerscanner

Quelle: [ARPDATA]
Dabei werden die Daten nur nach erfolgreicher Authentifizierung mittels Fingerabdruck freigegeben. Nach der Authentifizierung ist der Speicher wie ein gewöhnlicher Wechselspeicher nutzbar. Fremdzugriffe mittels „nachgemachtem“ Fingerabdruck sollen laut Hersteller nicht möglich sein. Des weiteren sind die Daten zusätzlich intern hardware-verschlüsselt, so dass Unberechtigte keinen Zugriff erlangen können. Die biometrischen Daten werden in einen extra Biometrie-Einheit gespeichert.

Lacie SAFE Hard Drive
Nach dem selben Prinzip arbeitet auch die externe USB-Festplatte von Lacie.

Quelle: [LACIE]

Notebooks mit Fingerabdruck-Sensor
Einige Notebook werden ab Werk schon mit einem Fingerabdruck-Sensor ausgestattet, somit ist das Anmelden am Notebook mit einem Finger anstatt oder ergänzend der persönlichen Passworteingabe möglich.

Mäuse mit Finger-Sensor
Erfüllen den selben Zweck wie bei den Notebooks mit Fingerabdruck-Sensor.

Quelle: [MSHW]

Türschloss mit Fingerscanner

Quelle: [ECE]
Das ECE 1000 speichert 50 Fingerabdrücke. Fälschliche Zurückweisung: einmal unter 1.000, fälschliche Zulassung: einmal unter 100.000. Zutritt ist auch über Eingabe eines Zugangscode möglich.

Filmverleih mit Fingerabdruck

Quelle: [FILM]
DVD-Verleih am Automaten ohne Verkäufer. Der Käufer wählt den Wunschfilm aus. Mit Hilfe der Mitgliedskarte und seinem Fingerabdruck kann der Käufer identifiziert werden. So ist auch mit dem System eine Alterskontrolle möglich.

DVD-DRM (Digital Rights Management) auf Basis des Fingerabdruckes
In den USA wird zur Zeit ein System entwickelt, bei dem das Anschauen einer DVD-DRM nur von dem eigentlichen Käufer möglich sein soll. Dies soll so realisiert werden, dass beim Kauf der DVD-DRM der Fingerabdruck des Kunden auf einen RFID-Speicher auf der DVD-DRM gespeichert wird. Der Film lässt sich dann nur abspielen, wenn der Käufer sich am DVD-Player mit dem Fingerabdruck identifiziert. Somit könnten Filmstudios den Zuschauerkreis eingrenzen. Ob dieses Methode wirklich realisiert werden wird, ist auf Grund des immensen Aufwands fraglich.

Kopierschutz mit Fingerabdruck
Einen ähnlichen Plan verfolgt der Biometrie-Anbieter Veritouch mit einem digialen Walkman, der nur Zugriff auf die Mediendaten nach erfolgreicher Authentifizierung mit dem Fingerabdruck zulässt. Das britische Onlinemagazin *The Register* meldet, dass Veritouch sein Produkt bereits der US-Musikindustrieorganisation RIAA vorgestellt hat.

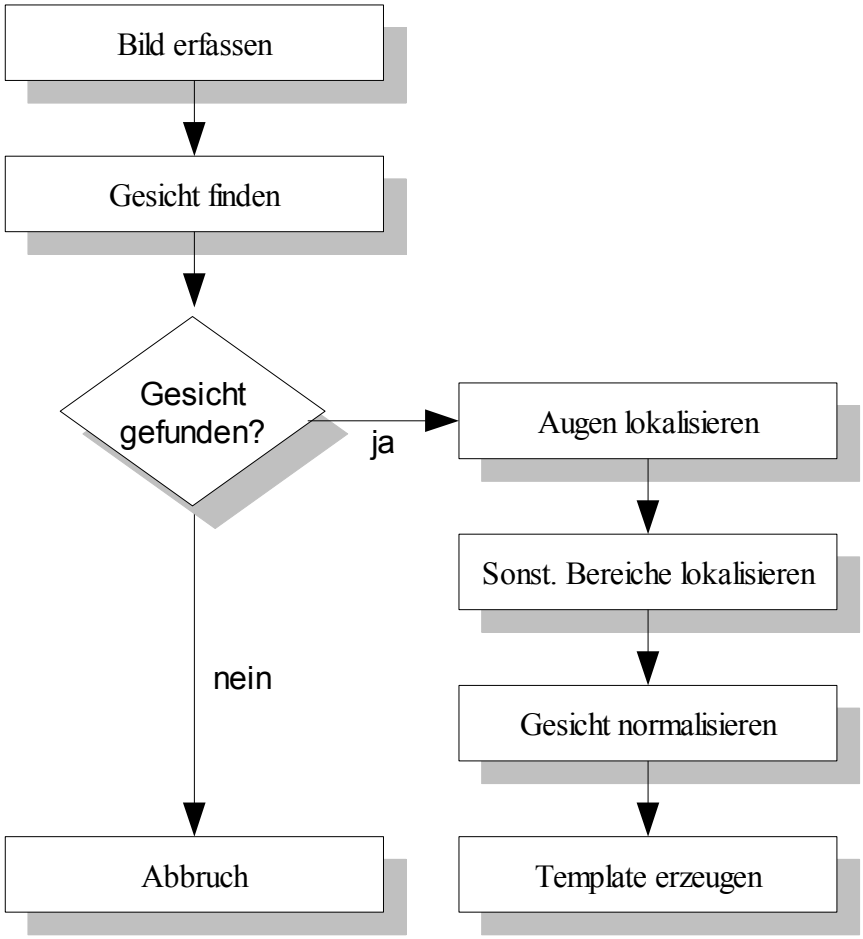
Gesichtserkennung

Die Gesichtserkennung ist ca. 10 Jahre alt und wird bis jetzt in Zugriffskontrollsystemen für Firmenarbeiter, Ausstellungsbesucher und in Spielkasinos verwendet.

Bild des Gesichts als Frontalaufnahme z. B. für den ePass

Ein Vorteil der Gesichtserkennung ist, dass das Gesicht frei zugänglich und dadurch einfacher zu fotografieren ist. Die Verwendung der weit komplizierteren Fläche eines Gesichtes hat aber zur Folge, dass die Bildverarbeitung aufwendiger wird.

Anlegen eines (Referenz-)Templates



Quelle: [BSI02]

Bild erfassen
Das Gesicht wird mittels einer Kamera aufgenommen.

Gesicht finden
Das aufgenommene Bild wird nach einer gesichtähnlichen Form untersucht. Wenn kein Bild gefunden wurde, wird das aufgenommene Bild verworfen.

Augen lokalisieren
Zu Zentrierungszwecken werden die Augen gesucht. Augen sind dunklere Punkte gegenüber dem Gesicht und lassen sich somit leicht lokalisieren.

Weitere Gesichtsbereiche lokalisieren
Von den Augen aus werden nach weiten Gesichtsbereichen gesucht, wie Nase, Mund und Gesichtsränder. Dadurch ist die gefundene Augenposition wichtig für die Lokalisierung der Gesichtsbereiche.

Gesicht normalisieren
Die Gesichtsbilder werden in diesem Schritt auf ein einheitliches Maß gebracht. Dabei werden die Bilder auf die Augenposition zentriert.

Merkmale extrahieren
Es wird nach weiteren Merkmalen gesucht.

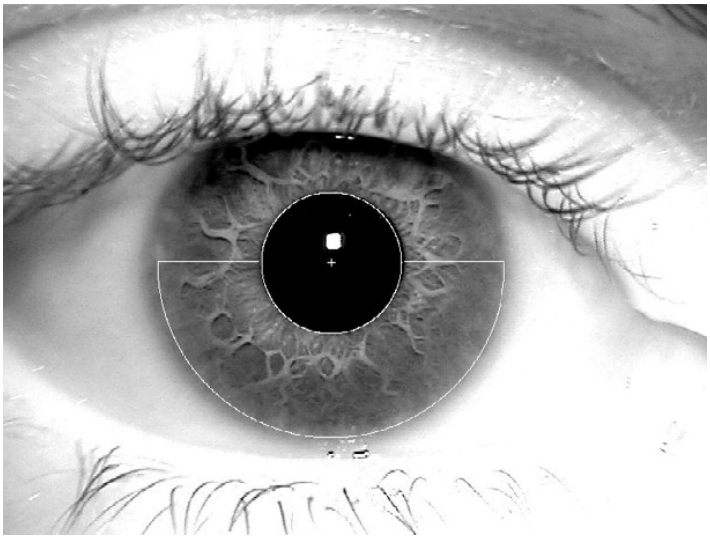
Template erzeugen
Durch mathematische Formeln werden die Merkmaldaten codiert und auf eine Größe von 1000 bis 1300 Byte komprimiert.

Referenzdatensatz erzeugen
Wird ein Template erfolgreich erzeugt, wird dieses qualitativ mit Gesichtern aus der Referenzdatenbank verglichen. Werden dabei genügend Unterschiede festgestellt, wird das Template gespeichert.

Vergleich von Templates
Um einen Vergleich zweier Tamplates vorzunehmen, werden sie byteweise mittels eines mathematischen Algorithmus kombiniert. Die Höhe des Ergebnisses bestimmt den Grad der Ähnlichkeit der Templates. So kann bei einem bestimmten Schwellenwert bestimmt werden, dass es sich bei den beiden Bildern, um die selbe Person handelt.

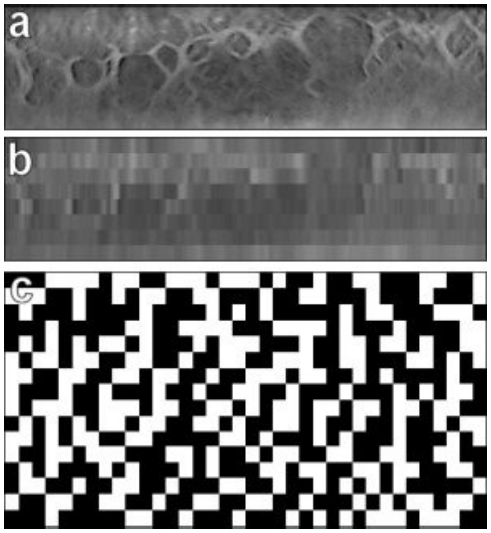
Iriserkennung

Es wurde festgestellt, dass die zwischen der Iris und der Hornhaut des menschlichen Auge liegende band- und kammartige Bindegewebsstruktur bei jedem Menschen einmalig ist. Die Struktur unterscheiden sich auch bei eineiigen Zwillingen. Da sich die Struktur im Verlaufe des Lebens kaum ändert, eignet sie sich gut als eindeutiges Identifikationsmerkmal.
Der erste einsatzfähige biometrische Algorithmus wurde Anfang der neunziger Jahre von John Daugman entwickelt und zum Patent angemeldet.
Beim Erzeugen der Templates wird die Iris mit einer im Abstand von ca. einem Meter entfernten Lichquelle im nahen Infrarotbereich aufgenommen. Ist das Bild aufgenommen, sucht das System wie bei der Gesichtskennung nach einem zentralen Punkt - in diesem Fall der Iris.



Aufnahme einer Iris bei einer Wellenlänge von 850 nm, Quelle: [BSI03]

Wurde die Iris von dem System gefunden, wird ein Kreissegment der Bindegewebsstruktur ausgeschnitten und in einen Streifen konstanter Breite transformiert.



Veranschaulichung der Grundschritte zur Erzeugung eines Templates aus einem Bild der Iris, Quelle: [BSI03]

Dieser Streifen wird mittels mathematischer Verfahren bearbeitet und in Binärcode umgewandelt. Die typische Größe von Iristemplates ist je nach Verfahren im Bereich einiger hundert Bytes.

IE-System von SD Industries zur Erstellung von Iris-Templates, Quelle: [BSI04]

ePass – interdisziplinäres Beispiel

Der neue Reisepass, vereint gleich zwei biometrische Systeme, den Fingerabdruck und das Gesichtsbild.
Die Einführung des neuen ePasses ist der letze Schachzug des mit dem letzten Regierungswechsel scheidenden Innenminister Otto Schily. Das erklärte Ziel, des Ende 2005 eingeführten Dokuments ist es, ein modernes, fälschungssicheres und maschienenlesbares Ausweispapier zu etablieren. Diese Eigenschaften sollen zum einen durch die Unterstützung von Funkchips, sogenannten RFID-Etiketten (radio frequency identification), zum anderen durch die Speicherung biometrischen Daten im Ausweis erreicht werden. Seit der Einführung der neuen Ausweise im November 2005 ist das biometrische Gesichtsbild des Inhabers im ePass gespeichert, ab Januar 2007 ist die Speicherung von Fingerabdrücken EU-weit Pflicht. Mit Hilfe des ePasses soll unter anderem eine schnellere, personalminimierte Grenzkontrolle erreicht werden, im Idealfall sollen die Grenzbeamten nur noch eingreifen müssen, wenn die vom Nutzer selbst durchgeführte Authentifizierung mehrfach fehlschlägt.

Bild-Quelle: [GOLEM]

Zusammenfassung: Vergleich der Systeme

Quelle: [BSI04]

Merkmal	Positiv	Negativ
Fingerabdruck	- Beste Erkennungsleistung - Hohes Sicherheitsniveau möglich	- Stabile Sensoren trotz kontaktbehaftetem Einsatz
Gesichterkennung	- Kaum Training erforderlich	- Ausgesprochen homogene Ausleuchtung nötig - Bei hohem Sicherheitsniveau nicht akzeptable Rückweisungsrate
Iris	- Hohes Sicherheitsniveau möglich	- Bedienungsschwierigkeiten für Wenignutzer - FAR signifikant höher als angegeben (Mythos: feste Schwelle)

3. Gesetze, Vorschriften und Standards

Gesetze und Vorschriften
Zwar ist die Verwendung von biometrische Merkmalen zur Identifikation und Authentifikation von Personen nicht ganz neu, jedoch ergeben sich in gewisser Weise Neuerungen bzw. der Bedarf der Überarbeitung von bestehenden Gesetzen, Vorschriften und Regelungen. Spätestens mit der Einführung von biometrischen Merkmalen in Ausweisedokumenten betrifft die Verarbeitung, Speicherung und Erhebung von biometrischen Daten Millionen von Menschen. Aus diesem Grund ist es notwendig einen juristischen Rahmen zu schaffen, der auf einer Seite erlaubt, sicherheitsfördernde Technik zu etablieren, andererseits die Daten der Nutzer zuverlässig vor Mißbrauch schützt.

In diesem Abschnitt finden Sie eine Auflistung von Gesetzen, die nach den Recherchen der Autoren in Zusammenhang mit Biometriefragen stehen.

Signaturverordnung (SigV)
Die Signaturenverordnung erlaubt es nach § 16 Abs. 2 die Speicherung von zusätzlichen biometrischen Merkmalen, um Menschen eindeutig identifizieren zu können.

Bundesdatenschutzgesetz
Das Bundesdatenschutzgesetz beschreibt Vorschriften für die Erhebung, Speicherung und die Verarbeitung von personenbezogen Daten, also auch biometrischen.

Grundgesetz
Nicht direkt im Grundgesetz verankert, aber im sog. Volkszählungsurteil aus den Paragraphen für Menschenwürde und Handlungsfreiheit abgeleitet, ist das Recht auf informationelle Selbstbestimmung.

Terrorismusbekämpfungsggesetz
Das nach den Anschlägen des 11. Septembers 2001 beschlossene Gesetzespaket zur Prävention von terroristischen Anschlägen besonders in Deutschland, bildet u.a. die Grundlage zur Speicherung von biometrischen Daten in Ausweisdokumenten.

Standards
Neben der Notwendigkeit auf Schaffung eines gesetzlichen Rahmens, spielt selbstverständlich auch die technische Realisierung der Systeme eine wichtige Rolle. Hierzu haben verschiedene Gremien und Institiutionen Standards entwickelt bzw. deren Vorschläge liegen zur Zeit zur Standardisierung vor.

Biometriespezifische Standards sind derzeit noch in Arbeit oder wurden zur Standardisierung bei ISO eingereicht. Abgeschlossene Projekte mit IS-Status (International Standard) sind fett gedruckt. Zu den zu bearbeitenden Themen gehören u.a. (Stand 2006-10-21):

Quelle: [BROMBA]

Working-Number	*Title*
19784-1	**Biometric Application Programming Interface Part 1: The BioAPI Specification**
19784-2	Biometric Application Programming Interface Part 2: Biometric Archive Function Provider Interface
19784-3	Biometric Application Programming Interface Part 3: BioAPI Lite
19785-1	**Common Biometric Exchange Framework Format - Part 1: Data Element Specification**
19785-2	**Common Biometric Exchange Framework Format - Part 2: Procedures for the operation of the biometric registration authority**
19785-3	Common Biometric Exchange Framework Format - Part 3: Patron Format Specification
19794-1	**Biometric data interchange formats Part 1: Framework**
19794-2	**Biometric data interchange formats Part 2: Finger Minutiae Data**
19794-3	**Biometric data interchange formats Part 3: Finger Pattern Spectral Data**
19794-4	**Biometric data interchange formats Part 4: Finger Image Data**
19794-5	**Biometric data interchange formats Part 5: Face Image Data**
19794-6	**Biometric data interchange formats Part 6: Iris Image Data**
19794-7	Biometric data interchange formats Part 7: Signature/Sign Time Series Data
19794-8	**Biometric data interchange formats Part 8: Finger Pattern Skeletal Data**
19794-9	Biometric data interchange formats Part 9: Vascular Biometric Image Data
19794-10	Biometric data interchange formats Part 10: Hand Geometry Silhouette Data
19794-11	Biometric data interchange formats Part 11: Signature/Sign Processed Dynamic Data
19794-12	Biometric data interchange formats Part 12: Face Identity Data
19795-1	**Biometric Performance Testing and Reporting - Part 1: Principles and Framework**
19795-2	Biometric Performance Testing and Reporting - Part 2: Testing Methodologies for Technology and Scenario Testing
19795-3	Biometric Performance Testing and Reporting - Part 3: Modality-Specific Testing
19795-4	Biometric Performance Testing and Reporting - Part 4: Interoperability Performance Testing
19795-5	Biometric Performance Testing and Reporting - Part 5: Scenario Evaluation of Biometric Access Control Systems
19795-6	Biometric Performance Testing and Reporting - Part 6: Testing Methodologies for Operational Evaluation
24708	Biometric Interworking Protocol (BIP)
24709-1	BioAPI Conformance Testing – Part 1: Methods and Procedures
24709-2	BioAPI Conformance Testing – Part 2: Test Assertions for Biometric Service Providers
24709-3	BioAPI Conformance Testing – Part 3: Test Assertions for BioAPI Frameworks
24709-4	BioAPI Conformance Testing – Part 4: Test Assertions for Biometric Applications
24713-1	Biometric Profiles for Interoperability and Data Interchange - Part 1: Biometric Reference Architecture
24713-2	Biometric Profiles for Interoperability and Data Interchange - Part 2: Physical Access Control for Employees at Airports
24713-3	Biometric Profiles for Interoperability and Data Interchange - Part 3: Biometric-Based Verification and Identification of Seafarers
24714-1	Technical Report on Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies - Part 1: Guide to the Accessibility, Privacy, and Health and Safety Issues in the Deployment of Biometric Systems for Commercial Application
24714-2	Technical Report on Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies - Part 2: Practical Application to Specific Contexts
24722	Technical Report on Multi-Modal and Other Multi-Biometric Fusion
24741	Technical Report For a Biometric Tutorial
24779	Pictograms, Icons and Symbols for use with Biometric Systems
29794-1	Biometric Sample Quality Standard Part 1: Framework
29794-4	Biometric Sample Quality Standard Part 4: Finger Image
29794-5	Biometric Sample Quality Standard Part 5: Face Image

4. Chancen und Vorteile

Einen großen Pluspunkt bei der Einführung biometrischen Systeme sehen seine Vertreter bei der Terrorismusbekämpfung. Im Terrorismusbekämpfungsgesetz, das am 09.01.2002 in Kraft getreten ist, wurden die Rechtsgrundlagen für die Aufnahme biometrischer Merkmale in Pässe und Personalausweise geschaffen.
Mit Hilfe des ePasses soll unter anderem eine schnellere, personalminimierte Grenzkontrolle erreicht werden, im Idealfall sollen die Grenzbeamten nur noch eingreifen müssen, wenn die vom Nutzer selbst durchgeführte Authentifizierung mehrfach fehlschlägt.

„Autocontroll-Spur“ am Flughafen Frankfurt/Main (im Rahmen der „BioP II“-Studie [BSI04]), Quelle: [RAVEN]

Für Einzelanwender, die sich ihre Passwörter nicht merken wollen oder können, scheint die Authentifizierung mit Hilfe biometrischer Merkmale eine gute Lösung zu sein – ein „Vergessen“ gibt es hier nicht.
Einen weiteren Vorteil bieten die biometrischen Verfahren, dass sie trotz relativ hoher Anschaffungskosten, die Kosten für den langfristigen Betrieb gering halten. Dadurch dass sich die meissten biometrischen Merkmale im Laufe der Jahre kaum verändern, ist die langfristige Authentifizierbarkeit gesichert. Des weiteren soll nach Herstelleraussagen die Fälschungssicherheit sehr hoch sein.
Das Erfassen vieler Biometriemerkmale geht relativ schnell. Ein Fingerabdruck ist ebenso wie die Iris in wenigen Sekunden eingelesen. Je nach Vergleichsverfahren dauert die Erkennung ebenfalls wenige Sekunden.
Für die Zukunft denkbar ist auch, dass gefundene biometrische „Hinterlassenschaften“ (Fingerabdruck, Haare, etc.) an Tatorten kriminellen Handelns nicht nur mit den Datenbeständen der Polizei, sondern im Zweifel mit den Datenbeständen von ausweisdokumentausstellenden Behörden verglichen wird. So ist eine rasche Identifizierung bei Ersttätern wahrscheinlich.
Bankgeschäfte oder Bezahlungen z.B. im Supermarkt könnten auch ein neues Einsatzgebiet im Rahmen von biometrischen Systemen sein. Der „Future Store“ der Metro Gruppe testet dieses Verfahren zur Zeit mit ausgewählten Kunden. Nach dem Einkauf identifiziert sich ein Kunde mit Hilfe einer RFID-gespickten Kundenkarte und verifiziert seinde Person mit Hilfe eines Fingerscans. Die Kosten seines Einkaufes werden dann bequem von seinem vorher hinterlegten Konto abgebucht.

5. Risiken und Nachteile

FAR vs. FRR
Fehlerhafte Zulassungssrate (FAR) und fehlerhafte Abweisungsrate (FRR) hängen untrennbar von einander ab. Der Wunsch nach Minimierung der zu unrecht authentifizierten oder identifizierten Nutzer erhöht zwangsläufig die Anzahl von Nutzern die fäschlicherweise abgewiesen werden oder unerkannt bleiben.

FTE
Bei den z. Zt. besten Identifikationssystemen am Markt (vgl. [BSI04]) liegt die Rate der Nutzer, die nicht in das System „enrolled“ (eingepflegt) werden können (FTE) je nach verwendetem System und Merkmal bei bis zu 0,99%. Das heißt bei rund 680 Millionen EU-Bürgern würden 6,8 Millionen Personen (oder nahezu alle Einwohner der Schweiz) ein System (hier beispielsweise den ePass) nicht nutzen können. Allein in Deutschland würde dies noch 800.000 Einwohner betreffen. Die Gründe waren merkmalsbedingt sehr unterschiedlich. Der häufigste Grund für Fehler während des Enrolments für Fingerprinttemplates waren zu feuchte Finger. Der zweithäufigste Grund war zu trockene Finger. Beim Merkmal Iris war ein Grund für das Scheitern des Enrolments, die Unfähigkeit von kurzsichtigen Personen das Merkmal richtig zu präsentieren, da diese nach den Empfehlungen des Systemherstellers ihre Sehhilfe entfernten.

Öffentlichkeit der Merkmale vs. dauerhafte Nutzung
Problematisch ist ebenfalls, dass biometrische Merkmale in der Regel öffentlich sind, d. h. es ist nur eine Zeitfrage, bis die biometrischen Daten Angreifern zur Verfügung stehen.

Beispiele:

- Unzureichend gesicherte Datenbestände in Arztpraxen und Krankenhäusern
- (hochauflösende) Videoüberwachung in Eingangsbereichen von zahlreichen Gebäuden
- ...

Diese Tatsache widerspricht dem Bedürfnis der Industrie, biometrische Merkmale zur Authentifizierung zu nutzen, die möglichst lange von Bestand sind. Ein Ausweg könnte sein, die biometrischen Daten mit konventionellen Zugangsverfahren zu kombinieren. So wird aus der Authentifizierung eine Verifizierung. Bei Bedarf ist so leicht möglich, den konventionellen Teil (z. B. Chipkarte) auszutauschen. Diese Kopplung macht jedoch den großen Vorteil, Identität nicht mehr entwenden zu können (Schlüssel) oder vergessen zu können (PIN) zu nichte.

Mehrfachidentitäten und Zeugenschutzprogramme
Weiterhin kann es zu der Vernichtung gewünschter Mehrfachidentitäten kommen. Ausländische Staaten werden ebenso wie das organisierte Verbrechen Datenbanken mit biometrischen Merkmalen anlegen, um leichter verdeckte Ermitller oder Personen in Zeugenschutzprogrammen identifizieren zu können. (Quelle: [INFO29])

Gefahren für Freiheit und Demokratie
Der Zwang, biometrische Daten für Ausweisdokumente zur Verfügung zu stellen, verstößt gegen das Recht auf infomationelle Selbstbestimmung, das heißt das Recht zu entscheiden, ob und wo ein Bürger der Bundesrepublik Deutschland seine Daten

hinterläßt, wird ausgesetzt.
Die zentrale Speicherung von biometrischen Daten der EU-Bürger wird von nahezu allen EU-Innenministern befürwortet. Dass es zur Zeit noch keine zentrale Datei für Biometriemerkmale gibt, ist einzig den Zweifeln des EU-Parlamentes zu verdanken.
Würde aber eine solche Datei existieren (im 3. Reich hieß diese "zentrale Datensammlung", unter dem DDR-Regime "Zentralkartei"), würde dort auch das biometrische Gesichtsbild eines jeden Bürgers, das zum Beispiel im ePass verwendet wird, gehortet werden. Mit Hilfe dieser Daten und den zahllosen Überwachungskameras überall in den Innenstädten, Einkaufspassagen, Tankstellen, Bahnhöfen, Flughäfen, Staßenbahnen etc. könnte problemlos ein umfassendes Bewegungsprofil von Menschen erzeugt werden.
Auch auf einen der Grundpfeiler der Demokratie, der Versammlungs- bzw. Demonstrationsfreiheit hätte dieses Szenario Einfluß: Ein Mensch der weiß, dass die Feststellung seiner Identität abgeschlossen ist, noch bevor die Demonstration beendet ist, wird im Zweifel lieber nicht teilnehmen. Wer möchte schon vom Chef identifiziert werden, während er auf einer Gewerkschaftskundgebung ein besonders provokantes Plakat schwenkt? Oder wer möchte dann noch für die gleichgeschlechtliche Ehe demonstrieren, wenn der konservative Arbeitgeber zusehen (und identifizieren lassen) könnte.

Safety-Problem
Ein weiteres Problem ist das von Prof. Pfitzmann (TU Dresden) getaufte Safety-Problem. Es beschreibt das Horrorszenario, dass kriminelle Personen entführen oder Körperteile von Personen abtrennen, um sich so Zugang zu Systemen verschaffen, die mit Hilfe biometrischer Verfahren geschützt sind.(Quelle: [INFO29])

Quelle: [DS8701]

Biometrie und Datenschutz
"Jede biometrische Messung liefert potentiell sensitive persönliche Daten, z. B. offenbart ein Netzhaut-Scan Daten über den Alkoholkonsum der vergangenen zwei Tage, und es wird diskutiert, ob Fingerabdrücke Informationen über die sexuelle Orientierung von Männern liefern."
(Quelle: [INFO29])

Ein Puzzleteil zum Überwachungsstaat
"Die Einführung der biometrischen Ausweisdokumente reiht sich ein in eine Folge von Verletzungen dieses Grundrechtes [Recht auf Infomationelle Selbstbestimmung]. Die sich immer weiter ausdehnende Videoüberwachung, die automatisch Kennzeichnerkennung, der große Lauschangriff, die Jahr für Jahr steigenden Telefonüberwachungsmaßnahmen, die Speicherung von genetischen Informationen in digitaler Form, die Aufhebung des Bankgeheimnisses, die noch immer diskutierte Vorratsdatenspeicherung von Telefon- und Internetdaten; die Liste auf dem Weg zum Überwachungsstaat ließe sich noch fortsetzen."
(Quelle: [DS8701])

Anhang A – Glossar

In diesem Anhang sind die wichtigsten Begriffe in aller Kürze zusammengefaßt. Sie sollen ein Hilfsmittel und Startpunkt für die weitere Recherche sein und sind bei Bewertungen von biometrisches System unerläßlich.

Enrolment
Anlegen eines Referenzdatensatzes mit dem der Vergleich des (Anfrage-)Templates stattfindet. Während des Enrolments wird die Erfassung des gleichen Merkmals mehrfach wiederholt und ein Mittel gebildet.

FAR (false acception rate)
Mathematische Größe, die die Häufigkeit von fälschlicherweise zugelassenen Personen angibt.

FRR (false rejection rate)
Mathematische Größe, die die Häufigkeit von fälschlicherweise abgewiesenen Personen wiedergibt.

FTA (failure to acquire)
Wahrscheinlichkeit, mit der ein Merkmal nicht vom Sensor aufgenommen werden kann.

FTE (failure-to-rerolment)
Fehlerrate während des Enrolmentprozesses.

LDS (logical data structure)
Standardisiertes Datenformat für biometrische Daten zur Speicherung und zum Austausch.

Template
Die Daten, die aus dem Sensorabbild bei jedem Authentifikationsversuch erzeugt werden, nennt man (Abfrage-)Template. Dieses wird mit einem, in der Regel auf einer Smartcard oder dezentral auf einem Dauerspeicher abgelegten, (Referenz-)Template vergleichen, das vorher beim Enrolment erzeugt wurde.

Anhang B - Quellen

[ARPDATA] http://www.arp.com, Artikel-Nummer: 299332, Stand: 22.11.2006

[BROMBA] http://bromba.com/faq/biofaqe.htm, „Bioidentifikation – Fragen und Antworten“, Stand: 18.11.2006

[BSI01] Bundesamt für Sicherheit in der Informationstechnik, Publikation „Biometrie-Fingerabdruckerkennung“, Stand: 20.01.2005

[BSI02] Bundesamt für Sicherheit in der Informationstechnik, Publikation „Biometrie-Gesichterkennung“, Stand: 24.01.2005

[BSI03] Bundesamt für Sicherheit in der Informationstechnik, Publikation „Biometrie-Iriserkennung“, Stand: 27.01.2005

[BSI04] Bundesamt für Sicherheit in der Informationstechnik, Studie: „Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II“, Stand: 24.08.2005

[DS8701] CCC e. V., Organ: „Datenschleuder“ Nr. 87/2005, Seite 8 ff., „Sicherheit durch Biometrie?“

[ECE] CRM-Vertrieb, http://www.crm-vertrieb.de/pdf/ECE-370.pdf, Stand: 22.11.06

[FILM] http://www.cityinfonetz.de/tagblatt/kino/index.php?aktion=thema&filmid=663752, Artikel „Filmverleih mit Fingerabdruck“, Stand: 26.10.2006

[GOLEM] http://www.golem.de/print.php?a=38374, Veröffentlicht: 01.06.2005, Stand: 22.11.2006

[INFO29] Informatik_Spektrum, Band 29, Heft 5, Oktober 2006, Seite 353 ff.

[LACIE] http://www.lacie.com/de/products/product.htm?pid=10806, Stand: 22.11.06

[MSHW] http://www.microsoft.com/hardware/mouseandkeyboard/ProductDetails.aspx?pid=036&active_tab=overview, Stand: 22.11.2006

[RAVEN] http://kai.iks-jena.de/livejournal/bilder/12-02-04-bgsiriskontrolle1.jpg, Stand: 22.11.2006, Bild „Autocontroll-Spur am Flughafen Frankfurt/Main“