

# **Biometrische Verfahren**

**(auf der Basis von Projektarbeiten von  
Christian Dreiskämper, Jens Lohmann und Johanna Stronzik)**

**Dortmund, Oktober 2004**

# Inhalt

	<u>Seite</u>
<b>Vorwort</b>	<b>3</b>
<b>Einleitung</b>	<b>4</b>
<b>Verfahren im Einzelnen</b>	<b>7</b>
<b>Zusammenfassung</b>	<b>45</b>
<b>Kombinierte Biometricsysteme</b>	<b>46</b>
<b>Schlussbetrachtung</b>	<b>48</b>
<b>Literaturverzeichnis</b>	<b>50</b>
<b>Internet-Links</b>	<b>51</b>

## Summary

**Jeder Mensch hat ganz persönliche Merkmale wie Stimme, Aussehen und Verhalten, wodurch er erkannt und identifiziert werden kann.**

**Der Begriff Biometrie stammt aus dem Griechischen und bildet sich aus den Wörtern „bios“ für Leben und „metron“ für Maß. Danach ist die Biometrie die Wissenschaft der Körpermessung an Lebewesen.**

**Biometrische Merkmale, welche heute von Sensoren ausgewertet werden können, sind unter anderem das Fingerbild, die Handgeometrie, das Gesicht, die Stimme und die Unterschrift.**

**Ziel dieses Vortrages ist, die biometrischen Verfahren zu beschreiben und zu zeigen, wie eine Authentisierung mit ihrer Hilfe durchgeführt werden kann.**

**Biometrische Verfahren können auch missbraucht werden, um personenbezogene Daten zu sammeln und systemübergreifend Benutzerprofile zu erstellen. Daher findet der Datenschutz besondere Beachtung, und es wird eine Möglichkeit vorgestellt, wie Authentisierung anonym erfolgen kann.**

## Einleitung

### Verfahren im Einzelnen

### Seite

- **Fingerbildererkennung** 7
- **Gesichtserkennung** 16
- **Iriserkennung** 24
- **Spracherkennung** 31
- **Unterschriftenerkennung** 38



## ... Einleitung

### ➤ Arten der Erkennung

- **Identifikation**: hier soll die Identität einer Person durch einen 1:n-Vergleich erfolgen und festgestellt werden, um welche Person es sich handelt.



- **Verifikation**: hier soll durch einen 1:1-Vergleich die Identität einer Person bestätigt werden, ob es sich bei der Person, die erkannt werden will, auch um diejenige handelt, für die sie sich ausgibt.



### ➤ Voraussetzungen:

- Grenzwert muss jeweils definiert werden ( d.h. eine 100%ige Übereinstimmung muss nicht vorliegen, da der Vorgang sonst zu lange dauern würde )
- es muss gewährleistet sein, dass sich die Verfahren nicht überlisten lassen ( → durch Foto, Tonband, Videoaufnahme )
- es muss eine Lebenderkennung eingebaut sein ( z.B. Messung von Puls, Temperatur, Augenblinzeln ), so dass gewährleistet ist, dass z.B. keine Gesichtsmaske oder sogar abgeschnittene Finger benutzt werden.

## ...Einleitung

### ➤ Enrollment

- Beim Enrollment wird ein Referenzdatensatz erzeugt, den das System später mit aktuell gewonnenen Daten vergleichen kann. Der Referenzdatensatz muss sehr sorgfältig aufgenommen werden, damit er ein breites Spektrum der entsprechenden Person abdeckt. So ist es z.B. möglich, dass der Finger in einem etwas veränderten Winkel auf den Sensor aufgelegt wird oder dass die Kamera das Gesicht aus einer leicht veränderten Perspektive aufnimmt. Auch in diesen Fällen sollte es noch möglich sein, die betreffende Person sicher zu verifizieren.

### ➤ es ist zwischen

- aktiven Merkmalen ( basierend auf Verhaltensmerkmalen wie Stimme, Lippenbewegung beim Sprechen, Bewegungsablauf beim Gehen )                      und
- passiven Merkmalen ( basierend auf Körpermerkmalen wie Gesichtsform, Handlinienmuster, Handvenenmuster, Ohrenmuschelform, Irismuster, Fingerabdruck )

zu unterscheiden

- ### ➤ Die einzelnen Verfahren sollten teilweise miteinander kombiniert werden, um die Sicherheit der Ergebnisse zu verbessern.

## Fingerbildererkennung

- **Einleitung**
- **Verfahrensbeschreibung**
- **Sensorprinzipien**
- **Probleme**
- **Grundformen**
- **Technische Daten**
- **Lebenderkennung**
- **Merkmalscharakteristika**
- **Applikationen in der Praxis**
- **Bewertung**
- **Fingerbildscanner**



## ... Fingerbildererkennung

### ➤ Einleitung

- **Jeder Finger hinterlässt einen einmaligen Abdruck. Nicht zwei Finger auf der ganzen Welt haben identische Papillarlinien, also Fingerabdrücke. Weil sich die Muster erst während der Embryonalentwicklung in Zufallsprozessen ausbilden, haben sogar eineiige Zwillinge unterschiedliche Papillarlinien. Bei jedem Menschen bleibt das Muster das ganze Leben lang unverändert.**
- **Auf der Haut der Fingerspitzen bilden Erhebungen ein Linienmuster. In den Erhebungen befinden sich Poren, die Schweiß absondern. Dieser Schweiß bildet entlang der Erhebungen einen Film. Kommt der Finger mit einer Oberfläche in Berührung, wird ein Teil des Schweißfilms auf der Oberfläche zurückgelassen, wodurch ein Fingerabdruck entsteht.**

## ... Fingerbildererkennung

### ➤ Verfahrensbeschreibung

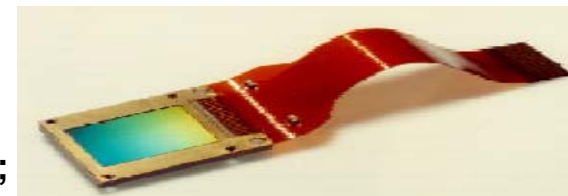
- das Verfahren ist nicht berührungslos, zur Authentisierung wird ein Finger auf einen Sensor gelegt; dieser vergleicht die Merkmale mit den gespeicherten Referenzmustern ( 1:n → Identifikation ) oder mit einem angegebenen Referenzmuster ( 1:1 → Verifikation ) ( → Matching ) (s.o.)

### ➤ Sensorprinzipien

a) kapazitive Sensoren : Finger wird auf eine kleine Sensorplatte bestehend aus vielen einzelnen Kondensatoren gelegt; überall dort, wo die Erhebungen der Fingerspitze in Kontakt mit der Platte kommen, entladen sich die Kondensatoren; der Zustand der Kondensatoren ( geladen / entladen ) ergibt das Bild des Fingerabdrucks

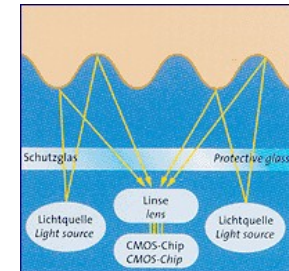


b) Infrarot-Sensoren : ähnlich wie bei kapazitiven; hier wird nur keine Ladung, sondern Wärme, die die Erhebungen abgeben, ausgetauscht; die Wärmedifferenzen auf dem Sensor ergeben das Bild des Fingerabdrucks



## ... Fingerbildererkennung

c) **optische Sensoren** : ein Lichtstrahl wird in einem Winkel von 45 Grad zum aufgelegten Finger gesendet; anhand der Reflexion kann der Sensor die Linienstruktur des Fingerabdrucks erkennen



### ➤ Probleme

- verschiedene Faktoren können die Authentisierung erschweren/ verhindern:
  - a) zuviel Feuchtigkeit auf dem Finger ( es entstehen zwischen den einzelnen Erhebungen Flächen, die die Struktur verfälschen)
  - b) zuwenig Feuchtigkeit auf dem Finger ( einige Sensoren können das Linienmuster der Erhebungen nicht mehr vollständig erfassen, so dass wichtige Charakteristika unerfasst bleiben )
  - c) Schmutz auf Finger oder Sensor ( Linienstruktur kann überdeckt werden )
  - d) temporäre Veränderungen am Finger ( Einschnitte oder Abschürfungen )
  - e) fehlerhafte Positionierung des Fingers auf dem Sensor



Abbildung 4: Zu feuchter, zu trockener- und beschädigter Fingerabdruck

## ... Fingerbildererkennung

### ➤ Grundformen

- es gibt drei Grundformen bei Fingerabdrücken: Wirbel, Schlingen und Bögen
- die weißen Punkte in den Fingerabdrücken in der folgenden Abbildung sind Poren, die sich in den Erhebungen befinden



### ➤ Technische Daten

- für die Klassifikation eines eingelesenen Fingerabdrucks in Original oder Fälschung wird für eine Verifikation im Mittel eine Sekunde benötigt, für eine Identifikation in Abhängigkeit zur Größe der Datenbank und Geschwindigkeit der verarbeitenden Einheit entsprechend länger; die Auflösung beträgt üblicherweise 500 dpi
- die Größe eines Datensatzes liegt zwischen 256 Bytes und 2000 Bytes, so dass dieser problemlos auch auf eine Chipkarte Platz findet
- die gesamte Dauer der Verifikation ( von Ankunft bis zum Verlassen ) beträgt im Mittel etwa 7 Sekunden

## ... Fingerbildererkennung

### ➤ Lebenderkennung

- der Fingerabdruck ist ein statisches ( = passives ) Merkmal und erfordert während der Authentisierung selbst keine Aktion vom Benutzer
- somit ist es bei hohem Sicherheitsbedarf erforderlich, dem Sensor einen Scanner hinzuzufügen, um zu überprüfen, ob es sich um einen echten, lebendigen Finger handelt
- es soll also verhindert werden, dass das System durch einen Wachsfinger oder einem auf einem Finger aufgetragenen Latexabdruck getäuscht werden kann
- es kann z.B. durch zusätzliche Sensoren überprüft werden, ob ein Fingerpuls vorhanden ist

### ➤ Merkmalscharakteristika

- die einfachste Methode ein Vergleichsmuster zu erstellen ist, die Grauwertbilder des Fingerabdrucks und des Musters zu verwenden ( jedoch aus datenschutzrechtlicher Sicht bedenklich, da sie Rückschlüsse auf den jew. Besitzer erlauben, z.B. durch Vergleich mit einer Verbrecherkartei )

## ... Fingerbildererkennung

### ➤ Merkmalscharakteristika

- eine weitere Methode ist die Ermittlung von Minuzien ( Linienenden, Verzweigungen, Schlingen und Wirbel ), wo ein Muster gebildet werden kann; zwölf dieser Minuzien genügen, um den Fingerabdruck eines Menschen zu identifizieren



diese Minuzien werden über Vektoren miteinander verbunden; es wird nur das resultierende Muster gespeichert ( ausreichend für eine juristisch eindeutige Identifikation ); benötigt wird eine Sensorauflösung von ca. 500 dpi



Abbildung 6: Bildung eines Musters aus einzelnen Minutiae

- eine dritte Möglichkeit ist die Ermittlung von Poren ( genauer als über Minuzien ), hier ist eine Auflösung von ca. 800 dpi notwendig

## ... Fingerbildererkennung

### ➤ Applikationen

- es gibt Geräte in verschiedenen Variationen:
  - wandmontiert als Zugangskontrolle zu Räumen oder Gebäuden
  - als eigenständiges Gerät, das z.B. über die serielle Schnittstelle an einen PC angeschlossen werden kann oder integriert in Eingabegeräte wie Tastatur oder Maus

Die Bundesrepublik Deutschland prüft zur Zeit, ob in Zukunft die Einreise-Visa zusätzlich zum neu eingeführtem Lichtbild mit dem biometrischen Merkmal Fingerabdruck verbunden werden sollen.

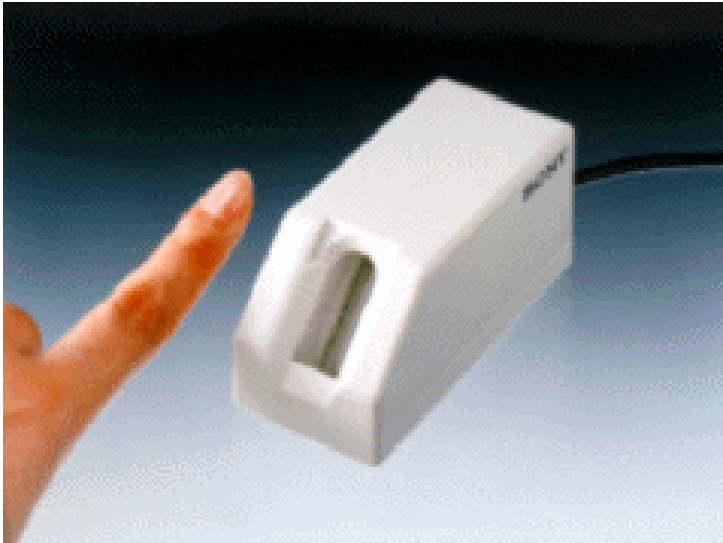
### ➤ Bewertung

- Vorteile:
  - lange Erfahrungen auf diesem Gebiet
  - sehr kleine Scannergröße, daher auch geringe Anschaffungskosten für Hardware
  - geringer Speicherbedarf
- Nachteile:
  - schmutzempfindlich
  - möglicherweise gestörtes Hygieneempfinden der Benutzer
  - mögliche Akzeptanzprobleme wegen der Assoziation von Fingerabdrücken mit einer Verbrecherkartei



## ... Fingerbildererkennung

### ➤ Fingerbildscanner



## Gesichtserkennung

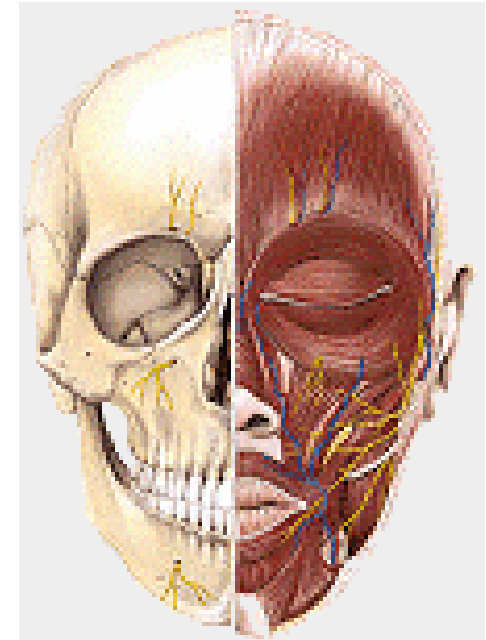
- **Einleitung**
- **Verfahrensbeschreibung**
- **Scannerarten**
- **Technische Daten**
- **Lebenderkennung**
- **Merkmalscharakteristika**
- **Mögliche Applikationen in der Praxis**
- **Bewertung**



## ... Gesichtserkennung

### ➤ Einleitung

- Menschen erkennen einander bei einer Begegnung vor allem am Gesicht, die charakteristischen Gesichtszüge eines Mitmenschen prägen sich uns besser ein als andere Eigenschaften.
- Bei der automatischen Gesichtserkennung wird über eine Videokamera das Gesicht einer Person aufgenommen und mit einem oder mehreren zuvor gespeicherten Gesichtern verglichen.
- Es wird zwischen zwei Verfahren unterschieden:
  - a) visuelle Gesichtserkennung
  - b) thermische Gesichtserkennung



## ... Gesichtserkennung

### a) Visuelle Gesichtserkennung:

#### ➤ Verfahrensbeschreibung

- eine Kamera nimmt ein Bild des Gesichts auf und analysiert es anhand verschiedener Kriterien
- die Gesichtserkennung kann sowohl im Verifikationsmodus wie auch im Identifikationsmodus erfolgen (s.o.)
- dieses statische Verfahren ist ( im Gegensatz zur z.B. Fingerbildererkennung ) berührungslos

#### ➤ Scannerarten

- die Scannergröße ist variabel ( von Größe einer Webcam für den Rechnerzugang bis hin zu über einen Meter hohen, schmalen Säulen, in die die Kamera in einem schräg nach oben zeigenden Winkel montiert ist für den Zugang zu Räumen oder Gebäuden )



## ... Gesichtserkennung

### ➤ Technische Daten

- die Zeit für eine Verifikation beträgt ca. 1 - 5 Sekunden, für eine Identifikation in Abhängigkeit zur Größe der Datenbank und Geschwindigkeit der verarbeitenden Einheit entsprechend länger
- die Größe eines Datensatzes beträgt etwa 2-4 Kilobytes, so dass er problemlos auf einer Chipkarte gespeichert werden kann
- ein eventuell zu Audit – Zwecken gespeichertes Originalbild belegt 16 Kilobytes

### ➤ Lebenderkennung

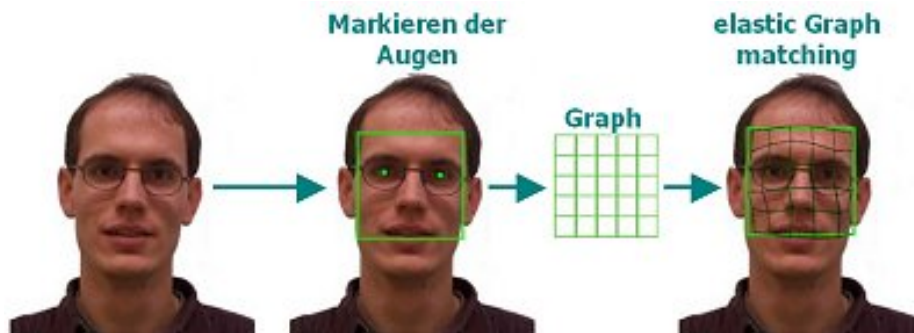
- eine Lebenderkennung ist notwendig, um das System vor Nachbildungen, wie z.B. einem Photo, zu schützen
- auch gegen äußere Veränderungen des Gesichts wie z.B. ein Bart oder eine Sonnenbrille muss das System unempfindlich sein



## ... Gesichtserkennung

### ➤ Merkmalscharakteristika

- eine Methode, wie aus dem Bild eines Gesichts ein Merkmalsatz erstellt werden kann, ist es, verschiedene markante Punkte ( z.B. Haaransatz, Augenbrauen, Augen, Nase, Mund, Kinn ) über Vektoren miteinander zu verbinden, das resultierende Muster zu speichern und es für den Vergleich zu verwenden (Elastic Graph Matching)



- eine weitere Methode ist, eine Art Gitter über das Gesicht zu legen; die dreidimensionalen Eigenschaften des Gesichts werden in das Gitter übertragen, das in Erzeugung eines Merkmalsatzes verwendet wird



## ... Gesichtserkennung

### ➤ mögliche Applikationen in der Praxis

- Computerzugang (Biometrisches Logon)
- Zutrittskontrolle zu Räumen oder Gebäuden (Biometrische Zutrittssicherung)
- Geldausgabeautomat



### ➤ Bewertung

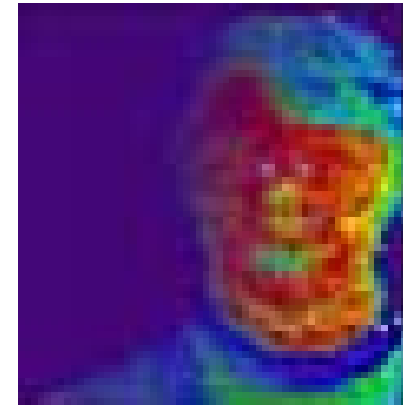
- Vorteile: - potentiell hohe Benutzerakzeptanz, da das System berührungslos, unaufdringlich, einfach bedienbar ist
  - niedrige Anschaffungskosten für Hardware für den Zugang zu einem Computer
- Nachteile: - hohe Anfälligkeit des Systems gegen zu geringe Beleuchtung
  - hohe Falschakzeptanzrate bei Benutzergruppen von über 100 Personen ( bei dem derzeitigen technischen Standard )

## ... Gesichtserkennung

### b) Thermische Gesichtserkennung:

#### ➤ Verfahrensbeschreibung

- hier zeichnet eine Infrarot – Kamera ein Bild des Gesichts auf
- Dabei wird das Thermobild des Gesichtes, das aufgrund der Durchblutung der Haut entsteht
- ( benutzerspezifische Rotfärbung) , mit einer Wärmebildkamera aufgenommen und ausgewertet



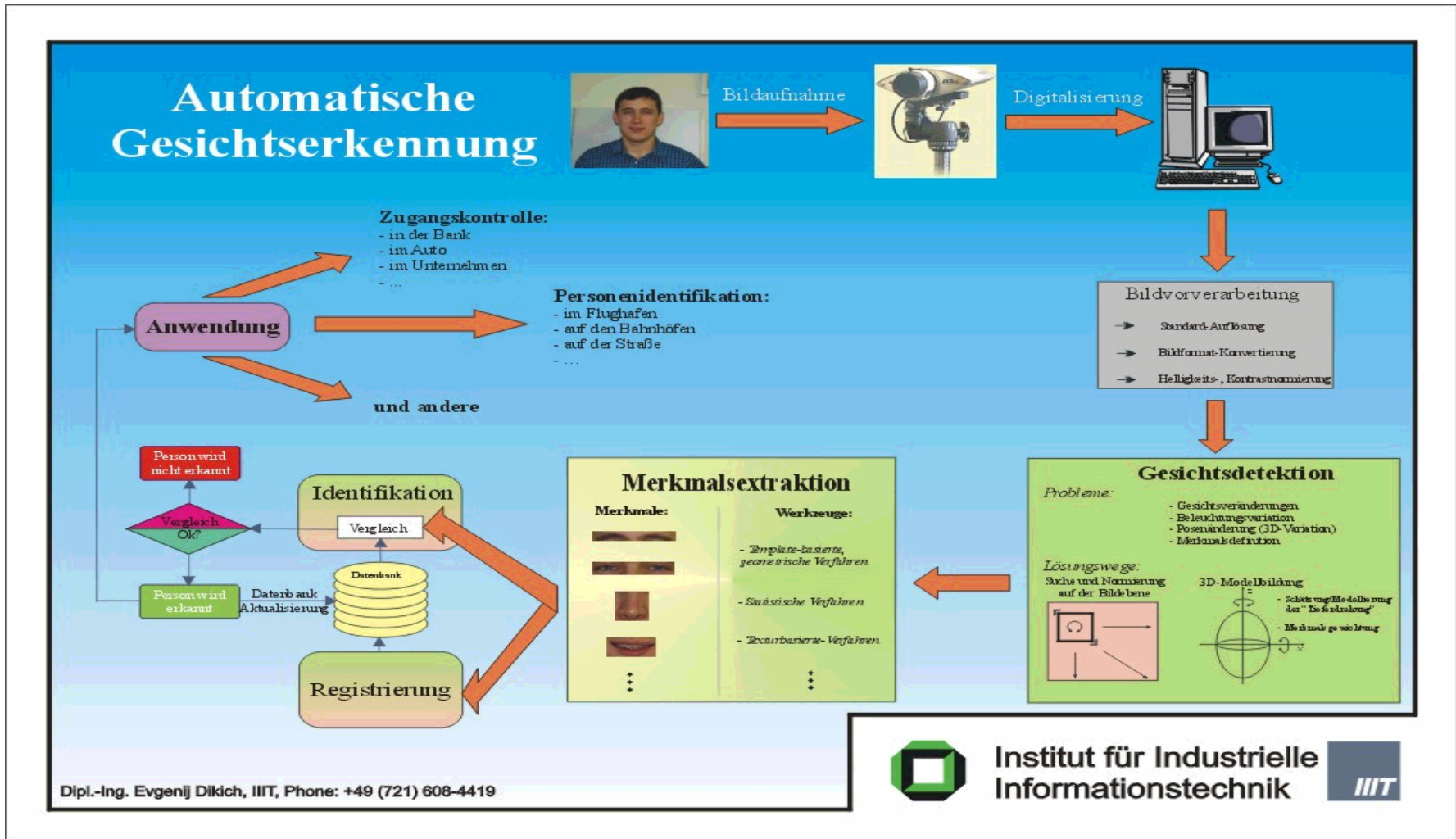
#### ➤ Lebenderkennung

- eine Lebenderkennung ist durch die Verwendung einer Infrarot – Kamera nicht erforderlich, da Fälschungen nahezu ausgeschlossen sind

#### ➤ Bewertung

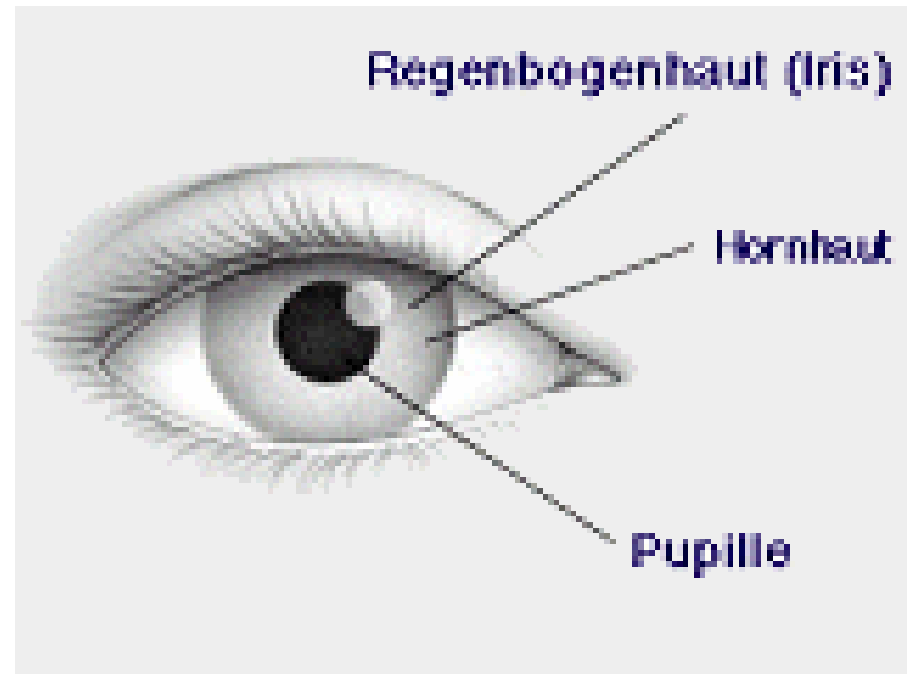
- Vorteile: - Unabhängigkeit der Beleuchtung ( im Gegensatz zur visuellen Gesichtserkennung )  
- Fälschungssicherheit bezüglich der Verkleidung oder der plastischen Chirurgie
- Nachteil: - relativ hoher Preis für die Hardware

# ...Gesichtserkennung



## Iriskennung

- **Einleitung**
- **Verfahrensbeschreibung**
- **Technische Daten**
- **Lebenderkennung**
- **Merkmalscharakteristika**
- **Applikationen in der Praxis**
- **Bewertung**
- **Irisscanner**



## ... Iriserkennung

### ➤ Einleitung

- Ähnlich dem Fingerbild ist die Iris bei jedem Menschen verschieden. Ihre Eigenarten (Äderchen, Pigmentkrausen, Streifen usw.) werden von Zufälligkeiten während der Embryoentwicklung bestimmt und ändern sich im Laufe des normalen menschlichen Lebens nicht. Ausnahmen können hier auftreten, wenn es zu einer Erkrankung oder Verletzung des Auges kommt.
- Die Wahrscheinlichkeit für zwei völlig identische Iris-Codes ist  $1: 10^{1078}$ , selbst genetisch identische Zwillinge bzw. das rechte und das linke Auge einer einzelnen Person haben so unterschiedliche Codes, wie zwei völlig verschiedene Menschen.
- Mit über 450 Freiheitsgraden bietet die Iris sogar sechs- bis achtmal soviel Variablen wie der menschliche Fingerabdruck. Da jeder dieser Freiheitsgrade hunderte oder tausende von Variationen haben kann, sind tausende Datenpunkte vorhanden, auf denen die Identifikation aufsetzen kann. In der Praxis haben statistische Analysen ergeben, dass etwa 244 Freiheitsgrade von den Systemen verwendet werden.



## ... Iriserkennung

### ➤ Verfahrensbeschreibung

- Mit einer Kamera wird das Gesicht des Benutzers gesucht und die exakte Position der Augen bestimmt. Das Muster der Iris wird erfasst und in ein Binärmuster umgewandelt. Die Erkennung findet, je nach Sensortyp, aus einer Entfernung von 10-50 cm statt.
- Das Verfahren ist berührungslos und somit ist die Erkennung auch von der Umgebung des Sensors abhängig. Bei der Iriserkennung ist die Helligkeit der Umgebung wichtig, da diese Einfluss auf die Größe der Pupille hat. Außerdem muss es hell sein, damit der Sensor die Merkmale eindeutig erkennen kann.
- Das Muster der Iris wird erfasst und in ein Binärmuster umgewandelt. Die Erkennung findet, je nach Sensortyp, aus einer Entfernung von 10-50 cm statt.

### ➤ Technische Daten

- Es gibt theoretisch  $10^{78}$  verschiedene Irismuster. Um diese eindeutig in einem Datensatz abbilden zu können, müsste jeder Datensatz mindestens  $2^{260}$ , also 260 Bit = 33 Bytes groß sein. Die tatsächliche Größe eines Datensatzes beträgt etwa 512 Bytes.
- Die benötigte Zeit der Verifikation beträgt in Abhängigkeit zur Größe der Datenbank etwa 2 Sekunden.

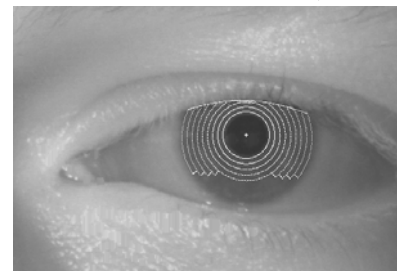
## ... Iriserkennung

### ➤ Lebenderkennung

- Die Iris ist ein statisches Merkmal. Eine Lebenderkennung ist notwendig, um das System vor Nachbildungen, wie zum Beispiel ein Glasaugen oder das Foto eines Benutzers, zu schützen.
- Die Equal Error Rate ist nach Angaben der Hersteller  $<10^{-2}\%$  beziehungsweise  $<10^{-4}\%$ . Probleme könnten sich bei Personen ergeben, die farbige Kontaktlinsen oder eine getönte Brille tragen. Auch wechselnde Lichtverhältnisse könnten sich negativ auf die Erkennung auswirken.

### ➤ Merkmalscharakteristika

- Eine Kamera nimmt ein Bild des Auges in schwarzweiß auf. Über das Bild wird ein Gitter gelegt. Ein Algorithmus generiert aus den hellen und dunklen Bereichen der Iris innerhalb des Gitters einen „menschlichen Code“, der eindeutig ist. Dieser Barcode ist das Muster, das dann mit dem Referenzmuster verglichen werden kann.



## ... Iriserkennung

### ➤ Merkmalscharakteristika

- **Robuste Darstellungen für die Mustererkennung müssen invariant sein gegenüber Veränderungen der Größe, Position und Orientierung der Muster. Im Fall der Iriserkennung bedeutet dies, dass man eine Darstellung ableiten muss, die invariant ist...**
  - a) gegenüber der Abbildungsgröße der Iris im Gesamtbild (diese Abbildungsgröße hängt vom Abstand zwischen Kamera und Auge sowie von der optischen Vergrößerung der Kamera ab)**
  - b) von der Pupillengröße innerhalb der Iris (die zu einer nichtaffinen Musterverzerrung führt)**
  - c) vom Ort und von der Orientierung der Iris im Bild (die von der Kopfneigung abhängen)**
  - d) sowie vom Kamerawinkel im Zusammenwirken mit Spiegeln und sonstigen optisch-mechanischen Bildsuchmaßnahmen, die zusätzliche Bildrotationsfaktoren in Abhängigkeit von Augenposition, Kameraposition und Winkelstellung der Spiegel einführen.**

**Glücklicherweise ist es problemlos möglich, gegenüber allen Faktoren dieser Art eine Invarianz zu erreichen.**

## ... Iriserkennung

### ➤ Applikationen in der Praxis

- Pilotprojekte, wie das Eye-Scanning wurden in der Vergangenheit zum Beispiel an Flughäfen in Frankfurt/Main und in Charlotte (North Carolina) durchgeführt. Dabei unterstützte die Technologie der Firma EyeTicket aus Virginia ( [www.eyeticket.com](http://www.eyeticket.com) ) die Identifizierung des Flughafenpersonals und der Besatzungscrew. Dabei liest eine digitale Videokamera die Iris ein und weist ihr einen binären Code zu. Dieser wird beim Gegencheck geprüft und bei Übereinstimmung wird das Personal autorisiert. Bald soll die Technik der Iriserkennung den Reisepass ersetzen. Das verkürzt die Flughafen-Abfertigungszeit.

### ➤ Bewertung

- Vorteile: - hohe Erkennungsgenauigkeit  
- berührungsfreie Benutzung  
- geringer Speicherbedarf
- Nachteile: - bei blinden Menschen funktioniert diese Form der biometrischen Authentisierung nicht  
- eine sichere Lebenderkennung ist nötig, um den hohen Sicherheitsansprüchen gerecht zu werden



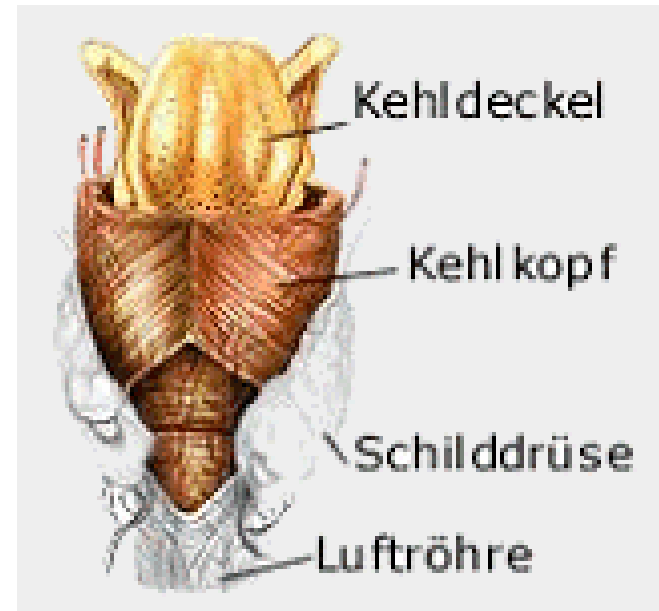
## ... Iriserkennung

### ➤ Irisscanner



## Spracherkennung

- **Einleitung**
- **Begriffserklärung**
- **Verfahrensbeschreibung**
- **Scannerarten**
- **Lebenderkennung**
- **Merkmalscharakteristika**
- **Probleme**
- **Mögliche Applikationen in der Praxis**
- **Bewertung**



## ... Spracherkennung

### ➤ Einleitung

- **Das Frequenzspektrum der menschlichen Stimme kann grafisch sichtbar gemacht werden und hat charakteristische Merkmale je nach Sprecher. Damit eignet sich auch die Stimme zur Identifizierung einer Person.**
- **Schaut man sich Zeitsignale verschiedener Sprecher an , die das gleiche Wort gesprochen haben, scheint eine automatische Erkennung eines bestimmten Sprechers zunächst relativ einfach.**
- **Eine Betrachtung der Zeitsignale des gleichen Wortes vom Sprecher, das zu unterschiedlichen Zeiten aufgenommen wurde, weist schon die eigentliche Problematik hin: Das reine Zeitsignal reicht nicht aus, um die Variationsvielfalt in den Griff zu bekommen.**
- **Welche Verfahren hinter einer automatischen Sprechererkennung stehen und welche Probleme im täglichen Betrieb entstehen können, soll nachfolgend erläutert werden.**

## ... Spracherkennung

### ➤ Begriffserklärung

- Sprecherverifikation („Ist er es?“): Der Sprecher ist durch Eingabe einer Kennung beispielsweise auf seiner Chipkarte und/oder seine PIN bekannt. Es soll geprüft werden, ob tatsächlich dieser Sprecher spricht.
- Sprecheridentifikation („Wer ist es?“): Es wird geprüft, welcher von den bekannten Sprechern spricht.

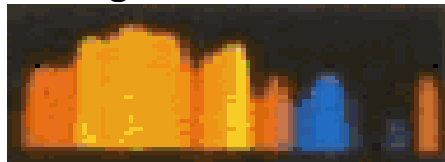
Bei beiden Prinzipien müssen Merkmale der Sprecher vor dem Erkennungsvorgang dem System bekannt gemacht werden, das System muss trainiert werden. Letztlich hängt es vom Training und der Speicher- und Entscheidungsverwaltung ab, ob eine Sprecherverifikation oder –identifikation erfolgt.

## ... Spracherkennung

### ➤ Verfahrensbeschreibung

Der automatische Sprechererkennungsvorgang besteht aus vier wesentlichen Abschnitten:

- der Sprachanalyse zur Gewinnung der sprecherspezifischen Merkmale, es wird aus den aufgezeichneten Frequenzen ein Muster gebildet



- dem Vergleich mit im Training gespeicherten Merkmalssätzen (Referenzmuster), wobei es sich dabei um textabhängige oder textunabhängige Sprachproben handeln kann
- der eigentlichen Schwellwertung über Annahme oder Ablehnung bei der Verifikation oder Sprecherauswahl bei der Identifikation
- einer Adaption der Referenzen und der Entscheidungsschwellen an die zeitlichen Stimmveränderungen, die für den praktischen Betrieb vorteilhaft ist.

## ... Spracherkennung

### ➤ Scannerarten

- Das Verfahren ist berührungslos und als Scanner kommt ein Mikrofon in Betracht.

### ➤ Lebenderkennung

- Die Sprache ist ein dynamisches Merkmal. Die Sprachfrequenzen variieren von mal zu mal, die Charakteristika der Sprache bleiben jedoch gleich. Eine Lebenderkennung ist dennoch notwendig, um sich vor Wiedereinspielung einer mit Tonband aufgezeichneten Authentisierung zu schützen.

### ➤ Merkmalscharakteristika

- Von jedem gesprochenen Wort wird sowohl die Lautstärke, als auch das Frequenzspektrum analysiert und daraus ein Frequenz-Lautstärke-Profil für den Benutzer erstellt. Aus jedem Wort werden 14 Merkmale extrahiert, die den Merkmalsvektor des Wortes bilden. Eine Abfrage von drei Ziffern ergibt somit einen Vektor aus 42 Merkmalen.

## ... Spracherkennung

### ➤ Probleme

Verschiedene Faktoren können die Authentisierung erschweren oder verhindern.  
Diese sind...

- **Variabilität durch sprecherunabhängige Faktoren, wie zum Beispiel Husten, Heiserkeit, emotionale Verfassung, Trunkenheit**
- **Artikulationsabhängige Faktoren, also ob Wörter zusammengezogen werden oder einzeln gesprochen werden**
- **Umgebungsabhängige Faktoren, wie zum Beispiel verschiedene Räumlichkeiten, Hintergrundgeräusche, Reflektionen oder die unbewusste Anpassung an die jeweilige akustische Umgebung**

## ... Spracherkennung

### ➤ Mögliche Applikationen in der Praxis

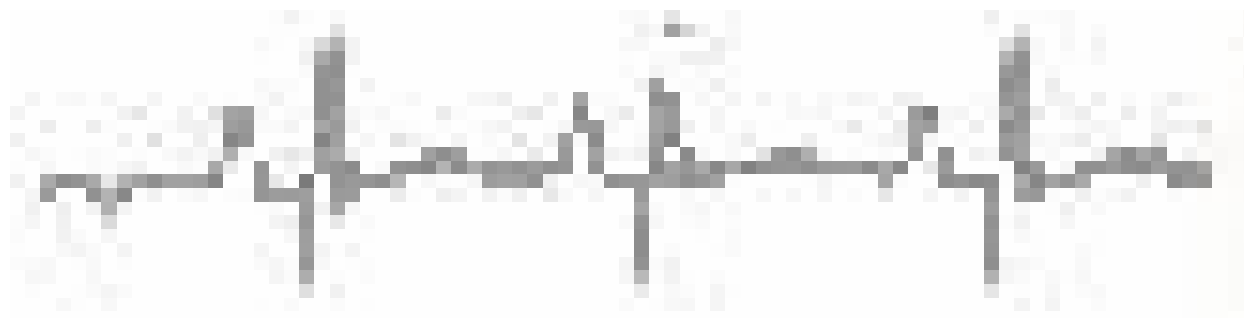
- Wegfahrsperre für Automobile
- für telefonische Transaktionen

### ➤ Bewertung

- **Vorteile:**
  - Möglichkeit der Authentisierung via Telefon
  - Bei vorhandener Hardwareplattform niedrige zusätzliche Hardwarekosten für ein Mikrofon
  - geringer bis mittlerer Speicherbedarf
- **Nachteile:**
  - relativ langsame Verifikation
  - relativ hohe Fehlerrate
  - Verfahren bei stummen oder sprachbehinderten Menschen nicht anwendbar
  - Stimme verändert sich durch Alter und Krankheit
  - Empfindlichkeit auf Nebengeräusche relativ hoch

## Unterschriftenerkennung

- **Einleitung**
- **Grundprobleme**
- **Verfahrensbeschreibung**
- **Sensorarten**
- **Technische Daten**
- **Merkmalscharakteristika**
- **Applikationen in der Praxis**
- **Bewertung**



## ... Unterschriftenerkennung

### ➤ Einleitung

- Auch die Unterschrift lässt sich als Beleg der eigenen Identität nutzen. Die manuelle Analyse wird in der Medizin und Schriftpsychologie seit langem praktiziert. Erst in den letzten Jahren wurde begonnen, die Handschrifterkennung durch Verfahren der Mustererkennung zu objektivieren und zu automatisieren.
- Eine Unterschrift lässt sich vielleicht fälschen. Aber der Schreibdruck und die Dynamik, mit der der Stift geführt wird, ist nicht erfassbar oder nachahmbar. Jeder Mensch schreibt mit einer individuellen Schreibzeit und macht individuelle Pausen zwischen den Buchstaben
- Das Verfahren der Unterschriftenerkennung ist dann interessant, wenn nicht nur die bildliche Repräsentation der Handunterschrift mit dem hinterlegten Template verglichen wird, sondern an einem Sensor die Dynamik der Handschrift bewertet wird, wie beispielsweise Geschwindigkeit und Druck.
- Dazu werden mit speziellen Sensoren die Kräfte und Beschleunigungen, die bei der Bewegung des Stiftes auftreten, gemessen. Daraus ermittelt eine Auswertlogik die individuellen Merkmale der Unterschrift.

## ... Unterschriftenerkennung

### ➤ Grundprobleme

- ***Entwicklung von Handschriften:*** Die Handschrift vollzieht sich in der Auseinandersetzung mit der in der Grundschule gelehrtten Ausgangsschrift. Sie ist vom jeweiligen Zeitstil geprägt. Aufgrund verschiedener Schreibvorlagen und Lerntechniken variiert das Schriftbild.
- ***Physiologische Einflussfaktoren:*** Der persönliche Schreibstil ist durch ein personenspezifisches Schreibtraining zu einer sensorischen Fertigkeit ausgebaut worden. Für das Schreiben mit der Hand werden Arm-, Handgelenk- und Fingerbewegungen überlagert. Die Überlagerungen müssen exakt aufeinander abgestimmt sein und in einer festen zeitlichen Abfolge verlaufen. Trotz dieses hohen Maßes an notwendiger Koordination und Exaktheit der Bewegungen schreibt der geübte Schreiber nahezu unbewusst.
- ***Konstanz und Konsistenz in Schriftproben:*** Konstanz ist in der Schrift niemals in dem Sinne gegeben, dass bei wortgleichen Schriftzügen völlige Deckungsgleichheit zu erwarten ist. Vielmehr weist jede Schrift auch unter gleich bleibenden Bedingungen eine mehr oder minder große natürliche Schwankung auf.

## ... Unterschriftenerkennung

### ➤ Verfahrensbeschreibung

- **Beim biometrischen Unterschriftenverfahren wird die Unterschrift eines Benutzers in geeigneter Weise aufgezeichnet, um daraus ein Muster zu erstellen. Der reine zweidimensionale Vergleich zweier Unterschriften auf Papier ist nicht sicher. Daher werden bei diesem Verfahren weitere Kriterien hinzugezogen.**
- **Das Verfahren ist dynamisch und berührungslos. Die benötigte Zeit für die Verifikation beträgt etwa eine Sekunde. Die Fehlerraten sind nicht bekannt.**
- **Die Unterschrift einzelner Benutzer kann sich im Laufe der Zeit ändern. Das Verfahren ist deshalb adaptiv, um mögliche Änderungen berücksichtigen zu können. Probleme bei der Authentisierung können auftreten, wenn ein Benutzer zum Beispiel durch kaltes Wetter klamme Finger hat und dadurch die Unterschrift von seinem Muster deutlich abweichen kann.**

**Dieses Verfahren bietet sich als Ersatz für herkömmliche Unterschriftenprüfungen an. So könnten auf diese Weise zum Beispiel in den Banken Transaktionen autorisiert werden.**

## ... Unterschriftenerkennung

### ➤ Sensorarten

Um eine Unterschrift auszulesen, können zwei verschiedene Arten von Sensoren zum Einsatz kommen. Es gibt...

- Einen speziellen Stift           oder
- Eine spezielle Unterlage

In beiden Sensortypen sind einzelne Sensoren implementiert, die die Bewegung des Stiftes bei der Unterschrift auslesen und digitalisieren. Im ersten Fall befinden sich diese Sensoren im Stift selbst, im zweiten Fall in der Unterlage, auf der mit einem beliebigen Stift unterschrieben werden kann.



## ... Unterschriftenerkennung

### ➤ Merkmalscharakteristika

Bei einer Unterschrift werden vier verschiedene Merkmale aufgezeichnet:

- Die Bewegungen des Stiftes in X-Richtung
- Die Bewegungen des Stiftes in Y-Richtung
- Der Druck, den der Stift auf die Unterlage ausübt
- Die Zeit, die die Größe der X-Achse bestimmt

Die daraus resultierenden Kurven werden ausgewertet und zur Erstellung eines Merkmalsvektors verwendet.

### ➤ Applikationen in der Praxis

- bei Kreditinstituten (Unterschriftenprüfung bei Transaktionen)
- Sicherer E-Commerce, insbesondere zwischen Geschäftspartnern, wird erst durch die Kombination von klassischer Unterschrift und elektronischer Signatur gewährleistet.
- Bekämpfung von Betrug mit Kreditkarten

## ... Unterschriftenerkennung

### ➤ Applikationen in der Praxis

- Am Bsp. HESY (Handschriftenerkennungssystem):
  - HESY wird zur Zeit in einem Pilotprojekt im Hotel Consul, Bonn eingesetzt
  - Es dient zur elektronischen Archivierung der Unterschriften der Gäste, so dass die jahrelange Archivierung der Papiermeldezettel entfällt.
  - HESY besteht aus einer Schreibunterlage (Platte), die auf vier Drucksensoren gelagert und mit dem Computer verbunden ist.
  - Wenn der Gast oder Kunde darauf unterschreibt, werden dabei je 1046 Druckwerte pro Sekunde erfasst. Es entsteht ein schlichtes Faksimile der Unterschrift auf dem Bildschirm, dem ein komplexes System aus Kurvendiagrammen hinterlegt ist, das die Unterschrift "einmalig" macht.



# Zusammenfassung

Biometrische Verfahren								
Methode*	Fingerabdruck	Hand	Gesicht	Iris	Retina	Stimme	Schrift	Tastenschnal
								
biometrisches Merkmal	Fingerlinien auf der Fingerkuppe	Geometrie der Hand (z. B. Lage der Knöchel)	Gesichtsgeometrie (Lage von Augen, Nase usw.)	Gewebemuster rund um die Pupille	Muster der Blutgefäße auf der Netzhaut	Klangmuster und Sprechrhythmus der Stimme	Tempo, Druck, Beschleunigung der Schreibbewegung	Tipprhythmus an der Computertastatur
Vorteile	günstiger Preis, sehr kompakt, geringer Speicherbedarf, in viele Geräte integrierbar, schnell	Große Erfahrung (z. B. Olympiade 1996 in Atlanta), sehr geringer Speicherbedarf, einfache Bedienung	einfach zu bedienen, schnell, berührungslos, leicht integrierbar in Überwachungssysteme	schnell, geringer Speicherbedarf	schnell, geringer Speicherbedarf	geringer bis mittlerer Speicherbedarf, billig, auch über Telefon einsetzbar	billig, geringer bis mittlerer Speicherbedarf, menschliche Aktion erforderlich – daher Lebenderkennung integriert	permanente Überwachung des PC, Anwendung bei Computerarbeitsplätzen
Nachteile	Verletzungen (Narben) verschlechtern die Erkennung, schmutzempfindlich	Probleme bei sehr großen oder sehr kleinen Händen	lichtabhängig, relativ teuer, Gesicht verändert sich	teuer, beleuchtungsabhängig	teuer, Beleuchtung des Auges nötig, Auge muß ruhig gehalten werden, funktioniert nicht bei Grauem Star	langsam, Stimme verändert sich durch Alter und Krankheit, Erkennungsprobleme übers Telefon	natürliche Schwankungen in der Unterschrift reduzieren Erkennungsleistung	Tipprhythmus abhängig von Tastatur und Stimmung, gute Erkennung nur bei geübten Schreibern
Sicherheit	hoch Aber: System muß gewährleisten, daß Fingerabdruck von lebender Person stammt	mittel System muß erkennen, ob Hand von lebender Person stammt	mittel System muß Masken oder Fotos erkennen	extrem hoch theoretisch Täuschung mit Iris einer anderen Person möglich	extrem hoch Täuschung durch Retina-Attrappen muß verhindert werden	mittel Täuschung durch Bandaufnahmen muß verhindert werden	mittel Dynamik fremder Unterschrift kann eventuell trainiert werden	noch nicht bekannt
Akzeptanz	hoch Aber: eventuell hygienische Bedenken	hoch eventuell hygienische Bedenken	mittel bis hoch je nach Einsatz Furcht vor versteckter Überwachung denkbar	hoch Furcht vor versteckter Überwachung denkbar	mittel Aufmerksamkeit nötig, Angst vor Augenschäden denkbar	mittel Zeitaufwand und Aufmerksamkeit erhöht, Überwachung möglich	hoch in Situationen, wo schon heute unterschrieben wird	hoch in gewohnter Arbeitsumgebung

Photos: Orosio, V. Steiger, Archiv (8)

\*Weitere Verfahren: DNA-Analyse durch Entnahme von Hautzellen, Wärmebild des Körpers, chemische Analyse des Körpergeruchs

# Kombinierte Biometricsysteme



## ... Kombinierte Biometricsysteme

- **Durch die Kombination einer Vielzahl von Gesichts- und Verhaltensmerkmalen, beispielsweise der menschlichen Stimme oder der Bewegung der Lippen, lässt sich die Zuverlässigkeit der biometrischen Gesichtserkennung zusätzlich erhöhen.**
- **So wird z.B. eine Sekunde lang das Gesicht einer zu identifizierenden Person, die ein bestimmtes Wort in die Kamera spricht, aufgenommen. Ein Algorithmus ermittelt den optischen Fluss aus jeweils zwei aufeinander folgenden Bildern. Zusätzlich wird die Wellenform des gesprochenen Wortes mit einer zuvor aufgenommenen Wellenform verglichen.**
- **Ausweis mit Fingerabdruck und digitaler Signatur. Die Kombination von On-card Fingerabdruck-Verifikation und digitaler Signatur auf der Ausweiskarte bieten dem Bürger in Zukunft die Möglichkeit sämtliche Behördengänge (von der Ummeldung über die Kfz-Anmeldung bis zum Wählen) von daheim zu erledigen.**
- **Das fränkische Sicherheitsunternehmen Sitec stellte auf der Cebit eine Personenschleuse vor, die Zugangsberechtigte anhand von Fingerabdruck und Körpergewicht erkennt. Gedacht ist die Schleuse vor allem für die Sicherheitszonen in Zweigstellen von Banken. Die Gewichtskontrolle soll sicher stellen, dass der Bankangestellte alleine Zugang verlangt - und nicht mit einer Waffe an der Schläfe von einem Bankräuber zum Eintritt gezwungen wird.**

## Schlussbetrachtung

- **Der Umsatz im Bereich der Biometrie-Hardware wird bis 2007 stark ansteigen. Derzeit werden von Biometrik-Unternehmen rund zwei Drittel durch Services und ein Drittel aus dem Verkauf von Hardware erwirtschaftet.**
- **Biometrische Anwendungen dringen unterdessen immer mehr ins alltägliche Leben vor. So ersetzen derzeit immer mehr Firmen die Karten der Stechuhren mit Handscannern. Aber auch die US-Einwanderungsbehörde setzt verstärkt auf Biometrie zur Erkennung von Vielfliegern, die sich nicht jedes Mal in die Schlange am Personencheckpoint einreihen wollen. Im vergangenen Jahr nutzte die Polizei in Florida biometrische Geräte um die Fans beim Super- Bowl zu scannen. Sogar in Disneyland wird begonnen einen Fingerscanner als Eintrittskarte zu nutzen.**
- **Nach Ansicht von Experten wird Biometrie in Zukunft an PCs für Augen, Gesicht, Hand und Finger eingesetzt werden. Bereits heute können User spezielle Keyboards oder eine spezielle Mouse nutzen um etwa die Finger scannen zu lassen. Augen und Gesicht können mit einfachen PC-Kameras gescannt werden.**

## ... Schlussbetrachtung

- **Die hohe Sicherheit, die viele biometrische System bieten und die mögliche Eindämmung der "Passwortflut", mögen manche Anwender euphorisch stimmen.**
  
- **Doch wie zuverlässig und sicher sind Biometricsysteme?**  
**Bei Praxistests von Biometricsystemen stellte sich heraus, dass die Fehlerrate höher war als die der Hersteller. Unbefugte Personen erhielten zum Teil Zugriff zu Daten und befugten Personen wurde teilweise der Zugang nicht gewährt. Die Ursache liegt in den sich zum Laborumfeld der Entwickler unterscheidenden Umweltbedingungen wie Geräuschpegel oder Beleuchtungswechsel.**
  
- **Es muss daher darauf geachtet werden, dass der Schutz persönlicher Daten gewährleistet ist, um den "gläsernen Menschen" niemals Wirklichkeit werden zu lassen.**

## Literaturverzeichnis

- **Armin Medosch / Janko Röttgers (Hrsg.): Netzpiraten. Die Kultur des elektronischen Verbrechens, Hannover: Heinz Heise Verlag 2001**
- **Udo Ulfkotte (2001): Wirtschaftsspionage: Wie deutsche Unternehmen von ausländischen Geheimdiensten ausgeplündert und ruiniert werden, Goldmann-Verlag, München**
- **Michael Behrens/Richard Roth(Hrsg.): Biometrische Identifikation.Grundlagen,Verfahren Perspektiven, Wiesbaden: Vieweg Verlag 2001**

## Internet-links

- <http://www.marquiswhoswho.net/ULFKOTTE/>
- <http://www.sicherheit-im-internet.de/themes/print.phtml?ttid=14&tdid=23>
- <http://www.kecos.de/script/35biometrie.htm>
- <http://www.uni-karlsruhe.de>
- <http://www.biometrie.inos.de>
- <http://www.hesy.de>
- <http://www.teletrust.de>
- <http://www.eyeticket.com>