# Biometrische Authentifizierungssysteme

Denitsa MANOVA und Daniela PÖLL

18. Jänner 2013

# Inhalt der Präsentation

# Definition

## Wortherkunft

Biometrie wird von den griechischen Wörtern “bios“ (Leben) und “metron“ (Maß) abgeleitet.

## Definition

Biometrie ist als Lehre von der Anwendung mathematisch-statistischer Methoden auf die Mess- und Zahlenverhältnisse der Lebewesen und ihrer Einzelteile definiert.

# Definition

## Im Bereich der Personenerkennung

Man definiert Biometrie im Bereich der Personenerkennung als automatisierte Erkennung von Individuen, basierend auf ihren verhaltensbasierten und biologischen Eigenschaften.

Sie wird im Bereich der Computerwissenschaften in der Form von Identifizierung und Zugriffskontrolle verwendet.

# Methoden - Körperbiometrie

- DNA
- Fingerabdruck
- Fußabdruck
- Gesichtsgeometrie
- Handgeometrie
- Iris
- Ohrform
- Retina
- Venenstruktur

# Methoden - Verhaltensbiometrie

- Stimme
- Tippverhalten
- Unterschrift

# Begriffserklärungen

## Identifizierung

Identifizierung bedeutet die Feststellung der Identität einer Instanz aus einer größeren Menge von Instanzen.

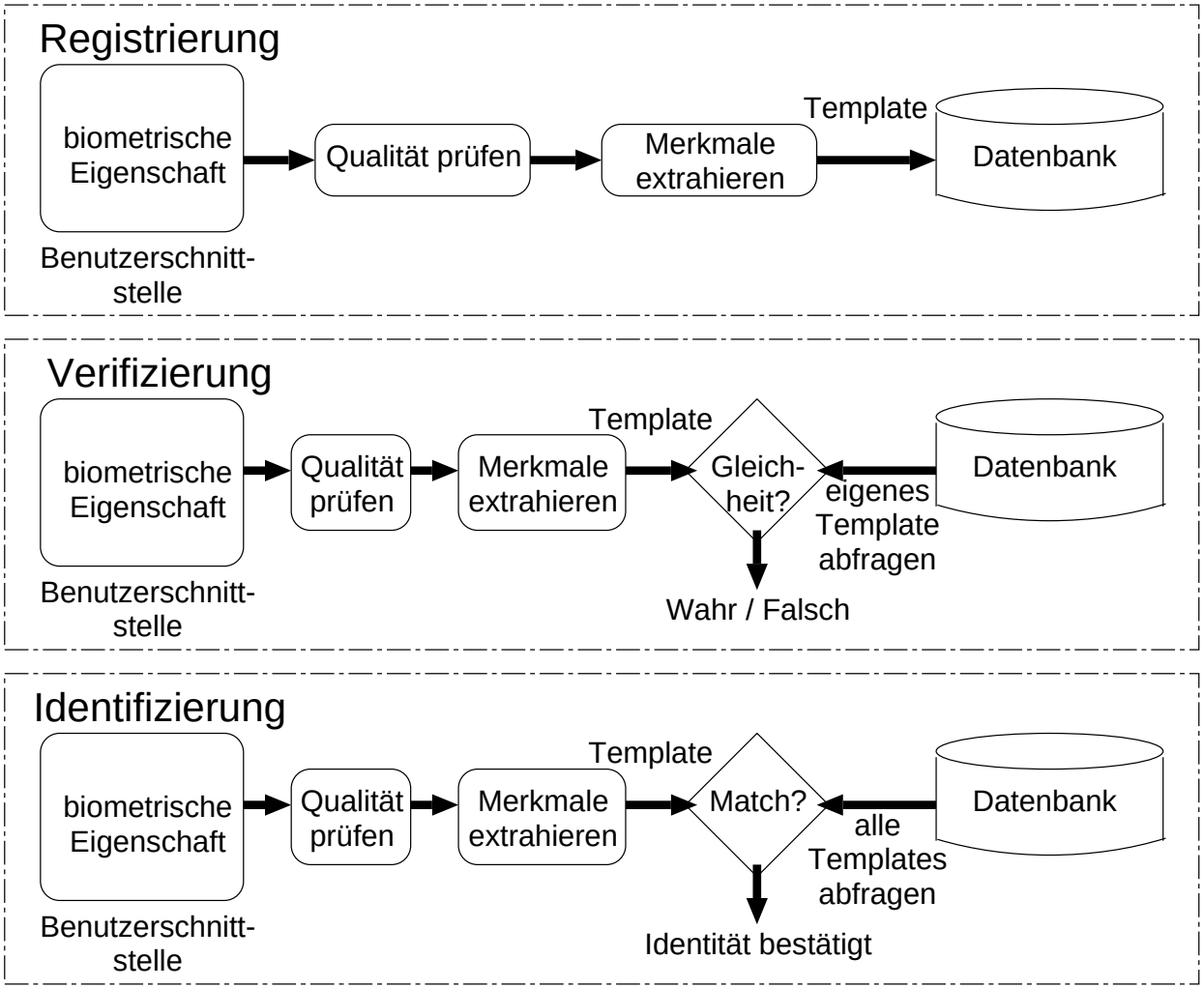
z.B. Identifizierung im Alltag durch Angabe des Namens.

## Authentifizierung / Verifizierung

Authentifizierung / Verifizierung einer Instanz ist der Nachweis dieser Identität, stellt also fest, ob die betreffende Instanz diejenige ist, die sie zu sein behauptet.

z.B. Authentifizierung / Verifizierung durch Vorlage eines Personalausweises.

# Registrierung - Verifizierung - Identifizierung



# Anforderungen

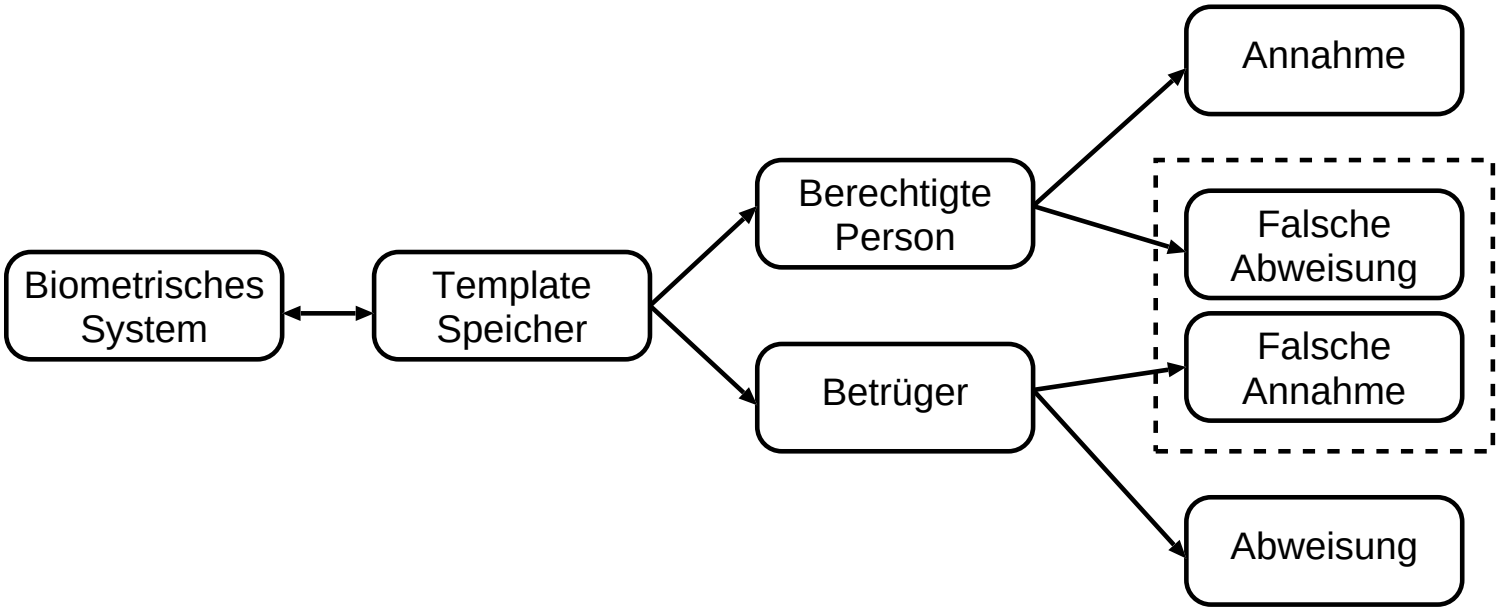
## Anforderungen an biometrische Eigenschaften

- Beständigkeit
- Beständigkeit gegenüber Missbrauch
- Effizienz
- Einzigartigkeit
- Messbarkeit
- Nutzerfreundlichkeit
- Universalität

# Fehlerrate bei der Erkennung

## Fehlerrate

- FRR (False Rejection Rate) Falsch-Abweisungsrate
- FAR (False Acceptance Rate) Falsch-Annahmerate
- EER (Equal Error Rate) FRR und FAR sind gleich



# Angriffsmöglichkeiten

## Wichtig zu beachten

Biometrische Authentifizierungssysteme werden häufig als sehr sicher dargestellt und gelten als das Authentifizierungssystem der Zukunft schlechthin, aber leider gibt es auch hier Angriffsmöglichkeiten, die man nicht unterschätzen sollte.

# Angriffsmöglichkeiten

- Fingerabdruck:
  - Dummy oder Fake-Fingerabdruck
  - Gummibärchen-Attacke
  - Anhauchen des Scanners
- Gesichtsgeometrie:
  - Foto vom Gesicht mit hoher Qualität
- Handgeometrie:
  - Fake-Hand
  - Papierschablone bei Formerkennung
- Iris:
  - Kopie wird auf Kontaktlinse übertragen
  - Foto vom Auge mit sehr hoher Qualität

# Fingerabdruck - Allgemeine Infos

- Ist eine der am häufigsten verwendeten biometrischen Methoden.
- Viele Systeme kombinieren Fingerabdruck mit:
  - Überprüfung des Blutflusses oder
  - Messung des Herzschlages.
- Jeder Fingerabdruck ist eine einzigartige Kombination aus Erhöhungen, Vertiefungen und Minutien.

# Auftreten von Fingerabdrücken

## Drei Arten

- Sichtbare Fingerabdrücke
- Verborgene Fingerabdrücke
- Eingeprägte Fingerabdrücke

# Grundsätzliche Unterteilung in drei Gruppen

- Wirbel (30%)
- Schleife (65%)
- Bogen (5%)

Die angeführten Werte wurden bei Forschungsarbeiten ermittelt und stellen das %-mäßige Vorkommen einer Gruppe dar.

# Linien-Typen

- Bogen
- Ellipse
- Gabelung
- Gerade Linie
- Insel
- Minutien Punkt
- Schleife
- Schweißdrüse
- Spirale
- Zeltartiger Bogen

# Optischer Scanner

- Finger wird auf einer Glasplatte platziert.
- Beim Scan wird ein Array von LEDs verwendet, mit denen der Finger beleuchtet wird.
- Mittels CCD (charge coupled device) wird ein Bild vom Fingerabdruck erstellt.
- Das produzierte Bild wird auf Qualität überprüft.

# Kapazitäts-Scanner

- Arbeitet ähnlich wie optischer Scanner.
- Anstatt Licht wird elektrischer Strom verwendet.
- Es wird die Distanz zu den Erhöhungen und Vertiefungen gemessen. Je nach Länge des Weges unterscheidet sich die Kapazität.
- Die Kapazität wird in ein digitales Grauwertbild übersetzt.
- Das produzierte Bild wird auf Qualität überprüft.

# Ultraschall Scanner

- Ist die neueste Technologie und deshalb noch nicht so häufig verwendet.
- Mittels Ultraschallwellen wird die Distanz zu den Erhöhungen und Vertiefungen gemessen.
- Resultierende Werte werden zur Erstellung des Bildes verwendet.
- Das produzierte Bild wird auf Qualität überprüft.

# Weiterverarbeitung der Bilder

Die durch den Scan erhaltenen Bilder werden weiterverarbeitet:

- Merkmale extrahieren
- Template erstellen
  - in Datenbank speichern
  - für Vergleich verwenden.

# Mögliche Probleme

Folgende Probleme können dazu führen, dass sich die Haut an den Fingerkuppen verändert. Da sich somit der aktuelle Fingerabdruck stark vom Template, welches in der Datenbank gespeichert ist, unterscheidet, kann die betreffende Person nicht authentifiziert werden.

- Alter
- Chemische Produkte
- Raue Haut und Hornhautbildung

# VIELEN DANK FÜR DIE AUFMERKSAMKEIT!

# Literatur

Skizzen wurden in Anlehnung an [1] erstellt.

[1] Charles A. Shoniregun und Stephen Crosier.
*Securing Biometrics Applications*.
Springer, 2008.
ISBN 0-201-52983-1.

[2] Andreas Uhl und Peter Wild.
Footprint-based biometric verification.
*Journal of Electronic Imaging*, 2008.

[3] Peter Rechenberg und Gustav Pomberger.
*Informatik Handbuch*.
Hanser, 4th edition, 2006.
ISBN 3-446-40185-7.

[4] H. Chen et al.
Fake hands: Spoofing hand geometry systems.

[5] Minhaz Fahim Zibran.
Eye based authentication: Iris and retina recognition.
Technical report, University of Saskatchewan, 2009.

[6] http://computer.howstuffworks.com.

[7] http://de.wikipedia.org.

[8] http://www.lechitel.bg.

[9] http://www.griaulebiometrics.com.

[10] http://www.seniorwomen.com.