Humboldt Universität Informatik

HUMBOLDT-UNIVERSITÄT ZU BERLIN

Biometrie und Datenschutz

Ralf Cremerius und Leonid Snurnikov

Seminar Überwachungstechnologien und informationelle Selbstbestimmung, 2006

Gliederung

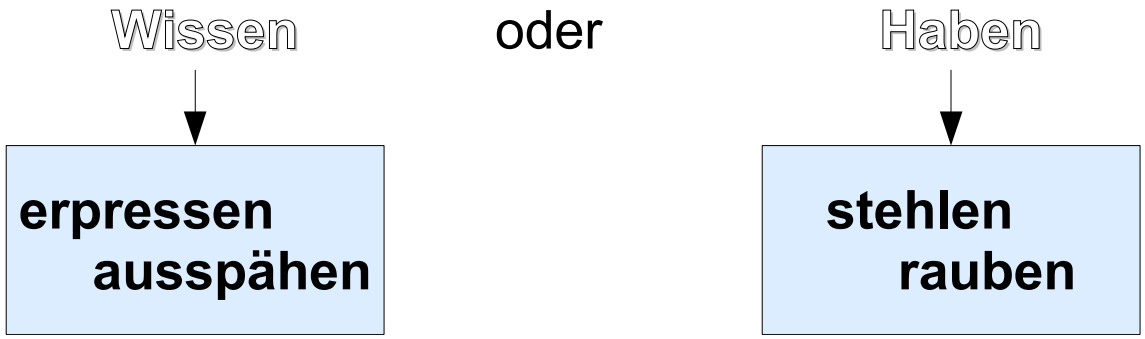
- Einführung und Grundlagen
  - Definition, biometrische Vorgehensweise, Authentifikation
  - Eigenschaften und Merkmale biometrischer Systeme
- Einschränkungen
  - Fehlerquellen und -arten, Sicherheitsaspekte
  - praktische Einschränkungen
- Technische Umsetzungen und Verfahren
  - Technische Ansätze
  - Möglichkeiten der Überwindung
- Datenschutzaspekte und juristische Fragen
  - Rechtlicher Rahmen, Besonderheiten biometrischer Daten
  - Speicherung und Datenschutz, weitere juristische Fragen
- Fazit und Ausblick

Definition

- Biometrie = Bio + Metron = Leben + Maß
- Vermessung ***quantitativer*** Merkmale
- statistische Verfahren
- Klassische Biometrie
  - Biostatistik
- Moderne Biometrie
  - Menschen
  - Authentifikation (1:1) und Identifikation (1:N)
  - Ziel: Zuordnung einer Identität und entsprechender Rechte zu physischen Personen

Biometrische Vorgehensweise

- traditionelle Authentifikationstechniken:



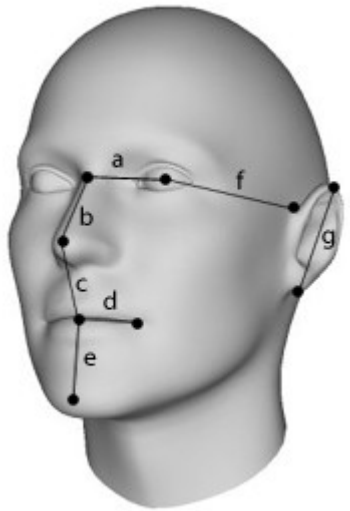
- Biometrie:
  - Authentifikation über ***Physiologie*** oder ***Verhalten (SEIN)***
  - ***personengebundene*** und nicht nur ***personenbezogene*** Merkmale/Daten
  - Merkmale schwer zu stehlen oder zu kopieren

Möglichkeit der Überprüfung des zu identifizierenden Merkmals zusammen mit dessen zulässigen Besitz

Grundprinzip der Authentifikation

1. Einlernphase = ***User-Enrollment***
   - Referenzmuster erfassen
2. Aktuelles Probemuster mit Referenzmuster vergleichen
3. Grad der Ähnlichkeit entscheidet

- Maß der Sicherheit der Identifikation bzw. Verifikation:
  - Falschakzeptanzrate (***FAR***)
    = Zulassungsrate Unberechtigter
  - Falschrückweisungsrate (***FRR***)
    = Abweisungsrate Berechtigter
- Weitere Eigenschaften biometrischer Systeme:
  - Erkennungszeit
  - Sicherheit, Zuverlässigkeit und Verfügbarkeit
  - Usability



Merkmale moderner Biometrie

- Kategorisierung nach:
  - aktiv / passiv
  - verhaltens-/physiologiebasiert
  - dynamisch/statisch

- langfristig stabile ***verhaltensbasierte*** Merkmale:

  Stimme, Handschrift,Tippverhalten, Gangdynamik ...
- langfristig stabile ***physiologische*** Merkmale:

  Fingerabdruck, Iris, Handgeometrie, DNA ...

- Grenzbereiche der Unterscheidung:

  Ist z.B. die Stimme wirklich nur verhaltensbasiert?

Merkmalseigenschaften

- Einzigartigkeit
- Konstanz
- Möglichkeit zur willentlichen Beeinflussbarkeit durch den Benutzer
- Merkmalsverbreitung
- Merkmalsakzeptanz
- Ausspähbarkeit
  - offene Merkmale
  - leicht verdeckte Merkmale
  - verdeckte Merkmale
  - diskrete bzw. schwer verdeckte Merkmale

Fehlerraten

- keine theoretische Abschätzung der Sicherheit (→ Empirie)
- Festlegung von Toleranzbereichen notwendig

Jedes biometrische System hat immer eine unvermeidbare Restfehlerquote

- Schwellwert entscheidet über Komfort und Sicherheit
  - abhängig von dem Anwendungszweck!
- zusätzlich zu FAR und FRR:
  - *equal error rate* (***ERR***): Fehlerrate, bei der FAR=FRR
  - *failure-to-enroll rate* (***FTE***):
    - Merkmal fehlt
    - Einschränkungen in der Erfassung
    - fehlendes oder unzureichendes technisches Verständnis
    - Systemprobleme (z. B. Sensorqualität)
    - fehlende Akzeptanz

Zur Einführung

- Praktische Einschränkungen
  - Fehlerraten zu groß
  - Überwindungssicherheit mangelhaft
- Sicherheitsaspekte biometrischer Verfahren
  - Verfahren ***nicht deterministisch***
  - Statistische Untersuchungen notwendig
- Anwendung <=> Risiko
  - Mehr Sicherheit oder mehr Überwachung?

Physiologische Ansätze - heute

Fingerabdruck

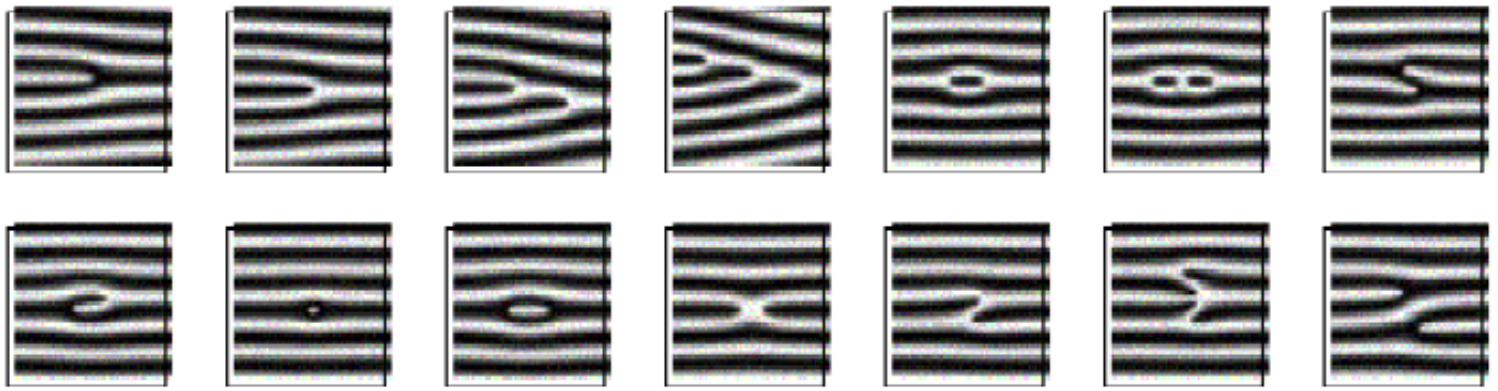
Handgeometrie

Iris

Gesicht

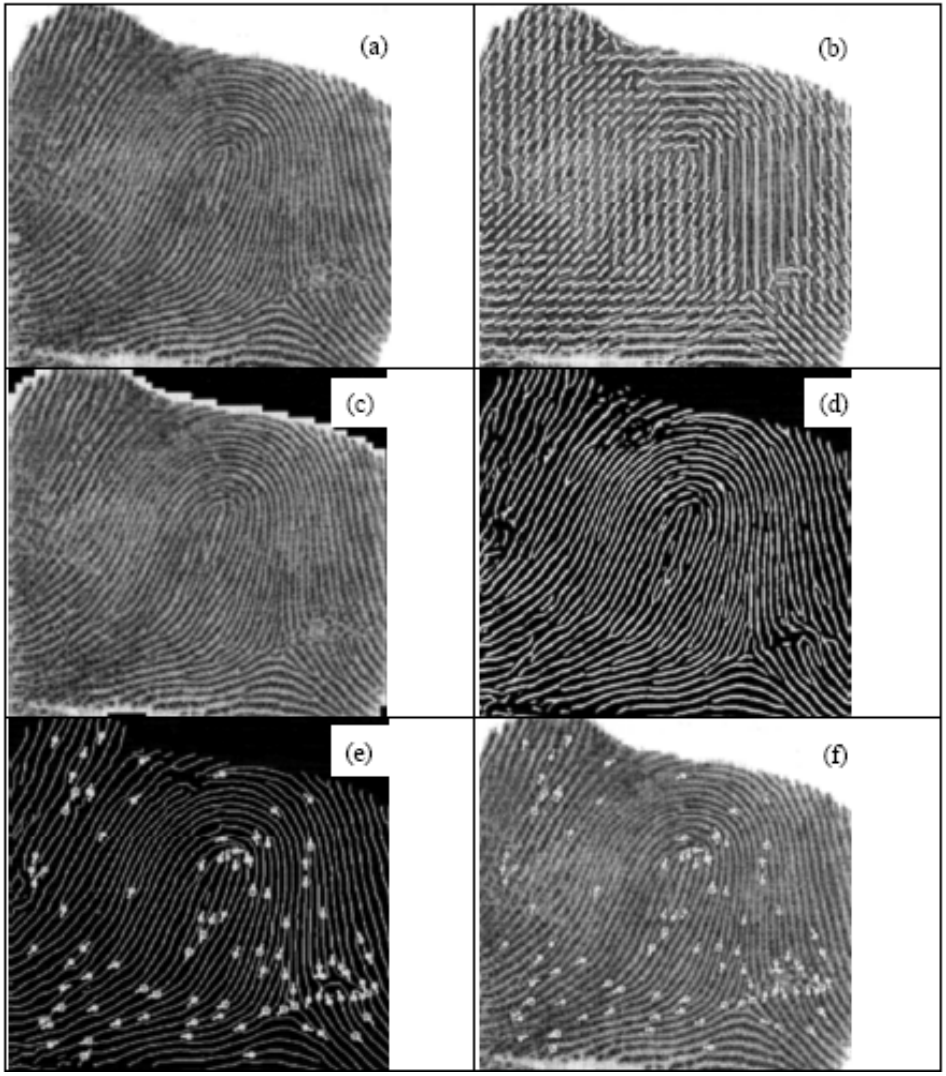
Fingerabdruck

- viel Erfahrung durch Daktyloskopie
- Muster der Papillarleisten individuell und stabil
- Probleme mit vielen Senioren - und Asiaten



http://www.bsi.bund.de/fachthem/biometrie/dokumente/Fingerabdruckerkennung.pdf

Fingerabdruck (2)



http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf

Verfahren

(a) Graustufenbild

(b) Berechnung Richtungsfeld

(c) Extraktion Vordergrundanteil

(d) Herausfilterung Hintergrund

(e) Berechnung des Skelettes mit den markierten Minuzien

(f) Überlagerung Minuzien mit Original-Graustufenbild

Fingerabdruck (3)

Überwindung einfacher Sensoren:

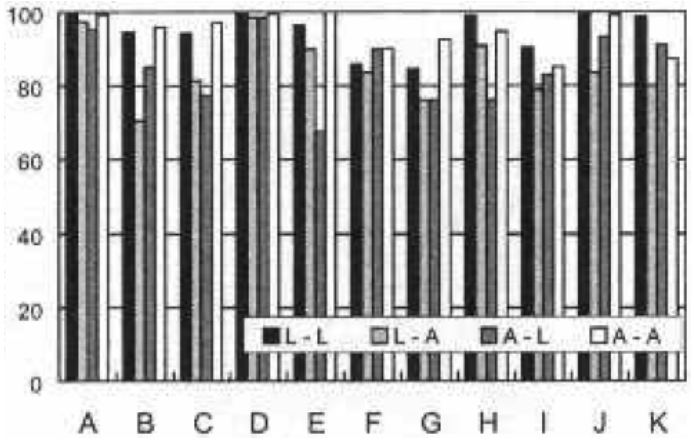
Mit Klebestreifen oder Wasser in einer Tüte

http://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/09Ueberwindung/ueberwindung.pdf

Fingerabdruck (4)

Matsumoto, 2002:

- Verfahren mit Abnahme des Fingerabdrucks
- in 68% - 100% der Fälle erfolgreich
- Verfahren mit latentem Fingerabdruck
- durchschnittlich in 67% der Fälle erfolgreich
- Täuschung aller 11 Testsysteme
  (teilweise Lebenderkennung, optische + kapazitative S.)



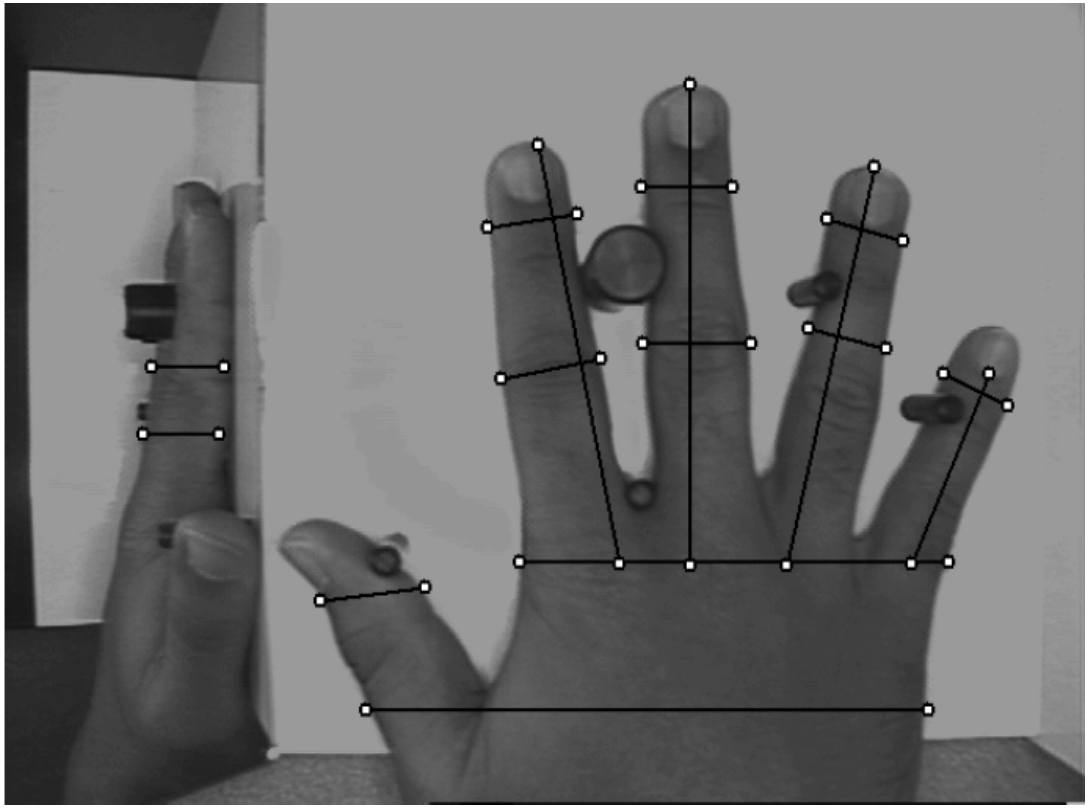
http://cryptome.org/gummy.htm

Handabdruck

- Handgeometrie einzigartig und ab Alter > 20 stabil
- 25 – 90 Meßpunkte für:
- Längen und Breiten der einzelnen Finger
- Dicke der Hand
- markante Punkte
- Fingerkrümmung ggü. Mittelpunkt
- Genauigkeit verschieden bewertet
- Lebendüberprüfung unverbreitet
- USA: In 50% der Kernkraftwerke und bei Einreisekontrolle

Handabdruck (2)

http://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/07Hand_Retina/Handerkennung-Ausarbeitung.pdf



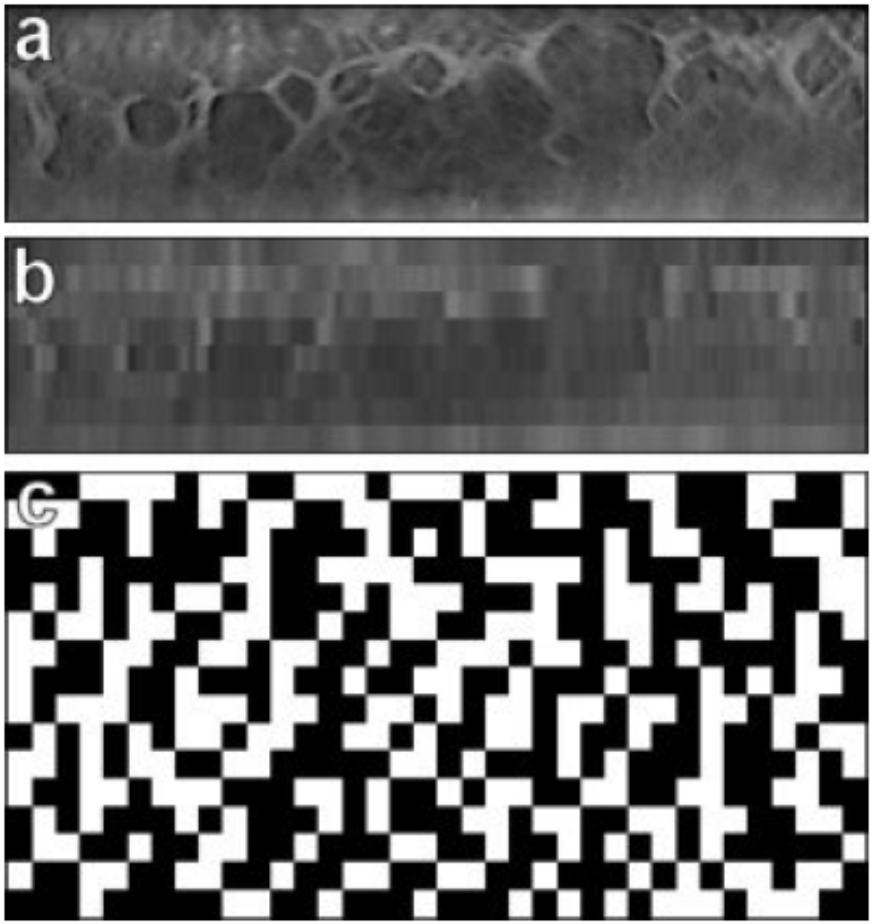
http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf

Iriserkennung

- hochindividuelles Merkmal
- langzeitstabil bei gesunden Augen

- Verwendung „normaler“ CCD-Kamera und Infrarotbeleuchtung
- hochkomplexe Struktur, Geräte bieten hohe Erkennungsleistung
- BSI-Studie: < 1% nicht in Enrollment erfaßbar
- erfordert erhebliche Nutzerkooperation und -eingewöhnung

Iriserkennung (2)



a) -> b)

- Partitionierung
- Mittelwertbildung Helligkeit je Partition

b) -> c)

- Vergleich Helligkeit Partitionen - Gesamtbild
- heller => 0
- dunkler => 1

www.bsi.de/fachthem/biometrie/dokumente/Iriserkennung.pdf

Iriserkennung (3)

Überwindung

- Farbausdruck von Irisfotographie oder Video
- Kontaktlinse mit Irisabbildung oder Irishologramm
- PC-Simulation echter Pupillenbewegungen
- Augenmodelle

Lebenderkennung

- Pupillenerweiterung durch Helligkeit
- Wölbung der Augen
- Reflexionseigenschaften
- Pupillenbewegungen

Gesichtserkennung

- Merkmal im Kindes- und im hohen Alter sehr instabil
- Untersuchung nichtmimischer Bereiche
- starke Abhängigkeit von Aufnahmesituation und Umgebungsbedingungen
- Gesichtserkennung oft Komponente in Hybridsystemen

Gesichtserkennung (2)

Ansätze

- Eigengesichtsanalyse
- Eigenschaftsanalyse
- weitere Varianten

Arbeitsschritte

- Aufnahme und Gesichtslokalisierung
- Normierung und Modifikation
- Merkmalsextraktion
- Abgleich / Matching

Gesichtserkennung (3)

- generell schlechte FAR und FRR
- Aufnahmekontext und Stilveränderungen problematisch

Überwindung

- Benutzung Fotografie oder Videosequenz

  => ohne Lebenderkennung oft ausreichend
- Angriff auf Datenübertragung und Einspielen einer Videosequenz
- Kunstkopf anfertigen

Verhaltensbasierte Ansätze - heute

Stimme

Unterschrift

Tastaturanschlag

Stimmerkennung

- Stimmapparat und Sprechgewohnheiten individuell
- ortsunabhängiges Merkmal
- Merkmal nicht stabil über Zeit oder bei Krankheiten
- Standardgeräte ausreichend
- Enrollment aufwendig

Überwindung

- Nutzerimitation
- Hochwertiges Abhören und Wiedereinspielen
- Erstellen eines akustischen Profils

Verfahren in der Entwicklung

Ohrform

DNA

Nagelbett

Gangerkennung

Ohr

- Individualität noch ungeklärt => ergänzendes Merkmal
- Erkennung durch 2D- und 3D-Abbildungen
- neues und relativ unerprobtes Verfahren
- Ohr zugänglich und leicht chirurgisch veränderbar
- Rechtsstatus noch unklar
- Anwendungsbeispiel „OISIN“

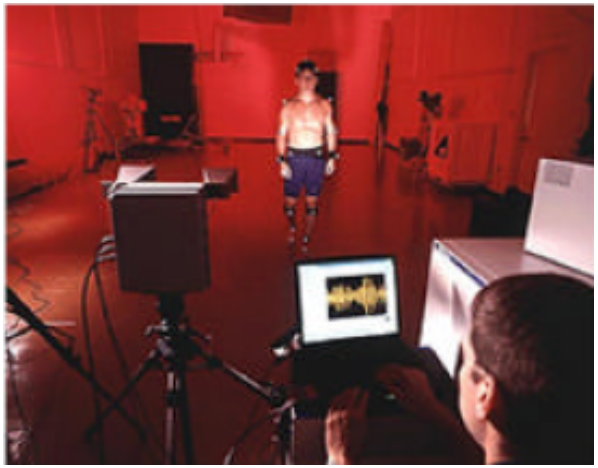
DNA

- eindeutiges Merkmal, stets und eindeutig meßbar
- geringe Fehlerrate
- noch sehr zeitaufwendig und kostenintensiv
- schwer abschätzbare Mißbrauchsszenarien

=> Eignung als Alltagsverfahren zweifelhaft

Gangerkennung

- Ziel: Identifizierung von Menschen in einer Masse
- noch in der Erforschung
- sehr verschiedene Herangehensweisen
- Eindeutigkeit des Gangs bisher ungeklärt
- vor allem polizeilicher Einsatz in Zukunft denkbar



http://www.impulse.de/downloads/biometrie_studie.pdf

Weitere Verfahren

BCI-EEG-Ansatz

Geruch

– UK: Mastiff Electronic Systems: „Scentinel“

Gesichtswärmeverteilung

Herzschlag

Körpersalzgehalt

Nagelbett

Zähne

– Bisher keine schnelle und hygienische Aufnahme

=> Methode bisher nicht umgesetzt

Abschlußbemerkungen Angreifbarkeit

Passive / physiologische Merkmale

– meist offen erkennbar und zugänglich

– Erfassung kann trotz Widerstand erzwungen werden

Aktive / verhaltensbasierte Merkmale

– immer wieder vom Nutzer veränderbar

– weniger genau und zuverlässig

– bisher störungsanfällig und leicht zu überwinden

– Erzwingen von Merkmalsausübung ebenfalls möglich

Hybridsysteme

– vereinen Vorteile und reduzieren Fehleranfälligkeit

– könnten Mängel einzelner Merkmale tolerieren

Bewertung biometrischer Verfahren - 1

Merkmal	*Univer-salität*	*Einzig-artigkeit*	*Beständig-keit*	*Messbar-keit*	*Leistung*	*Akzep-tanz*	*Resis-tenz**
Fingerbild	mittel	**hoch**	**hoch**	mittel	**hoch**	mittel	**hoch**
Handgeometrie	mittel	mittel	mittel	**hoch**	mittel	mittel	mittel
Iris	**hoch**	**hoch**	**hoch**	mittel	**hoch**	*gering*	**hoch**
Retina	**hoch**	**hoch**	mittel	*gering*	**hoch**	*gering*	**hoch**
Gesicht	**hoch**	*gering*	mittel	**hoch**	*gering*	**hoch**	*gering*
+Thermogramm	**hoch**	**hoch**	*gering*	**hoch**	mittel	**hoch**	**hoch**
Unterschrift	gering	*gering*	*gering*	**hoch**	*gering*	**hoch**	*gering*
Stimme	mittel	*gering*	*gering*	mittel	*gering*	**hoch**	*gering*
Handvenen	mittel	mittel	mittel	mittel	mittel	mittel	**hoch**
Tastenanschlag	*gering*	*gering*	*gering*	mittel	*gering*	mittel	mittel

http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf

Bewertung biometrischer Verfahren - 2

Merkmal	*Kostenfaktor*	*Anwenderfreundlichkeit*	*Wartungsanforderungen*
Fingerbild	mittel	*gering*	mittel bis **hoch**
Handgeometrie	**hoch**	mittel	mittel
Iris	**hoch**	**hoch**	mittel
Retina	**hoch**	**hoch**	mittel
Gesicht	mittel	**hoch**	mittel
+Thermogramm	mittel	**hoch**	mittel
Unterschrift	mittel	*gering*	mittel
Stimme	*gering*	*gering*	*gering*
Handvenen	mittel	*gering*	mittel
Tastenanschlag	*gering*	*gering*	*gering*

http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf

Bewertung biometrischer Verfahren - 3

Merkmal	*Templategröße (Bytes)*	*Verifikations-/ Registrierungszeit (sec)*	*FAR (%)*	*FRR (%)*
Fingerbild (Minuzien)	900-1.200	0,5-20/10-30	0,01-0,0001	1,0-5,0
Handgeometrie	10-20	2-5/k.A.	0,1-5,0	0,2-5,0
Iris	bis 512	0,5-10/k.A.	0,01-1,0	0,1-2,0
Retina	40-96	ab 1,5/bis 30	0,0001	bis 12
Gesicht	bis 1.300	1-5/bis 30	0,5-2,0	1,0-3,0
Unter/Handschrift	400-1.500	5-15/30	1,6-20	2,8-25
Stimme	1.500-3.000	ab 1,5/k.A.	k.A.	k.A.

http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf

Datenschutzaspekte

- Biometrische Informationen sind immer personenbezogene Daten
  - unter dem Schutz des ***informationellen Selbstbestimmungsrechts***
- Bei breitem Einsatz im staatlichen Bereich muss ***Verhältnismäßigkeitsgrundsatz*** beachtet werden
- wichtigste rechtliche Grundlage:

Bundesdatenschutzgesetz (***BDSG***)

„Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.“

(§3 Abs. 9 BDSG)

Datenschutzaspekte 2

- ***Zweckbindung*** biometrischer Daten:

  „Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.“

  (§31 BDSG)

- Einwilligung ***freiwillig***, ***informiert*** und ***bestimmt*** (§4a BDSG)
- Allgemeine Grundsätze:

  Datenvermeidung und ***Datensparsamkeit***

- Im BDSG auch Vorschriften, die für biometrische Verfahren sprechen
  - höheres Sicherheitsniveau
- Wann ist der Einsatz biometrischer Verfahren ***optimal***?

Besonderheit biometrischer Daten

- Zusatzgehalt, überschüssige Informationen
  - Langzeitproblematik
- Nicht in jedem Fall „offenkundige Daten“
  natürliche Person ↔ biometrische Daten
- Gefahr der elektronischen Form
- lebenslange Bindung
  - keine Rückrufmöglichkeit
- automatische Überwachung
  - Grundsatz der offenen Datenerhebung
  - aktive Mitwirkung der Betroffenen

Speicherung

zentrale Speicherung ◄——► **dezentrale Speicherung**

Vorteile:

- keine Kartenpersonalisierung
- einfache Handhabung
- Besserer Schutz der einzelnen Daten

Nachteile:

- Gefahr für informationelle Selbstbestimmung
- *single point of failure*
- Profilbildung

Vorteile:

- Kontrolle über die Daten

Nachteile:

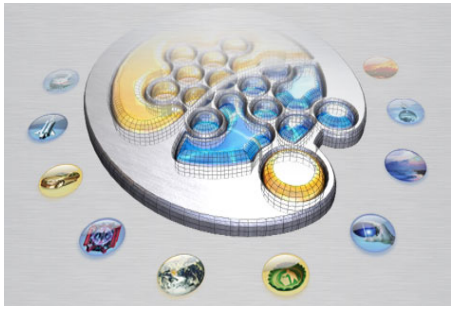
- Kosten
- Verlust / Diebstahl

Weitere juristische Fragen

- Biometrische Daten als Willenserklärung
- Gerichtliche Würdigung biometrischer Verfahren
- Risiken der Betreiber
- Vermeidung von Diskriminierung

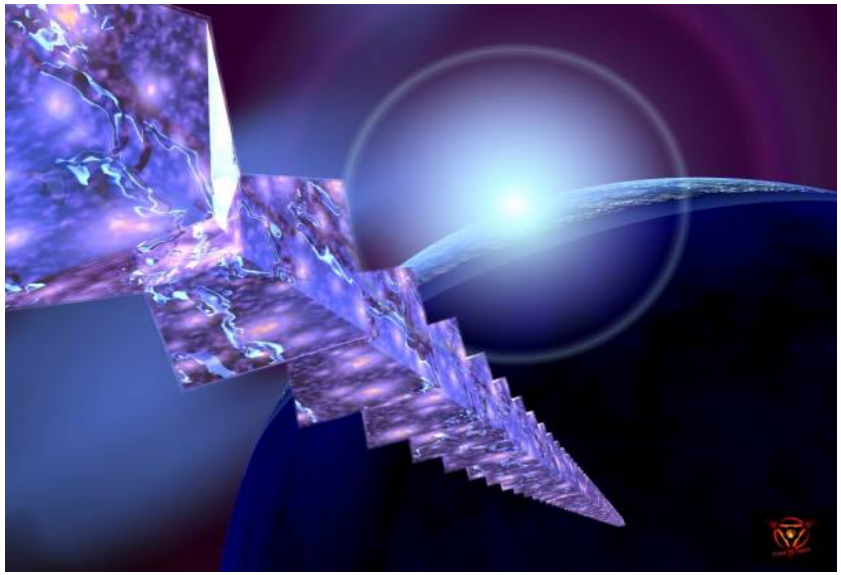
Fazit und Ausblick 1

- Möglichkeit für Verbesserung der Datensicherheit
  - Sicherheit muss ***zweiseitig*** betrachtet werden
- Gefährdung für grundrechtliche Positionen
  - Persönlichkeitsrecht
  - Menschenwürdegarantie
- Langzeitrisiko durch Standardisierungsbemühungen
  - Abhilfe durch ***templatefreie Verfahren***
  - ***on-card-matching***
  - Sensoren direkt auf der Karte
- Ausweitung der Datenschutzkontrollinstanzen auf dem nicht-öffentlichen Bereich
- Umgang mit Zurückweisungen bei großflächigem Einsatz



Fazit und Ausblick 2

- Zertifizierung von Produkten notwendig
- Doch weitere Verletzung des Allgemeinen Persönlichkeitsrechts?
- Hat man später in der Praxis wirklich die Wahl?
- Sozialverträglichkeit ↔ Diskriminierung
- Verhältnismäßigkeit immer im Auge behalten



Quellen

1. www.bfdi.bund.de - Bundesbeauftragter für Datenschutz und Informationsfreiheit
2. www.teletrust.de - TeleTrusT Deutschland e.V. (Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik)
3. www.datenschutz.de - Virtuelles Datenschutzbüro (Landesbeauftragter für Datenschutz des Landes Schleswig-Holstein)
4. www.datenschutzzentrum.de - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
5. www.tab.fzk.de - Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)
6. www.kommune21.de - E-Government, Internet und Informationstechnik
7. www.tab.fzk.de - Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)

Quellen 2

8. www.wikipedia.de
9. **www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf**
10. blogs.23.nu/static/moe/files/Angriffe_auf_Authentifizierungssysteme.pdf
11. www.cosy.sbg.ac.at/~uhl/biometrie_slides.pdf
12. **www.impulse.de/downloads/biometrie_studie.pdf**
13. **cryptome.org/gummy.htm**
14. www.bsi.bund.de/fachthem/biometrie/dokumente/Fingerabdruckerkennung.pdf
15. http://www.bsi.de/fachthem/biometrie/dokumente/Iriserkennung.pdf
16. agn-www.informatik.uni-hamburg.de/papers/doc/diparb_christian_paulsen.pdf
17. www.semper.org/sirene/people/gerrit/papers/bioausweise.pdf
18. www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie
19. www.crypto.ruhr-uni-bochum.de/imperia/md/content/seminare/itsws04_05/seminar_sayin_biometrie.pdf
20. www2.informatik.hu-berlin.de/~reichard/publ/Die_Unterschrift_in_der_Biometrie.pdf
21. berlin.ccc.de/~starbug/congress04.pdf
22. chaosradio.ccc.de/media/ds/ds085.pdf