Biometrie

"I am my passport"

Jörn Clausen
joern@TechFak.Uni-Bielefeld.DE

Übersicht

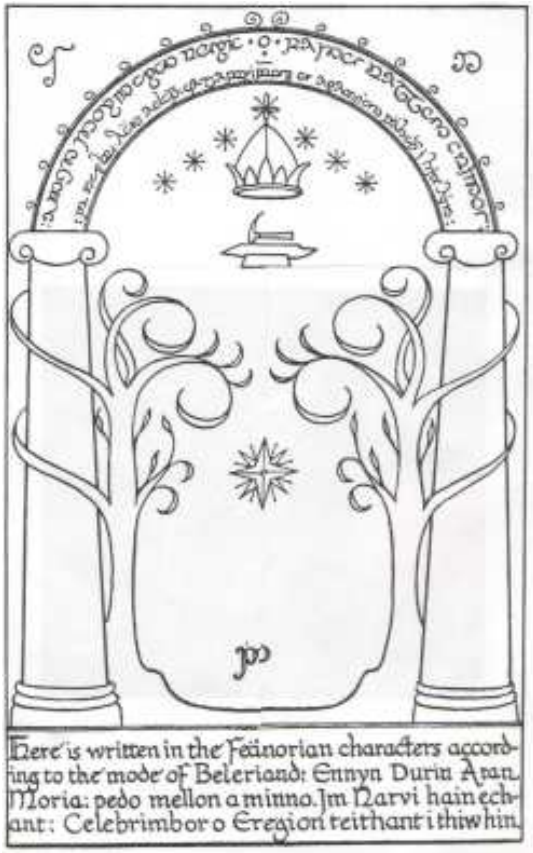
- Was ist Biometrie?
- Biometrische Verfahren
- Beispiele
- Entwicklungen

Begriffsklärung

- Begriff „biometrics“ mehrdeutig
- Biometrie: Bio-Mathematik, medizinische Statistik
- Biometrik: (automatisches) Messen eines biologischen Merkmals
- biometrische Identifikation

Authentisierung

- Authentisierung durch . . .
  - etwas, das ich weiß
    Paßwort, PIN, . . .
  - etwas, das ich habe
    Mensakarte, token, . . .
  - Kombination von beidem
    EC-Karte, . . .



Authentisierung, cont.

- Problem:
  - keine unmittelbare Überprüfung der Person
  - Wissen/Gegenstand kann weitergegeben werden

    . . . freiwillig, oder auch nicht
  - Mensakarte vergessen, account sharing
  - phishing, „ATM-frontends“, . . .
- Idee:

  Stelle Identität durch biometrische Merkmale fest.

Authentisierung durch Biometrie

- etwas, das nur ich kann
- etwas, das nur ich besitzen kann
- Fragen:
  - Geeignete Merkmale?
  - Zuverlässigkeit, Robustheit
  - Verarbeitung/Verwendung der Daten
  - Wirklich „nur ich“???

Merkmale

- Anforderungen (Roger Clark, 1994):

universality	exclusivity
uniqueness	precision
permanence	simplicity
indispensability	cost
collectibility	convenience
storability	acceptability

- kaum alle gleichzeitig erfüllbar

Anwendung

enrollment

- Erfassung des biometrischen Merkmals
- typisch: Generierung eines *templates*
- Speicherung von Merkmal oder template

verification

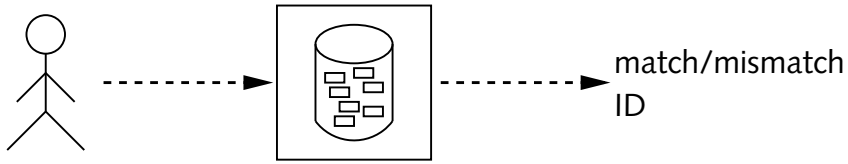
- Eingabe: ID + Merkmal
- Ausgabe: match/mismatch

identification

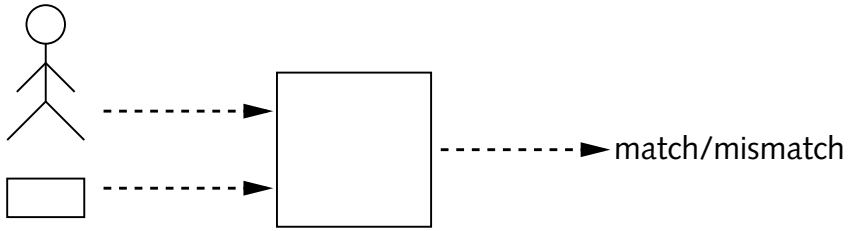
- Eingabe: Merkmal
- Ausgabe: ID

template-Verwaltung

- zentrale Sammlung von templates



- template beim Eigentümer



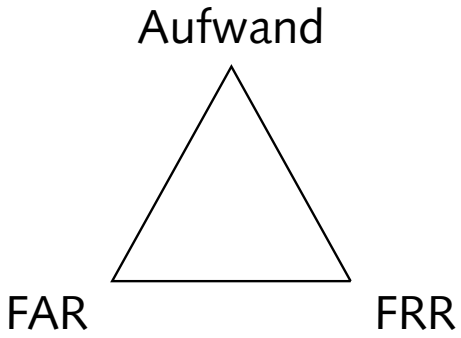
- dezentrale template-Verwaltung nur zur Verifikation geeignet
- Speicherung durch Barcode, Chip, . . . in Ausweis, token, . . .

Fehler

- Fehler bei der Erfassung (FTA, *failure to acquire*)
- Fehler beim enrollment (FTE, *failure to enroll*)
- kein standardisiertes Qualitätsmaß
- gebräuchliche Angaben:

  FAR *false acceptance rate*

  FRR *false rejection rate*

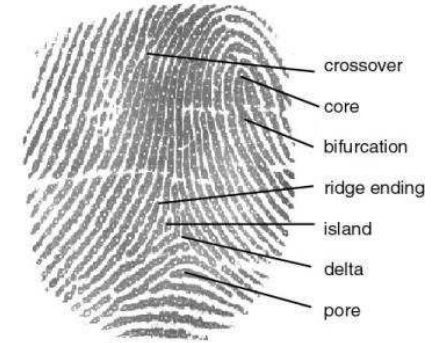


Biometrische Merkmale

- verbreitete Verwendung:
  - Fingerabdrücke, Handgeometrie, Gesicht
  - Iris, Retina, Venenmuster
  - Unterschrift, Schrift
  - Stimme
- (mögliche?) Merkmale:
  - DNA (genetischer Fingerabdruck)
  - Tippgeschwindigkeit/-verhalten
  - Geruch
  - ...

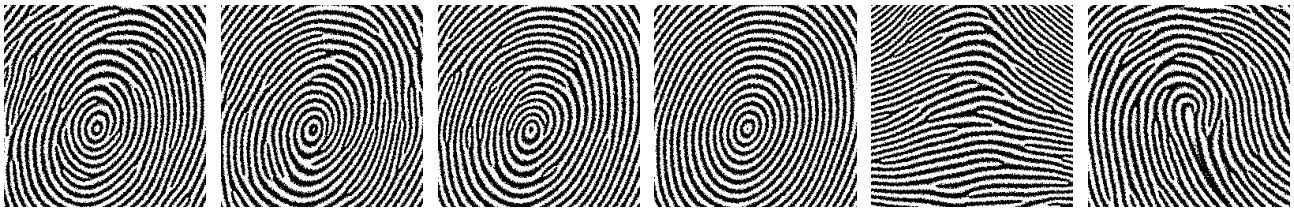
Fingerabdrücke

- seit Ende des 19. Jahrhunderts kriminalistisches Werkzeug
- Merkmale: Minutien
- verschiedene Meßverfahren:
  - optisch
  - kapazitativ
  - thermisch
  - akustisch



Probleme?

- Akzeptanz: erkennungsdienstliche Behandlung
- nie wissenschaftlich belegt
- Lesegeräte durch einfache Verfahren zu überlisten
- Tsutomu Matsumoto
  Impact of Artificial "Gummy" Fingers on Fingerprint Systems
- 80% Erfolgsrate, optische und kapazitative Systeme
- Beweismittel eßbar



Gesichtserkennung

- „natürlichstes“ Verfahren
- bereits im Einsatz (Paßbild)
- Originalbild oder Gesichtsgeometrie
- Besonderheit:
  - auf größere Entfernung anwendbar
  - ohne Einverständnis/Wissen anwendbar

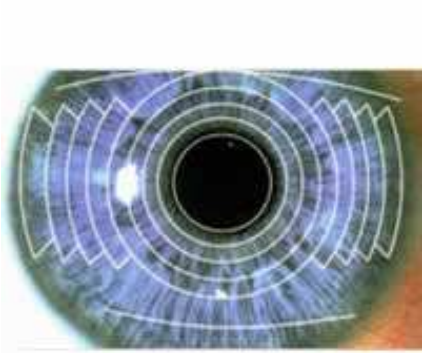
Probleme?

- Veränderungen (Alterung, Brille, Bart, Piercings, . . .)?

- schlechte Resultate
- kleiner Personenkreis, Verifikation oder sekundäres Merkmal

Iris

- (vermutlich) sehr individuelles Merkmal
- zeitlich konstant
- schwer ohne Kooperation des Besitzers zu erfassen



- Verfahren durch Iridian Technologies patentiert

Probleme

- Benutzervorbehalte (Verwechslung mit Retina-Scan?)
- schwierigere Bedienung
- Iris ungeeignet, nicht vorhanden, schlecht sichtbar

Beispiele 1

- Zoo Hannover: Smile & Go
- Identifikation durch Gesichtserkennung

- gute Akzeptanz bei den Besuchern
- Fehlschlag: Fingerabdruckerkennung

Beispiel 2

- Flughafen Frankfurt: Automated Border Controls (ABG)
- maschinenlesbarer Paß + Iris-Scan
- Speicherung der templates in lokaler Datenbank

Beispiel 3

- Flughafen Shiphol, Amsterdam: Automatic Border Passage (AGP)
- Iris-Scan + Smartcard („Privium Card“) mit template
- Abgleich mit aktueller Fahndungsliste
- Testphase ab Oktober 2001, seit Oktober 2002 in Betrieb
- kombiniert mit anderen Dienstleistungen, 119 €/Jahr
- Vorläufer (Fingerabdruck) aus kommerziellen Gründen eingestellt

Beispiel 4

- UNHCR Afghanistan
- Rückkehrer aus Pakistan
- Iris-Scan
- keine Verknüpfung von Name/Identität mit Bild/template

- 200000 Personen, 1000 entdeckte Betrugsversuche (10/2003)

zukünftige Entwicklungen

- International Civil Aviation Organization (ICAO):

  "The use of biometrics as an identity authentication [...] function will result in [...] the ability to know with more certainty, exactly who is getting onto flights."

- primäres Merkmal: Gesicht
- Interoperabilität: keine templates sondern Bilddaten (JPEG)
- Daten signiert (PKI), aber nicht verschlüsselt
- kontaktlose Datenübertragung
- offener Brief (FoeBuD, Big Brother Awards, EFF, ...)

  http://www.foebud.de/texte/aktion/icao/

zukünftige Entwicklungen, cont.

- Terrorismusbekämpfungsgesetz
- Ziel: Echtheit von Ausweisdokumenten gewährleisten
- Bundesbürger: keine bundesweite Speicherung
- Ausländer: Verwendung nicht geregelt
- zulässige Merkmale: Finger, Hände, Gesicht
- Daten können verschlüsselt werden
- Kosten: zwischen 22/4,5 M€ und 669/610 M€ (einmalig/p.a.)
- keine Erfahrung mit landesweitem Einsatz

Sinn und Unsinn

- Beispiel Stadionkontrolle (Bruce Schneier, *Beyond Fear*):
  - FAR = FRR = 0,1% (derzeit unrealistisch)
  - 1 in 10 Millionen Zuschauer: Terrorist
  - 75 Fehlalarme pro Spiel
  - 1 unerkannter Terrorist in 133 Spielen
- technische Angriffe (replay-Attacken, Lebenderkennung,...)
- Fälschungen, nicht-autorisierte template-Erzeugung
- *key revocation*
- inflationärer Einsatz, „digitale Spur“, Selbstbestimmung

Quellen

Die gezeigten Abbildungen stammen aus frei zugänglichen Quellen im WWW. Die Mehrzahl von ihnen dürfte einem Copyright unterliegen. Sollte ein Copyright-Inhaber Einwände gegen die Veröffentlichung innerhalb dieser Präsentation haben, möge er sich bitte an den Autor wenden.

The images shown in this presentation were downloaded from publicaly available sources in the WWW. Most of them are probably copyrighted. If a copyright owner objects to the use and publication of his/her images in the context of this presentation, please contact the author.