

21C3 – Biometrie in Politik und Technik

Biometrie in Technik und Politik

starbug@berlin.ccc.de

Fragen

bei Fragen:

- bemerkbar machen
- auf die Mikrofonengel warten
- Frage stellen

Inhalt

Arten der Authentifikation

Was ist Biometrie?

Funktionsweise biometrischer Systeme

Überwindungsmöglichkeiten

Politische Rahmenbedingungen zum Einsatz

Ergebnisse der Studien BioFinger und BioP

Forderungen zur Einführung biometrischer Merkmale

Demonstration der Überwindbarkeit versch. Systeme
politisch-technische Diskussion

Arten der Authentifikation

	Weitergabe	Verlust	Wechsel
Haben (Token, SmartCards)	ja	verlieren	austauschen
Wissen (Passwort, PIN)	ja	vergessen	wechseln
Sein (Biometrie)	nein ?	Krankheit/ Unfall	bedingt wechselbar

Was ist Biometrie?

aus dem Griechischen

Bios = Leben

Métron = Maß

Biometrie ist eine Technik zur Authentifikation und Identifikation von Personen anhand von spezifischen Körpermerkmalen.

Probleme mit biometrischen Systemen

- Merkmale sind nicht konstant
- Aufnahmebedingungen sind nie identisch

-> Nur eine Wahrscheinlichkeit der Übereinstimmung

Merkmale sind manchmal nicht verfügbar oder erfassbar
(körperliche oder kulturelle Einschränkungen)

-> Ausweichmerkmale oder separate Prüfung

Anforderungen an das Merkmal

Universalität

bei jeder Person vorhanden

Konstanz

geringe Veränderung über langen Zeitraum

Einzigartigkeit

grosser Unterschied gegenüber anderen Personen

Erfassbarkeit

durch technische Systeme messbar

Fälschungssicherheit

schwer zu kopieren

Aufbau von biometrischen Systemen

jedes biometrische System besteht aus:

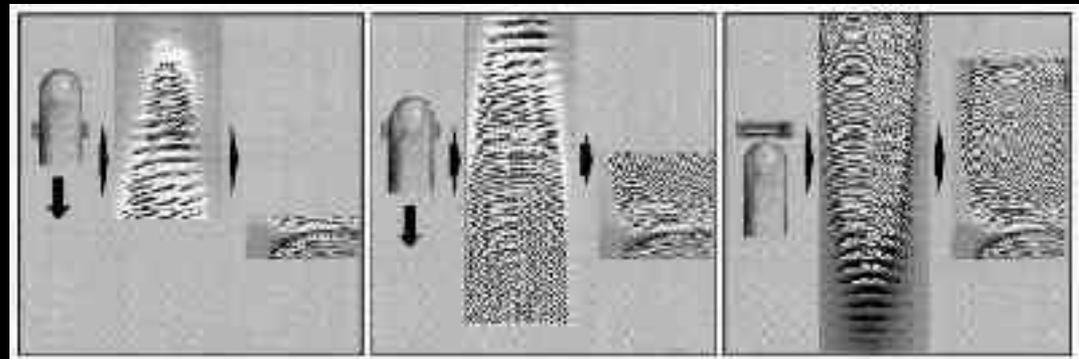
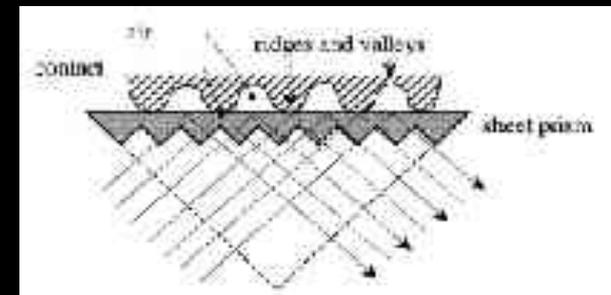
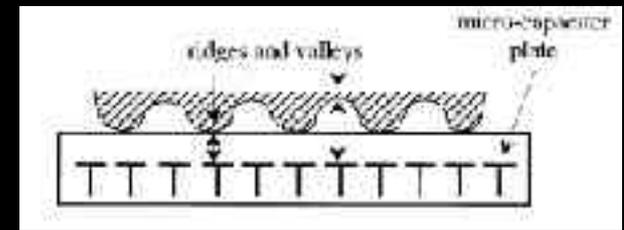
- Sensor
- Vorverarbeitung (Filter)
- Merkmalsextraktor
- Datenbank
- Vergleicher



Fingerabdruckerkennungssysteme

Fingerabdruck :: Sensorarten

- Kapazitiv
 - Ultraschall
 - Optisch (Berührungslos, gestörte Totalreflexion)
 - Druck
 - Elektrisch
 - Thermisch
-
- touching
 - sweeping



Fingerabdruck :: Merkmale

global

loop (delta und 1 core)

wirbel (delta und 2 cores)



local

Minutien



very-fine

Schweissporen



Fingerabdruck :: Verfahren

- Pattern matching über das gesamte Bild
- Minutienbasiert
Position und Ausrichtung von
endings und bifurcations
evtl. Weiterverfolgen der Papillarsegment
- Position der Schweißporen



Fingerabdruck :: Lebenderkennung

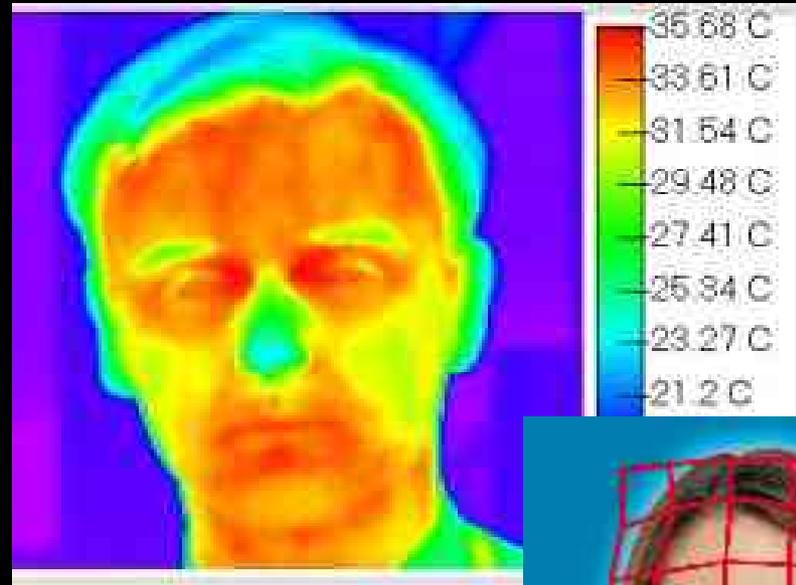
- Puls
- Eigenschaften der Haut (spezifischer Widerstand)
- Farbe/Absorptionseigenschaften der Haut und des Blutes
- Reflexionseigenschaften im Ultraschallbereich
- Schweißaustritt

Gesichtserkennungssysteme

Gesichtserkennung :: Sensorarten

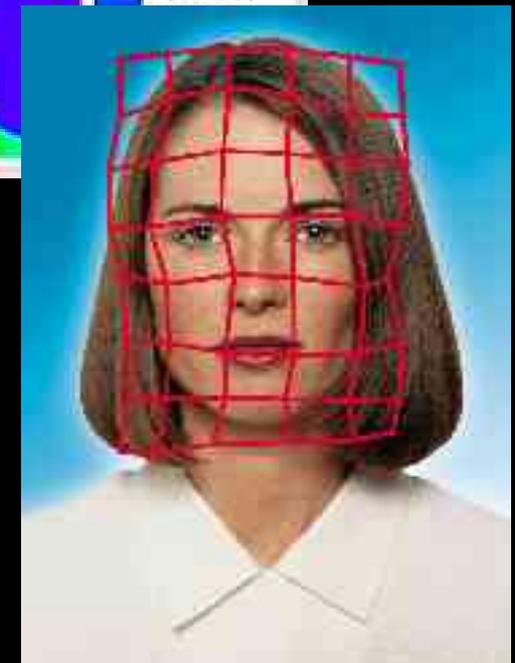
Aufnahmevarianten:

- 2 Dimensional
- 3 Dimensional



Sensortypen:

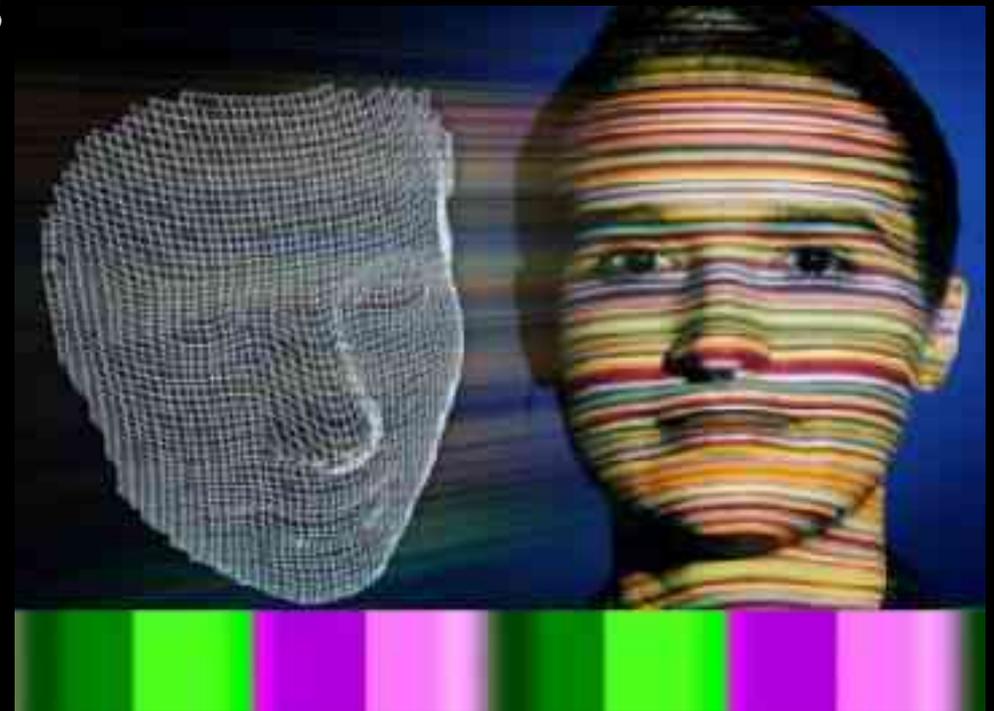
- Infrarot
- optisch sichtbarer Bereich



Gesichtserkennung :: 3D Aufnahme

- Projektion farbiger Linien
- Krümmung an Strukturen des Gesichts
- Ermitteln des 3D Bildes

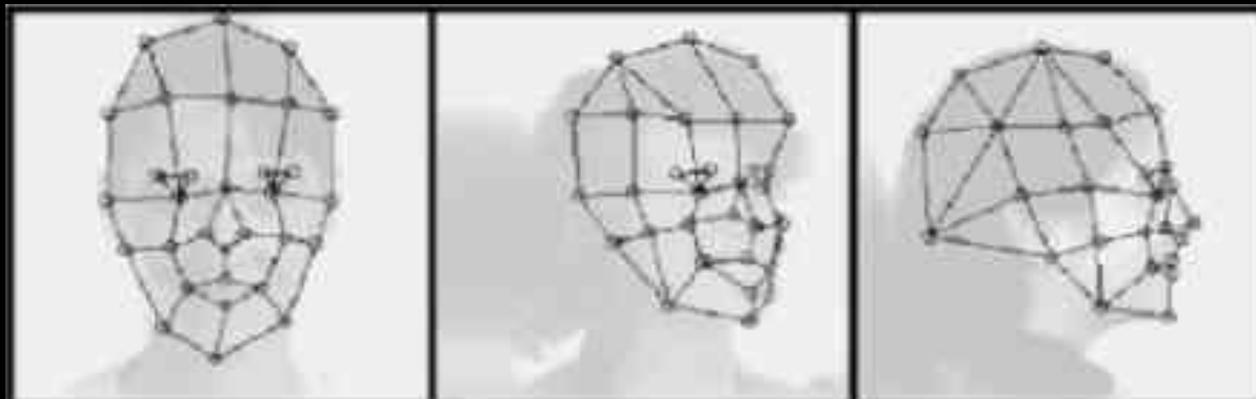
laut Siemens Auflösung
0,2 x 0,2 x 0,2 mm



Gesichtserkennung :: Gesichtsmetrik

Vergleich der Position markanter Gesichtspunkte

- Elastic Graph Matching
 - flexibles Gitter
 - Ecken an markanten Gesichtspunkten
 - Gitter bleibt auch bei Kopfbewegung bestehen

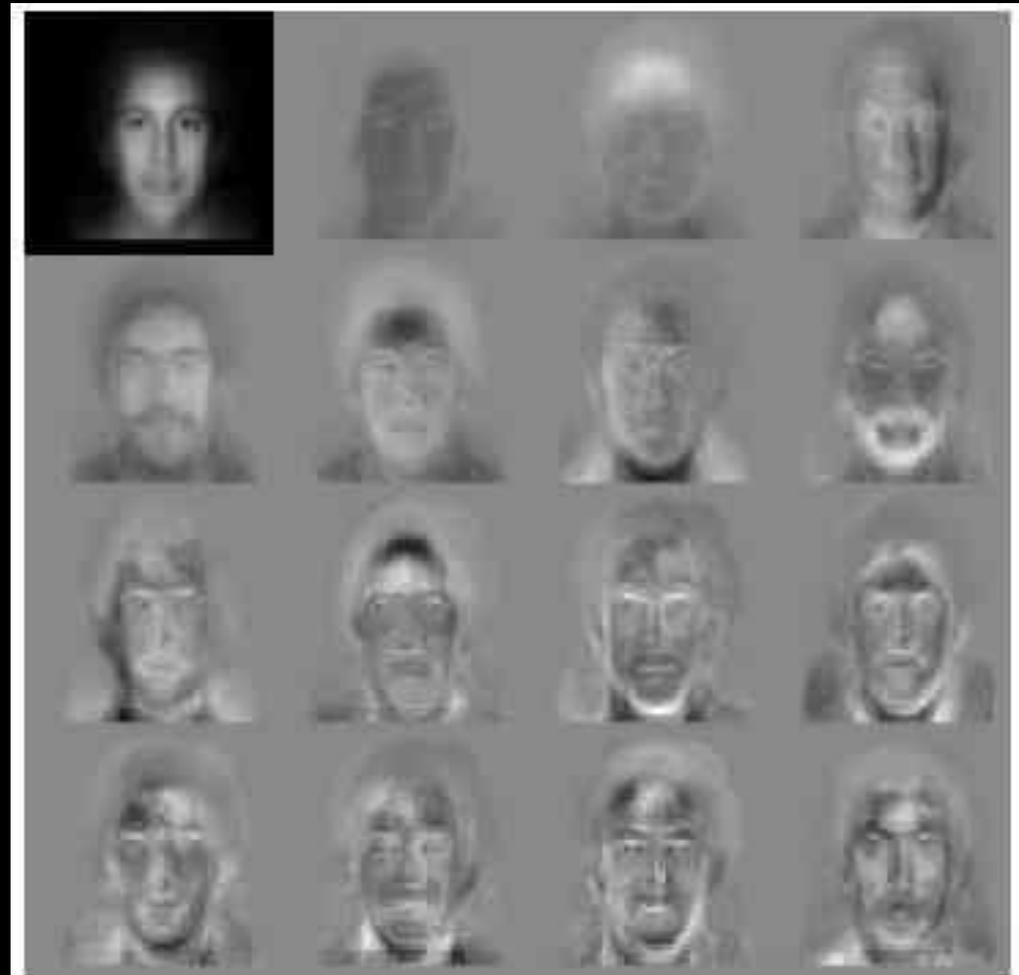


Gesichtserkennung :: Eigenface

Eigenface
(Durchschnittsgesicht)

Kombination aus ca. 100
Basisgesichtern

ähnlich dem Phantombild



Quelle: MIT Face Recognition Demo Page, nach Beltrani/Roth 2001, S. 21.

Gesichtserkennung :: Lebenderkennung

Bewegung des Gesichts bzw. des Kopfes

Bewegung im Gesicht (Blinzeln)

Reflexionseigenschaften der Haut

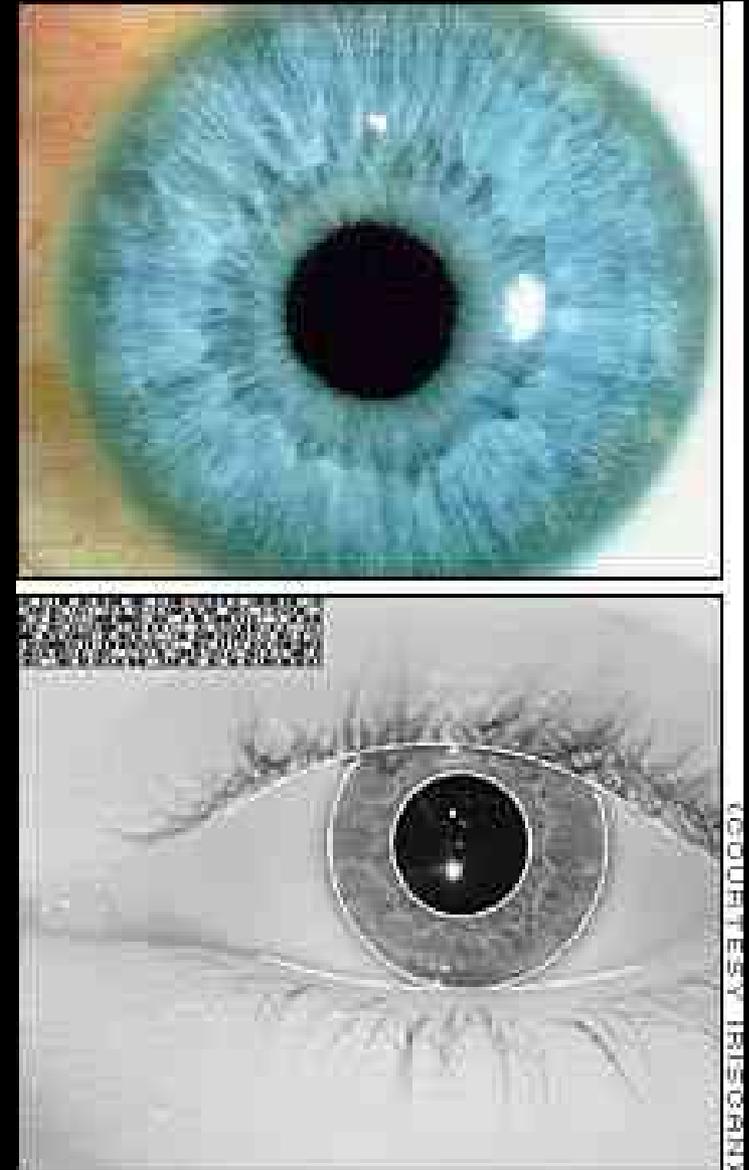
Iriserkennungssysteme

Iriserkennung :: Funktionsweise 1

Anstrahlen mit Infrarotlicht

Makroaufnahme des Auges im
nahen Infrarotbereich

Extraktion der Iris



Iriserkennung :: Funktionsweise 2

Aufteilen der Iris in 8 konzentrische Kreise

Erkennen markanter Muster und deren Position
(Corona, Krypten, Fasern, Flecke, Narben, radiale
Furchen, Streifen)

Erzeugen des Iriscodes

weitere Verfahren

Handschrift (statisch, dynamisch)

Handgeometrie

Tippdynamik

Gangdynamik

Sprechererkennung

Ohrform

Retinaerkennung (Aderhaut)

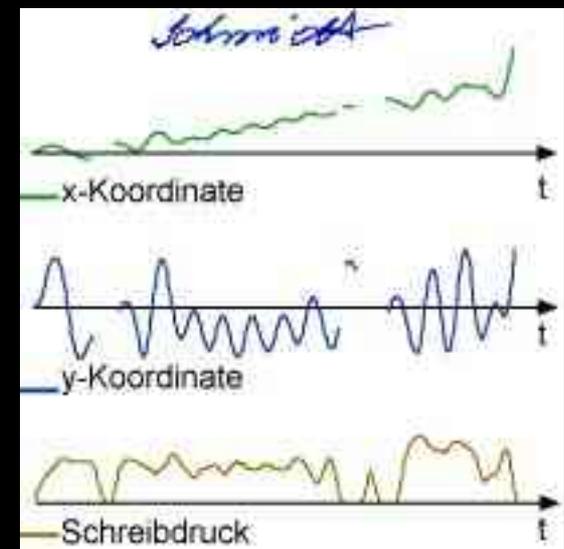
Bewegungserkennung (Gang)

Thermobild von Hand oder Gesicht

Venenmustererkennung

Geruchserkennung

DNA



Überwindung biometrischer Systeme

Überwindung :: Angriffe auf die Referenzdaten

- Manipulation beim Enrollment
(falsche Merkmale)
- Austauschen, Löschen oder Manipulieren der Templates

Gegenmaßnahmen:

- Überwachung des Enrollments
- Zugriff nur zum Sensor
- definierte Zugriffsrechte auf die Templatedateien

Überwindung :: Angriff auf die Kommunikation

- Wiedereinspielen gesniffter Datensätze (Replay Attacke)
- Einspielen von selbst generierten Datensätzen

Gegenmaßnahmen:

- Zugriff nur zum Sensor
- physikalische Absicherung der Kommunikationswege und Anschlüsse
- Abschirmung der Kabel
- definierte Zugriffsrechte auf die Treiber

Überwindung :: Fingerabdruck

Latenzbildreaktivierung auf dem Sensor
Anhauchen, Graphit- oder Farbpulver

Wiederauflegen der Latenzabdrücke
Graphitpulver mit Tesafilm

Anfertigen einer Fingerabdruckatrappe
aus Gelatine oder Holzleim



Überwindung :: Gesichtserkennung

Vorspielen eines Bildes oder einer Videosequenz

Anpassen des Gesichts (Schminken, Modellieren)

Vollmaske

Nachbildung des Kopfes



Überwindung :: Iriserkennung

Vorspielen eines Bildes oder einer Videosequenz

Kontaktlinse mit gedruckter oder handgemalter Iris

Kontaktlinse mit Irishologramm



<http://www.heise.de/ct/english/02/11/114/>

Politische Rahmenbedingungen

politische Rahmenbedingungen in Deutschland

9. Jan.2002 Terrorismusbekämpfungsgesetz
(Otto Katalog)

Änderung von 21 Gesetzen oder Rechtsvorschriften
(Pass- und Personalausweisgesetz sowie
Ausländer- und Asylverfahrensgesetz)

Aufnahme von Merkmalen:

- der Finger ODER der Hand ODER des Gesichts
(keine Kombination und keine Iris)
- auch in verschlüsselter Form (Informationsfreiheit
durch Auskunftspflicht der Behörden (Art.16,
Abs.6 PassG))

Gesetzesziele

Computergestützte Identifikation von Personen
(Effektivierung von Grenzkontrollen)

Ist der Besitzer des Dokuments auch der Inhaber?

Zweifelsfreie Feststellung der Echtheit von
Dokumenten

Erschweren der Fälschungen vom Pässen

Verbesserung behördlicher Infoaustausch zur
Verhinderung der Einreise von Terroristen

Ausländerausweise (Aufenthaltsgenehmigung)

- Aufnahme der Merkmale in eine Zentrale DB
- keine Zweckbindung !
- Verwendung der Daten für polizeiliche Spurensuche erlaubt
- Gleichheitsgrundsatz und informationelle Selbstbestimmung verletzt
- Weiteres klärt NUR eine Rechtsverordnung, (widerspricht Bundesverfassungsgerichtsurteil nach dem alle wesentlichen Entscheidungen vom Parlament selbst zu regeln sind)
- Problem mit der Gültigkeit biometrischer Merkmale in „unbefristeter“ Aufenthaltserlaubnis

Beschlüsse der EU

Verordnungen zur einheitlichen Visagegestaltung (23.2.2002)

- Integration von Lichtbild in Visa
- verpflichtende Aufnahme von zwei Fingerabdrücken
(gute Eignung für Datenbankabgleich)

Ziel: Personen aufspüren, die mit gefälschten amtlichen Dokumenten in die EU einreisen wollen

Eurodac (seit 15.1.2003)

- Erfassung der Fingerabdrücke von Asylbewerber und illegalen Zuwanderern und Speicherung in EURODAC

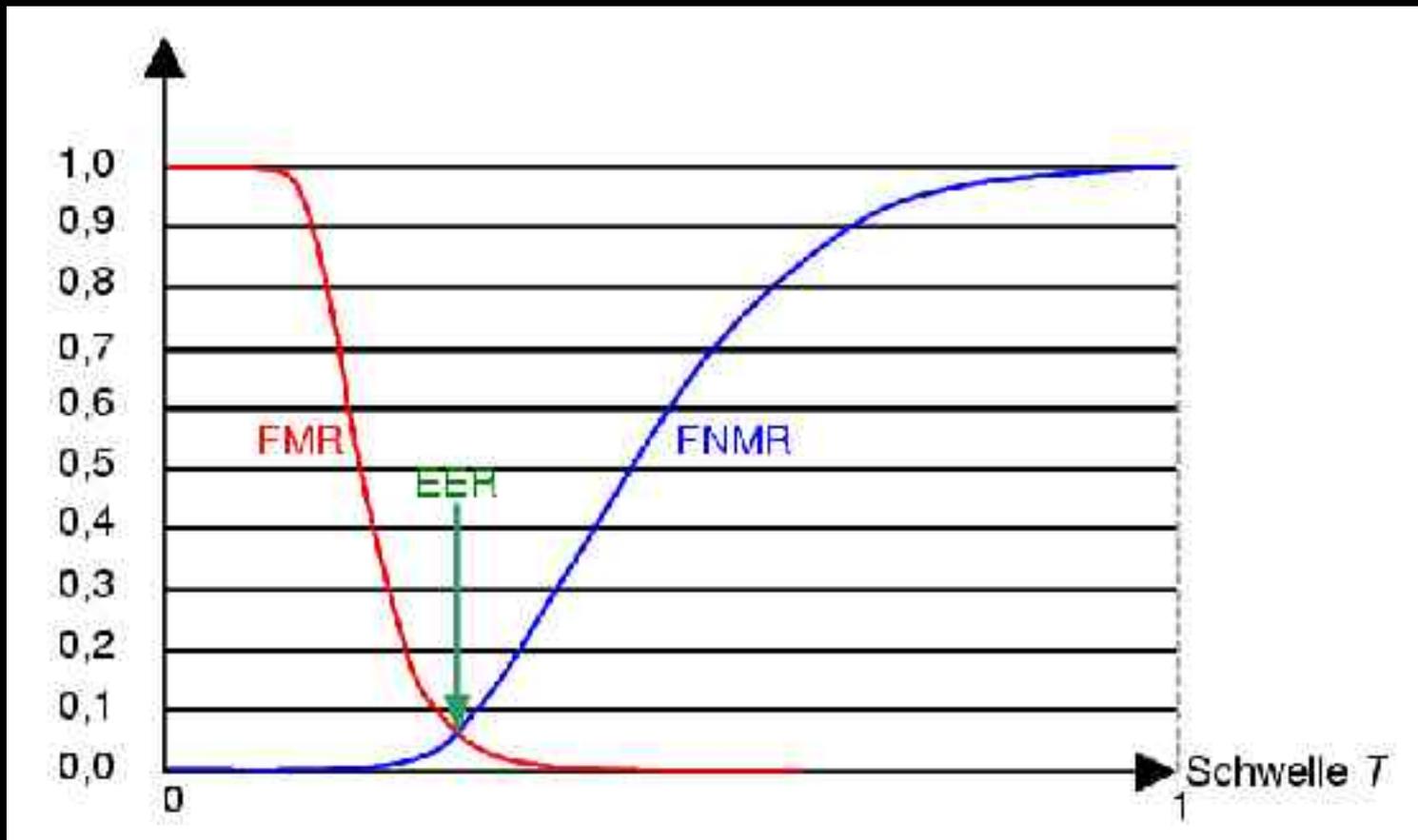
Ziel: Verhindern von Mehrfachanträgen eines Asylbewerbers und evtl. Rückführung ins Ausgangsland

Schritte der Einführung

- 01.01.04 Fingerabdrücke und Gesichtsbild bei Einreise in die USA für Personen mit Reisedokumenten ohne Biometrie
- 26.10.04 auch für Bürger aus VisaWaivers Staaten
- Beschluss des EU-Parlaments (Coelho-Bericht)
- Beschluss des Rates der Innen- und Justizminister bzw. der Regierungschefs
- nach 16 Monaten: Aufnahme von digitalen Gesichtsbildern
- nach 32 Monaten: zur Aufnahme von Fingerabdrücken
- Einführung in Ausweise?

Ergebnisse von Tests biometrischer Systeme

FAR (FMR) – FRR (FNMR) – EER



BioFinger I

Testergebnisse :: BioFinger :: 1

FTA (hardwarebedingter Fehler):
zwischen 0% und 1,2%

FTE (softwarebedingter Fehler):
4 Algorithmen mit 0%
sonst zwischen 0,05% und 23%

EER der Algorithmen (gemittelt aus allen Sensoren):
20% bis 39%

FRR (FAR = 0,1%)
50% der Systeme < 10%
23% der Systeme < 3%

Testergebnisse :: BioFinger :: 2

Einfluss des Templatealters auf die FRR:

10 Jahre – Faktor 1,4

30 Jahre – Faktor 2,5

Sensorfläche hat keinen Einfluss auf
Erkennungsleistung

Biometrische Zwillinge unterscheiden sich (aber nur im
niedrigen einstelligen Prozentbereich)

Testergebnisse :: BioP :: 1

Aktuelle Personalausweise sind nicht für die biometrische Gesichtserkennung geeignet

- schlechter Bildqualität (Kontrast)
- Gesicht im Halbprofil

Musterausweis nach ICAO

- Vergleich mit, vom Ausweis gescanntem Bild möglich
- Ergebnisse aber noch nicht zufriedenstellend

Testergebnisse :: BioP :: 2

Kompression:

75kB - vernachlässigbarer Einfluss

14kB (Vorschlag der ICAO) - noch akzeptabel

11kB - deutlicher Abfall der Erkennungsleistung

Bildauflösung:

Verringerung führt zu leicht schlechteren Ergebnissen

Lichteinfall:

Von der Seite – extreme Verschlechterung des Ergebnisses
aus dem Hintergrund – Einfluss vernachlässigbar

Testergebnisse :: BioP :: 3

Alter der Ausweise:

keine fundierten Erkenntnisse möglich, weil die
Erkennungsraten zu schlecht waren

Leistung nimmt mit zunehmenden Alter des Bildes ab

FRR nimmt nach einer Gewöhnungsphase von
einigen Tagen ab

Überwindung mit einfachsten Mitteln möglich:

- Foto (Farbe und s/w)
- Video

Testergebnisse :: BioP :: Nutzerbefragung

Mehrheit der BKA Beamten fordert,
Gesichtserkennung nicht isoliert einzusetzen

Generelle Nützlichkeit wird nur von 1/3 gesehen!

Beide getesteten Systeme erhielten beim Punkt
Benutzerakzeptanz, Überwindungssicherheit und
Lichteinfluss die Note 5 (5,16 bzw. 4,93)
(Schulnotensystem)

TAB Bericht

Fingerabdruck

- 2% ohne ausreichend ausgeprägte Merkmale
- mögliche Probleme mit der Langzeitstabilität

Iris

- mögliche Probleme bestimmter Ethnien,
- keine Belege über Einzigartigkeit in Grossanwendungen

Datensignierung/Verschlüsselung

- Pässe sind 10 Jahre gültig, die Signatur aber nur 5 (Signaturgesetz)

Forderungen an die Entscheidungsträger

Forderungen :: 1

- **Keine Aufnahme biometrischer Merkmale !**
leichte Zuordnung von Pass und Person durch unveränderlichen und eindeutigen Datensatz
- Öffentliche Debatte und die Aufklärung der Bevölkerung über die Risiken und Kosten
- Verfahren, die aktive Mitwirkung verlangen
- Keine Zentrale DB oder länderübergreifende Vernetzung lokaler Register
- Keine Speicherung überschüssiger (Roh-)Daten (Rückschlüsse auf Krankheiten, Ethnie, Drogenkonsum)
- Verwendung von Match on Card Verfahren
- Strenge Zweckbindung der erhobenen Daten

Forderungen :: 2

- Einsatz fälschungssicherer Systeme und Klärung der Haftungsfrage bei Missbrauch
- Test der Systeme durch unabhängige Organisationen
- Feldtests mit ausreichender Probandenzahl und Dauer **vor** der Einführung
- Öffentliche und wissenschaftliche Begleitung des Einsatzes

Forderungen :: 3

- Keine Speicherung der Daten in RFID Chips ?
- Verschlüsselung der im Pass gespeicherten biometrischen Daten ?
- Einsatz von starken und offenen Verschlüsselungsalgorithmen für den Kommunikationsweg
- keine Diskriminierung von Personen durch regelmässig Zurückweisungen
- Manipulationssichere und Haltbare Dokumente
- **Keine Einführung in Personalausweise !**

Offene Fragen

Warum sollen biometrische Merkmale wirklich aufgenommen werden?

Welche biometrischen Merkmale und welche Systeme (Verfahren, Hersteller) kommen zum Einsatz?

Welche Ausweissysteme (Smartcard, RFID) werden verwendet?

Wie hoch sind die Kosten und wer trägt sie?

Wo werden die Daten gespeichert und wer hat Zugriff auf sie?

ToDo

Klären der offenen Fragen

Beobachten und Beeinflussen der politischen Entwicklung!

Weigerung der Abgabe von Fingerabdrücken

Aufklärung der nationalen und europäischen
Entscheidungsträger und der Bevölkerung

Zeigen der Unsicherheit der Systemen und der Auslesbarkeit
der Fingerabdruckdaten

Rechzeitig einen nichtbiometrischen Pass beantragen !

Optionen zur Einführungen neuer Dokumente

Annahme für die Kostenkalkulation

6500 Meldestellen für Pass/PA Beantragung

laufende Kosten p.a. = 20% Anschaffungspreis

200 Kontrollpunkte an Grossflughäfen und 200 an
Landes- und Seegrenzen

Baumassnahmen:

20kE pro Kontrollpunkt

15kE innerhalb von Gebäuden

Einführung neuer Dokumente :: Option 1

Biometrische Nutzung der bestehenden Dokumente
(Livescan eines aufgedruckten Bildes)

Standardisierung der Passbildqualität
(aktuellen Bilder mit schlechtem Kontrast und
Gesichtern im Halbprofil (BioP 1))

Kosten:
einmalig 21Mio, laufend 4,5Mio

Einführung neuer Dokumente :: Option 2

Technische Aufwertung bestehender Dokumente

Speicher: Barcodes oder digitale Speicherelemente
zentrale (2a) oder dezentrale (2b) Erfassung und
Verarbeitung der biometrischen Merkmale

Kosten:

2a) einmalig 179Mio, laufend 55Mio

2b) einmalig 614Mio, laufend 332Mio

Einführung neuer Dokumente :: Option 3

Smardcard mit elektronischem Speicherelement

Flächeneinsatz der elektronischen Unterschrift
wirtschaftliche Innovation

Impulse für den elektronischen Rechts- und
Geschäftsverkehr

Kosten:

einmalig 669Mio, laufend 610Mio

Danke

Demonstration der Überwindbarkeit und
politisch technische Diskussion

im Anschluss
in Saal 3

Informationen und Kontakt

starbug@berlin.ccc.de

<https://www.ccc.de/biometrie>

biometrie@lists.ccc.de

biometrie-subscribe@lists.ccc.de