Biometrische Identifikations- Lösungen und Anwendungen

Dr. Bernd Reinhold
Senior Vice President & Chief Technology Strategist

27. März 2007

Biometrie ist aus Sicht der...

1. Anwendung

...ein automatisiertes Verfahren zur Feststellung oder Überprüfung der Identität einer lebenden Person, das sich auf ein charakteristisches und messbares physiologisches oder Verhaltens- Merkmal der Person stützt.

2. Wissenschaft

eine statistische Analyse biologisch determinierter Merkmale einer Person mit dem Ziel einer Diskriminierung nach Merkmalsähnlichkeiten.

3. Hersteller

eine technische Lösung

- ***zum Erfassen der biometrischen Charakteristika (Sensoren)***
- ***mit Modulen, die den Charakteristika zugeordnete Muster extrahieren, komprimieren, verarbeiten, sowie diese als Templates speichern, vergleichen und aus dem Vergleich ein Resultat ableiten***
- ***mit einem Interface zur Übergabe des Resultats an Anwendungs- Systeme.***

Biometrisch relevante Begriffe (Definitionen nach US NSTC 2006)

„Erkennung“

...wird in Verbindung mit einem biometrischen Merkmal generisch benutzt, um ein biometrisches System funktionell zu beschreiben: Gesichts- Erkennung, Iris- Erkennung, Sprach- Erkennung etc.

„Verifikation“

... ist für ein biometrisches System die Aufgabe, die Identität einer Person über einen Vergleich mit einem oder mehreren vorher gespeicherten Templates zu bestätigen. Diese Definition entspricht einer biometrischen Variante für Aufgaben, die traditionell PIN oder Passwort erfüllen.

„Identifikation“

...das biometrische System bekommt die Aufgabe, das biometrische Merkmal einer Person mit in einer Datenbank gespeicherten Templates abzugleichen um eine Referenz zu finden. Ist bekannt, dass die Person in der Datenbank zu finden ist, spricht man von einer geschlossenen (closed- set) DB; ansonsten von einer offenen (open- set) DB.

Die wichtigsten biometrischen Merkmale

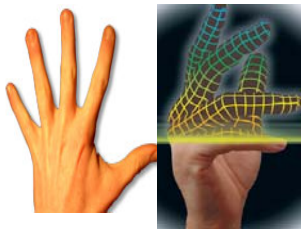
Biometrische Merkmale

Physiologische Charakteristika

Verhaltenscharakteristika

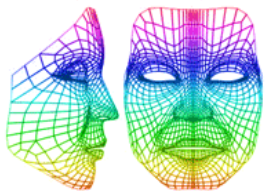
Finger/ Hand abdruck

Hand-Geometrie



Iris

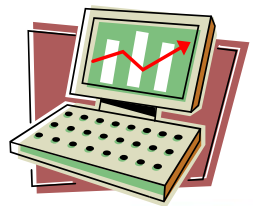
Gesicht



Stimme

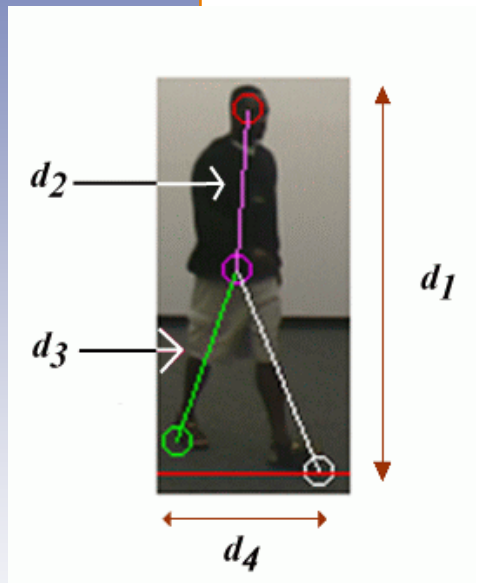
Signatur

Key Stroke

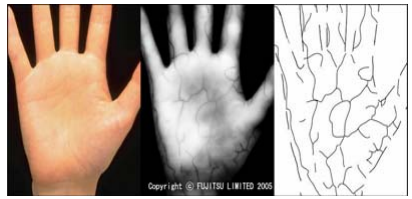


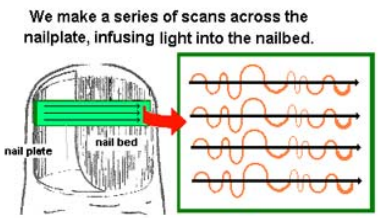
Weitere Merkmale

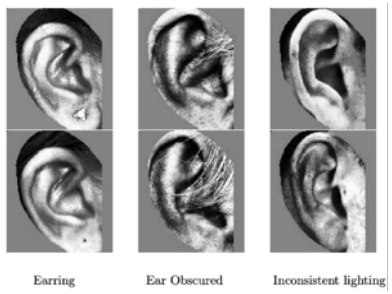
…zwischen *“erfolgreich eingeführt” und “Jahre weg von praktischer Nutzung”:*



- **Retina**
- **Venenmuster (z. B. des Handrückens)**
- ***Gesichts- Thermographie***
- ***Blutpulsmessung***
- **Hautmerkmale**
- **Nagelbett**
- ***Gang***
- **Ohrform**
- ***Geruch***
- **DNA**







Biometrische Systeme

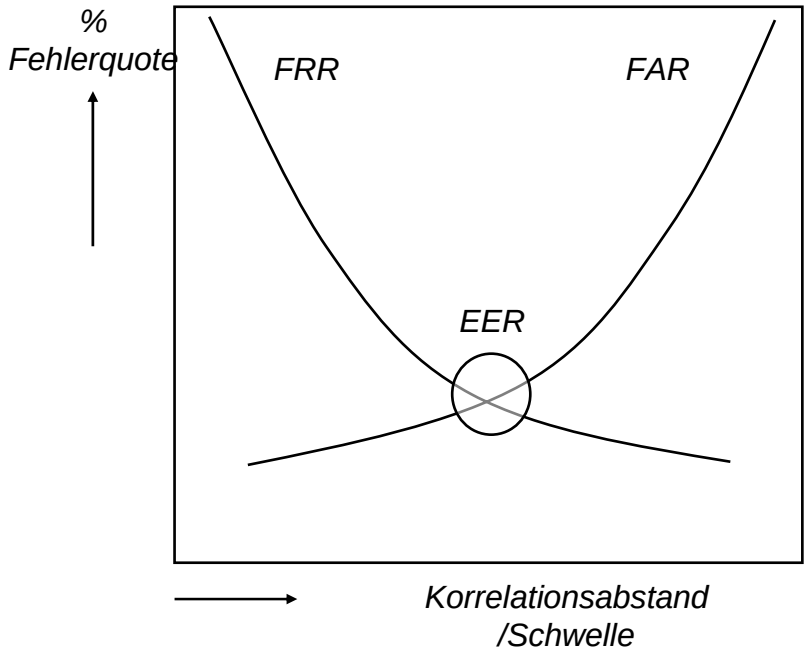
“Bin ich diese Person?”

“Sind meine Referenzdaten im System gespeichert?”

Die Biometrie vergleicht immer nichtidentische Muster. Es wird ein Korrelationsabstand gemessen und eine Schwelle eingeführt. Unterhalb der Schwelle wird ein Muster einer Person zugeordnet und das System antwortet auf obige Frage mit „JA“. Dabei kann das System recht haben – dann liegt eine „True Match“ vor, oder sich irren, dann liegt ein „False Match“ vor. Jenseits der Schwelle ist die Antwort „NEIN“, auch diese kann richtig oder falsch sein. Die Genauigkeit des Systems wird durch die statistischen Werte „False Match Rate – FMR“ und „False Non Match Rate -FNMR“ gebildet. In Bezug auf eine Anwendung werden daraus die falsche Akzeptanz- rate FAR und die falsche Rückweisungsrate FRR abgeleitet.

Systemeigenschaften

Bin ich diese Person?	Das System hat recht	Das System irrt
JA	Ich bin identifiziert 1	Ich bin falsch identifiziert FMR 3
NEIN	Ich bin nicht diese Person 2	Ich bin nicht identifiziert FNMR 4



In allen biometrischen Verfahren werden nichtidentische Muster auf ihre maximale Übereinstimmung überprüft. Die Biometrie liefert Korrelationen aus einer Muster- Erkennung mit einer Fehlerrate.

Einige ausgewählte Test Resultate

FRVT Test (NIST 2002):

Gesichtserkennung:

71,5% richtige Erkennung bei 0,01% FAR
90,3% richtige Erkennung bei 1% FAR

1- Fingererkennung:

99,4% richtige Erkennung bei 0,01% FAR
99,9% richtige Erkennung bei 1% FAR

Für Identifikationsaufgaben ist der Fingererkennung wesentlich besser als die Gesichtserkennung geeignet.

Quelle: NIST Fingerprint Group

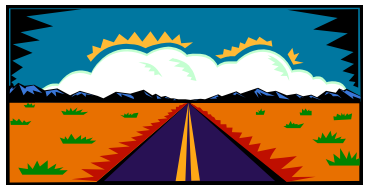
Die Biometrie verspricht:

Mehr Sicherheit .....und weniger Betrug

Polizei

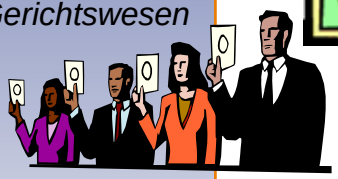
Gefängnisse

Auf absehbare Zeit bleiben
Regierungen und öffentlicher Sektor
Hauptanwender



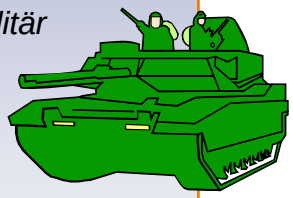
Reisen und Verkehr

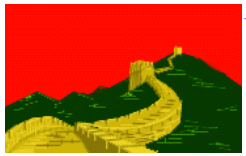
Gerichtswesen

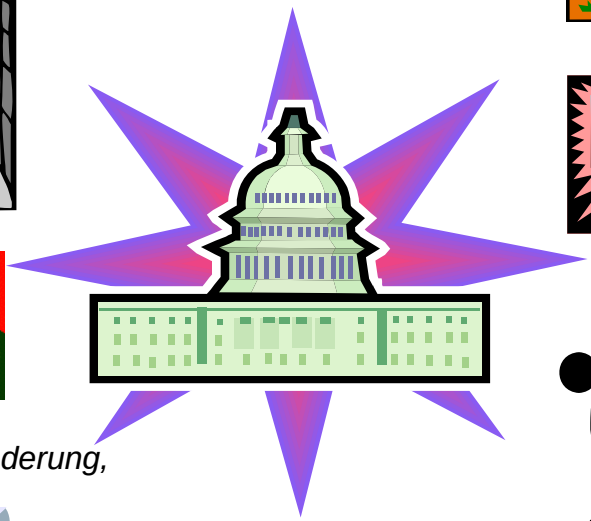


Finanzen: Banken,
Points of Sales

Militär

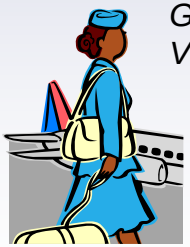




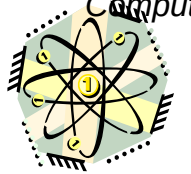


Gesundheitswesen
Wohlfahrt

Grenzübergänge, Zoll, Einwanderung,
Visa, Asylanten



Sicherheit von Gebäuden,
Computern und Kommunikation



Flughäfen
Seehäfen

Öffentlicher, halböffentlicher und privater Sektor

Ausgewählte Biometrie- Projekte

Die Bedrohung durch den internationalen Terrorismus hat die sichere Identifizierung von Personen in den Mittelpunkt öffentlichen Interesses gerückt.

USA

US Visit
TWICS
Hazmat
HSPD 12 – PIV
REAL ID
Registered Traveller
IAFIS NGI

EU & Weltweit

EURODAC
IDENT 1
VIS
e- Passport
e- Identity
e- Citizen Card

Seafarer ID

Identifikation - Das Skalierungsproblem

In der Datenbank sollen sich sehr viele Datensätze N aber nur eine zur Anfrage passende Referenz befinden.

Der Match wird gefunden oder nicht – dafür gibt es nur eine einzige Chance. Die FNMR ist für Identifikation und Verifikation gleich.

Alle anderen Anfragen müssten eigentlich mit NEIN beantwortet werden. Diese Frage kann aber (N-1) mal richtig oder falsch beantwortet werden. Die FMR ist von der Größe der Datenbank abhängig:

$$TFMR = N \times FMR(1).$$

Ein weiteres Skalierungsproblem entsteht, wenn n verschiedene Personen eine Anfrage an eine Datenbank mit N Daten starten:

$$TFMR(n, N) = n \times (1-(1-FMR(1))^N .$$

Quelle: Higgins 2003

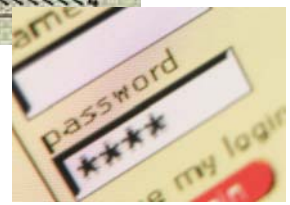
Biometrie und Authentifizierung

…mit Gegenständlichem:

- Schlüssel
- Ausweis, Pass
- Plakette, Abzeichen etc.

…mit Insider- Kenntnis:

- Passwort
- PIN
- Persönliche Erinnerungen



…mit sich selbst:

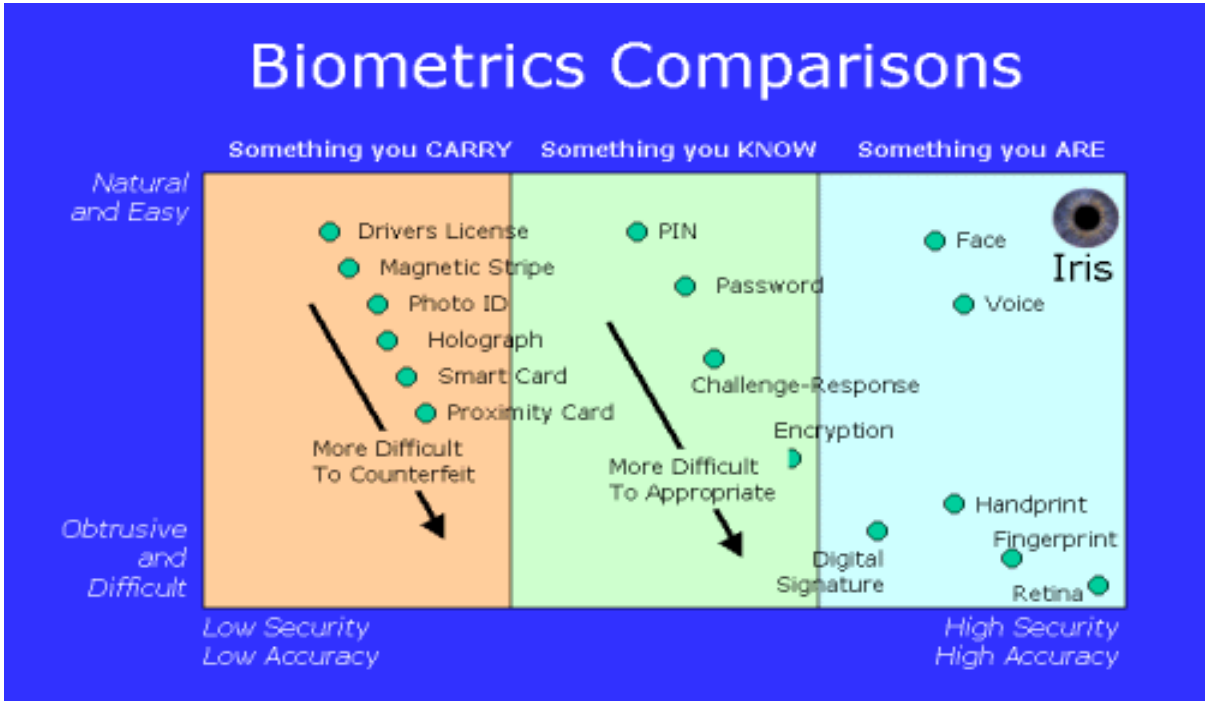
- Biometrie

CROSSMATCH® TECHNOLOGIES

Warum Biometrie?

- **Mehr Sicherheit**
  - **Kann nicht vergessen werden**
  - **Kann nicht verloren werden**

- **Mehr Sicherheit**
  - **Kann nicht gestohlen werden**
  - **Kann nicht (leicht) kopiert werden**



ID Dokumente und Biometrie

ID Dokumente (Reisepässe, Personalausweise, Führerschein etc.) sind im grenzüberschreitenden Verkehr Standard und in den meisten Ländern dieser Welt akzeptiertes Mittel für die Personen- Identifikation.
Trotz zunehmender Zahl und Raffinesse von Sicherheitsmerkmalen haben sie das Manko, dass sie ein „ Ding“ getrennt von der Person sind. Dinge können gefälscht, verloren oder gestohlen werden.
Das Sicherheits- Niveau von ID Dokumenten ist in verschiedenen Staaten höchst unterschiedlich.

Die Biometrie anderseits hat als statistisches Verfahren das Manko der Volumen- Skalierung. Je größer die Datenbank, desto größer die Fehlerrate.

Viele Identifikations- Projekte setzen deshalb auf eine Verbindung von ID Dokumenten und biometrischen Merkmalen.

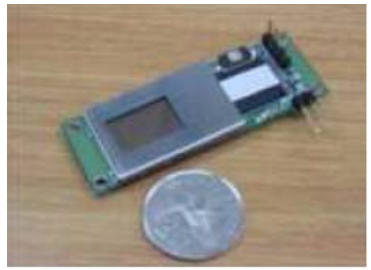
Zusammenwirken verschiedener Technologien

Biometrische Modalitäten auf ID Dokumenten gespeichert

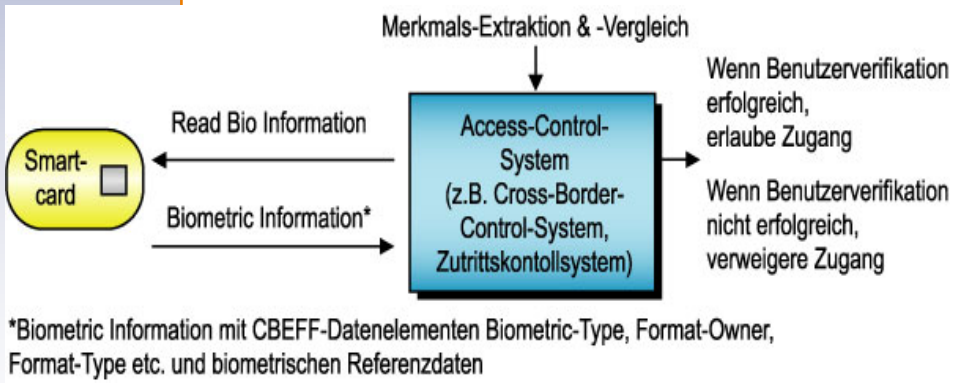
…als Bild

…auf 2D Barcode

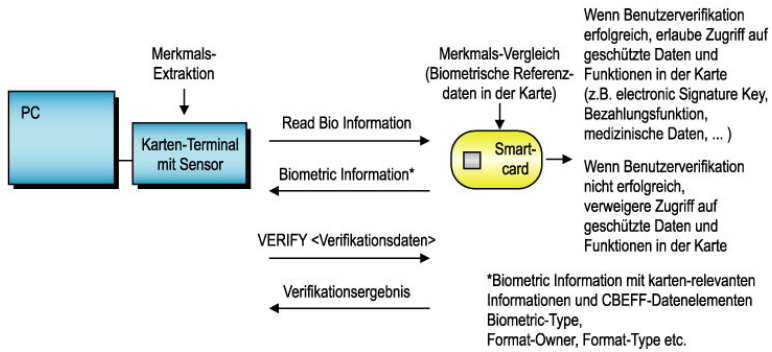
…auf RFID



oder aktuell gescannt



Off- Card Match

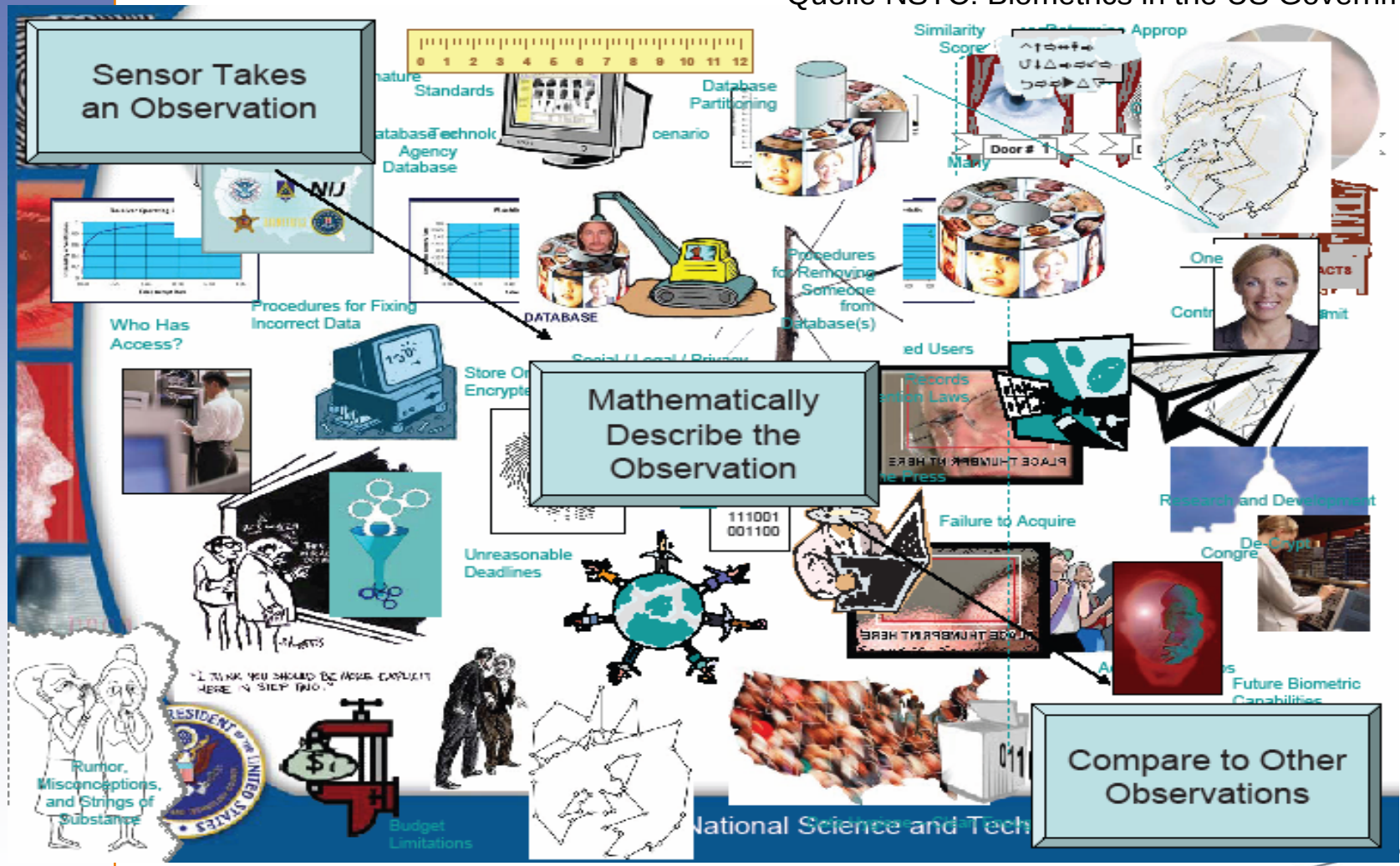


On- Card Match

Interoperabilität, Standards, Datenaustausch

Ordnung im biometrischen Universum

Quelle NSTC: Biometrics in the US Government



Standards

Standards: Regeln, Richtlinien und Vorschriften für Produkte, Verfahren und Systeme

- Formate für den Austausch biometrischer Daten (z. B. EFTS, EBTS, ANSI INCTS…für diverse biometrische Modalitäten))
- Technische Interfaces für das Zusammenwirken biometrischer Komponenten (z. B. BioAPI, CBEFF…)
- Anwendungsprofile (z. B. Data Integrity of Biometric- Based personal Identification for Border Management, PIV/ FIPS 201, ANSI INCITS 238- 2003 Biometric- Based Verfification…)
- Metrik für Leistungstests, Berechnungsvorschriften, Resultatbewertung (z. B. ANSI INCITS 409.2-2005 Biometric Performance Testing…)

Wer macht die Standards?

ICAO International Civil Aviation Organization

NIST National Institute of Standards and Technology

EU Commission

INCITS InterNational Committee for Information Technology Standards

JTC 1 Technology Joint Technical Committee 1; Subcommittee 37

OASIS Organization for the Advancement of Structured Information Standards

Benchmark- und Interoperabilitäts- Tests

Performance Evaluierungen für

- Technologien
- Szenarien
- Operationen

Konformitätsbeurteilungen

Interoperabilitätstests

Biometrische Fallstudien, Pilot- Tests und Förderprojekte

Nationaler und internationaler Datenaustausch

In dem Maße wie man Identitätsdiebstahl als nationale oder globale Bedrohung wahrnimmt entstehen Forderungen und Projekte nach Austausch von gesammelten Daten, z. B. Daten über Terroristen und terroristische Organisationen , Sexual- oder Gewaltverbrecher, Mitglieder von internationalen Verbrecherbanden usw.

Neben der reinen Verbrechensbekämpfung gibt es ein wachsendes Bedürfnis auch für Personengruppen wie Asylanten, Ausgewiesenen, Einreisenden aus bestimmten Ländern, Sozialflüchtlingen usw. Daten zu sammeln und auszutauschen.

Die Tendenz sowohl mehr persönliche Daten zu sammeln und parallel die Datensammlungen zu vernetzen macht die Identifikationssysteme sowohl effizienter als auch anfälliger gegen Missbrauch und Angriffe.

Sicherheitsrisiken biometrischer Systeme

Spoofing: Dem Sensor werden unechte biometrische Merkmale offeriert.

Umgehung des Sensors: Einspielen aufgezeichneter Merkmale.

Substitution: Das gespeicherte Template wird verändert oder ersetzt.

Maskerade: Es wird ein künstliches Tempate generiert.

Systembestandteile der Datenbank oder des Matches werden durch ein „Trojanisches Pferd“ ersetzt, das immer die gewünschten Ergebnisse erzeugt.

Manipulation an den Systemeinstellungen.

Überschreiben des Ergebnisses.

Quelle: Biometric Encryption; März 2007
http://www.eubiometricsforum.com/dmdocuments/bio-encryp.pdf

Resümee: Aktuelle Herausforderungen

Die Biometrie braucht für ihren weiteren Erfolg Systemlösungen, die dem komplexen Charakter ihrer Nutzung gerecht werden:

- **Weiterer technologischer Fortschritt in den biometrischen Verfahren**
- **Bessere Integration in Anwendungen und Zusammenarbeit verschiedener Technologien**
- **Interoperabilität, Standards, Datenaustausch**
- **Akzeptanz, Kommunikation, Daten- Verschlüsselung, Schutz der Privatsphäre**

CROSSMATCH
TECHNOLOGIES

Biometric Solutions Made In Europe

Livescanners

Facial Recognition Systems

Document Readers

www.crossmatch.com

from Cross Match Technologies

The One-Stop Solution Provider

ID Management: Finger, Gesicht, Ausweis

Live Scanner – Front End für AFIS

AFIS Automatische Fingerabdruck Identifizierungssysteme

Criminal AFIS:

In der Datenbank werden abgerollte Finger, flache Finger, Handflächenabdrücke gespeichert.

Aufgabe: Suche nach einer Referenz für eine verdächtigte Person/ Spur einer Person in der Datenbank.

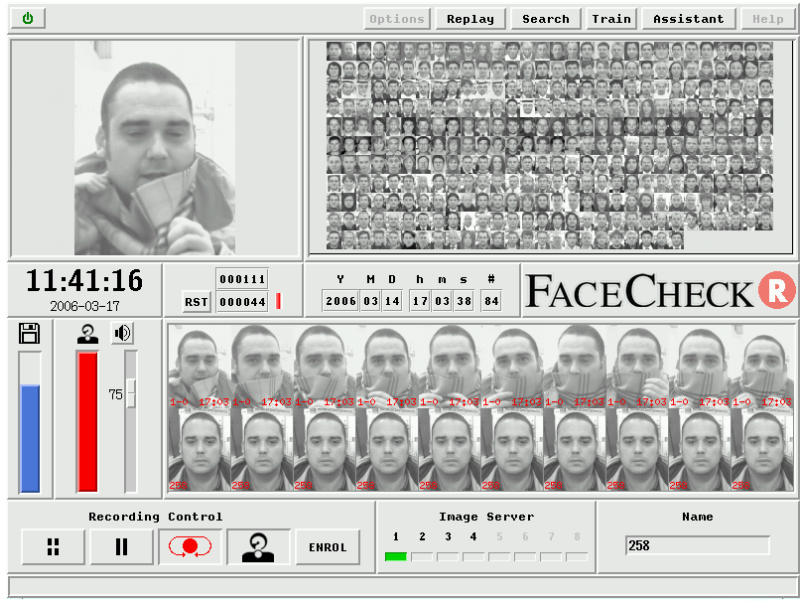
Civil AFIS

Eine Person soll eine überprüfbare Identität zugeordnet werden.

Die Datenbank kann aus einer einzigen Referenz bestehen (Fingerabdruck im Reisepass) bis zu einer umfassenden Einwohner- Datenbank.
Es werden 1,2,4,8,oder 10 flache Finger gespeichert. Für große Datenbanken sind Mehrfinger- Datensätze vorteilhaft.

Live Scan Produkte

Produkte für die Gesichtserkennung



Lesegeräte für ID Dokumente

Quelle: CrossMatch

Weiterführende Links

http://www.biometrics.gov/

http://www.biometricscatalog.org/

http://www.biometrics.org/

http://www.crossmatch.com

Haftungsausschluss

Dieser Vortrag enthält öffentlich zugängliches Bild- und Textmaterial aus Firmenpublikationen, Präsentationen und wissenschaftlichen Arbeiten. Quellenangaben wurden nach besten Wissen beigefügt.

Die Darstellung reflektiert ausschließlich die Sicht des Referenten.