

Biometrische Zugangskontrolle durch Gesichtserkennung

Christian Maier

Vortrag am Lehrstuhl für IT-Sicherheit
02. November 2005

Gliederung

Ziele der Arbeit

Authentifizierung

- Vorstellung der Verfahren
- Grundlagen der Biometrie

Anforderungen an die Verfahren

Gesichtserkennung

- Spezifische Probleme
- Verfahren
- Ergebnisse bedeutender Evaluationen
- Prototypische Implementierung

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren
Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme
Verfahren
Ergebnisse bedeutender
Evaluationen
Prototypische
Implementierung

Ziele der Diplomarbeit

- ▶ Darstellung der Grundlagen der Authentifizierung.
- ▶ Vorstellung verschiedener Verfahren (insbesondere der Biometrie).
- ▶ Erarbeitung von Anforderungen.
- ▶ Analyse, inwieweit die verschiedenen Verfahren die Anforderungen erfüllen.
- ▶ Detailliertere Betrachtung der Gesichtserkennung.

Was ist Authentifizierung?

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

- ▶ Überprüfung und Feststellung der **Identität einer Person**

Wo wird Authentifizierung eingesetzt?

- ▶ Berechtigungsprüfung in Informations- und Kommunikationssystemen
- ▶ Personenkontrolle (z.B. an Grenzübergängen, Flughäfen. . .)
- ▶ Zutrittskontrolle (z.B. zu einem Gebäude, Firmengelände. . .)
- ▶ Überall dort, wo die Identität einer Person relevant ist.

Formen der Authentifizierung

- ▶ Unterscheidung nach dem Abgleichsverfahren
- ▶ **Verifikation**: Überprüfung einer vorgegebenen Identität (1:1 Vergleich)
- ▶ **Identifikation**: Feststellung der Identität einer zunächst unbekanntem Person (1:n Vergleich)

Gruppierung der Verfahren

Authentifizierung durch. . .

- ▶ Wissen
- ▶ Besitz
- ▶ personenspezifische Merkmale (Biometrie)

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Authentifizierung durch Wissen

- ▶ Prüfen, ob die zu authentifizierende Person eine bestimmte Information kennt.
- ▶ Passwort, Kennwort, PIN, TAN...
- ▶ Eingabe über eine Tastatur

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Authentifizierung durch Besitz

- ▶ Prüfen, ob die zu authentifizierende Person einen bestimmten Gegenstand besitzt.
- ▶ Ausweisdokument, Magnetstreifen- oder Chipkarte, RFID-System
- ▶ (Karten-)Lesegeräte, kontaktbehaftet oder kontaktlos.

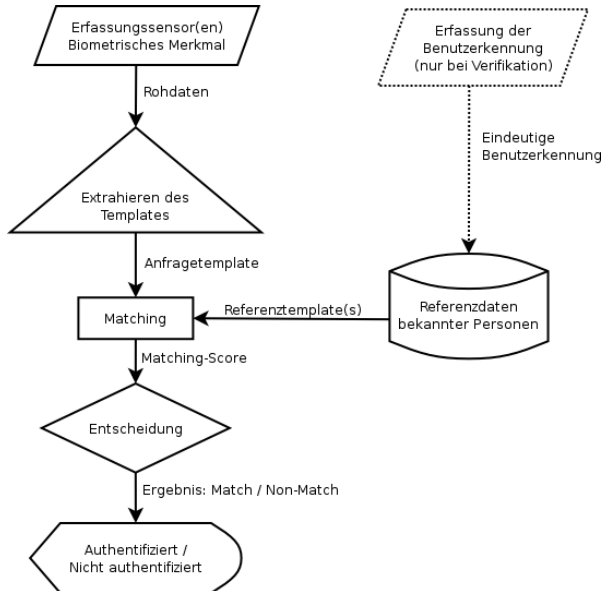
Authentifizierung durch personenspezifische Merkmale

- ▶ Prüfen, ob die zu authentifizierende Person individuelle physiologische und verhaltenstypische Merkmale aufweist.
- ▶ Biometrie: Bios (Leben), Metron (Maß).

Ablauf biometrischer Authentifizierung

- ▶ Erfassung des Merkmals.
- ▶ Extraktion bestimmter Ausprägungen (Anfragetemplate).
- ▶ Vergleich mit zuvor erfasstem Referenztemplate.
- ▶ Entscheidung anhand eines Ähnlichkeitswertes: Match oder Non-Match

Ablauf biometrischer Authentifizierung



Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Anforderungen an biometrische Merkmale

- ▶ Einzigartigkeit
- ▶ Verbreitung
- ▶ Dauerhaftigkeit
- ▶ Messbarkeit
- ▶ Benutzerfreundlichkeit
- ▶ Lebenderkennung

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Ursachen der Einzigartigkeit

- ▶ Genotypisch (ererbte)
- ▶ Randotypisch (zufällig)
- ▶ Konditioniert (erlernt)

Klassifizierung der Merkmale

- ▶ Aktive Merkmale: Ein bestimmtes Verhalten muss ausgeführt werden.
- ▶ Passive Merkmale: Erfassung einer physiologischen Eigenschaft des Körpers.
- ▶ Verfahren: Statisch (passive Merkmale) und dynamisch (aktive Merkmale).

Beispiele passiver Merkmale

- ▶ Fingerabdruck
- ▶ Gesicht
- ▶ Iris
- ▶ Retina
- ▶ Handgeometrie

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

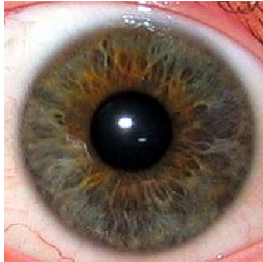
Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Beispiele passiver Merkmale



Iris



Retina

Quelle beider Bilder: <http://de.wikipedia.org>

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Beispiele aktiver Merkmale

- ▶ Dynamik der Unterschrift
- ▶ Stimme
- ▶ Dynamik des Tastaturanschlages

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

- ▶ Erfassung eines Merkmals wird von vielen Faktoren beeinflusst.
→ Templates sind nicht eindeutig reproduzierbar.
- ▶ Entscheidung Match / Non-Match anhand einer Akzeptanzschwelle

Ermitteltes Ergebnis	Tatsächlich sind die Merkmale	
	affin (Genuines)	nicht affin (Imposters)
Match	True Acceptance	False Acceptance
Non-Match	False Rejection	True Rejection

Kennzahlen biometrischer Systeme

- ▶ **False Acceptance Rate (FAR)**: Wahrscheinlichkeit, dass ein nicht affines Merkmal akzeptiert wird.



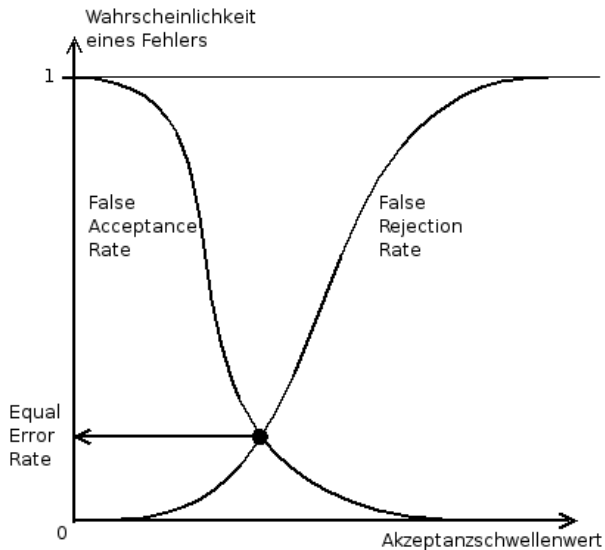
$$FAR = \frac{\text{Anzahl der False Acceptances}}{\text{Gesamtzahl der Vergleiche nicht affiner Merkmale}}$$

- ▶ **False Rejection Rate (FRR)**: Wahrscheinlichkeit, dass ein affines Merkmal zurückgewiesen wird.



$$FRR = \frac{\text{Anzahl der False Rejections}}{\text{Gesamtzahl der Vergleiche affiner Merkmale}}$$

Kennzahlen biometrischer Systeme



Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Authentifizierung einer Person

- ▶ Nur indirekte Identitätsprüfung durch Wissen und Besitz.
- ▶ Biometrie: Fester Personenbezug

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren

Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Sicherheit und Robustheit gegen Überwindungsversuche

- ▶ Bei allen Verfahren abhängig vom Angreifermodell.
- ▶ Biometrische Merkmale sind nicht geheim!
- ▶ Erfordert zuverlässige Lebenderkennung zum Schutz vor Attrappen.
- ▶ Bei hohen Sicherheitsanforderungen: Multi-Faktor-Authentifizierung

Reaktion bei Kompromittierung der Authentifizierungsdaten

- ▶ Wissen und Besitz meist problemlos auszutauschen.
- ▶ Biometrische Daten nicht geheim.
→ Bereits beim Systemdesign berücksichtigen.

- ▶ Schutz personenbezogener Daten
- ▶ Geringe Bedenken bei wissens- und besitzbasierten Verfahren.
- ▶ Biometrische Daten untrennbar mit Person verknüpft.
→ Hohes Schutzbedürfnis
- ▶ Datenschutzfreundliche Techniken: Dezentrale Speicherung, Verzicht auf Speicherung der Rohdaten.

Benutzerfreundlichkeit und Akzeptanz

- ▶ Wissen: Konflikt zwischen Sicherheit und Benutzerfreundlichkeit.
- ▶ Besitz: Relativ problemlos.
- ▶ Biometrie: Verspricht hohe Benutzerfreundlichkeit (z.B. durch berührungslose Erfassung).
- ▶ Trotzdem Akzeptanzschwierigkeiten (z.B. aufgrund hoher Fehlerraten oder gesundheitlicher Bedenken).

Kosten und Geschwindigkeit

- ▶ Einmalige und laufende Kosten
- ▶ Abhängig von Benutzerzahl, Anzahl an Authentifizierungsvorgängen. . .
- ▶ Wissensbasierte Verfahren meist mit geringem Kostenaufwand realisierbar.
- ▶ Bei zeitkritischen Anwendungen die FRR biometrischer Systeme beachten.

Spezifische Probleme der Gesichtserkennung

- ▶ Position und Größe
- ▶ Hintergrund
- ▶ Kopfhaltung
- ▶ Helligkeit
- ▶ Gesichtsausdruck
- ▶ Bedeckung

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren
Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme

Verfahren

Ergebnisse bedeutender
Evaluationen

Prototypische
Implementierung

Schritte der Templateerzeugung

- ▶ Erfassung (Bild, Bildsequenz, zwei- oder dreidimensional)
- ▶ Gesichtsentdeckung
- ▶ Normalisierung
- ▶ Berechnung des Templates

Ergebnisse bedeutender Evaluationen

- ▶ Face Recognition Vendor Test 2002, BioFace, BioP I und BioP II
- ▶ Unterschiedliche Zielsetzungen und Durchführungen.
- ▶ Momentan verfügbare Systeme nur bedingt praxistauglich.
- ▶ Bei hohen Sicherheitsanforderungen (niedrige FAR) inakzeptabel hohe FRR.

Das Verfahren der Eigenfaces

- ▶ Basiert auf Hauptkomponentenanalyse (principal component analysis).
- ▶ Vorgestellt von Turk und Pentland 1991
- ▶ Gut dokumentiert, Reduktion auf mathematisches Problem.

Das Verfahren der Eigenfaces

- ▶ Graustufenbild, N Pixel hoch, N Pixel breit ($N = 256$).
- ▶ Darstellung als Vektor der Länge N^2 ($N^2 = 65536$).
- ▶ Entspricht einem Punkt im N^2 -dimensionalen Raum.
- ▶ Bilder von Gesichtern stellen nur einen relativ kleinen Unterraum (Facespace) dar.

Eigenvektoren und Eigenwerte

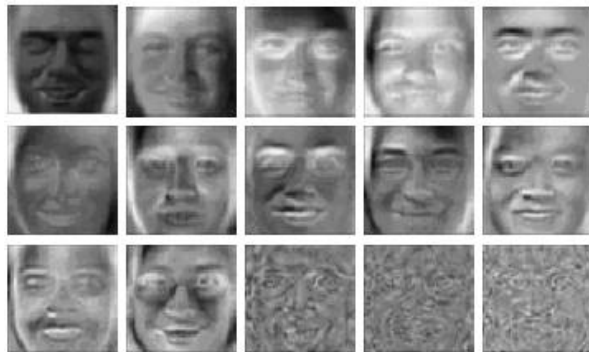
- ▶ Berechnung der Eigenvektoren und Eigenwerte des Facespace.
- ▶ Jeder Punkt (also jedes Gesicht) lässt sich durch Linearkombination von Eigenvektoren darstellen.
- ▶ Je höher der Eigenwert, desto größer ist der Informationsgehalt eines Eigenvektors.

Anwendung zur Gesichtserkennung (1)

Schritt 1: Berechnung der Eigenvektoren

- ▶ Trainingsdaten (Bilder von Gesichtern unterschiedlicher Personen) ergeben den Gesichtsraum (Facespace).
- ▶ Für diesen Gesichtsraum werden die Eigenvektoren berechnet.
- ▶ Geringe Anzahl (M) an Vektoren ausreichend für Gesichtserkennung.
- ▶ M Eigenvektoren mit den höchsten Eigenwerten als Basisvektoren.
- ▶ Darstellung eines Eigenvektors als Bild ähnelt einem Gesicht → Eigenface.

Anwendung zur Gesichtserkennung (1)



Quelle: Zehang Sun, Department of Computer Science,
<http://www.cse.unr.edu>

Biometrische
Zugangskontrolle
durch
Gesichtserkennung

Christian Maier

Ziele der Arbeit

Authentifizierung

Vorstellung der Verfahren
Grundlagen der Biometrie

Anforderungen an
die Verfahren

Gesichtserkennung

Spezifische Probleme
Verfahren
Ergebnisse bedeutender
Evaluierungen

Prototypische
Implementierung

Anwendung zur Gesichtserkennung (2)

Schritt 2: Projektion bekannter Personen in den Gesichtsraum

- ▶ Bilder der zu authentifizierenden Personen werden als Linearkombination der Basisvektoren dargestellt.
- ▶ „Projektion in den Gesichtsraum“
- ▶ Berechnete Eigenwerte beschreiben das Gesicht (Referenztemplate).
- ▶ Wenig Rechenaufwand und daher ausreichend schnell durchführbar.

Anwendung zur Gesichtserkennung (3)

Schritt 3: Gesichtserkennung

- ▶ Anfragebild wird ebenfalls in den Gesichtsraum projiziert.
- ▶ Vergleich der errechneten Eigenwerte des Anfragetemplates mit bekannten Referenztemplates.
- ▶ Errechnung eines bestimmten Ähnlichkeitswertes oder eines Distanzmaßes.

Demonstration des entwickelten Prototyps

Diplomarbeit und Präsentation im Internet:
`www.chmai.de`