Pseudonyme Biometrik: Ein signatur-basierter Ansatz

Biosig 2003 - Martin Johns - Universität Hamburg
mj@martinjohns.com

Inhalt

1. Motivation
2. Grundlegendes
3. Voraussetzungen und Ziele
4. Bestehende Ansätze
5. Der signatur-basierte Ansatz
6. Ein Beispiel

Motivation

- Die Beziehung zwischen einen biometrisches Merkmal und dem Merkmalsträger ist:
  - Eindeutig
  - Unveränderlich
  - Dauerhaft

Motivation (II)

- Diese Eigenschaft ermöglicht das Identifizieren von Personen unabhängig von eingelernter Identität
- Ziele des Papers:
  - Formale Formulierung der Anforderungen und Bedingungen
  - Angabe eines Beispiels

Pseudonymität

- Bewegt sich zwischen den Extremen "*anonymity*" und "*accountability*"
- Beinhaltet eine *1:n*-Relation zwischen Person und Pseudonym

Biometrische Authentikation

- Nachweis einer digitalen *Identität* durch ein biometrisches Merkmal
- Notation:

M	biometrische Rohdaten
S	biometrische Signatur
$f(M) = S$	biometrischer Algorithmus
$d(S,S')$	Abstandsmaß zweier Signaturen
$T > d(S,S')$	Schwellwert

Identifizieren von Signaturen

biometrische Rohdaten (*M*)

Identität A

Identität B

Ressource 1

S1: [00101001...]
S2: [11001010...]
S3: [11100011...]
...

Ressource 2

S1: [11100011...]
S2: [00111010...]
S3: [01010101...]
...

$d(S3,S1) < T$

Anforderungen

(F1) Möglichkeit der Nutzung eines Dienstes eines Anbieters unter zwei verschiedenen Identitäten

(F2) Möglichkeit der Nutzung zweier Dienste des selben Anbieters unter zwei verschiedenen Identitäten

(F3) Verhinderung der Zusammenlegung personenbezogener Datensätze

(F4) Verhinderung der illegalen Weitergabe der biomtrischen Signatur an dritte

Voraussetzungen

- Keine Speicherung der biometrischen Rohdaten
- Kontrolle über die Erfassungseinheit bestimmt den Erfolg der Pseudonymisierung

Bestehende Ansätze

- Verwendung verschiedener biometrischer Merkmale [Köh99]
- Hashen oder Verschlüsseln der Signaturen [Don99]
- Auslagerung von Teilen der biometrischen Authentikation [Ble98]

Der signatur-basierte Ansatz (I)

- Grundlegende Idee: Integration eines Maskierungs-Werts *k* in die Signaturberechnung
- *PS = f(M,k)*

Der signatur-basierte Ansatz (II)

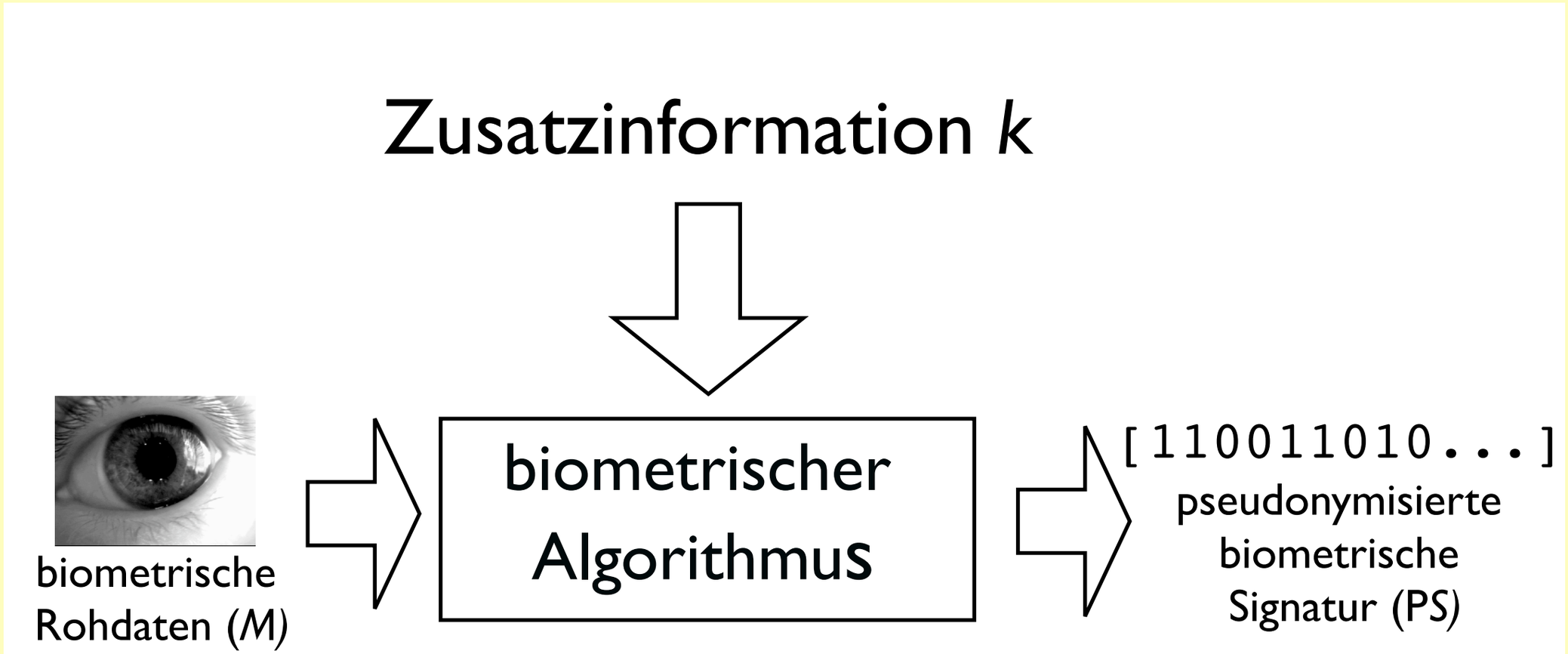
biometrische Rohdaten (*M*)

biometrischer Algorithmus

[10010101...]
biometrische Signatur (*S*)

Berechnung einer biometrischen Signatur

Der signatur-basierte Ansatz (III)



Berechnung einer pseudonymisierten biometrischen Signatur

Anforderungen: Pseudonymisierung

(P1) $d(f(M,k), f(M',k)) < T$, wenn M und M' von der selben Person stammen

(P2) $d(f(M,k), f(M',k)) > T$, wenn M und M' von verschiedenen Personen stammen

(P3) $d(f(M,k), f(M,k')) > T$, wenn k ungleich k'

Anforderungen: Robustheit

- Es darf keine Umkehrfunktion f^{-1} existieren, die *PS* in *S* überführt
- Es darf keine Vergleichsfunktion *d'* existieren, die eine Vergleich zweiser pseudonymisierter Signaturen *PS* und *PS'* bei Umgehung der Werte von *k* ermöglicht

Ansatzpunkte der Pseudonymisierung

1. Vor der Signaturberechnung:

$$PS = f(M,K) = f(t(M,k))$$

2. Während der Signaturberechnung

3. Kombination der beiden Ansatzpunkt

Geeignete Algorithmen

+	-
Verlustbehaftete Signaturerstellung (z.B. statistische Methoden)	Eindeutige Relation zwischen Teilen der Signatur und vorhanden Merkmalsausprägungen
“Syntaktische” Analyse	“Semantische” Analyse

Umgang mit *k*

- Eine Geheimhaltung des Maskierungs-Werts *k* ist nicht in jedem Fall notwendig
- Wenn unter Kenntnis von k_1 und k_2 eine Relation zwischen $PS_1 = f(M,k_1)$ und $PS_2 = f(M,k_2)$ hergestellt werden kann, ist eine Geheimhaltung unerlässlich

Beispiel (I)

- Algorithmus von John Daugman zur Iris-Erkennung [Dau93]
- Pseudonymisierung während der Signaturberechnung
- Grundalgorithmus: Berechnung komplexer Waveletkoeffizienten anhand fester Analyse-Punkte
- Signatur-Erzeugung aufgrund der Vorzeichen der Waveletkoeffienten

Beispiel (II)

- Methode: Verschiebung der Analyse-Punkte
- Durchschnittlicher Wechsel des Vorzeichens des Waveletkoeffizienten bei einer Verschiebung der Analyse-Punktes von etwa 10% der effektiven Breite des Wavelets

Beispiel (III)

- *vi* : zufällige Verschiebung der Analysepunkte in x/y-Richung:

$$v_i = (v_{i_x}, v_{i_y}), \qquad i \in [1, 1024] \qquad v_{i_{(x,y)}} \in [-b, b]$$

- Resultierende Formel:

$$h_{i_{\{Re,Im\}}} = \mathrm{sgn}_{\{Re,Im\}} \int_{\rho} \int_{\phi} I(\rho, \phi)\, e^{-i\omega(\theta_i + v_{i_x} - \phi)} e^{-\frac{(\tau_i + v_{i_y} - \rho)^2}{\alpha^2}} e^{-\frac{(\theta_i + v_{i_x} - \phi)^2}{\beta^2}}\, \rho\, d\rho\, d\phi.$$

Fazit

- Eine sigantur-basierte Pseudonymisierung von biometrischen Signaturen ist möglich
- Eine Auswahl geeigneter biometrischer Algorithmen und eine Erweiterung dieser in Hinsicht auf Pseudonymisierung steht noch aus

Zum Ende...

- Vielen Dank für ihre Aufmerksamkeit
- Fragen, Ergänzungen, Kommentare...???

Literatur

[Ble98] Gerrit Bleumer. Biometric yet Privacy Protecting Person Authentikation. In Information Hiding, LNCS, pages 99 – 110, Berlin Heidelberg, 1998. Springer.

[Dau93] John Daugman. High Con dence Visual Recognition of Persons by a Test of Statistical Independence. In Transactions on Pattern Analysis and Machine Intelligence, volume 15, pages 1148 – 1161, November 1993.

[Don99] Lutz Donnerhacke. Anonyme Biometrie. DuD, 3/99:151 – 154, 1999.

[GZT00] C. Garcia, G. Zikos, and G. Tziritas. Wavelet Packet Analysis for Face Recognition. In Image and Vision Computing, volume 18(4), pages 289 – 297, 2000.

[Joh03] Martin Johns. Anwendung von Wavelets in der biometrischen Authentikation. Diplomarbeit, Universität Hamburg, Fachbereich Informatik, Hamburg, 2003.

[Köh99] Marit Köhntopp. Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren. In Patrik Horster (Hg.): Sicherheitsinfrastrukturen; Proceedings zur Arbeitskonferenz Sicherheitsinfrastrukturen 1999. Vieweg, 1999.

[PK01] Andreas Pfitzmann and Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In H. Federrath, editor, Designing Privacy Enhancing Technologies, number 2009 in LNCS, page 1pp, Berlin Heidelberg, 2001. Springer.

[WFNM99] L. Wiskott, J.-M. Fellous, N. KrËuger, and C. Malsburg. Face Recognition by Elastic Bunch Graph Matching. In Intelligent Biometric Techniques in Fingerprint and Face Recognition, pages 375–373, London New York, 1999. CRC Press.