Sicherheitsevaluierung von Template Protection Systemen

TeleTrusT-interner Workshop 2010
10. Juni 2010, Saarbrücken

Alexander Nouak
Fraunhofer-Institut für Graphische Datenverarbeitung IGD
Abteilung Identifikation und Biometrie
alexander.nouak@igd.fraunhofer.de

Authentisierung

- Faktoren zur Authentisierung
  - Wissen
    - PIN, Passwort etc.
  - Besitz
    - Token, SmartCard, Bankkarte etc.
- Höhere Sicherheit durch Kombination der Faktoren
- Problematik
  - Beide können vergessen, verloren, gestohlen werden
- 3. Faktor
  - Sein
    - Körpereigene Merkmale, Biometrie

Studie zu Identitätsdiebstahl

- Identitätsdiebstahl und Identitätsmissbrauch im Internet Rechtliche und technische Aspekte
  - Im Auftrag des BMI und des BSI
  - Veröffentlichung am 9. Juni 2010
  - Kostenlos bis 23. Juni 2010 verfügbar unter:
    - www.bsi.bund.de/cae/servlet/contentblob/1086544/publicationFile/90903/Studie_Identitaetsdiebstahl_090610.pdf
  - Autoren
    - Prof. Dr. Georg Borges (Ruhr-Universität Bochum)
    - Prof. Dr. Carl-Friedrich Stuckenberg (Universität des Saarlandes)
    - Prof. Dr. Jörg Schwenk (Ruhr-Universität Bochum)
    - Dr. Christoph Wegener (Ruhr-Universität Bochum)

Herausforderungen

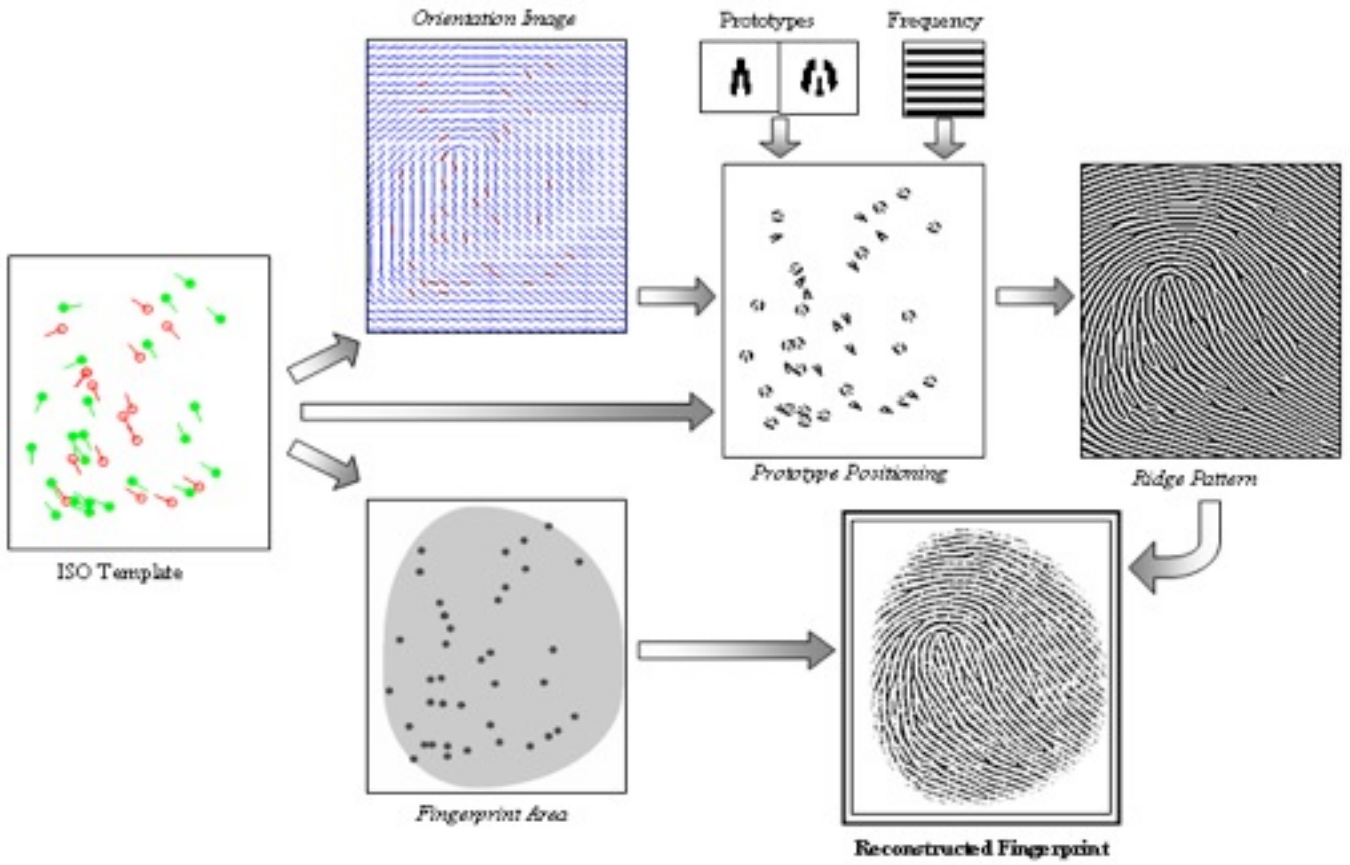
- Privatsphäre
  - Gefahr des Missbrauchs
- Sicherheit
  - Wahrscheinlichkeitsbasiert
  - Neues Subsystem – neue Sicherheitslücken
- Vertrauen
  - Medizinische Auswirkungen, Hygienebedenken
- Risikominderung
  - Fälschungsproblematik
- Interoperabilität
- Herstellerunabhängigkeit

Biometrische Daten

- Sicherheits- und Datenschutzprobleme in biometrischen Systemen
  - Verstärkter Identitätsdiebstahl
  - Unveränderlichkeit
  - Verknüpfung
  - Privatsphäre
  - Datenschutz und zentrale Speicherung

Sicherheits- und Datenschutzprobleme

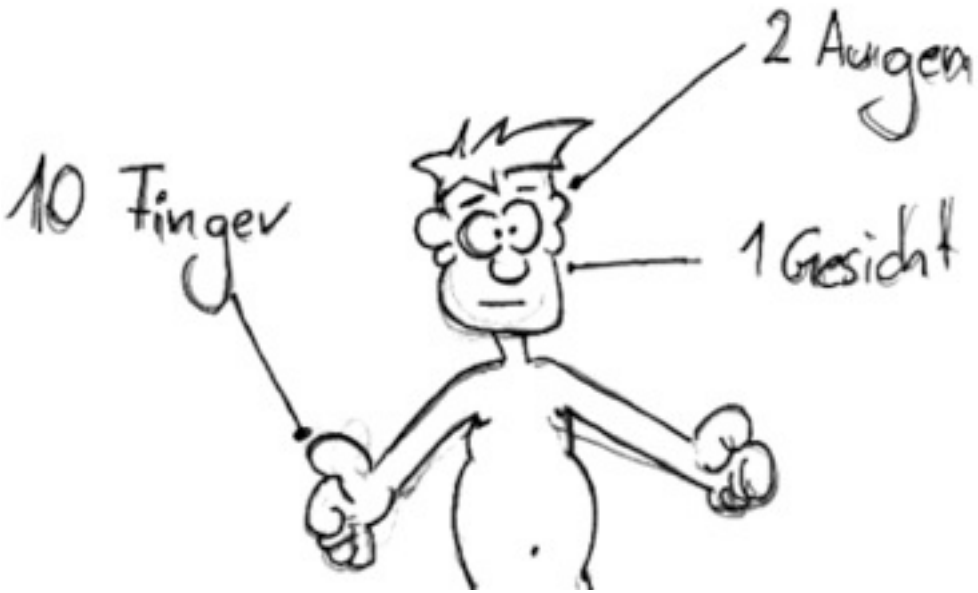
- Verstärkter Identitätsdiebstahl



* Biometric System Laboratory, DEIS, University of Bologna,
http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=15&pathSubj=111%7C%7C15&Req=&

Sicherheits- und Datenschutzprobleme

- Unveränderlichkeit



Sicherheits- und Datenschutzprobleme

- Verknüpfung

Sicherheits- und Datenschutzprobleme

- Privatspäre
  - Krankheiten:
    - Freischwebende Iriszyste*

  - Ca. 75% höhere Wahrscheinlichkeit einer durchgehenden Handlinie bei an Trisomie 21 oder Trisomie 13 Syndrom Erkrankten**
  - Genetische Informationen, Geschlecht, ethnische Zugehörigkeit…
  - *Für die Authentisierung sind diese Informationen irrelevant*

*www.eyecancerinfo.com/photogallery/8_47.jpg

** Julia Seidel, “Zusatzinformationen in Fingerbildern”, Hochschule Darmstadt, 2006

Sicherheits- und Datenschutzprobleme

- Datenschutz und zentrale Speicherung
  - Richtlinie 95/46/EC: Die Europäische Richtlinie zum Datenschutz sieht vor, dass jedermann das Recht hat, Kontrolle über Erfassung und Nutzung seiner persönlichen Daten auszuüben. (Informationelle Selbstbestimmung)
  - Bundesdatenschutzgesetz
  - Referenzen:
    - White Paper zum Datenschutz in der Biometrie, H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock, TELETRUST Deutschland e.V., March 2008
    - Biometric Systems and Data Protection Legislation in Germany, Martin Meints, Heinz Biermann, Manfred Bromba, Christoph Busch, Gerrit Hornung, Gisela Quiring-Kock;
      in: Proceedings of the 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008

Anforderungen an biometrische Templates

- Geschützte Templates
  - keine Rekonstruktion der biometrischen Daten
- Widerrufbare, erneuerbare, diversifizierbare geschützte Templates
- Universeller Ansatz
- Interoperabilität
- Datenminimierung
- Intrinsische Sicherheit
  - keine Reduktion der Zuverlässigkeit ggü. bisheriger System
- Integration in existierende Verifikationsmethoden
- Architekturflexibilität
  - Online Verifikation (zentrale Datenbanken)
  - Offline Verifikation (lokale Datenbank)

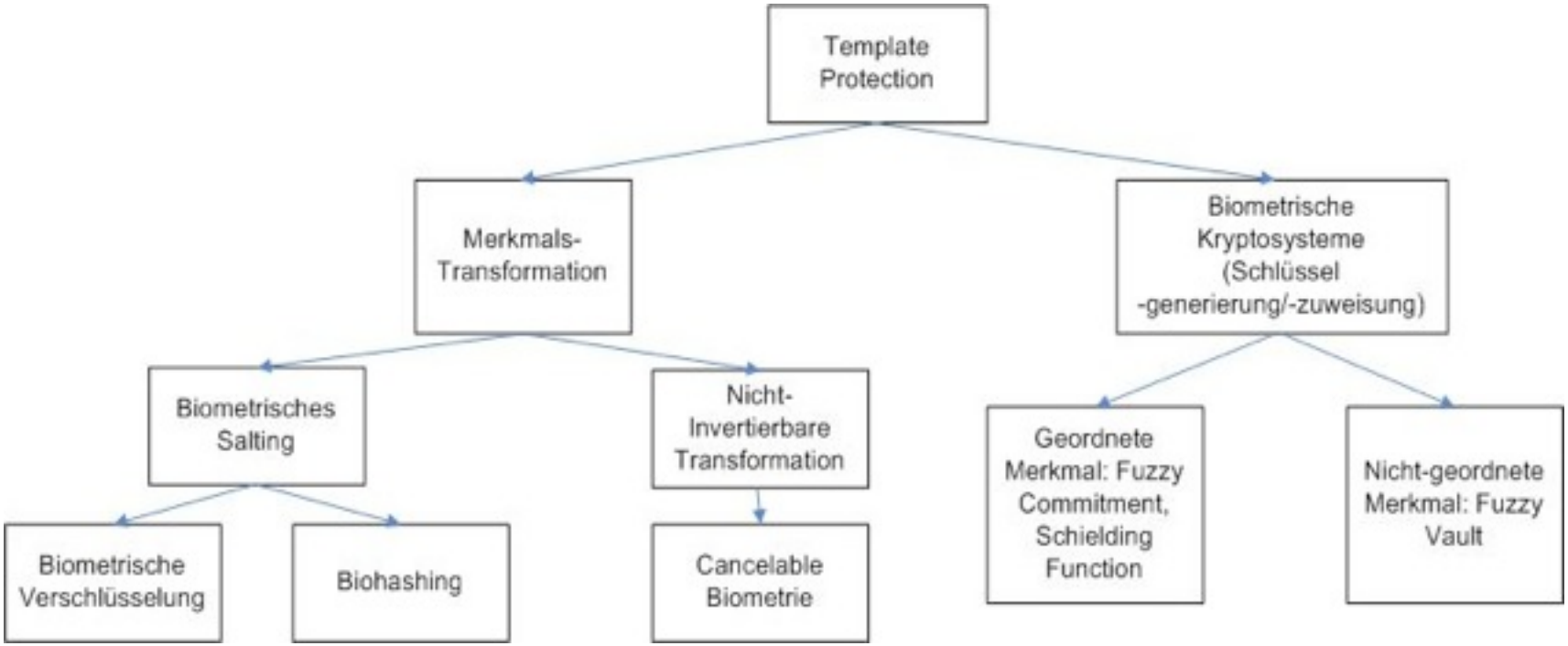
Alternative Schutzmethoden

- Schutz biometrischer Daten
  - Verschlüsselung
    - Empfindlich gegen Variationen biometrischer Daten
      - Entschlüsselung ist notwendig → Sicherheitslücke
    - (Komplexe) Schlüsselverwaltung ist erforderlich
    - Widerstandslos gegen interne Angreifer
  - Comparison-on-Card
    - Keine Datenschutzprobleme
    - Nicht möglich für alle biometrischen Charakteristika
    - Nur für Verifikation geeignet
    - Echtheit der Smartcard muss überprüft werden

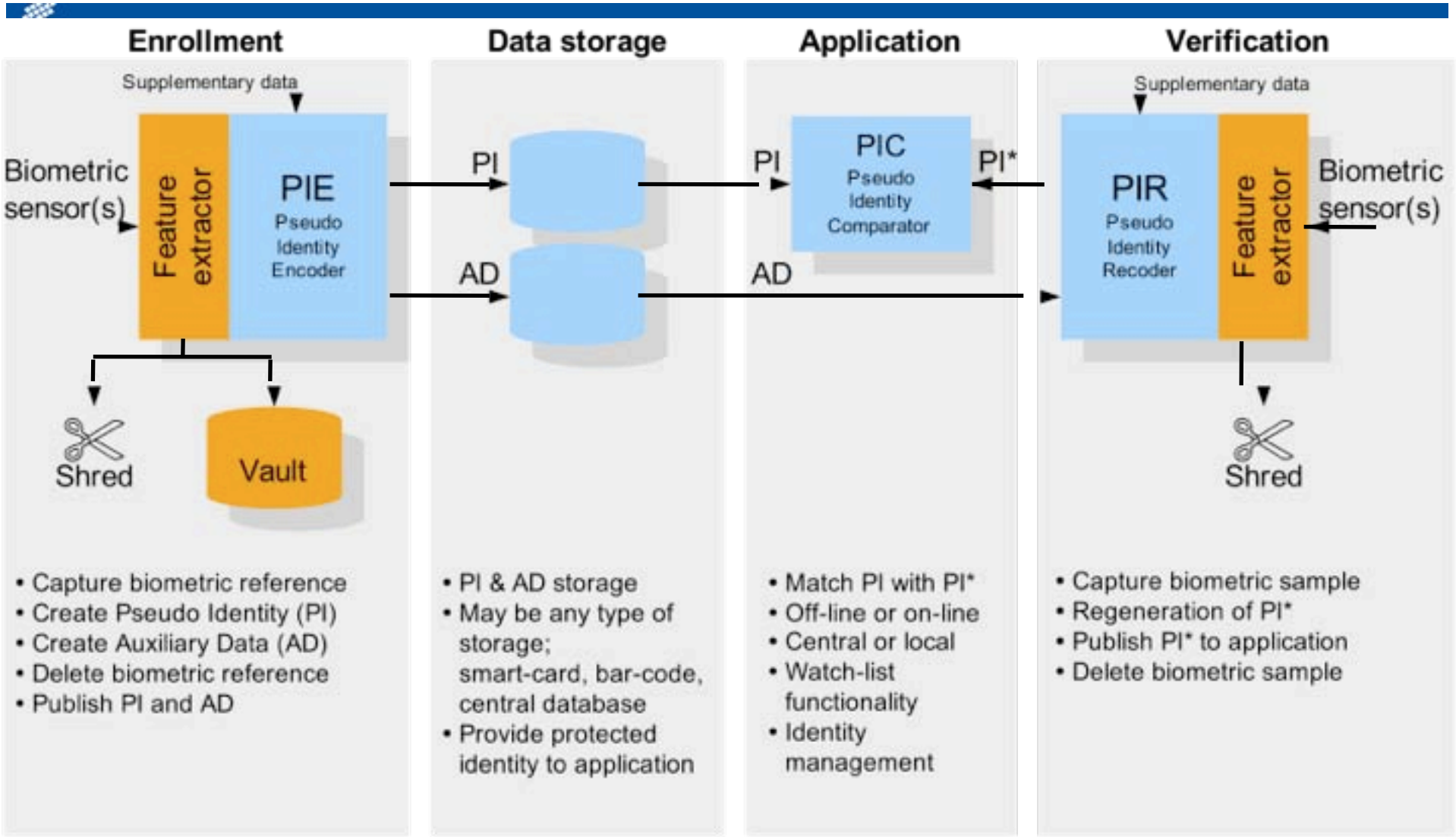
⇒ Template Protection

Template Protection Verfahren

- Template Protection
  - generiert unterschiedliche, unabhängige sichere Referenzen aus biometrischen Daten, die aus pseudonymen Identifikatoren (PI) und unterstützenden Daten (Auxiliary Data – AD) bestehen



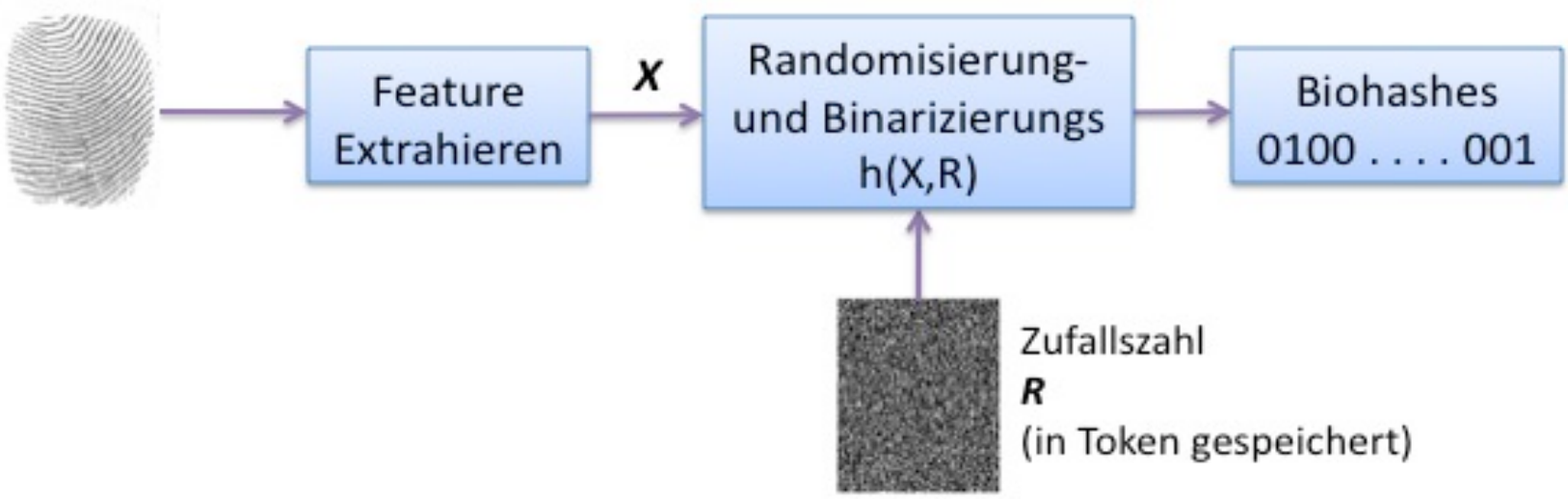
Architekturübersicht



J. Breebaart, C. Busch, J. Grave, E. Kindt: A Reference Architecture for Biometric Template Protection based on Pseudo Identities, in Proceedings BIOSIG 2008

Transformationsmethode: Biohashing

- Biohashing-Verfahren konvertieren biometrische Merkmale zu binären Kodes – so genannten Biohashes – mithilfe großer Mengen benutzerspezifischer Zufallszahlen
  - Zufällige Projektionsmethode + Binarisierung
  - Binarisierung mit zufälligen Schwellwerten
  - Bilden zufälliger Komplexzahlen und Binarisieren derer Phasen

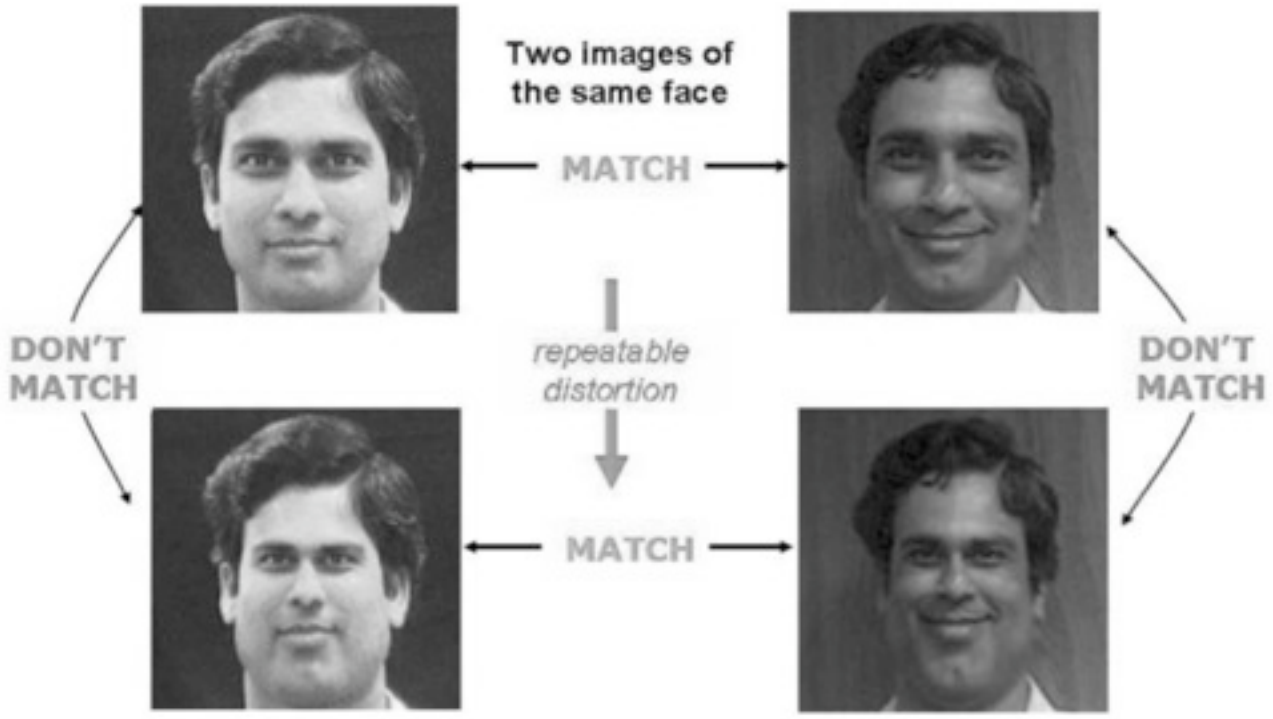


Transformationsmethode: Biohashing

- PI ist eine binäre Zeichenkette (der Biohash)
  - Zufallszahlen sollen bspw. in einem Token als zusätzliche Daten gespeichert werden
  - Vergleich der PIs basiert auf dem Hamming-Abstand
- Identifikation ist unmöglich
- Biohashing basiert auf zufälliger Projektion
  - Erfolgreich implementiert für Handflächen-, Fingerabdruck- und Gesichtserkennung
  - EER von Null kann im Fall der „Biometrics-Stolen“ erreicht werden
  - Erkennungsrate reduziert im Fall der „Token-Stolen“

Transformationsmethode: Cancellable Biometrie

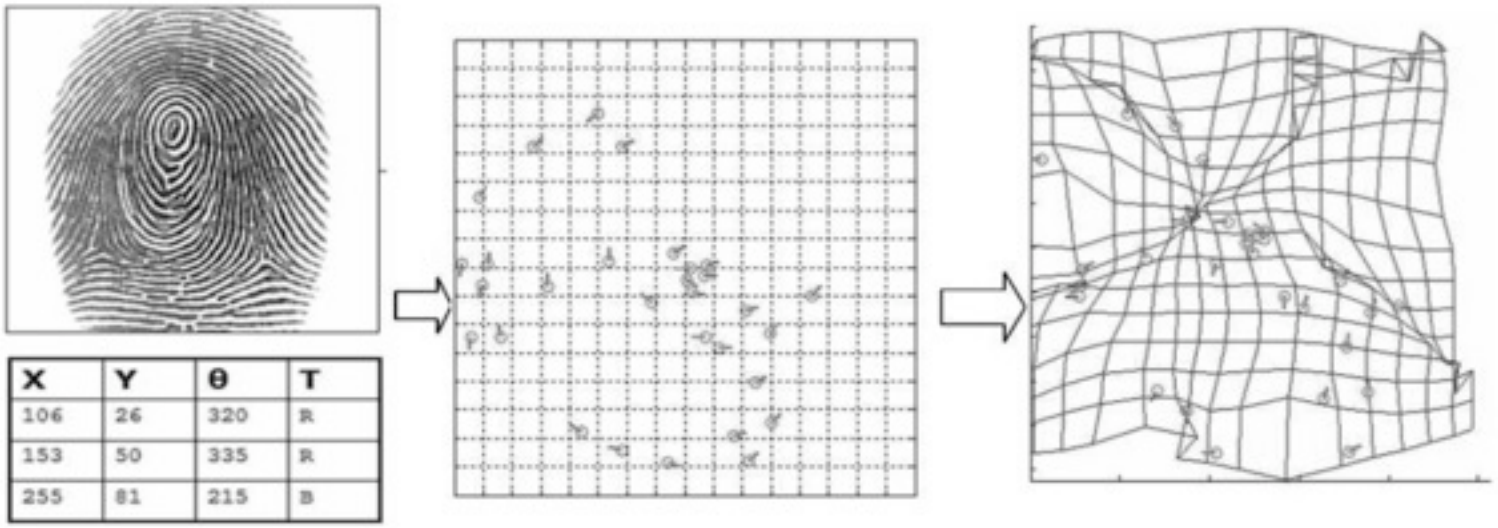
- Cancelable Biometrie
  - Nicht-Invertierbare Transformationsfunktionen werden benutzt
  - Morphing von Gesichtern



17 * K. Ratha, Sharat Chikkerur, Jonathan H. Connell, Ruud M. Bolle: Generating Cancelable Fingerprint Templates, April 2007

Transformationsmethode: Cancellable Biometrie

- Minutien von Fingerabdrücken
  - Transformation mittels Oberflächenfaltung



X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

* K. Ratha, Sharat Chikkerur, Jonathan H. Connell, Ruud M. Bolle: Generating Cancelable Fingerprint Templates, April 2007

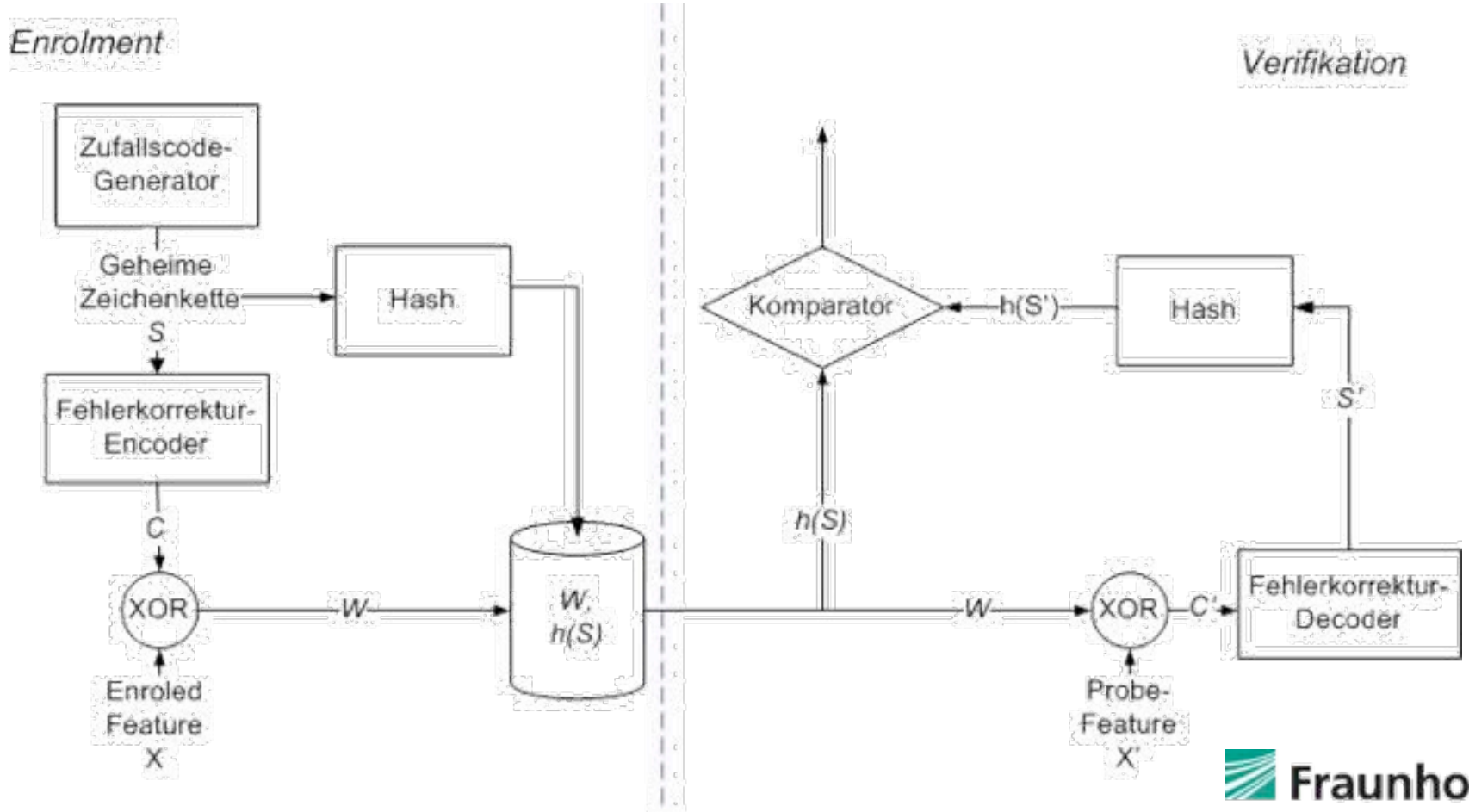
Transformationsmethode: Cancellable Biometrie

- Cancellable Biometrie
  - PI ist das transformierte Sample oder Merkmal
    - Transformationsparameter sollen als zusätzliche Daten geheim gespeichert werden
  - Kein Matching zwischen unterschiedlich transformierten Merkmalen
  - Im Prinzip funktioniert dieses Verfahren für alle biometrischen Charakteristika, aber es existiert keine allgemeine Transformation
  - Jedoch ist eine genaue Sicherheitsanalyse notwendig

Biometrische Kryptosysteme (BK)

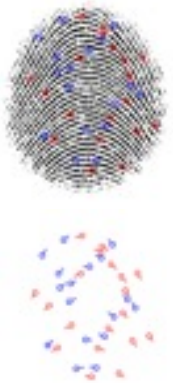
- Biometrische Kryptosysteme kombinieren Kryptografie mit Fehlerkorrekturverfahren
  - PI ist der Hash der geheimen Zeichenkette
    - unterstützende Daten müssen als Teil der geschützten Templates gespeichert werden
    - Vergleich basiert auf einem exakten Match
  - Geeignet für alle biometrische Charakteristika
    - 2-D- und 3-D-Gesichtserkennung
    - Iriserkennung
    - Fingerabdruckerkennung
    - Handflächenvenenerkennung
    - Ohrerkennung

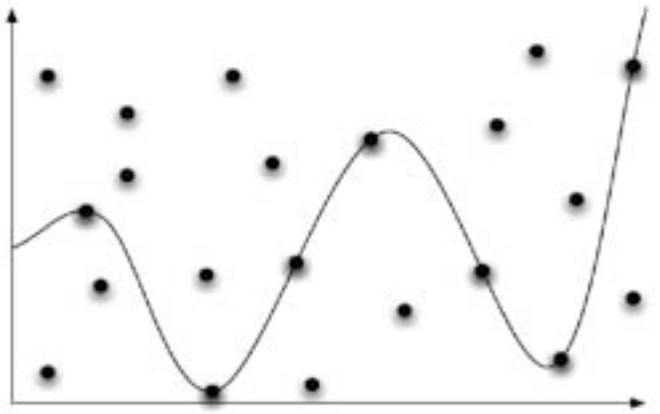
- Fuzzy Commitment Schema
  - kryptographische Verschlüsslung + Fehlerkorrekturkode



BK: Fuzzy Vault

- Secret Sharing
  - PI ist der Hash einer geheimen Zeichenkette
    - unterstützende Daten sind das Vault-Set
  - Sicherheit des Verfahrens
    - wie schnell kann ein echtes Minutienpunkteset im Vault-Set gefunden werden
  - „Helper Data“, z.B. Punkte auf den Fingerlinien, die an Stellen hoher Krümmung liegen, können verwendet werden, um die Leistungsfähigkeit zu erhöhen





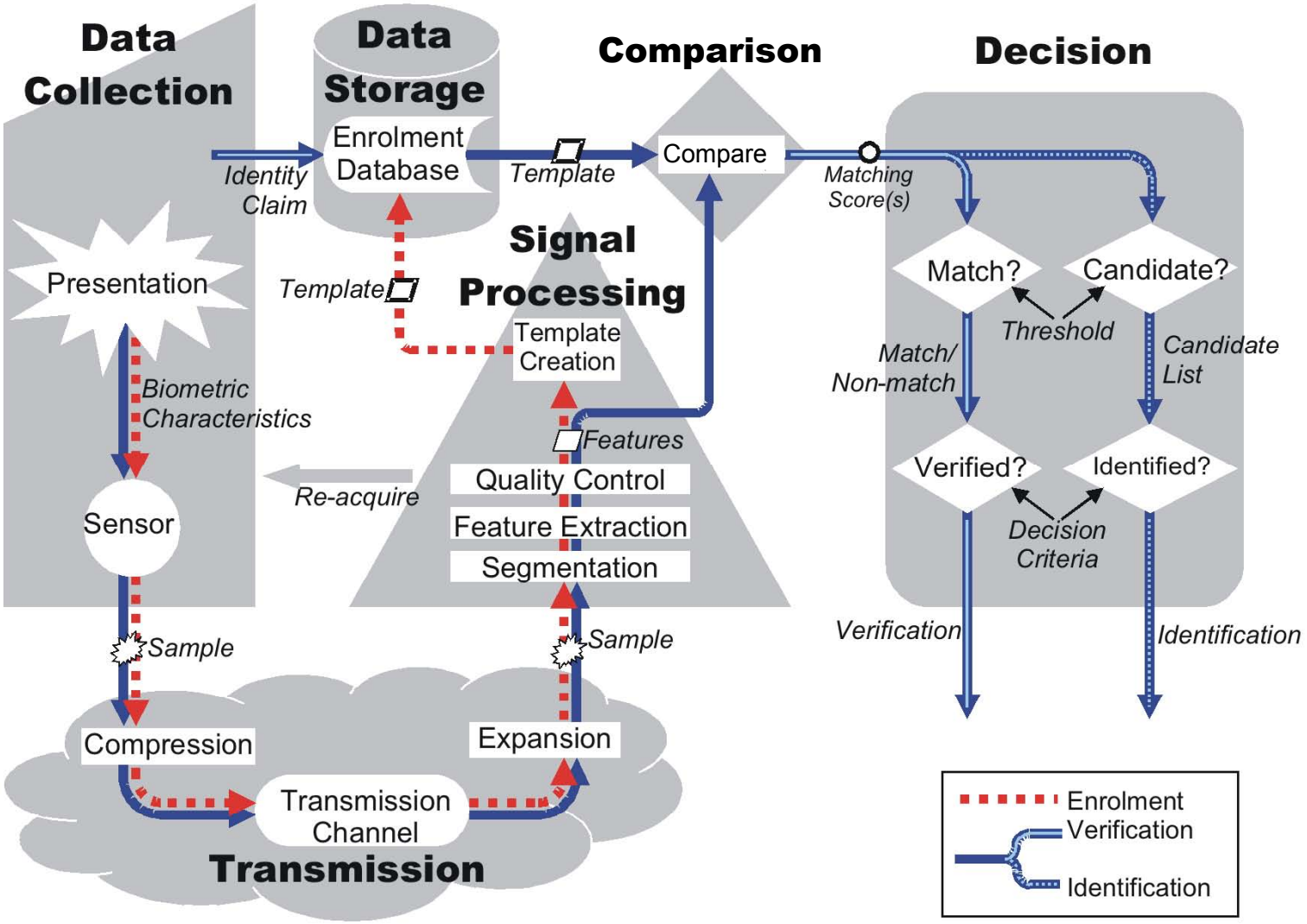
Sicherheit von Template Protection

- Resistenz gegen Angriffe:
  - Brute-Force-Angriffe
    - Die Komplexität, um pseudonyme Identifikatoren zu schätzen, z.B. die Länge einer geheimen Zeichenkette
  - Verknüpfungsangriffe
    - Die unterstützenden Daten enthalten benutzerspezifische Informationen. Biometrische Verschlüsselung ist anfälliger als Transformationsmethoden
  - Falsch-Akzeptanz-Angriff
    - Alle biometrischen Systeme sind anfällig, aber nur durchführbar, wenn der Angreifer eine große biometrische Datenbank besitzt

Schutzziele

- Ausreichende Sicherheit des PI
  - Ist es schwer genug, den richtigen Identifikator zu schätzen
  - Ist es schwer genug, das Sample od Feature Set zu rekonstruieren, wenn der identische Transformationsalgorithmus angewendet wird
- Keine Ableitung der biometrischen Informationen aus PI oder AD
- Gute Zufälligkeit des PI
  - Die Identifikatoren sollten unabhängig sein
  - Keine Verbindungen zwischen den PIs
- Keine persönlichen Daten in AD
  - AD sollte zufällig sein

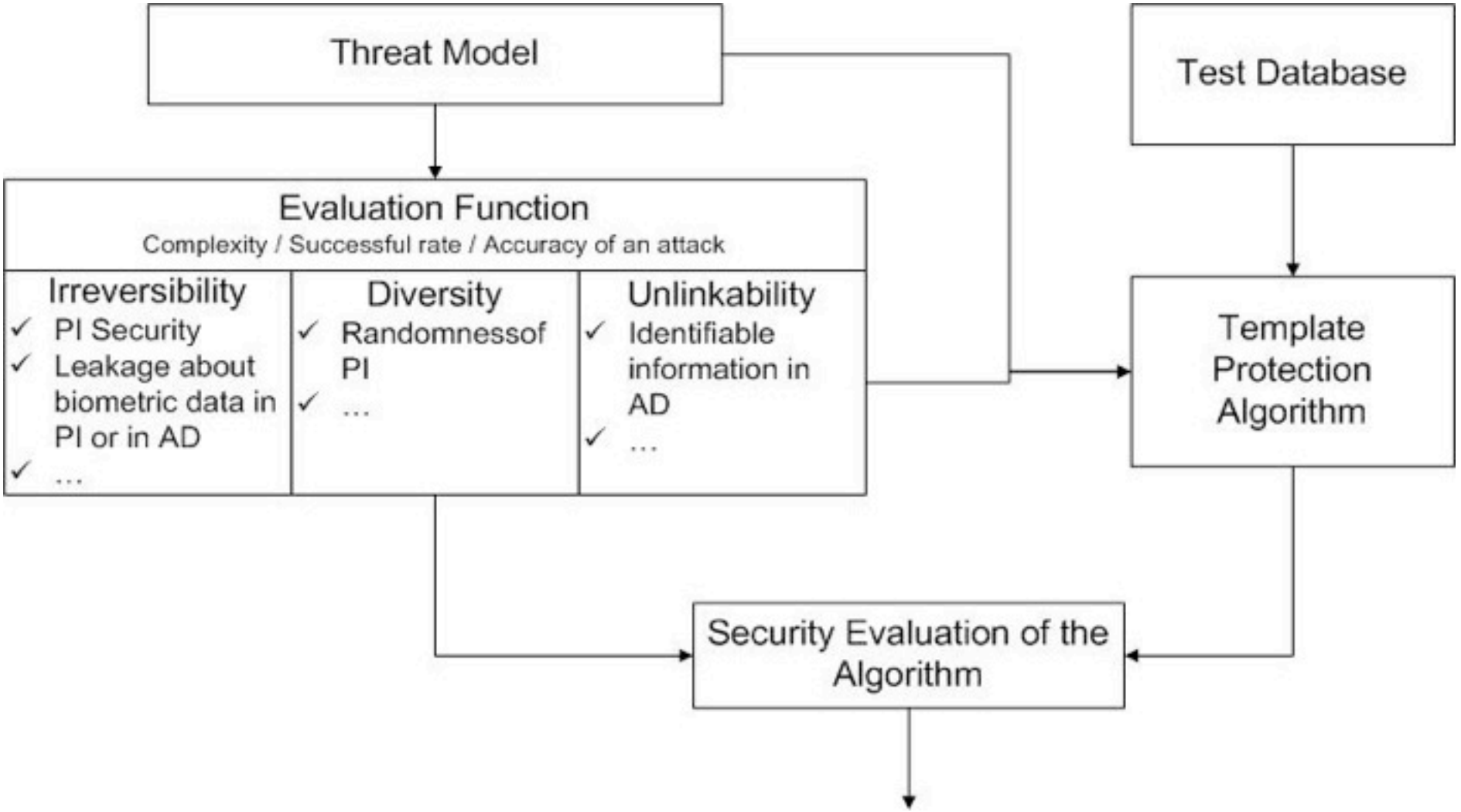
Generisches biometrisches System



Angriffsmodelle (AM)

- AM1 – Speicher
  - Das geschützte Template ist bekannt
- AM2 – Signalverarbeitung
  - Kerkhoff-Prinzip: Template Protection Verfahren ist öffentlich
    - Verknüpfung
      - Gespeicherte geschützte Templates ein und derselben Person sind aus unterschiedlichen Datenbanken bekannt
    - Systemparameter sind bekannt
    - (Geheime) Ergänzungsdaten (Supplementary Data – SD) sind bekannt
    - Die statistischen Eigenschaften der biometrischen Daten sind bekannt
- AM3 – Entscheidung
  - Eine umfangreiche biometrische Datenbank ist verfügbar

Evaluierungsframework



Evaluierungsframework

- Aufgaben des Evaluierungsframworks
  - Alle Anforderungen an Template Protection müssen mit geeigneten Evaluierungsfunktionen quantisiert werden
  - Aus Sicherheits- und Datenschutzsicht muss die Ableitung biometrischer limitiert werden
    - auf die Hilfsdaten (AD) des geschützten Templates in biometrischen Kryptosystemen
    - selbst dann, wenn unterstützende Daten (SD) des Transformationsalgorithmus kompromittiert werden
  - Es ist notwendig, Lücken im Privatsphärenschutz von geschützten Templates zu messen, inkl. Rekonstruktionsmöglichkeiten biometrischer Daten.
    - Gefahr der Verknüpfung

Fraunhofer
IGD

Alexander Nouak
Dipl. Informationsw. (FH), Dipl. Betriebsw. (FH)

Abteilungsleiter
Identifikation und Biometrie
Fraunhofer-Institut für Graphische Datenverarbeitung IGD

Fraunhoferstraße 5 · 64283 Darmstadt
Telefon +49 6151 155-147 · Fax -499
alexander.nouak@igd.fraunhofer.de