IT Sicherheit: Authentifikation

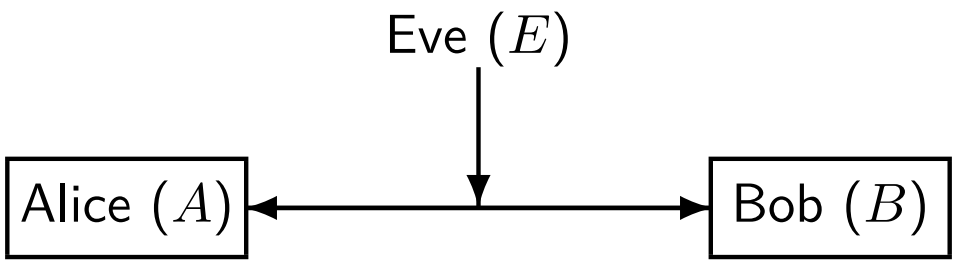
Dr. Christian Rathgeb

Hochschule Darmstadt, ATHENE, da/sec Security Group

11.06.2020

Authentisierung: Einführung I

- B (Prüfer) kann die Identität von A (Beweisender) zweifelsfrei feststellen
- Angreifer E versucht, Identität von A zu übernehmen



Feststellung der Identität z.B. über:

- eindeutige Merkmale
- charakteristische Eigenschaften

Authentisierung: Einführung II

Grundlage für alle kryptographischen Verfahren:

- Mit wem führe ich einen Schlüsselaustausch durch (vgl. Man-in-the-Middle-Angriff)
- Wem schicke ich vertrauliche Nachrichten
- Wer schickt mir vertrauliche Nachrichten
- Wer hat eine Nachricht signiert

Authentisierung: Einführung III

Faktoren für die Überprüfung:

- Wissen (z.B. ein Passwort, eine PIN)
- Besitz (z.B. ein Schlüssel in einer Chipkarte)
- Eigenschaften (z.B. ein biometrisches Merkmal)

$n-$Faktor-Authentisierung:

- 1-Faktor-Authentisierung: Nutzt nur einen Faktor
  z.B. Abrufen von E-Mails: Benutzername/Passwort (Wissen)
- 2-Faktor-Authentisierung: Nutzt zwei verschiedene Faktoren
  z.B. Auszahlung am Geldautomaten: Bankkarte (Besitz) und PIN (Wissen)

Passwörter

Typisches Beispiel: Benutzername/Passwort

- Anmeldung am Client
- Anmeldung an Webdiensten (E-Mail, Forum, Online-Banking)

Nachteile: Anfällig gegen

- Ausspähen (z.B. über Phishing, Keylogging, Abhören der Verbindung)
  Replay-Attacken: Abhören der Verbindung und Wiedereinspielen
- Man-in-the-Middle Attacken

Replay Angriffe

Der Angreifer E schleust eine bereits gesendete Nachricht in das Protokoll ein:

- Das Übermitteln des Geheimnisses geschieht offen/verschlüsselt
- Ein Angreifer kann damit das Geheimnis abhören und wieder einspielen
- Verschlüsselung schützt nicht vor Replay-Angriffen
- Statische Daten können von einem Angreifer E auch verwendet werden, selbst wenn er diese nicht interpretieren kann

Einmalpasswörter

Verbesserung: Einmalpasswörter

- Jedes Passwort wird nur einmal verwendet
- Verhindert somit Replay-Attacken

Problem: Beide Seiten müssen die Passwörter kennen
Zwei Möglichkeiten:

- Passwortlisten
- Passwortgeneratoren

Einmalpasswörter: Passwortlisten I

Typischer Anwendungsfall: Transaktionsnummern (TAN) im Online-Banking, z.B. zur Bestätigung von Überweisungen

- Beide Kommunikationspartner erhalten eine Liste mit Passwörtern
- Passwörter werden wie folgt verwendet:
  - Sequentielle Auswahl: von oben nach unten
  - Indizierte Auswahl: Prüfer gibt an, welches Passwort verwendet wird (z.B. Nummer in der Liste)

Einmalpasswörter: Passwortlisten II

Indizierte Auswahl ist ein Challenge-Response Protokoll:

$\boxed{B}$ Prüfer (Liste L)		$\boxed{A}$ Beweisender (Liste L)
wähle Index i		
(challenge)	$\xrightarrow{i}$	
		suche $i-$tes Passwort p_i
	$\xleftarrow{p_i}$	(response)
vergleiche		

Einmalpasswörter: Passwortgeneratoren

Ableitung verschiedener Passwörter aus einem vorab ausgetauschten Geheimnis g

Wir unterscheiden:

- zeitgesteuerte Generatoren
- ereignisgesteuerte Generatoren
- Challenge-Response-Generatoren

Zeitgesteuerte Generatoren

Hauptideen:

- Generierung der Einmalpasswörter aus
  - g (vorab ausgetauschtes Geheimnis) und
  - t (Zeitpunkt der Authentisierung)
- Beide Parteien (Prüfer und Beweisender) generieren das Einmalpasswort
- Prüfer vergleicht sein Einmalpasswort mit dem vom Beweisenden

Problem:

- Zeit beim Prüfer und Beweisenden nicht exakt gleich
- Man benötigt also einen Toleranzbereich (z.B. 30 Sekunden)

Zeitgesteuerte Generatoren

- key $= g$ (vorab ausgetauschtes Geheimnis)
- $t =$ time (in sec) (Zeitpunkt der Authentisierung)
- message $= t/30$ (Zeitintervall von 30 Sekunden)
- $p =$ mac(key, message) (Einmalpasswort für Zeit t)
  Message Authentication Codes (MAC), z.B. HMAC
- Beispiel: Google Authenticator

Ereignisgesteuerte Generatoren

Hauptideen:

- Generierung der Einmalpasswörter aus
  - g (vorab ausgetauschtes Geheimnis) und
  - t (Zähler, Anzahl der bereits durchgeführten Authentisierungen)
- Beide Parteien (Prüfer und Beweisender) generieren das Einmalpasswort
- Prüfer vergleicht sein Einmalpasswort mit dem vom Beweisenden

Ereignisgesteuerte Generatoren: Lamport-Hash I

Basiert auf einer kryptographischen Hashfunktion H

- g (vorab ausgetauschtes Geheimnis)
- Zufallszahl r (muss nicht geheim gehalten werden)
- Startwert $S = H(r||g)$
- Generierung der Einmalpasswörter:
  - Erstes Passwort: $p_1 = H^N(S)$ (N mal Anwenden von H)
  - Zweites Passwort: $p_2 = H^{N-1}(S)$ ($N-1$ mal Anwenden von H)
  - $t-$tes Passwort: $p_t = H^{N-(t-1)}(S)$

Ereignisgesteuerte Generatoren: Lamport-Hash II

- Aus $p_t = H^{N-(t-1)}(S)$ lässt sich nicht $p_{t+1} = H^{N-(t-2)}(S)$ berechnen
  $H^{N-(t-1)}(S) \mapsto H^{N-(t-2)}(S)$ ist die Umkehrung von H auf $H^{N-(t-1)}(S)$

Problem: Irgendwann wurden N Passwörter erzeugt

- Reinitialisierung: Wähle einen neuen Zufallswert r
- Bilde neuen Startwert $S = H(r||g)$

Challenge-Response gesteuerte Verfahren

z.B. auf Basis von Message Authentication Codes
Vorab ausgetauschtes Geheimnis: Der symmetrische Schlüssel k

B (Prüfer) Schlüssel: k		A (Beweisender) Schlüssel: k
choose random c		
(challenge)	$\xrightarrow{c}$	
		compute $r := \text{mac}(k, c)$
	$\xleftarrow{r}$	(Einmalpasswort, response)
compute $r' := \text{mac}(k, c)$		
if $r' = r$ then accept		
else reject		

Einmalpasswörter: Zusammenfassung

Vorteile:

- Sicher gegen passive Angriffe (Ausspähen): Jedes Mal ein neues Passwort
- Verfahren verhindert somit Replay-Attacken

Weiterhin möglich: Man-in-the-Middle-Angriff (aktiver Angriff)

- Angreifer E gibt sich als Prüfer B aus und erhält das Einmalpasswort von A
- E kann sich gegen über B als A ausgeben
- Verhinderung des Angriffs: Gegenseitige Authentisierung:
  - Nicht nur A muss sich gegenüber B authentisieren, sondern auch B gegenüber A

Faktor Besitz

- A (Beweisender) besitzt einen geheimen Schlüssel k
  - Für symmetrische Verfahren: Schlüssellänge ≥ 100 Bit
  - Für asymmetrisches Verfahren RSA: Schlüssellänge ≥ 4000 Bit
- Schlüssel ist irgendwo gespeichert
- Ziel: Sichere Speicherung des Schlüssels
  - Schlüssel soll von keinem Unbefugten ausgelesen werden können
  - Schlüssel soll von keinem Unbefugten genutzt werden können

Sicherheitselemente

Nutzung sicherer Hardware (Sicherheitschips)
Microprozessoren, die gege Angriffe geschützt sind, z.B. gegen

- physikalische Attacken (bohren, fräsen, ...)
- elektrische Angriffe (mehr Strom, als Spezifikation erlaubt)
- Angriffe mit Licht und Laser

Detektoren erkennen Angriffe, Schlüsselspeicher wird gelöscht

2-Faktor-Authentisierung

2-Faktor-Authentisierung basierend auf

- Besitz (Sicherheitselement) und
- Wissen (PIN)

Umsetzung

- Speicherung von Schlüssel und PIN im nicht-auslesbaren Bereich des Chips
- Authentisierung:
  - über Challenge-Response Verfahren
  - Nutzung des Schlüssels wird über PIN freigegeben

2-Faktor-Authentisierung

Anwendungsbeispiele:

- Bankkarten (Geldabheben an Bankautomaten)
- Kreditkarten (Bezahlen am Point of Sale)
- Personalausweis (Authentisieren mit der Online-Ausweisfunktion)

Überblick

- Eigenschaften biometrischer Verfahren
- Grundlagen biometrischer Verfahren
- Biometrische Charakteristika und Sensoren
- Merkmalsextraktion
- Biometrische Vergleichsverfahren
- Biometrische Erkennungsleistung
- Schutz biometrischer Daten
- Alterungsprozesse und Biometrie

Einführung

Was ist Biometrie?

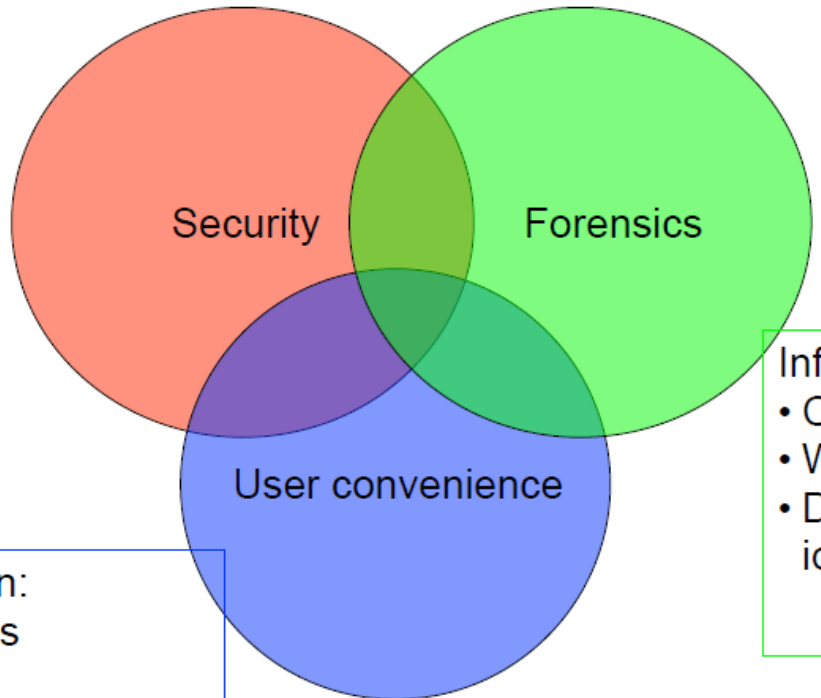
- Die Beobachtung und Messung von Charakteristika des menschlichen Körpers zum Zwecke der (Wieder-)Erkennung
- ISO/IEC Definition des Begriffs: **biometrics** *"Automated recognition of individuals based on their behavioral and biological characteristics."*

Einführung II

Anwendungsbereiche Biometrischer Verfahren:

Access control:
- information
- devices / token ownership
- locations

Immigration / Border Control



Information retrieval
- Camera surveillance
- Watch lists
- Disaster victim identification

Personalization:
- home systems
- computers
- social inclusion

Ease of use:
- no PINS/tokens
- ongoing authentication

Einführung III

Eine Authentisierung kann erreicht werden:

- durch Wissen: Password, PIN, ...
- durch Besitz: SmartCard, USB-token, ...
- durch Biometrie: Charakteristik des menschl. Körpers

Wissen oder Besitz kann man leicht verlieren,vergessen oder weitergeben, biometrische Charakteristika nicht ohne weiteres!

- Delegation, Abstreiten, etc. wird erschwert.
- Sicherheitslevel ist nicht abhängig vom Benutzer!

Grundlagen I

Generische Funktionsweise:

- Die biometrische Charakteristik des Benutzers wird aufgezeichnet und gespeichert (Enrolment).
- Der Benutzer wird dem System quasi vorgestellt.
- Beim Authentisierungsversuch wird die Charakteristik wiederum aufgenommen und mit der gespeicherten Referenz verglichen (Authentication).
- Wird ein festgelegter Schwellwert überschritten, gilt der Benutzer als authentisiert.

Grundlagen II

Identifikation vs. Verifikation:

- Identifikation: Erkenne die Identität einer Person ($1 : n$ - Vergleich).

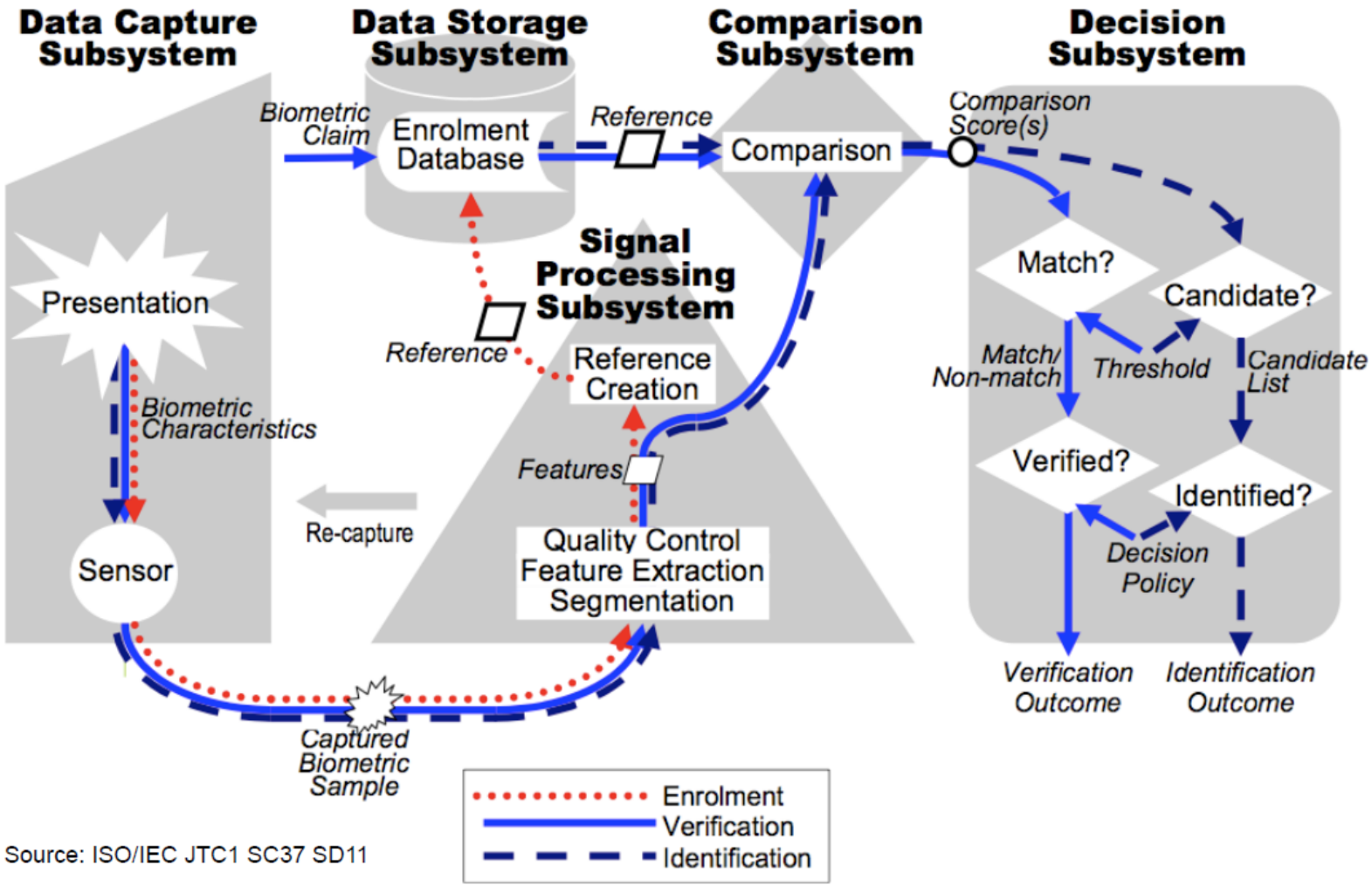
Mitarbeiter = Prof. Busch

- Verifikation: Validierung einer Identitätsbehauptung ($1 : 1$ - Vergleich)

Ähnlichkeit: „80%“

(Comparison-Score)

Grundlagen III



Biometrische Charakteristika

Wichtige Eigenschaften:

- *Verbreitung*: jede natürliche Person sollte die Char. haben
- *Einzigartigkeit*: die Char. ist unterschiedlich für jede Person
- *Beständigkeit*: die Char. verändert sich nicht mit der Zeit
- *Messbarkeit*: die Char. ist mit geringem Aufwand messbar
- *Performanz*: Erkennungsleistung und Geschwindigkeit
- *Akzeptabilität*: die Methode wird von der Zielgruppe angenommen
- *Sicherheit*: es ist schwer, ein Replikat der Char. zu erstellen

Wichtige Begriffe (ISO/IEC - Vokabular) I

- *Biometrisches Charakteristikum:*
  Biologisches oder verhaltensabhängiges Charakteristikum eines Individuum von welchem sich zur Unterscheidung verwendbare, reproduzierbare biometrische Merkmale ableiten lässt, die zum Zwecke der biometrischen Erkennungautomatischen Erkennung einsetzbar sind.
- *Biometrisches Sample:*
  analoge oder digitale Repräsentation biometrischer Charakteristika vor der biometrischen Merkmalssextraktion.
- *Biometrisches Merkmal:*
  Zahlen oder markante Kennzeichen die aus einem biometrischen Sample extrahiert wurden und zum Vergleich verwendet werden können.

Wichtige Begriffe (ISO/IEC - Vokabular) II

- *Biometrische Referenz:*
  eines oder mehrere gespeicherte biometrische Samples, biometrische Templates oder biometrische Modelle, die einer Person zugeordnet wurden und als Objekt zum biometrischen Vergleich verwendet werden.
- *Biometrisches Template:*
  Menge oder Vektor von gespeicherten biometrischen Merkmalen, die direkt vergleichbar zu den biometrischen Merkmalen einer biometrischen Probe.

Wichtige Begriffe (ISO/IEC - Vokabular) III

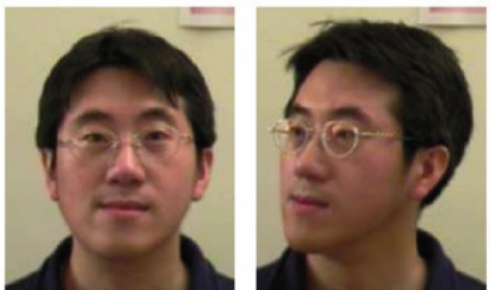
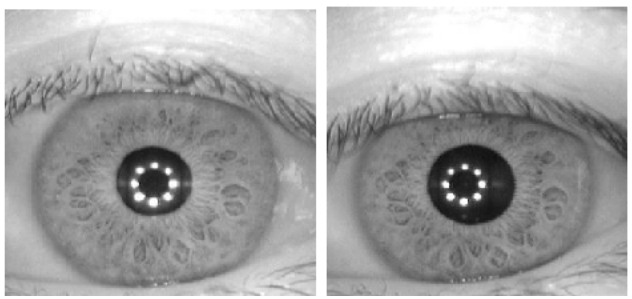
- *Biometrische Probe:*
  biometrische Samples oder biometrische Merkmale, die als Eingabe zu einem Algorithmus zum Vergleich mit einer biometrischen Referenz dienen
- *Biometrischer Vergleich:*
  Schätzung, Berechnung oder Messung der Ähnlichkeit oder Unterschiedlichkeit zwischen der biometrischen Probe und biometrischen Referenzen.

Wichtige Begriffe (ISO/IEC - Vokabular) IV

- *Merkmalsextraktion:*
  Vorgang, bei dem aus einem Sample ein Merkmalsvektor erzeugt wird.
- In der Enrolmentphase erzeugen wir ein Template (= Menge oder Vektor von gespeicherten biometrischen Merkmalen, die direkt vergleichbar zu den biometrischen Merkmalen einer biometrischen Probe)
- In der Wiedererkennungsphase erzeugen wir einen Proben-Merkmalsvektor.

Wichtige Begriffe (ISO/IEC - Vokabular) V

- Biometrische Charakteristika, zB Fingerabdruck, Iris, Gesicht, etc. erlauben jedoch keinen exakten Vergleich von Merkmals-Vektoren (Templates)

- Exakter Vergleich durch Intra-Klassen-Varianz unmöglich!
- Passwörter oder PINs erlauben einen exakten Vergleich.

Wichtige Begriffe (ISO/IEC - Vokabular) VI

- *Vergleichswert (engl. comparison score):*
  Numerischer Wert oder auch Menge mehrerer Werte, die das Resultat eines Vergleichs sind.
- *Ähnlichkeitswert (similarity score):*
  Vergleichswert, der mit der Ähnlichkeit ansteigt
- *Distanzwert / Abweichungswert (engl. dissimilarity score):*
  Vergleichswert, der sich bei Ähnlichkeit verringert

In biometrischen Systemen wird anhand eines Vergleichswertes eine binäre Entscheidung (Accept/Reject) getroffen!

Bewertung Biometrie

Schwächen der Biometrie:

- Steigerung der Sicherheit bedingt Steigerung der Komplexität
- Unscharfes Ergebnis (Schwellwerte notwendig)
- Erneuerung der biometrischen Daten ist nicht möglich
- Angriffe auf den Sensor:



Biometrische Charakteristika:

Biologische Charakteristika:

- Fingerabdruck
- Gesicht
- Iris
- Venen
- Handgeometrie
- Handflächenabdruck
- Ohren
- DNA

Verhaltensbasierte Charakteristika:

- Tippverhalten
- Unterschrift
- Stimme
- Gang

Gesichtserkennung I

Motivation - Vergleich mit anderen Verfahren:

- Gesicht ist das Charakteristikum mit der größten Verbreitung
- potentiell hohe Benutzerakzeptanz (Bedienbarkeit)
- Erfassung erfolgt berührungslos
  (kein Eingabegerät erforderlich - Kameras sind Massenware)
- Anatomischer Einfluss:
  - Knochengerüst
  - Gesichtsmuskulatur
  - Faltenwurf
  - Haut-Textur
  - Haarwuchs

Gesichtserkennung II

Applikationen:

- Man findet Gesichtserkennung in verschiedenen Kategorien von Applikationen
- Beispiele: Entsperren von Smartphones, Grenzkontrolle, Überwachung



Gesichtserkennung III

Herausforderungen:

- Pose:
  - Orientation der Person zur Kamera
  - Abstand der Person zur Kamera
- Beleuchtung:
  - Sonnenlicht, wechselnde Umweltbedingungen
  - seitlicher Schattenwurf
- Ausdruck and andere Variationen:
  - emotionale Ausdrücke
  - Alterung etc.

Gesichtserkennung IV

Weitere Herausforderungen:

- Alterungsprozesse (im Gesicht sind stark heterogen)




- Medizinische Eingriffe (zB. Augenlidstraffung)

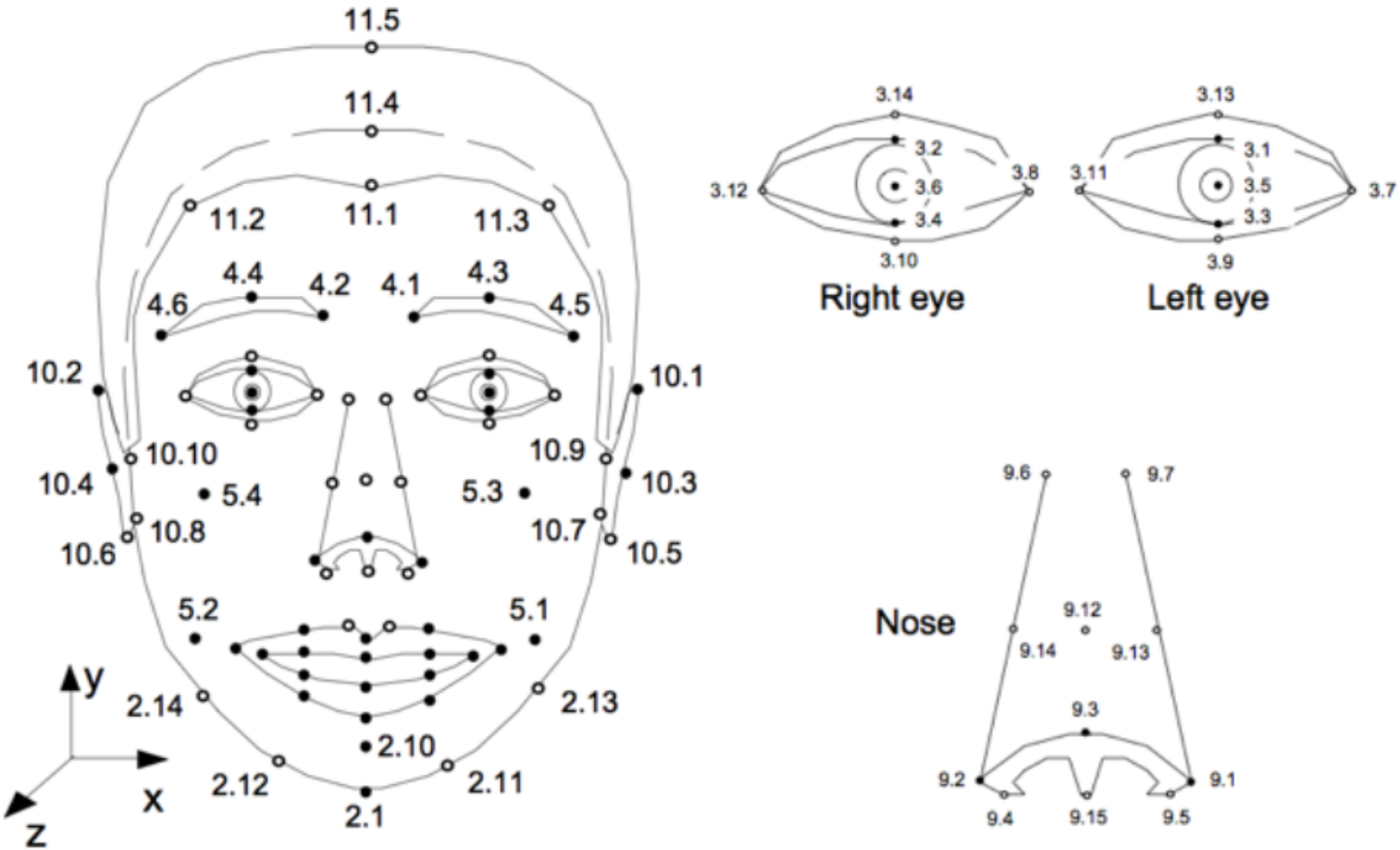

Gesichtserkennung V

Verarbeitungsschritte:

- Segmentierung des Gesichts
  - Bildbereich des Gesichts bestimmen
- Detektion der Landmarken
  - z.B. Innen- und Ausseneckpunkte von Augen oder Mund
- Berechnung von Merkmalen
  - für das gesamte segmentierte Gesicht oder Texturfenster um die Landmarken
- Vergleich zwischen
  - dem berechneten Merkmalsvektor aus dem Probenbild und dem hinterlegten Merkmalsvektor aus dem Referenzbild
  - Ergebnis ist ein Vergleichswert

Gesichtserkennung VI

Landmarken in der Gesichtserkennung:



Source: ISO/IEC 19794-5:2011

Gesichtserkennung VII

Merkmalsextraktion - Gesichtsbilder:

Grundsätzlich unterscheidet man zwei Ansätze.

1. *Holistisch*:
   das gesamte Gesichtsbild wird verarbeitet
   (z.B. Local Binary Patterns)
2. *Landmarken-basiert*:
   im Gesicht detektieren Texturfenster an der Landmarke
   beschreiben das lokale Muster

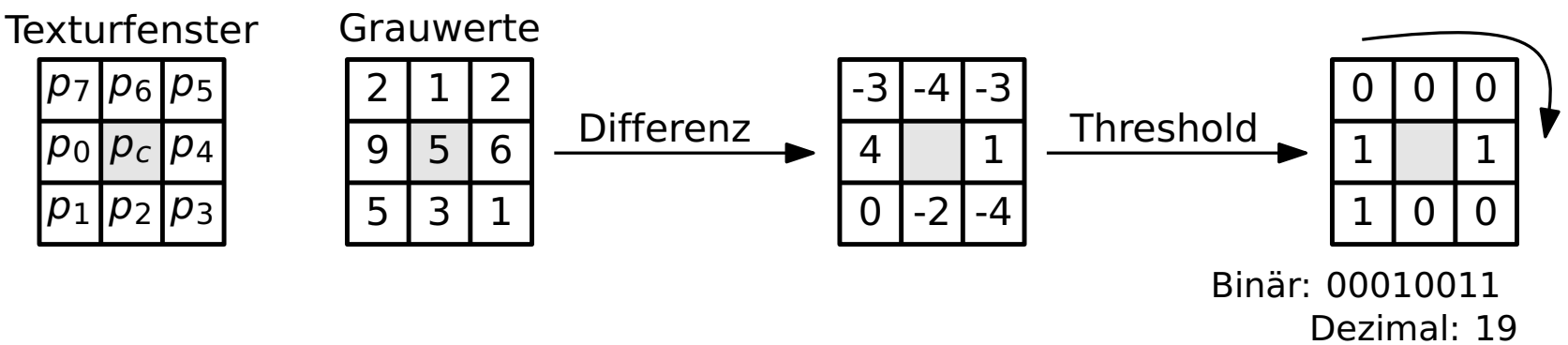
Gesichtserkennung VIII

Merkmalsextraktion - Local Binary Patterns:

Der Wert eines LBP-codes für ein Pixel $P = (x_c, y_c)$ ist definiert als,

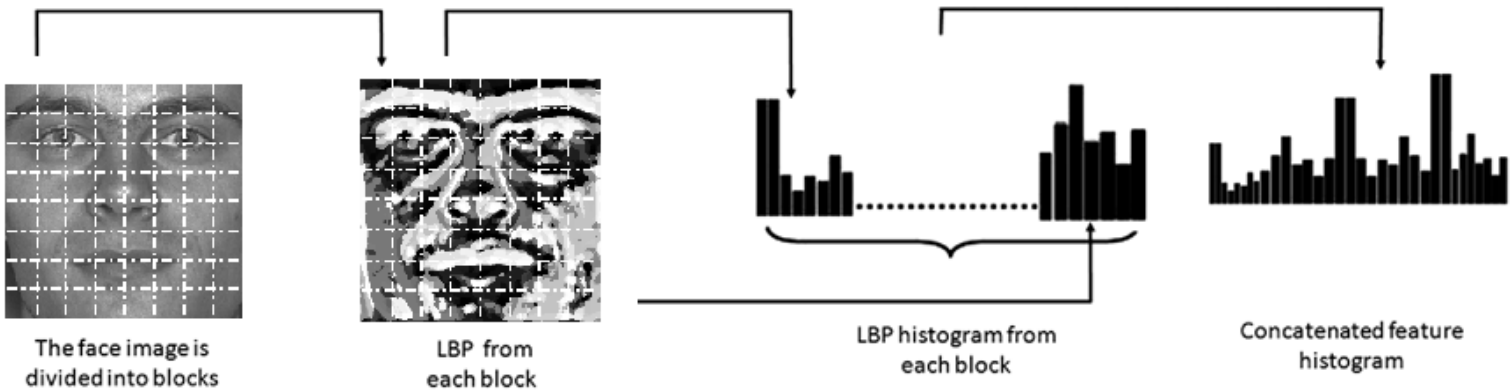
$$LBP_P = \sum_{i=0}^{7} sign(p_i - p_c) * 2^i$$

$$sign(x) = \begin{cases} 1, \text{wenn } x \geq 0 \\ 0, \text{sonst.} \end{cases}$$



Gesichtserkennung IX

Merkmalsextraktion - Local Binary Patterns:



- Zwei Histogamme $A = (a_1, \ldots, a_n)$ und $B = (b_1, \ldots, b_n)$ können mittels χ^2-Distanz ("Chi-Square") verglichen werden:

$$\chi^2(A, B) = \sum_{i=1}^{n} \frac{(a_i - b_i)^2}{a_i + b_i}$$

- Dh. es wird ein Distanzwert berechnet.

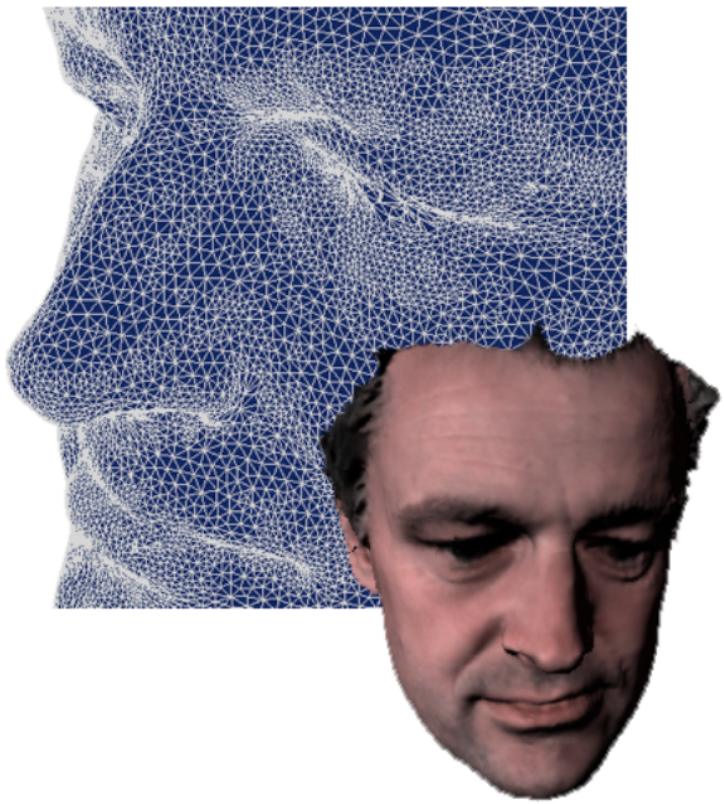
Gesichtserkennung X

Durchbruch in 2015 durch Google:

- Deep-Learning "FaceNet" Algorithmus von Google reduzierte Fehlerraten bei der gesichtserkennung um ca. 30%.
- Algorithmus basierend auf maschinellen Lernen mit neuronalem Netz (Convolutional Neural Net) bestehend aus 22 Schichten und 140 Millionen Parametern (!)
- Training: 2000 Stunden auf 200 Million Gesichtsbildern von 8 Millionen Personen.

Gesichtserkennung XI

2D vs. 3D Gesichtserkennung:



- 3D-Gesichtserkennung ist robuster gegen Angriffe!

Biometrische Erkennungsleistung I

Biometrische Verfahren arbeiten nicht fehlerfrei!

- Die Erkennungsleistung (engl. Biometric performance) wird in Fehlerwahrscheinlichkeiten (error rates) formuliert.
- Man unterscheidet zwischen sogenannten Algorithmenfehler und Systemfehler.

Biometrische Erkennungsleistung I

Es können zwei Arten von Algorithmenfehler auftreten:

- *False Match (FM)*: Vergleichsentscheidung hinsichtlich einer Übereinstimmung einer biometrischen Probe und einer biometrischen Referenz, die von verschiedenen erfassten Betroffenen Personen stammen.
- *False Non Match (FNM)*: Vergleichsentscheidung hinsichtlich einer Nicht-Übereinstimmung einer biometrischen Probe und einer biometrischen Referenz, die von der selben zu erfassenden Betroffenen Person und von dem selben biometrischen Charakteristikum stammen.

Biometrische Erkennungsleistung II

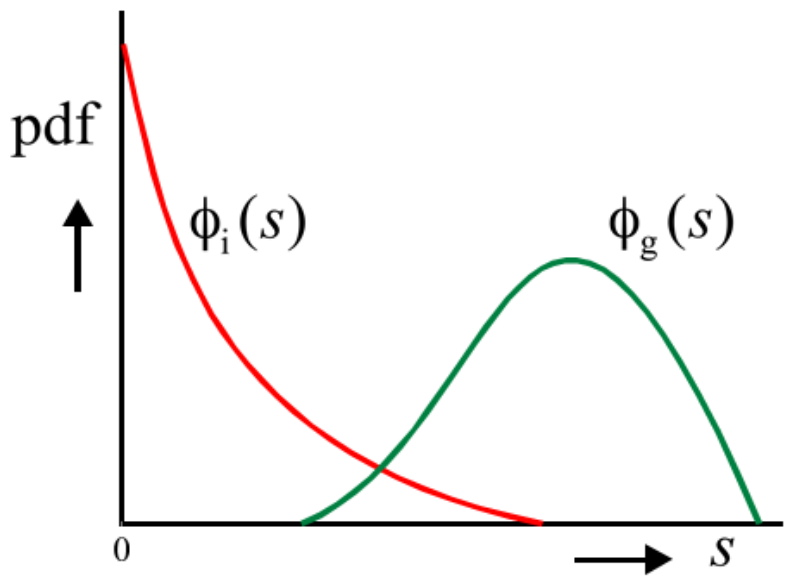
Evaluierung von Algorithmenfehler:

- Zur Abschätzung der Algorithmenfehler sind für jedes Individuum pro biometrischer Instanz ≥ 2 Sample vorliegen.
- Zwei Arten von Vergleichen werden durchgeführt:

1. *Genuine Vergleich* - engl. mated comparison trial: Vergleich einer biometrischen Probe und einer biometrischen Referenz von ein und derselben Betroffenen Person und derselben biometrischen Charakteristik als Teil eines Test der Erkennungsleistung.
2. *Imposter Vergleich* - engl. non-mated comparison trial: Vergleich von einer biometrischen Probe und einer biometrischen Referenz von unterschiedlichen Betroffenen Personen als Teil eines Test der Erkennungsleistung.

Biometrische Erkennungsleistung III

- Aus Genuine und Impostor Vergleichen ergeben sich zwei Wahrscheinlichkeitsdichtefunktionen (engl. Probability densitiy Distribution Function):
- $\Phi_g(s)$: PDF der Genuine Ähnlichkeitswerte s
- $\Phi_i(s)$: PDF der Impostor Ähnlichkeitswerte s

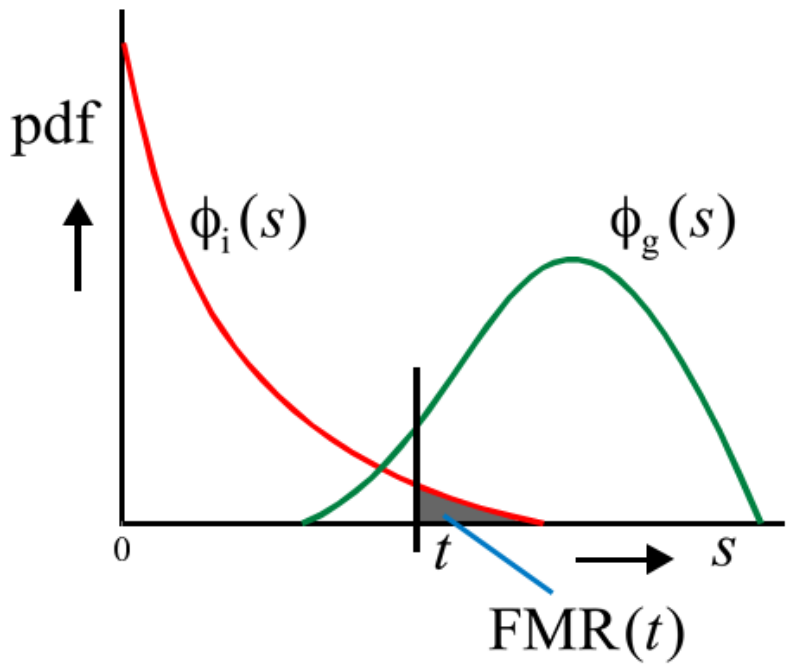


Biometrische Erkennungsleistung IV

- Die Wahrscheinlichkeit für beide Arten von Algorithmenfehler (*False Match* und *False Non Match* werden zu einem definieretn Schwellwert t evaluiert.
- Abhängig von der Wahl von t ändern sich die Wahrscheinlichkeiten für die jeweiligen Algorithmenfehler.
- In den meisten Fällen hat eine Senkung der einen Fehlerwahrscheinlichkeit eine Steigung der Anderen zur Folge (und umgekehrt).
- Der Schwellwert t sollten abhängig von der Applikation (und ihrer Sicherheitsanforderung) gesetzt werden.

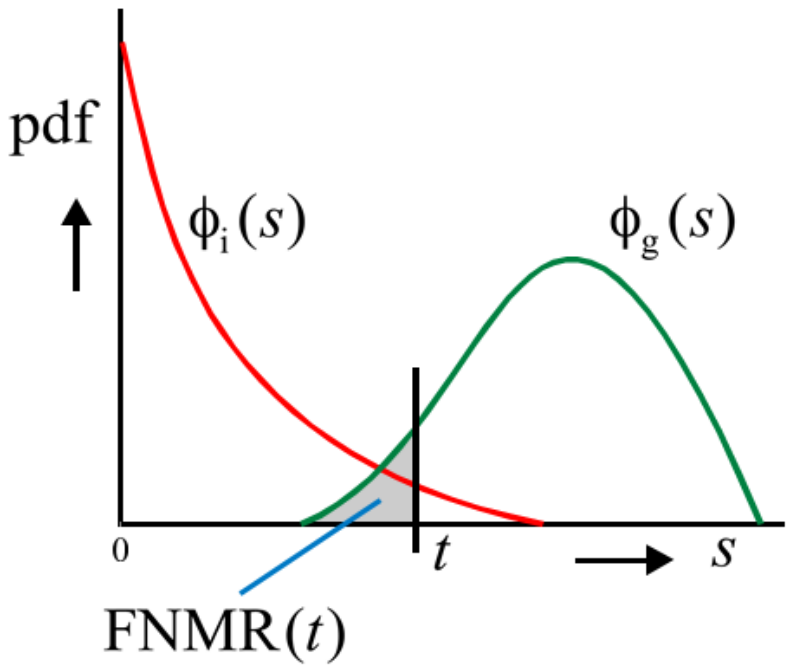
Biometrische Erkennungsleistung V

- *False Match Rate (FMR)*: Anteil der abgeschlossenen biometrischen Übereinstimmungsprüfungen von nicht-gepaarten Teilen, die zu einer Falschübereinstimmung führen.
- $FMR(t) = \int_t^1 \Phi_i(s)ds$



Biometrische Erkennungsleistung VI

- *False Non-Match Rate (FNMR)*: Anteil der abgeschlossenen biometrischen Übereinstimmungsprüfungen von gepaarten Teilen, die zu einer Falschnichtübereinstimmung führen.
- $FNMR(t) = \int_0^t \Phi_g(s)ds$



Biometrische Erkennungsleistung VII

- FNMR ist Maß für die Benutzbarkeit (Usability) eines biometrischen Systems.
- FMR ist Maß für die Sicherheit eines biometrischen Systems.
- In einem Biometrischen System werden Schlüssel durch biometrische Charakteristika ersetzt!
- In der Kryptographie wird die Sicherheit in Bits gemessen.
- Frage: eine FMR von 0.1% entspricht wieviel Bits Sicherheit?

Biometrische Erkennungsleistung VII

- FNMR ist Maß für die Benutzbarkeit (Usability) eines biometrischen Systems.
- FMR ist Maß für die Sicherheit eines biometrischen Systems.
- In einem Biometrischen System werden Schlüssel durch biometrische Charakteristika ersetzt!
- In der Kryptographie wird die Sicherheit in Bits gemessen.
- Frage: eine FMR von 0.1% entspricht wieviel Bits Sicherheit?
- FMR $= 0.1\%$ entspricht $\log_2(100/0.1) \simeq 10$ Bits Sicherheit
- Das gilt jedoch nur für Verifikation (1:1 Vergleich)!

Biometrische Erkennungsleistung VIII

- Wird ein biometrisches System im Identifikationsmodus betrieben muss die FMR noch niedriger sein.
- Sei P_1 die Wahrscheinlichkeit für ein FM in einer Verifikation und P_N die Wahrscheinlichkeit für ein FM in einer Identifikation (1:N Vergleich).
- Die Wahrscheinlichkeit, dass in einem Vergleich kein FM auftritt ist somit $(1 - P_1)$.
- Die Wahrscheinlichkeit, dass bei N unabhängigen Vergleichen kein FM auftritt ist somit $(1 - P_1)^N$.
- Somit ergibt $P_N = 1 - (1 - P_1)^N$.

Biometrische Erkennungsleistung IX

Beispiel:

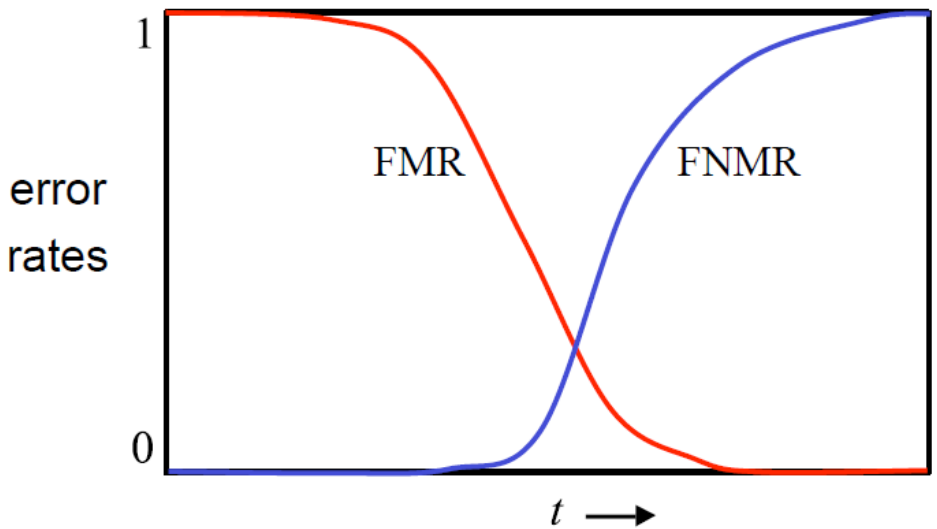
- Angenommen ein System hat eine FMR von 0.1%.
- Wahrscheinlichkeit für ein FM in Abhängigkeit von N:

$$N = 200 \rightarrow P_N \simeq 18\%$$
$$N = 2000 \rightarrow P_N \simeq 86\%$$
$$N = 10000 \rightarrow P_N = 99.995\%$$

- Identifikation ermöglichen biometrische Systeme nur wenn diese bei sehr niedriger FMR ($P_1 \ll 1/N \ll 1$) betrieben werden!
- Gesichtserkennung wird meist für FMR=0.1% durchgeführt, FaceNet: FNMR $< 5\%$.

Biometrische Erkennungsleistung X

- FMR und FNMR können als Funktion dargestellt werden.



- Rahmenbedingungen: $FMR(0) = 1$, $FNMR(0) = 0$ und $FMR(1) = 0$, $FNMR(1) = 1$.
- Gleichfehlerrate (Equal Error Rate): EER and der Stelle $FNMR = FMR$.
- Genuine Match Rate: $GMR = 1 - FNMR$.

Biometrische Erkennungsleistung XI

Wir betrachten vier Arten von Systemfehlern:

1. Failure-to-Capture: “Es konnte kein Sample erzeugt werden”.
2. Failure-to-eXtract: “Es konnte aus dem Sample kein Template erzeugt werden”.
3. Failure-to-Acquire: Ursache kann in der Erfassung (Failure-to-Capture) oder in der Verarbeitung (Failure-to-eXtract) liegen.
4. Failure-to-Enrol: “Für dieses Individuum kann niemals ein brauchbares Template erzeugt und gespeichert werden”.

Biometrische Erkennungsleistung XII

Wahrscheinlichkeit einer Erfassungsfehlfunktion,
Definition durch ISO/IEC:

"*Failure-to-Capture Rate (FTC)*: relativer Anteil der Akquisitionsfehler in einer spezifizierten Menge von biometrischen Akquisitionsprozessen."

$$FTC = \frac{N_{tca}+N_{nsq}}{N_{tot}}$$

- N_{tca}: die Anzahl der terminierten Erfassungsversuche.
- N_{nsq}: die Anzahl der erzeugten Samples in unzureichender Qualität.
- N_{tot}: die Anzahl der gesamten Erfassungsversuche.

Biometrische Erkennungsleistung XIII

Wahrscheinlichkeit einer Merkmalsextraktionsfehlers, Definition durch ISO/IEC:

"*Failure-to-eXtract Rate (FTX)*: relativer Anteil der Enrolmentfehler an einer spezifizierten Menge von Enrolmenttransaktionen."

$$FTX = \frac{N_{ngt}}{N_{sub}}$$

- N_{ngt}: die Anzahl der Versuche ist, in denen kein Template erzeugt werden konnte.
- N_{sub}: die Gesamtzahl der biometrischen Samples, auf welche die Merkmalsextraktion angewendet wurde.

Biometrische Erkennungsleistung XIV

Wahrscheinlichkeit einer Enrolmentfehlfunktion,
Definition durch ISO/IEC:

"*Failure-to-Enrol Rate (FTE)*: relativer Anteil der Enrolmentfehler an einer spezifizierten Menge von Enrolmenttransaktionen."

$$FTE = \frac{N_{nec}}{N}$$

- N_{nec}: die Anzahl der Enrolmentfehlfunktionen für Individuen, deren biometrische Charakteristika nicht erfasst werden können.
- N: die Gesamtzahl der natürlichen Personen, die in der Enrolmendatenbank aufgenommen werden sollen.

Biometrische Erkennungsleistung XV

Wahrscheinlichkeit einer Akquisitionsfehlfunktion, Definition durch ISO/IEC:

"*Failure-to-Acquire Rate (FTA)*: relativer Anteil der Akquisitionsfehler in einer spezifizierten Menge von biometrischen Akquisitionsprozessen."

$$FTA = FTC + FTX * (1 - FTC)$$

- Die Ursache eines Failure-to-Acquire kann in der Erfassung (Failure-to-Capture) oder in der Verarbeitung (Failure-to-eXtract) liegen.

Biometrische Erkennungsleistung XVI

- False-Accept-Rate (FAR):

$$FAR = FMR * (1 - FTA)$$

- False-Reject-Rate (FRR):

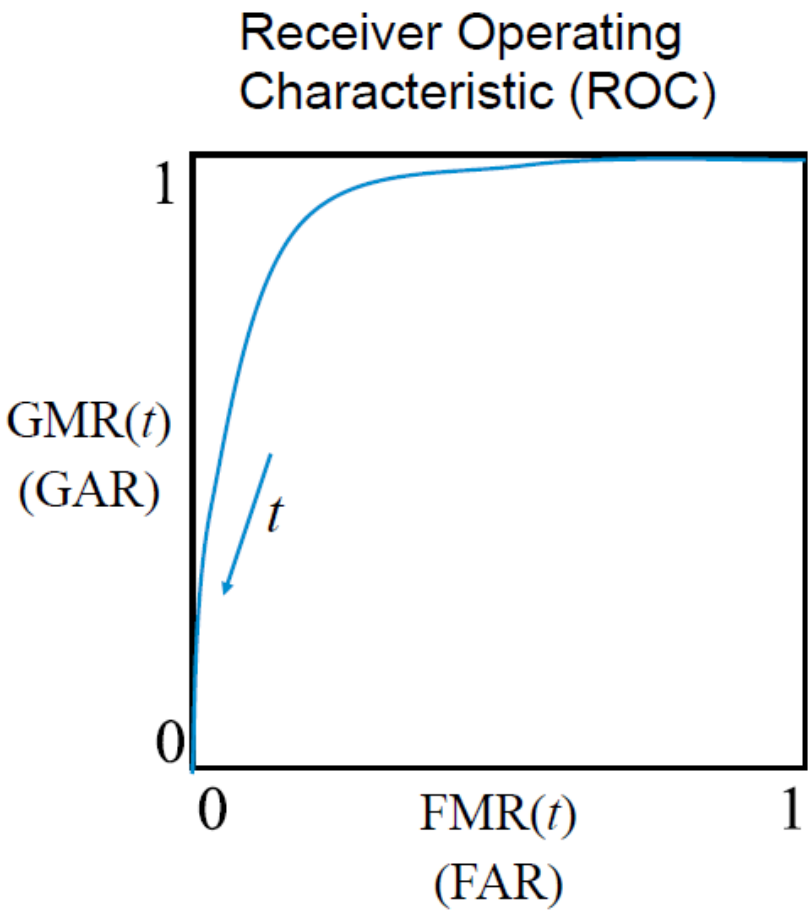
$$FRR = FTA + FNMR * (1 - FTA)$$

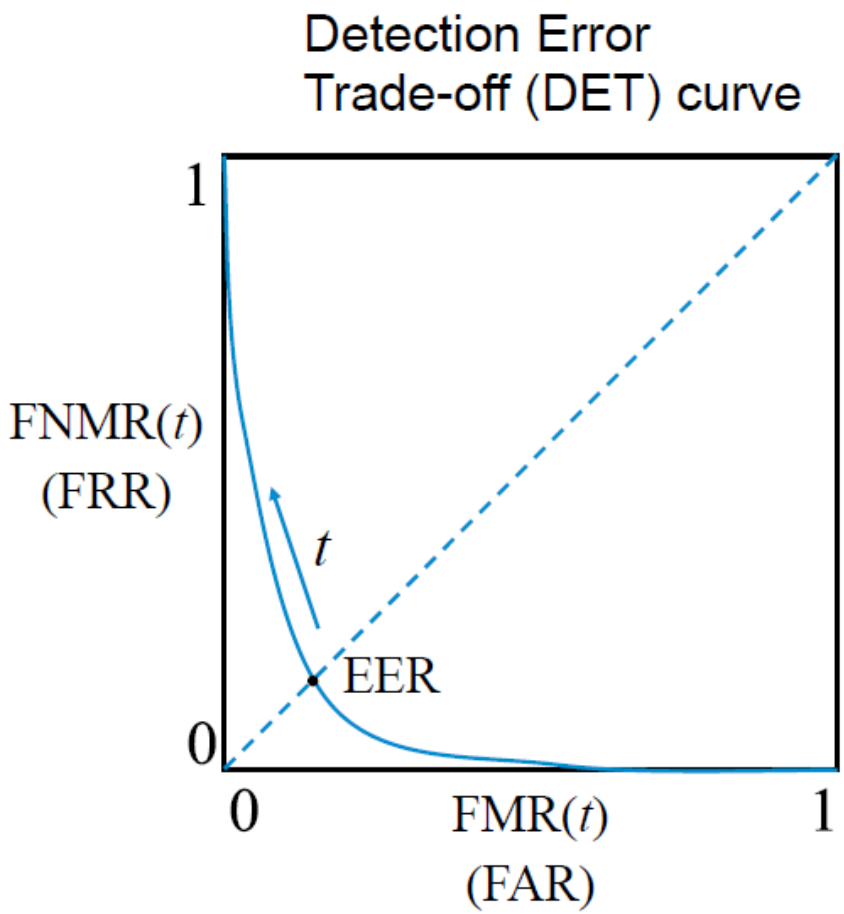
- Genuine-Accept-Rate (GAR):

$$GAR = 1 - FRR$$

Biometrische Erkennungsleistung XVII

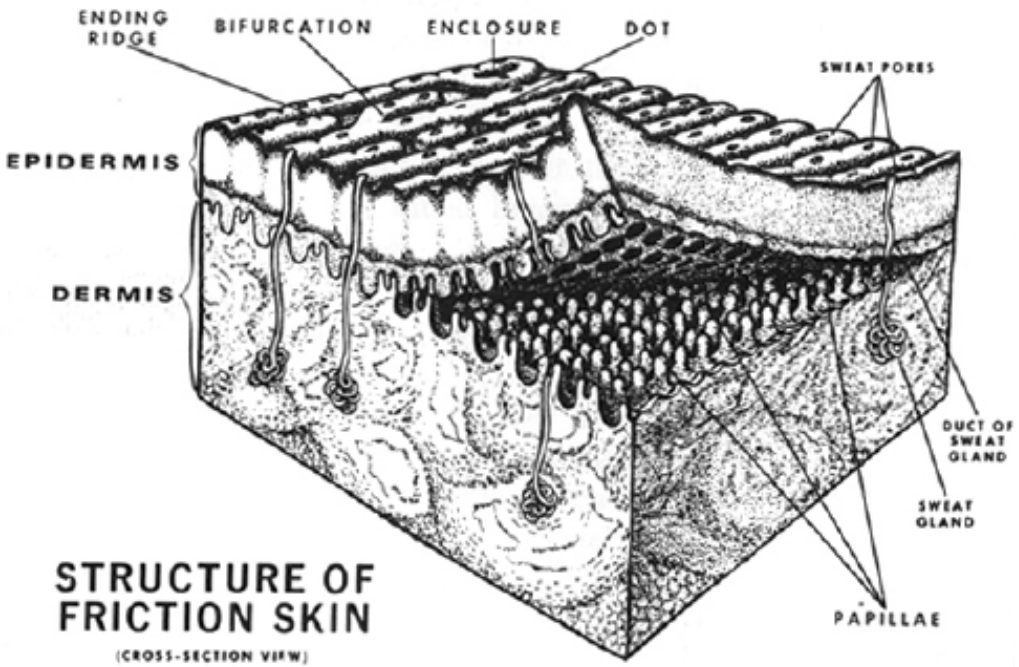
Graphische Darstellung Erkennungsleistung:





Fingerabdruckerkennung I

- Bildung der Papillarleisten zufällig
  (in den ersten Lebenswochen)
- Im Abdruck sind Papillarlinien erkennbar
- Muster bleibt konstant mit der Alterung



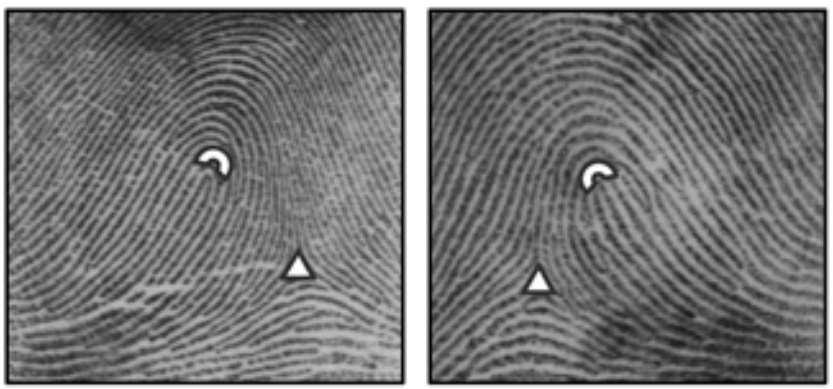
Fingerabdruckerkennung II

Linke Schleife - engl. Left Loop:

- Das Schleifenmuster enthält eine typische Delta Struktur
- Die Papillarlinien beginnen und enden links des Kerns

Rechte Schleife - engl. Right Loop:

- Das Schleifenmuster enthält eine typische Delta Struktur.
- Die Papillarlinien beginnen und enden rechts des Kerns.



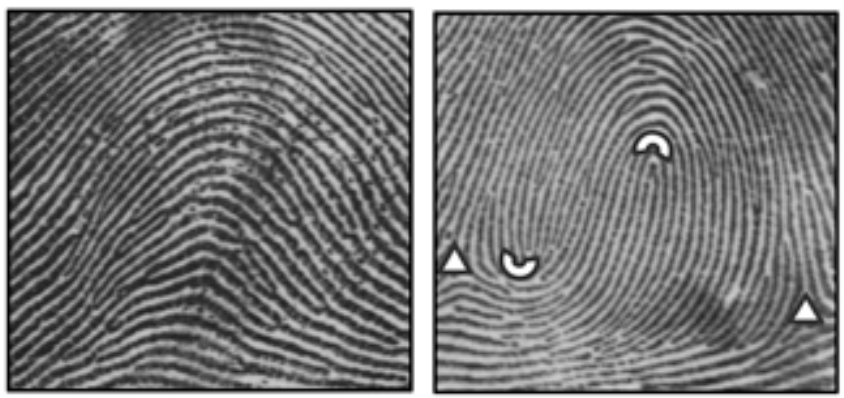
Fingerabdruckerkennung III

Bogen - engl. Arch:

- Das Grundmuster enthält keine Delta Struktur.
- Die Papillarlinien im Zentrum des Grundmusters sind nach oben gebogen. Sie verlaufen vom linken zum rechten Bildrand.

Wirbel - engl. Whorl:

- Das Grundmuster enhält zwei Delta Strukturen.
- Die Papillarlinien sind um den Kern geringelt.



Fingerabdruckerkennung IV

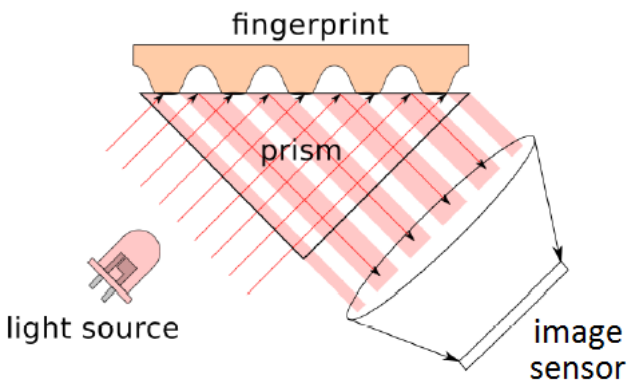
Analoge/digitale Repräsentation der Papillarleisten:

- Landmarken im Fingerbild werden als *Minutien* bezeichnet.

Fingerabdruckerkennung VI

Optische Sensoren:

- Finger liegt auf Oberfläche eines Prismas auf und wird mit einfarbigem Licht bestrahlt.
- Gute Bildqualität, aber große Bauart (Auflösung bis 1000 dpi).
- Total Internal Reflection (TIR), die Reflexion in den Kontaktbereichen wird unterdrückt.

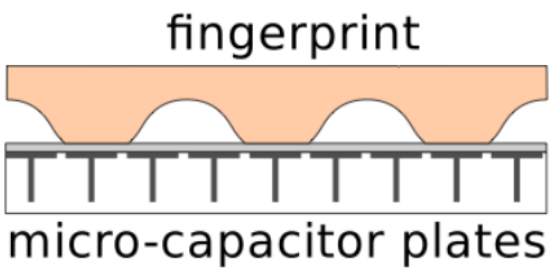


Source: Cross Match

Fingerabdruckerkennung VII

Kapazitive Sensoren:

- Raster von Kondensatorplatten als Sensorelemente.
- Messung der Leitfähigkeit an Hautoberfläche: Kapazität an aufliegenden Hautlinien größer.
- Umformung in digitale Signale.
- Klein und integrierbar, aber anfällig gegen elektr. Aufladung.

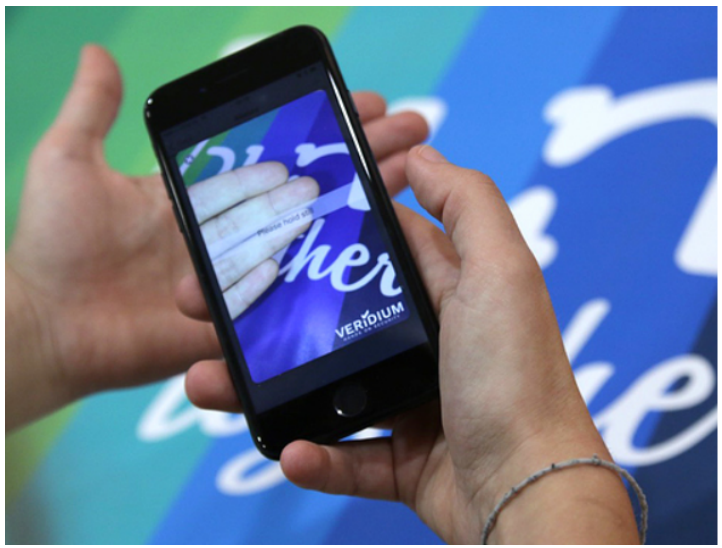


Kapazitiver Sensor von Infineon
Bildgröße: 224 x 288 Pixel
Sensor-Fläche: 11,3 mm x 14,3 mm

Fingerabdruckerkennung VIII

Kontaktlose Sensoren:

- Fotos von ein oder meherern Fingern gleichzeitig.
- Höhere Anfälligkeit gegen Angriffe.



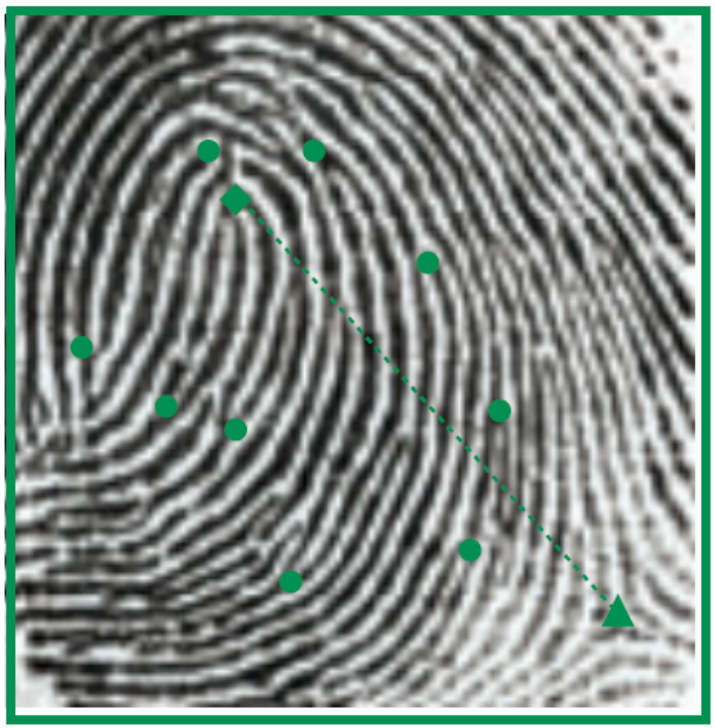
Fingerabdruckerkennung VIII

Kontaktlose Sensoren:

- Fotos von ein oder meherern Fingern gleichzeitig.
- Höhere Anfälligkeit gegen Angriffe.

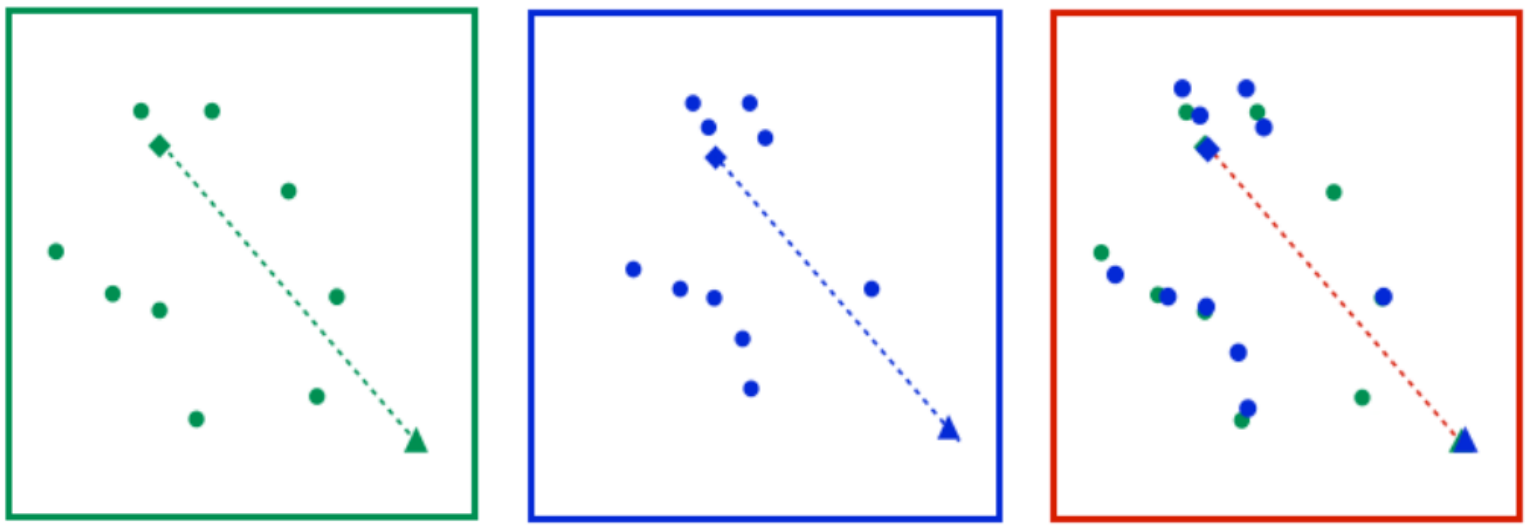
Fingerabdruckerkennung XII

Ausrichtung (engl. alignment) des Referenz Bild und des Probe Bild:



Fingerabdruckerkennung XIII

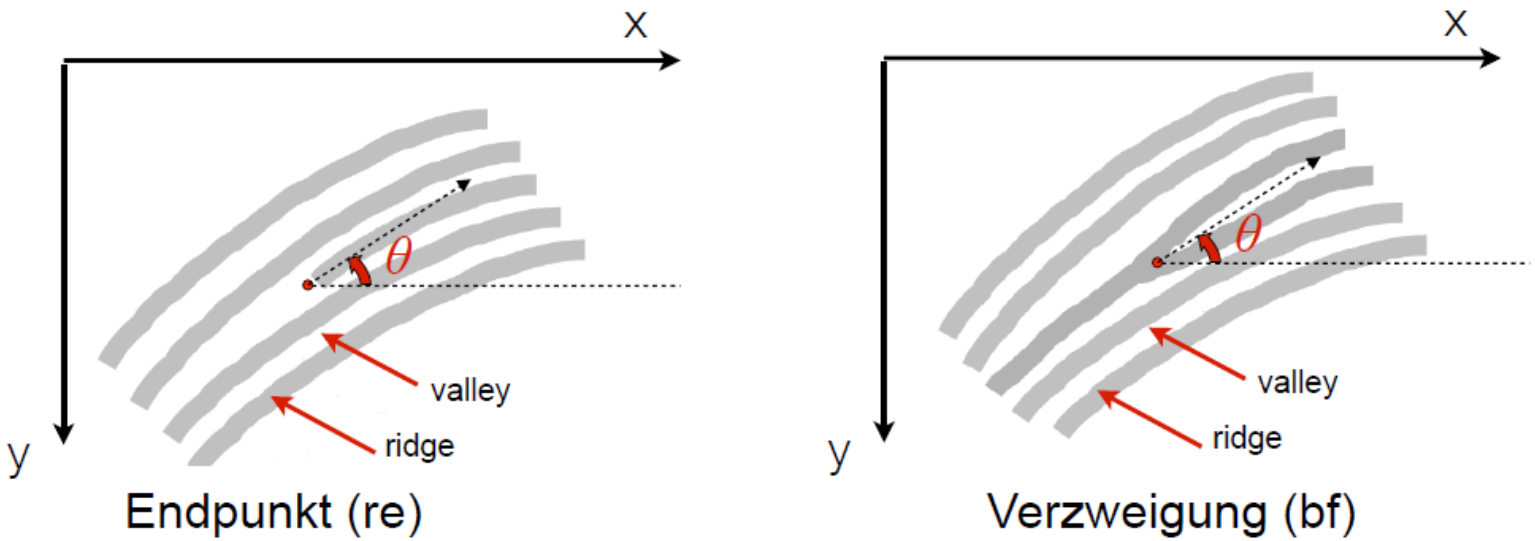
Vergleich des Referenz Bild mit dem Probe Bild:



- für wieviele Minutien-Punkte in der Probe lässt sich in der Referenz-Wolke ein passender Partner finden?

Fingerabdruckerkennung XIV

Suche nach einer korrespondierenden Minutien:



- Minutien wird definiert durch ein Tupel $m = \langle x, y, \theta, t \rangle \in \mathcal{M}$.
- Absolute Position: x, y
- Winkel: θ
- Minutien Typ: $t \in \{re, bf\}$

Fingerabdruckerkennung XV

Suche nach einer korrespondierenden Minutien:

- Für eine Referenz R und Probe Q werden zum Vergleich nur Koordniaten und Winkel verwendet.

$$R = \{m_1, m_2, \ldots, m_n\} \subseteq \mathcal{M}, m_i = \langle x_i, y_i, \theta_i \rangle \in R$$
$$Q = \{m'_1, m'_2, \ldots, m'_k\} \subseteq \mathcal{M}, m'_j = \langle x_j, y_j, \theta_j \rangle \in Q$$

  wobei n und k die Anzahl der Minutien R bzw. Q bezeichnen.

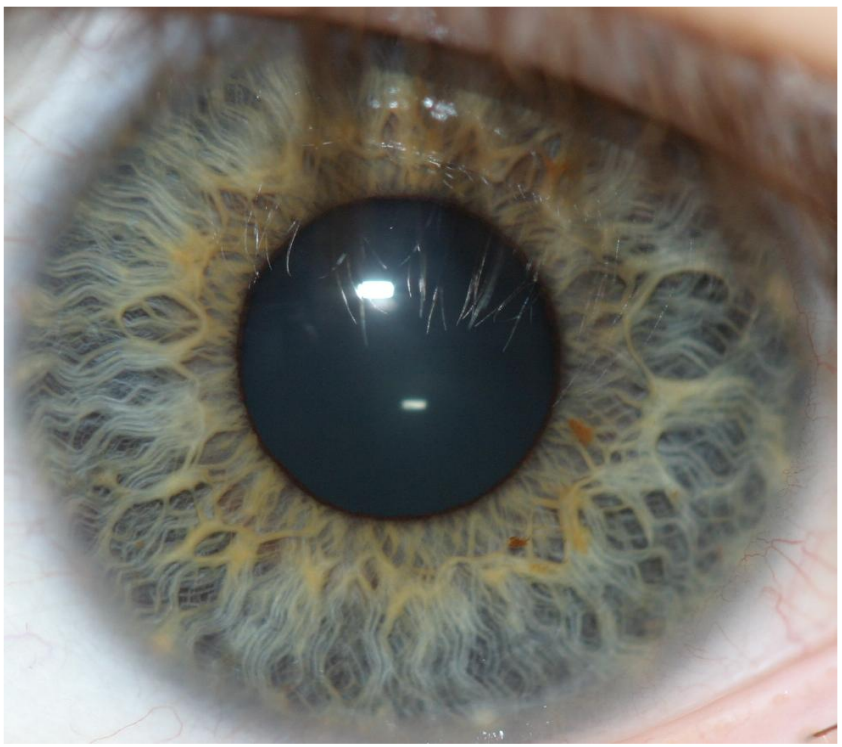
- 2 Minutien sind Partner, wenn die räumliche Differenz sd und die Differenz der Orientierungen dd innerhalb der Toleranz ist,

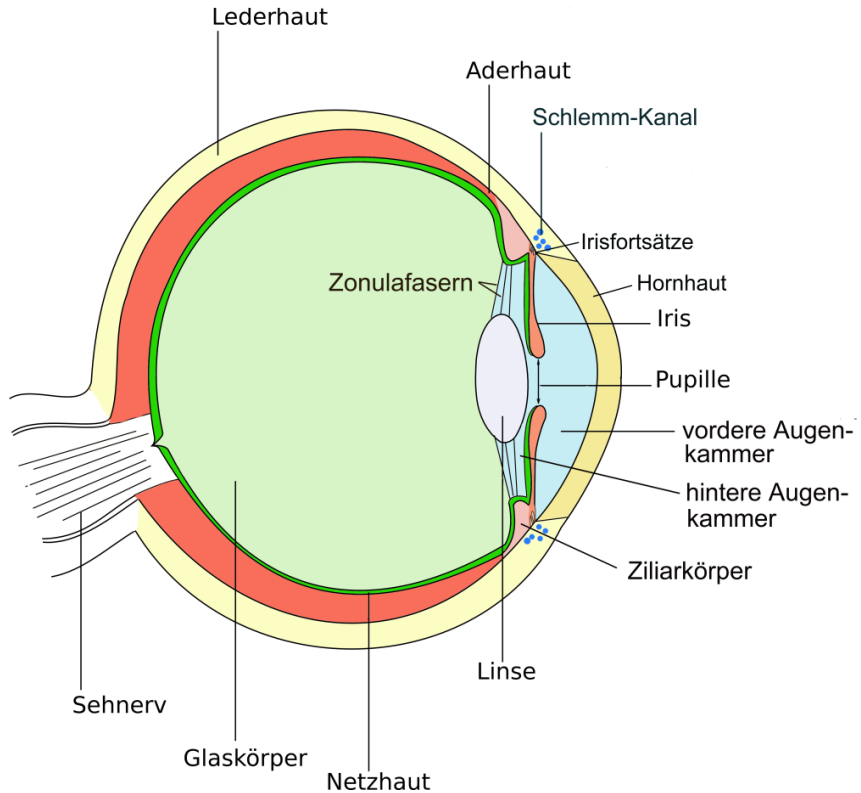
$$sd(m_i, m'_j) = \sqrt{(x_i - x'_j)^2 + (y_i - y'_j)^2} \leq r_0$$
$$dd(m_i, m'_j) = \min\{|\theta_i - \theta'_j|, 360 - |\theta_i - \theta'_j|\} \leq \theta_0$$

- Ähnlichkeitswert zw. R und Q wird durch die Anzahl der gefundenen Paare bestimmt.

Iriserkennung I

- Die Iris (Regenbogenhaut) ist die durch Pigmente gefärbte Blende des Auges welche sich ca. ab 21. Woche entwickelt.



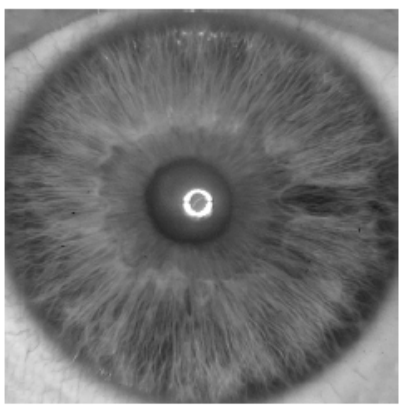


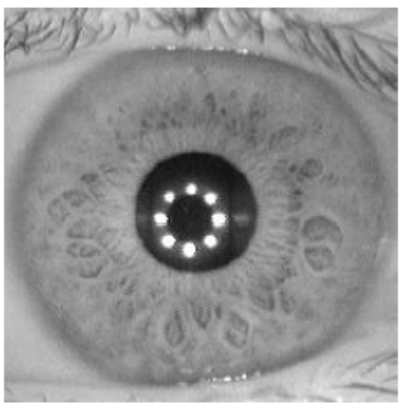
Iriserkennung II

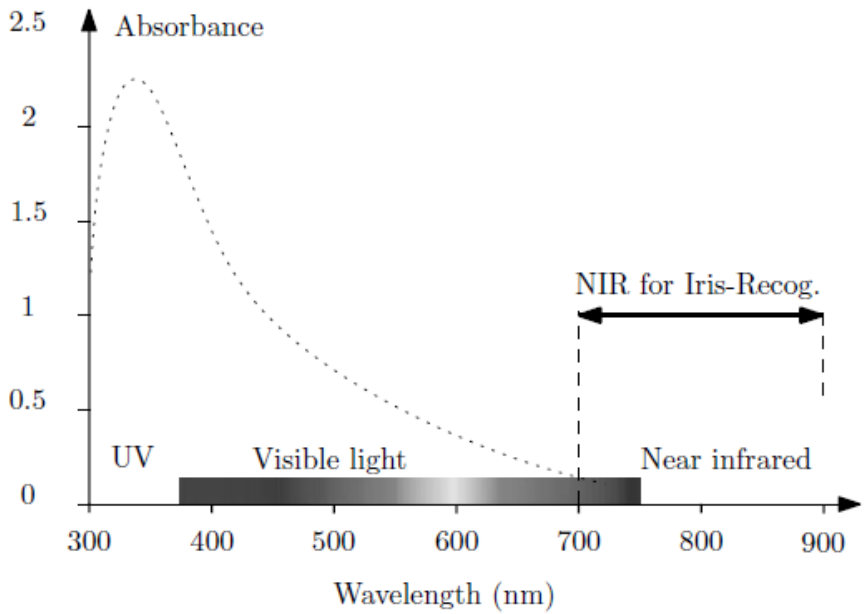
- Aufnahme eines Bildes eines Auges geschieht unter aktiver Teilnahme des Subjekts.

Iriserkennung III

- Aufnahme des Auges geschieht meist im nahe-Infrarot Bereich.
- Dies ermöglicht eine robuste Aufnahme des Iris-Musters.

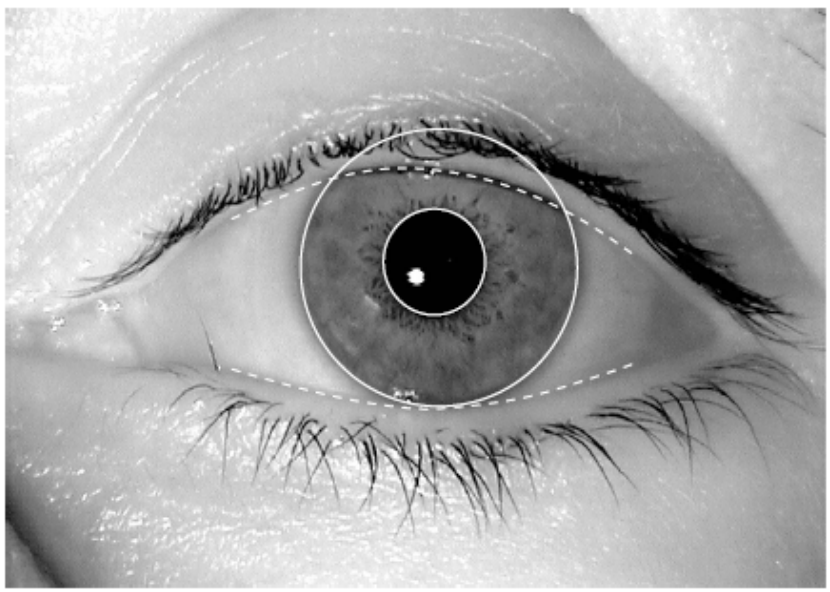






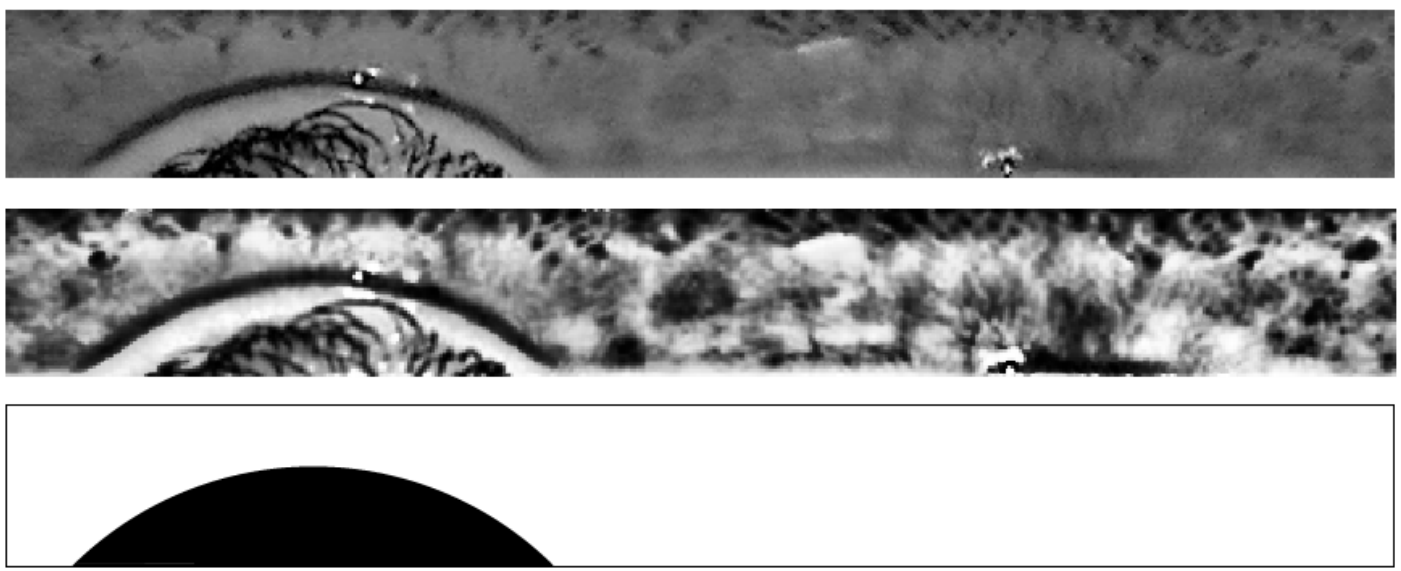
Iriserkennung IV

- Die Pupille und der äußere Iris-Rand werden detektiert und mittels Ellipsen approximiert.
- Augenlider und Wimpern werden detektiert und eine entsprechende (binäre) Maske wird berechnet.



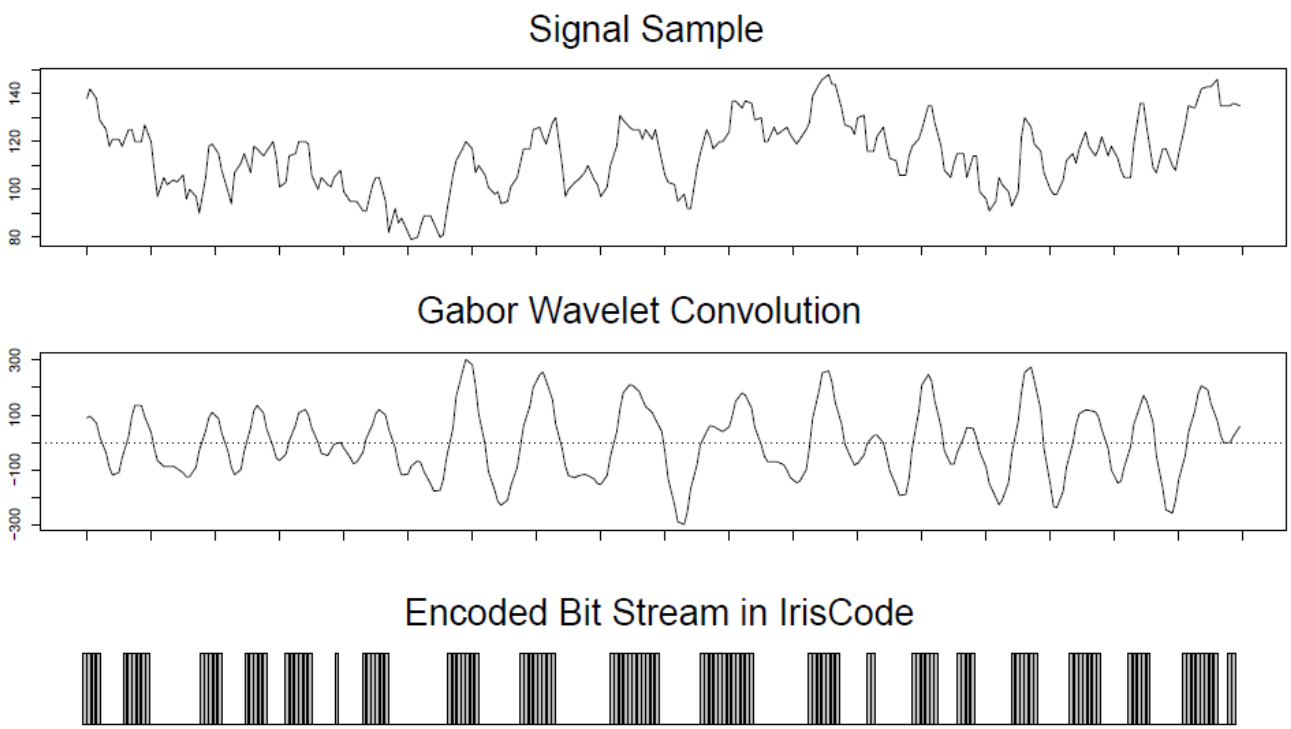
Iriserkennung V

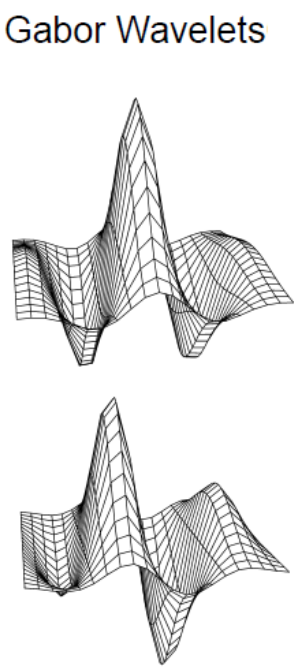
- Iris und die dazugehörige Maske werden zu einem rechteckigen Bild fixer Größe transformiert ("aufgerollt").
- Der Kontrast der aufgerollten Textur wird normalisiert.



Iriserkennung VI

- Die Textur wird zeilenweise als Signal betrachtet und Filter (zB Gabor Wavelets) werden darauf angewendet.





Iriserkennung VII

- Filterwerte werden am Ende binärisiert um einen sogenannten IrisCode (binäres Template) zu generieren.
- Dies ermöglicht eine kompakte Speicherung der Iris und der entsprechenden Maske in ca. 2,000-10,000 Bits.
- Beispiele für 1D LogGabor Merkmalsextraktoren:

- Korrelation zw. benachbarten Bits ist klar erkennbar da das Template aus einer natürlichen Textur extrahiert wird.

Iriserkennung VIII

- Die Hamming-Distanz (Anzahl unterschiedlicher Bits) dient als Distanz-Score zw. zwei Iris-Templates.
- Seien $\{codeA, codeB\}$ zwei Templates mit entsprechenden Masken $\{maskA, maskB\}$ so wird der Distanz-Score wie folgt berechnet:

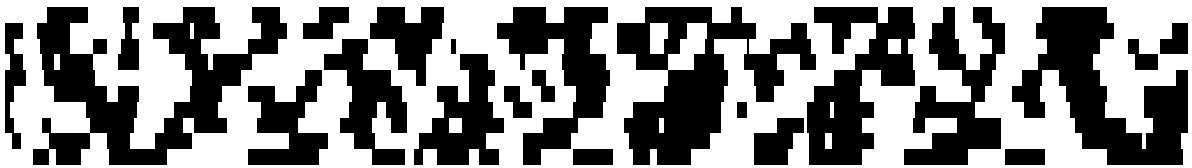
$$HD = \frac{||(codeA \oplus codeB) \cap maskA \cap maskB||}{||maskA \cap maskB||}$$

- Die Norm $||\cdot||$ gibt das Hamming-Gewicht (Anzahl 1er) an.
- Durch das Suchen einer minimalen Distanz für verschiedene Shifts können Rotationen der Augen kompensiert werden.

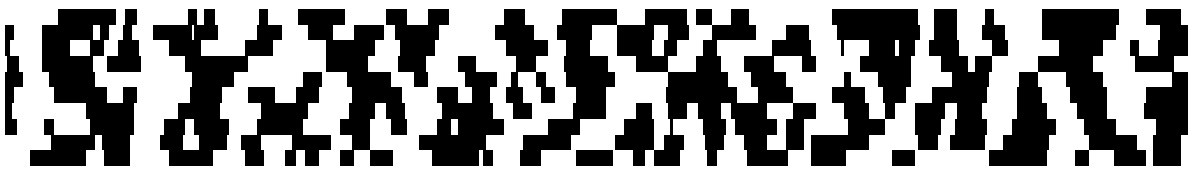
Iriserkennung IX

- Der Vergleich kann im Gegensatz zu anderen biometrischen Charakteristika (zB Fingerabdruck) sehr effizient durchgeführt werden.
- XOR, AND und das Hamming-Gewicht können für 64-bit in jeweils einem CPU-Zyklus berechnet werde.
- Ein 1:100,000 Vergleich kann auf einem herkömmlichen Desktop-PC im Sekundenbereich durchgeführt werden!
- Weiters lässt sich ein $1 : N$ vergleich einfach parallelisieren oder mittels Hardware beschleuningen (GPU).

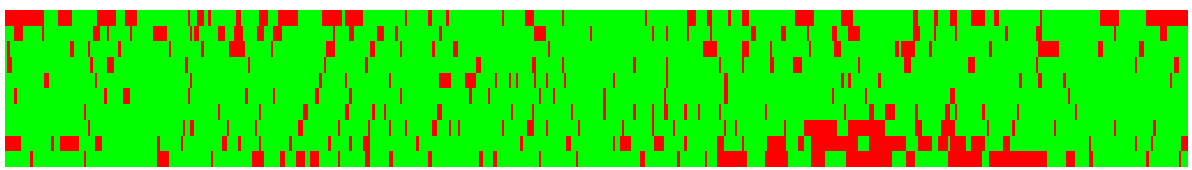
Iriserkennung X



(a) Referenz



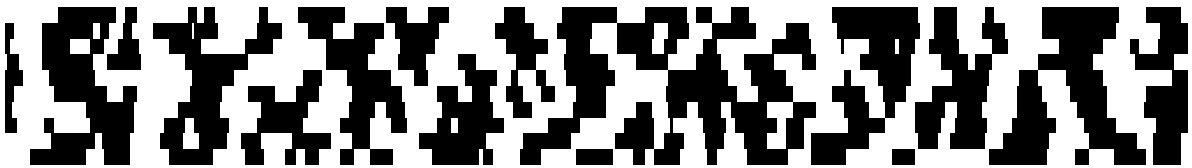
(b) Probe



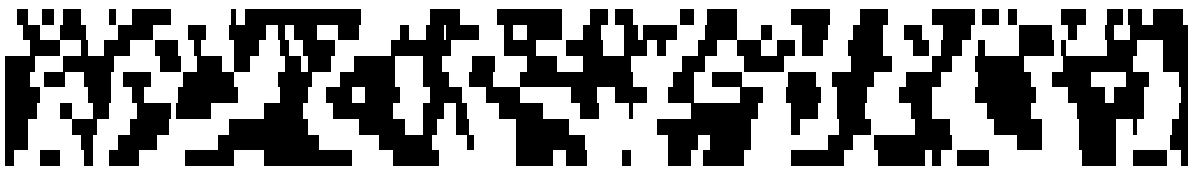
(c) (Non-)matching Bits

Abbildung: Referenz und Probe vom gleichen Auge, $HD = 0.149$.

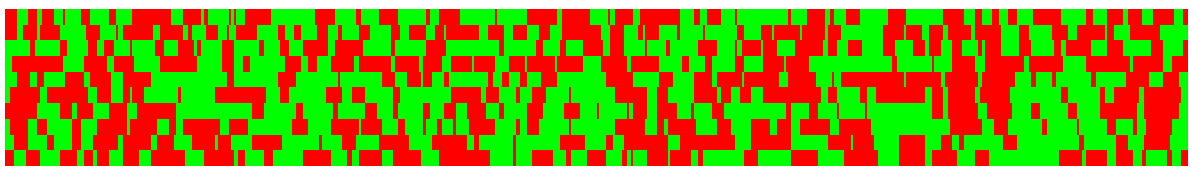
Iriserkennung XI



(a) Referenz



(b) Probe

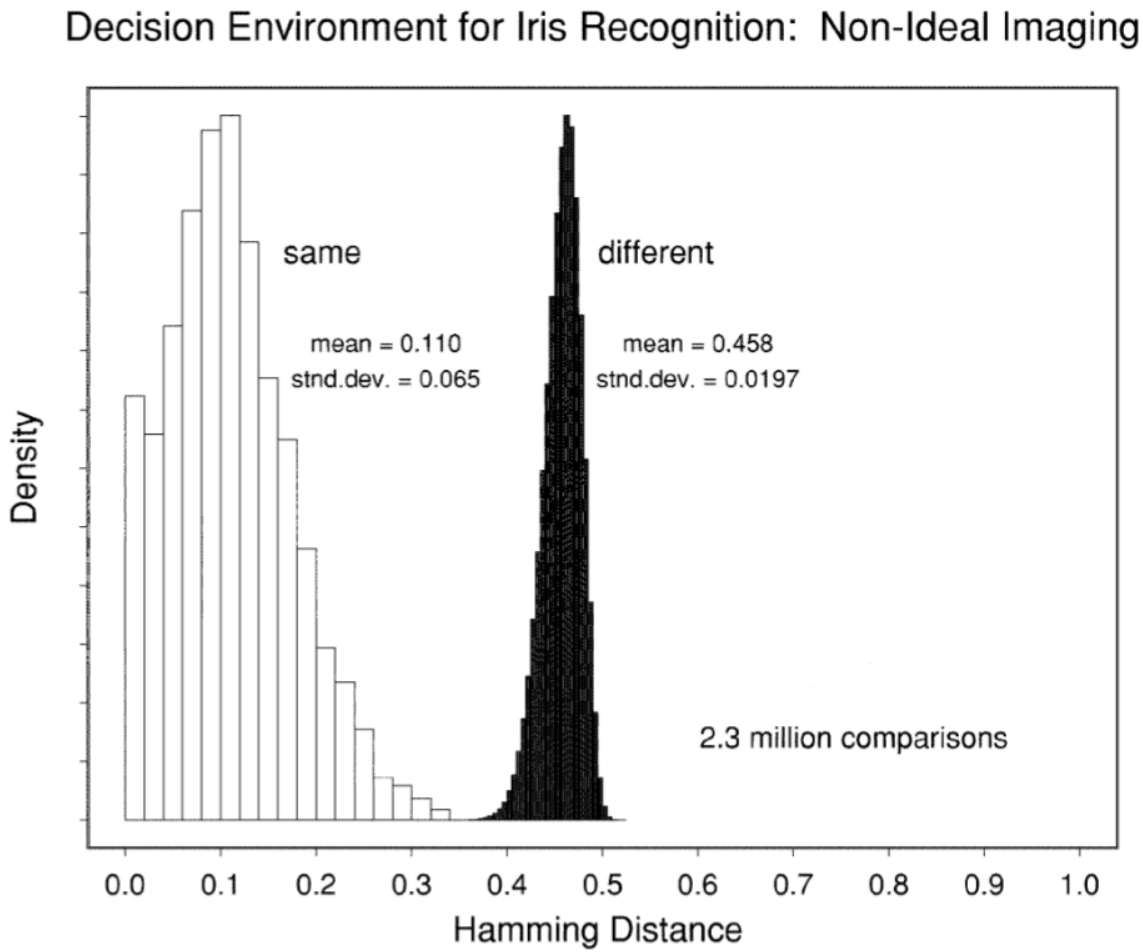


(c) (Non-)matching Bits

Abbildung: Referenz und Probe vom verschiedenen Augen, $HD = 0.484$.

Iriserkennung XII

- Iris Biometrie bietet sehr hohe Genauigkeit!



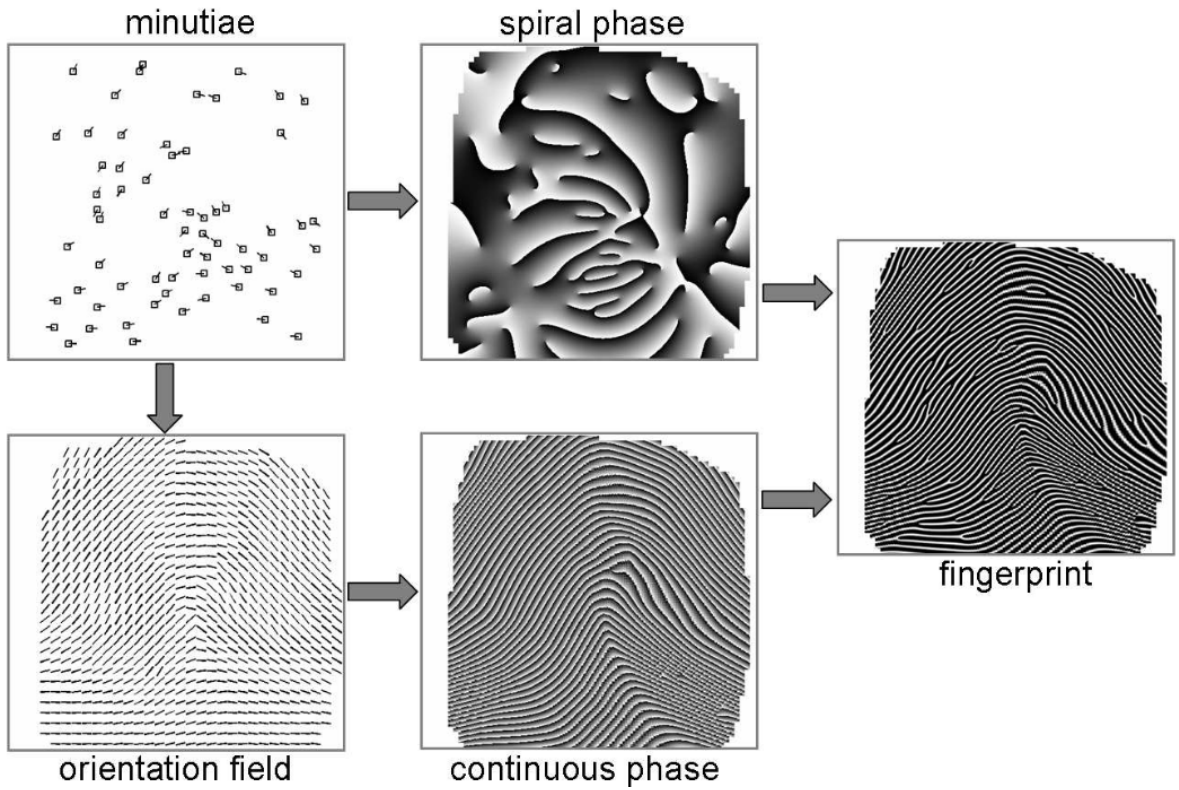
Iriserkennung XIII

- Zusammenhang von Schwellwert und FMR:

Hamming Distanz	Wahrscheinlichkeit für FM
0.26	1 in 10^{13}
0.27	1 in 10^{12}
0.28	1 in 10^{11}
0.29	1 in 13 Milliarden
0.30	1 in 1.5 Milliarden
0.31	1 in 185 Millionen
0.32	1 in 26 Millionen
0.33	1 in 4 Millionen
0.34	1 in $690,000$
0.35	1 in $133,000$

Schutz biometrischer Daten I

- Biometrische Daten sind personenbezogene Daten die geschützt werden müssen! Biometrische Charakteristika können aus gespeicherten Templates approximiert werden:



Schutz biometrischer Daten II

- Das Passwort eines Benutzers muss bei jeder Anmeldung überprüft werden.
- Damit ein Login-Passwort geschützt bleibt (zB beim Auslesen einer Festplatte) wird dieses nicht “plain” abgelegt.
- Das Passwort wird nach der Festlegung gehasht und in der Datei `/etc/passwd` abgelegt.
- Bei jeder Authentifikation wird die Eingabe des Benutzers gehasht und mit dem abgelegten Hash verglichen.
- Dh. das abgelegte Passwort bleibt permanent geschützt.

Schutz biometrischer Daten III

... mittels herkömmlicher Kryptographie?

- Wünschenswerte Eigenschaften von kryptographischen Methoden: *Diffusion* und *Konfusion*
- Geringe Änderung der Eingabe bewirkt drastische Änderung der Ausgabe (Lawinen-Effekt)
- Biometrische Varianz verhindert die Anwendung dieser Konzepte (kryptographische Methoden)!

Schutz biometrischer Daten IV

- Ein Workaround wäre Verschlüsselung zu verwenden und vor dem biometrischen Vergleich zu entschlüsseln, zB AES mit RSA
- Es ergeben sich zwei Probleme:

1. Das Problem wird nur verschoben ("shift of problem"): ich schütze meinen "Schlüssel" mit einem Schlüssel.
2. Bei jeder Authentifizierung muss entschlüsselt werden (Identifikation!) und das Template befindet sich ungeschützt im System.

Schutz biometrischer Daten V

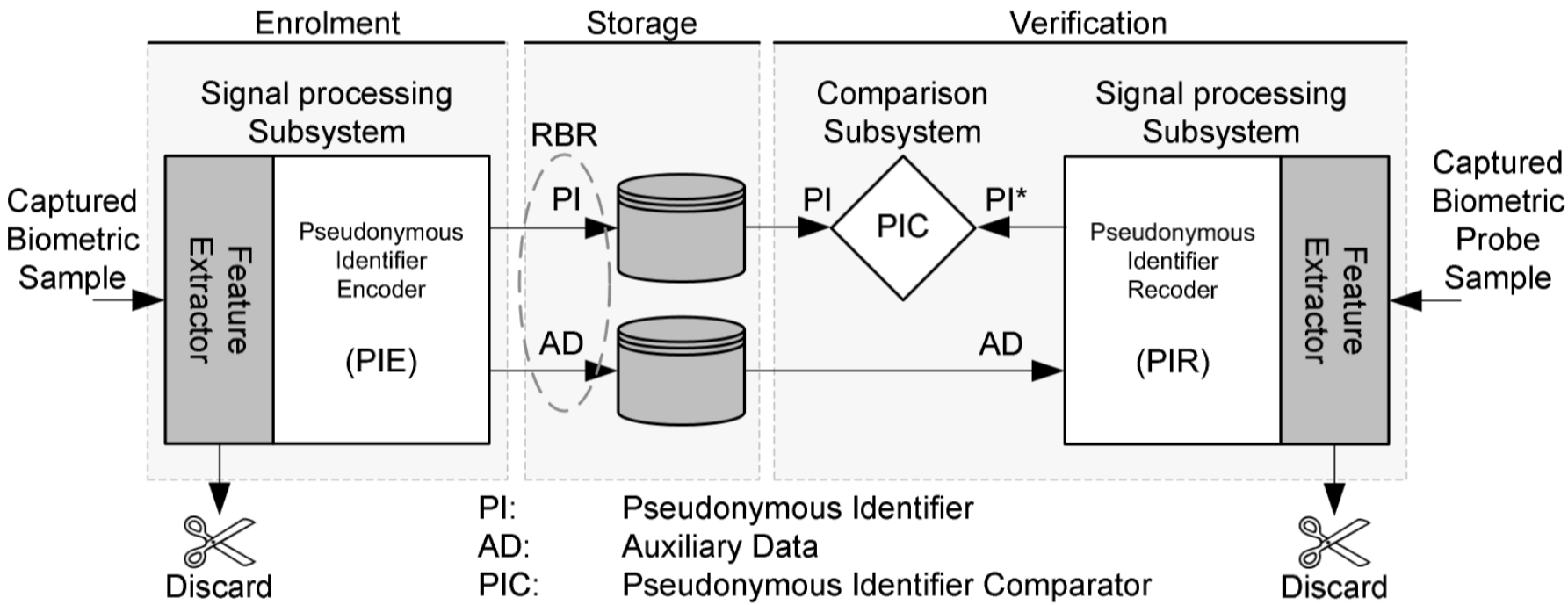
Bei binären biometrischen Templates (zb Iris) welche die Hamming Distanz zum biometrischen Vergleich verwenden ist eine einfache verschlüsselung mittels XOR (One-Time Pad) möglich:

- Für ein biometrisches System wird eine Schlüssel k gewählt.
- Die binäre biometrische Referenz R wird mit einem Schlüssel k der selben Länge verschlüsselt, $C = R \oplus k$.
- Die binäre biometrische Probe P wird ebenfalls mit k verschlüsselt, $C' = P \oplus k$.
- Der Vergleich findet im verschlüsselten Raum zw. C und C' statt: $s = HD(C, C')$.

Biometric Template Protection I

- Der Oberbegriff *Biometric Template Protection* umfasst Technologien welche eine Lösung für die zuvor beschriebene Problematik bieten.
- Die Anforderungen an solche Systeme sind im Standard ISO/IEC 24745 "Biometric Information Protection" definiert.
- Grund-Idee: originale biometrische Templates durch sogenannte Renewable Biometric References (RBRs) ersetzt.
- RBRs sollen einen biometrischen Vergleich im verschlüsselten Raum ermöglichen, dh. originale biometrische Templates sind permanent geschützt.

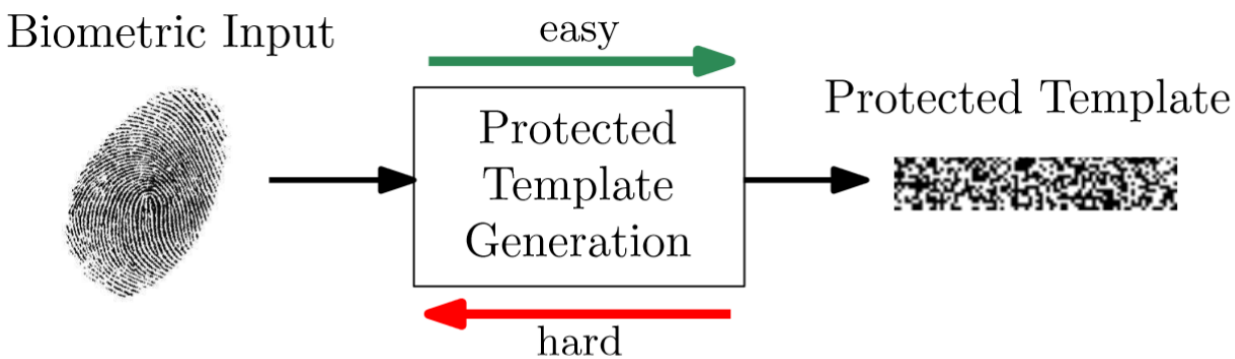
Biometric Template Protection II



- Grund-Idee: originale biometrische Templates durch sogenannte Renewable Biometric References (RBRs) ersetzt.

Biometric Template Protection III

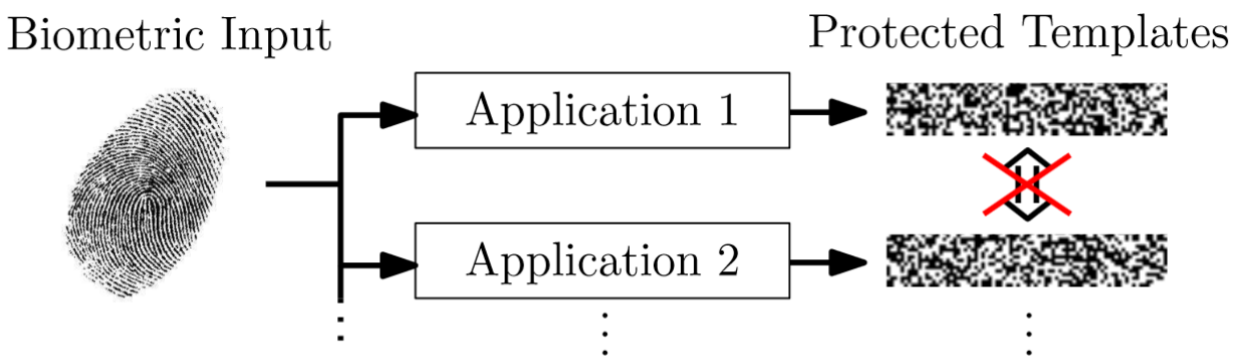
- *Nichtinvertierbarkeit*: es sollte praktisch nicht möglich sein aus dem RBR das originale biometrische Template/ Sample zu rekonstruieren.



- Diese Eigenschaft sollte vor Missbrauch (zB Presentation Attack $\simeq$ Replay Attack) von biometrischen Daten schützen.

Biometric Template Protection IV

- *Erneuerbarkeit*: es sollte möglich sein RBRs zurückzuziehen bzw. zu erneuern (vgl. Passwörter).
- *Unverkettbarkeit*: es sollte praktisch nicht möglich sein festzustellen ob verschiedene RBRs aus ein und demselben biometrischen Template. generiert wurden.

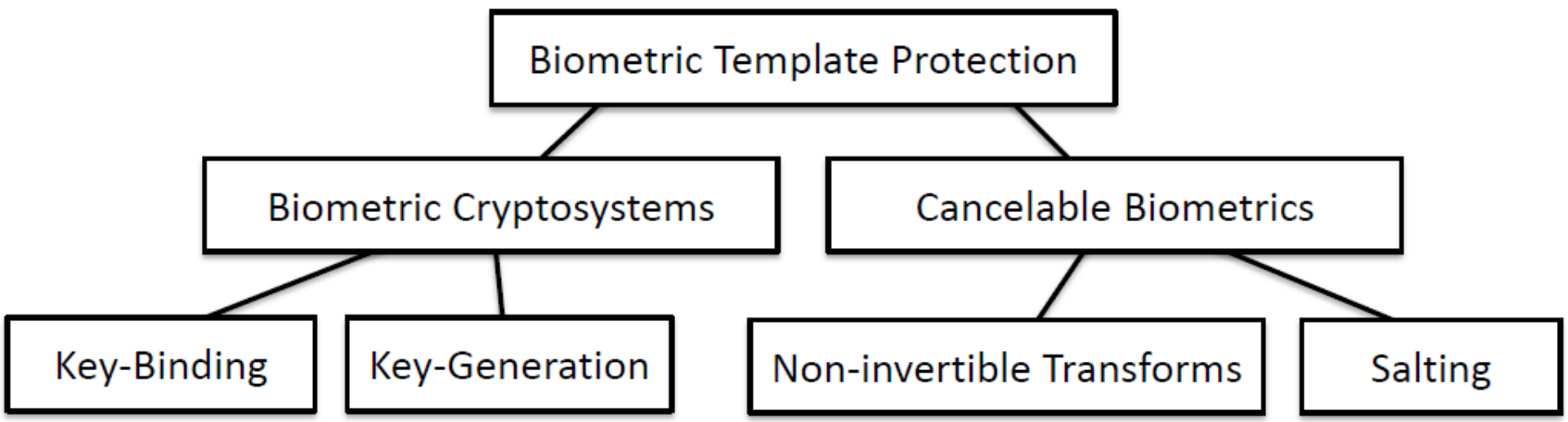


- Diese Eigenschaften schützen vor Cross-Matching Attacken.

Biometric Template Protection V

- Grundsätzlich werden zwei Arten von Techniken unterschieden:

1. Biometric Cryptosystems
2. Cancelable Biometrics



Biometric Template Protection VI

- Ziel von *Biometrische Kryptosysteme* ist es Biometrische Daten mit einem kryptographischen Schlüssel zu „verbinden“, sodass aus dem Resultat (Helper Data) der Schlüssel nur mittels Präsentation ähnlicher Biometrischen Daten errechnet werden können oder (parametrisierbar) einen stabilen Schlüssel aus Biometrischen Daten zu berechnen.
- Biometrische Vergleiche erfolgen indirekt über Schlüsselvergleiche $\rightarrow$ biometrische Daten bleiben permanent geschützt.
- Bei unterschiedlicher Schlüsselwahl bzw. Parametrisierungen sollten die resultierenden geschützten Templates nicht „matchen“.

Biometric Template Protection VII

- Fuzzy Commitment Scheme (FCS) ist ein kryptographisches Primitiv, welches zum Schutz von binären Daten entwickelt wurde

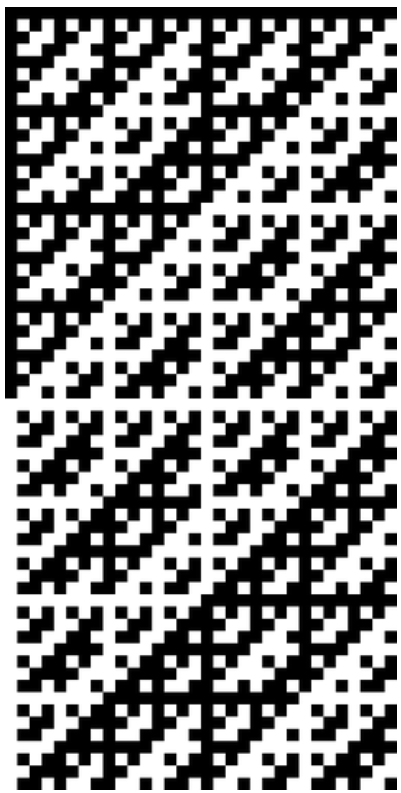
Enrolment (Key-Binding):

- Extrahiere ein binäres biometrisches Template x (zB aus Iris) und wähle einen Schlüssel k
- Bearbeite den Schlüssel mit Fehlerkorrektur $ECC_E(k) = c$, mit $|c| = |x|$. Dh. Teile des Schlüssels werden durch einsprechende Codewörter eines fehlerkorrigierenden Codes ersetzt.
- Berechne den Differenzvektor $\sigma = x \oplus c$ und den Hash von k, $h = H(k)$. Es wird nur das Commitment (σ, h) abgelegt, x und k werden gelöscht.

Biometric Template Protection VIII

- Fehlerkorrekturverfahren dienen dazu, Fehler bei der Speicherung und Übertragung von Daten zu erkennen und möglichst zu korrigieren (durch Redundanz).

- Beispiel: Hadamard Codes ersetzen Codewörter der Länge n durch Codeörter der Länge 2^{n-1}.
- Der Hammingabstand der Elemente (Zeilen) ist mindestens $2^{n-2} \Rightarrow$ man kann daher bis zu $2^{n-3} - 1$ Fehler korrigieren.
- Abbildung: Hadamard Code mit 64 Codewörtern der Länge 32.



Biometric Template Protection IX

Authentication (Key-Retrieval):

- Extrahiere ein neues binäres biometrisches Template x'. Es ist zu erwarten, dass $x \neq x'$ gilt.
- Berechne $c' = x' \oplus \sigma = x' \oplus x \oplus c$, dh. den fehlerbehafteten Code des Schlüssels.
- Führe die Fehlerkorrektur durch, $ECC_D(c') = k'$. Im Beispiel Hadamard Codes: finde das ähnlichste Codewort aus dem Alphabet.
- Berechne nun den Hash von k', $h' = H(k')$ und überprüfe ob $h = h'$ gilt. Ist dies der Fall kann k zurückgegeben werden.
- AD: Differenzvektor σ
- PI: Hash des Schlüssels h

Biometric Template Protection X

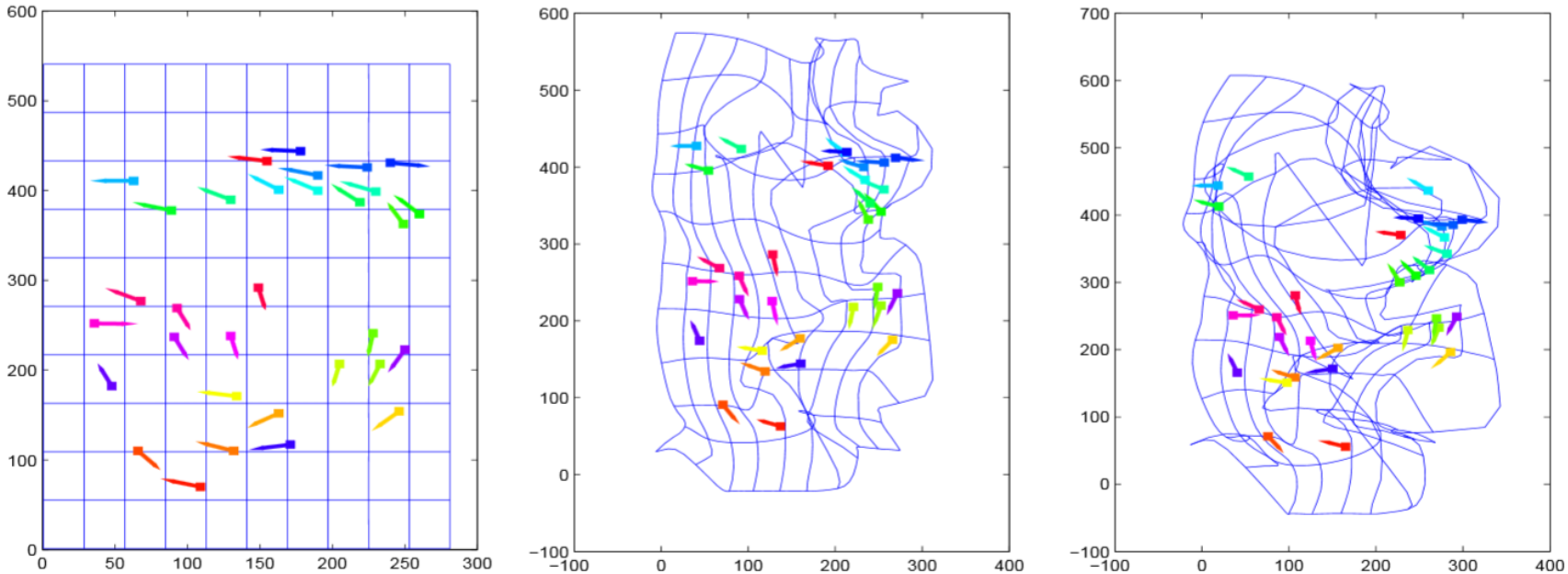
- Ziel von *Cancelable Biometrics* ist es auf biometrische Daten parametrisierte nicht-invertierbare Applikations-spezifische Transformationen anzuwenden welche einen biometrischen Vergleich in der transformierten (geschützten) Domäne erlauben.
- Durch veränderte Parametrisierung der Transformationen können mehrere geschützte Templates erzeugt werden.
- Bei unterschiedlicher Schlüsselwahl bzw. Parametrisierungen sollten die resultierenden geschützten Templates nicht „matchen“.

Biometric Template Protection XI

Surface Folding als Beispiel für Cancelable Biometrics:

- Bei Enrolment/Authentifikation wird das aufgenommene Bild bei dieser Technik vor der Merkmalsextraktion bearbeitet.
- Basierden auf gewählten Parametern wird das Bild wie Papier gefalten (zerknüllt).
- Der biometrische Comparator muss nicht ausgetauscht werden, man erhält weiterhin einen Vergleichswert (im Gegensatz zu biometrischen Kryptosystemen).

Biometric Template Protection XII



- AD: Parameter der nicht-invertierbaren Transformation
- PI: transformiertes (geschütztes) biometrisches Template
- RBR: $\{AD, PI\}$
- $PIE = PIR$: Surface folding Transformation
- PIC: Fingerprint Matcher

Biometric Template Protection XIII

- Die beiden wichtigesten Anwendung:

1. Pseudonymisierung biometrischer Datenbanken: Bei der Registrierung eines Benutzers wird durch Biometric Template Protection eine geschütztes Template in der Datenbank abgelegt. Dieses kann auf weitere verschlüsselte Einträge verweisen. Cross- Matching und Verfolgung von Aktivitäten ist nicht mehr möglich.
2. Biometrische Schlüsselvergabe: biometrische Kryptosysteme können dazu verwendet werden um basierend auf biometrischer Authentifizierung Kryptographische Schlüssel zu vergeben. Diese können entweder von biometrischen Daten abhängig sein oder zufällig gewählt werden.

Biometric Template Protection XIV

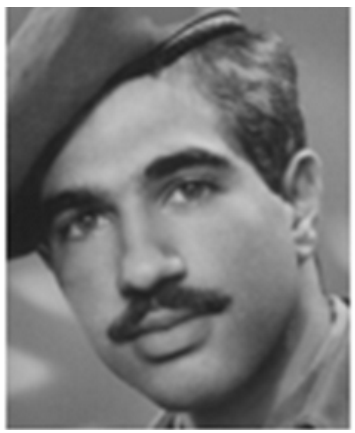
- Vorteile:
  1. Sicherheit wird erhöht indem biometrische Templates permanent geschützt werden
  2. Eine Erneuerbarkeit von Templates ist gewährleistet
  3. Cross-Matching von Datenbanken ist nicht möglich
  4. Biometrie-basierte Schlüssel-Vergabe kann realisiert werden
  5. Schutz von Privatsphäre erhöht soziale Akzeptanz von Biometrie
- Nachteile:
  1. Im Vergleich zu traditionellen Verfahren ist die Performance (Genauigkeit) signifikant schlechter
  2. Systeme können oft schlecht für Identifikation verwendet werden

Alterung biometrischer Templates I

Biometrische Charakteristika repräsentieren dynamische biologische Systeme und unterliegen somit Alterungsprozessen!

- Wir definierten *Beständigkeit*, "die Charakteristik verändert sich nicht mit der Zeit", als geforderte Eigenschaft.






Alterung biometrischer Templates II

Der Begriff *Biometric Template Ageing* beschreibt eine Erhöhung der Fehlerraten eines biometrischen Systems nach ansteigender zeit nach dem Enrolment (Registrierung).

- Anstieg der Fehlerraten bezieht sich auf $FNMR$, da Imposter Vergleiche unkorrelierte Samples vergleichen.
- Alterung biometrischer Templates wird nicht notwendiger Weise durch eine Alterung von biometrischen Charakteristika verursacht.
- Dh. keine Auswirkung auf die Sicherheit aber auf die Benutzbarkeit!

Alterung biometrischer Templates III

Es gibt viele Ursachen für die Alterung biometrischer Templates:

1. Alterung des Sensors
2. Sensor Interoperabilität
3. Umwelteinfüsse
4. (Un-)beabsichtigte Änderungen
5. Biologische Alterungseffekte
6. etc.

Alterung biometrischer Templates IV

Alterung des biometrischen Sensors:

- Bei der Alterung von Sensoren kann es zur Entstehung von defekten Pixel kommen.
- Die Verteilung solcher Pixel ist zufällig und kann somit gut simuliert werden.
- Auf simulierten Daten hat die Alterung biometrischer Sensoren nur sehr geringe Auswirkung auf die Alterung biometrischer Templates (für realistische Zeiträume).

Alterung biometrischer Templates IV

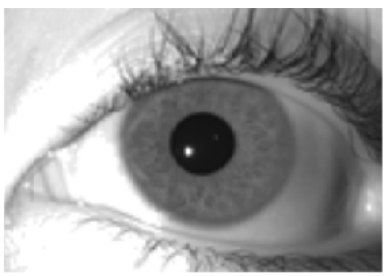
Sensor Interoperabilität ist von hoher praktischer Relevanz:

- Durch die Popularität biometrischer Systeme werden ständig neue Sensoren entwickelt.
- Werden Sensoren ausgetauscht wurde die Referenz evtl. mit einem anderen Sensor als die Probe aufgenommen.
- Eine erneute Registrierung ist teuer und aufwändig.
- Dies kann zu weiteren Variationen führen, welche wie folgt behandelt werden können:
  1. Identifiziere den Sensor und passe den Algorithmus entsprechend an;
  2. Isoliere vom Sensor unabhängige Merkmale;

Alterung biometrischer Templates V

Änderung von Umwelteinflüssen:

- Zeitliche Änderungen können Änderungen der Umwelteinflüsse mit sich bringen.
- Bsp: Änderung der Lichtverhältnisse kann zu Variationen in der Pupillenerweiterung führen (Iriserkennung).
- Bsp: Änderung der Luftfeuchtigkeit kann die Feuchtigkeit der Haut ändern (Fingerabdruckserkennung).


- Solche Variation können nach kurzer Zeit auftreten!

Alterung biometrischer Templates VI

(Un-)gewollte Änderungen biometrischer Charakteristika:

- Beispiele sind Verletzungen (zB. verbrannte Fingerkuppen) oder medizinische Eingriffe (zB. Augenlidstraffung).

- Auch solche Variation können nach kurzer Zeit auftreten und sind nur schwer zu kompensieren!
- Eine Detektion gewollter Veränderungen ist für biometrische Forensik wichtig.

Alterung biometrischer Templates VII

Biologische Alterungsprozesse:

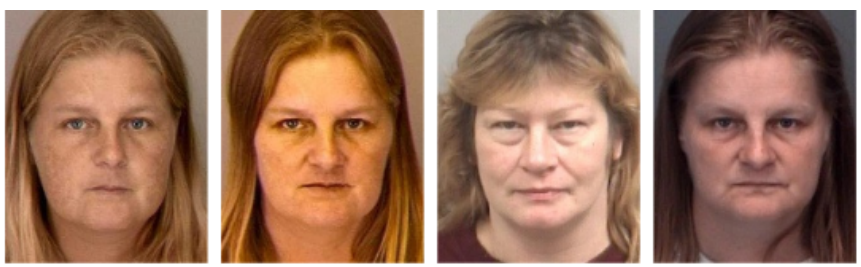
- Viele biometrische Charakteristika, zB. Gesicht oder Stimme, unterliegen offensichtlichen Alterungsprozessen.
- Verhaltensbasierte Charakteristika, zB. Gang oder Tippverhalten, sind grundsätzlich nicht für eine biometrische Erkennung über einen längeren Zeitraum brauchbar.
- Für verschiedene Charakteristika können gewissen Alterungsprozesse kompensiert werden, zB. Fingerwachstum.
- Untersuchungen von Alterungsprozessen sind grundsätzlich schwierig besonders für “neuere” Charkteristika, zB. Venen.

Alterung biometrischer Templates VIII

Biologische Alterungsprozesse für Gesicht:

- Abhängig von der Zeitspanne sind drastische Änderungen des Gesichts möglich.
- Alterungsprozesse im Gesicht sind stark heterogen!
- Erwachsene Menschen können bei $FMR \simeq 0.1\%$ über einen Zeitraum > 15 Jahre erkannt werden.

41.9 43.5 45.7 46.3



34.6 37.5 44.7 48.8

Alterung biometrischer Templates IX

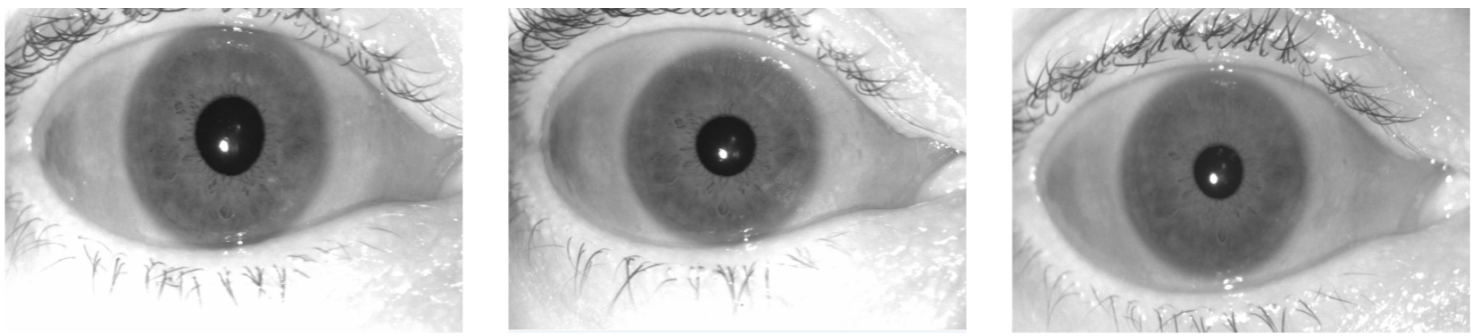
Biologische Alterungsprozesse für Fingerabruck:

- Ähnlichkeitswerte bei Genuine Vergleichen werden mit ansteigenden Zeitspannen kontinuierlich kleiner, Impostor Vergleiche bleiben konstant.
- Genauigkeit bei praktisch relevanten Schwellwerten bleibt jedoch annähernd stabil über Zeiträume > 12 Jahre.
- Wachstum von Fingern kann modelliert werden.
- Qualität der Fingerabdrücke spielt eine sehr wichtige Rolle!

Alterung biometrischer Templates X

Biologische Alterungsprozesse für Iris:

- Bis dato wurden keine Effekte von biologische Alterungsprozessen in der Iris gemessen.
- Für Zeitspannen von ca. 10 Jahren bleibt die Erkennungsleistung konstant.



2008 2009 2010

- Während minimale Erhöhungen von Fehlerraten gemessen wurden gibt es keinen fotographischen Beweis für Änderungen der Iristextur nach gewisser Zeit.

Alterung biometrischer Templates XI

Herausfordernungen bei der Untersuchung:

- Sehr große Datenbanken die über einen längeren Zeitraum aufgenommen wurden sind nötig um fundierte Schlüsse zu ziehen.
- Änderungen von Umwelteinflüssen müssen ausgeschlossen werden (Laborbedingung).
- Medizinische Forschung sollte eingebunden werden (Definition und Aufnahme von Meta-Daten).
- Simulation von Alterungsprozessen ist nur bedingt möglich.

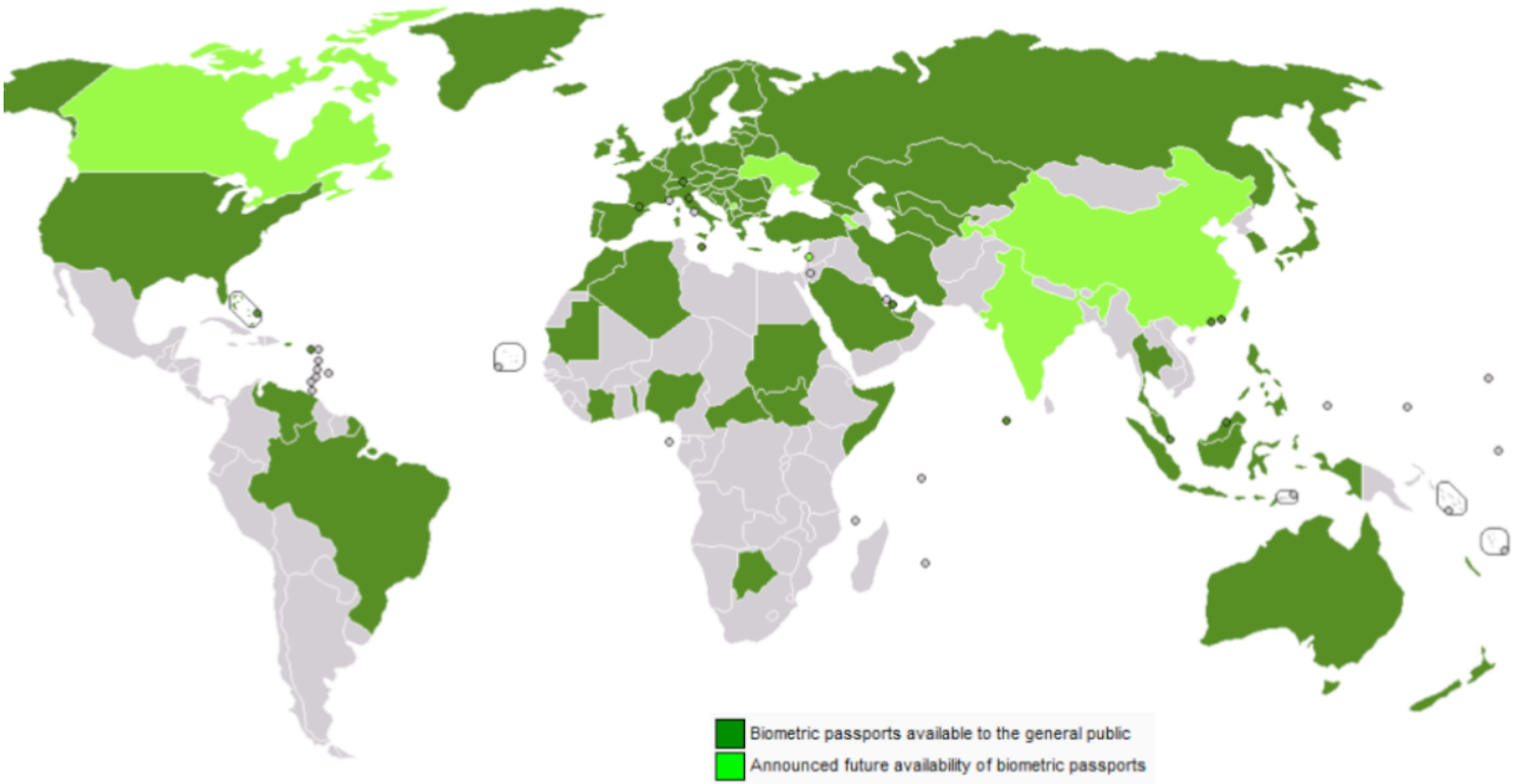
Biometrische Anwendungen I

Biometrische Reisepässe:

- Seit November 2005 nach ICAO Standard
- Contact-less IC Chip ISO/IEC14443 (Proximity)
- Gesichtsbilder und Fingerabdrücke
- Gültigkeit: < 25: 5 Jahre, > 25: 10 Jahre (nicht in allen Europäischen Ländern)

Biometrische Anwendungen II

489 Millionen ePassports ausgegeben von 101 Staaten (Schätzung der ICAO 2013):



Biometrische Anwendungen III

Grenzkontrolle - EasyPASS:

- Beamten kontrollieren die Spuren, Durchsatz der Passagiere sollte vergrössert werden.
- Pilotierung in 2009 in Frankfurt gestartet, derzeit Deutschlandweite Installation.
- Nutzung des Gesicht aus dem Reisepass für EU/Shengen (18+)

Biometrische Anwendungen IV

Trade-off zwischen Benutzbarkeit und Sicherheit:

Das perfekte biometrische System gibt es nicht!