

C⁴ (Chip, Card & Crypto Consulting)

E i n f ü h r u n g

i n d i e

B i o m e t r i e

SGRP Event 04

Freitag, 18. Juni 04

SwissRe, Zürich

C⁴(Chip, Card & Crypto Consulting)
Josef Schuler, dipl. Math.
Steiweidlistr. 3
6417 Sattel

j.schuler@bluewin.ch

DIE PRÄAMBEL

Stellen Sie sich vor, Sie bräuchten keine Schlüssel, keine Kreditkarten und keine weiteren Zutritts Hilfsmittel mehr, ausser Ihre eigenen Finger.

Sie kommen nach Hause, halten den Finger hin und die Türen öffnen sich. Sie können nie mehr einen Schlüssel verlieren. Oder Sie merken, Sie haben kein Geld mehr, Sie gehen zum nächstgelegenen Bancomaten, halten den Finger hin und beziehen so Ihr Geld. Oder noch besser, anstatt, dass Sie an der Kasse den Geldbeutel zücken und das Geld oder die ec-Karte herausnehmen, bezahlen Sie an der Kasse mit dem Finger; Sie könnten nie mehr Geld verlieren, und nie mehr zu wenig Geld im Portemonee haben.

Wäre das schön!! Aber, es ist auch zu schön um wahr zu sein.

DIE BIOMETRIE BESTEHT NICHT NUR AUS FINGERABDRUCKVERFAHREN

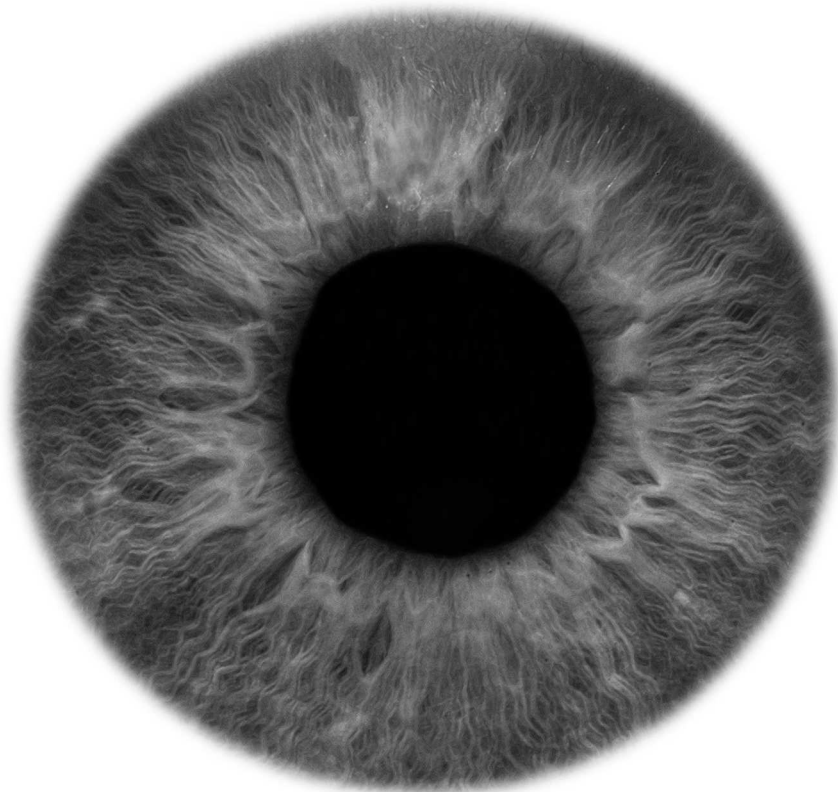


Bild stammt aus der Diplomarbeit von Roman Vögtli (NDS-INS 3), „BIOMETRISCHE VERFAHREN UND DEREN RECHTLICHER ASPEKT“, siehe Literaturverzeichnis [RV].

Bemerkung: Wenn sich jemand weiter ins Gebiet einlesen will, so seien ihm die obige Diplomarbeit (enthält z.B. eine gute Abhandlung in die Iris- und Retinaerkennung) und die Studienarbeit von Stefan Hanke [SH] empfohlen.

O. INHALTSVERZEICHNIS

1. EINLEITUNG	1
1.1. Definition und Begriffsklärung	1
1.2. Inhalt und Ziele des Vortrags	2
1.3. Ein Einführungstest	3
2. DIE BIOMETRIE	4
2.1. Die grundsätzliche Authentisierung	4
2.2. Der schematische Ablauf einer Verifikation	5
2.3. Die verschiedenen Verfahren; eine Übersicht	5
2.4. Notwendige Eigenschaften biometrischer Merkmale	5
2.5. Einfluss auf die Benutzerakzeptanz	9
2.6. Die wichtigsten Begriffe und Kennwerte	10
2.7. Verifikation versus Identifikation	12
2.8. Erkennungssicherheit versus Fehlerwahrscheinlichkeit	13
2.9. Vor- und Nachteile	14
2.10. Vergleiche	15
2.11. Marktzahlen	16
2.12. Anwendungen	17
2.13. Evaluationskriterien	18
3. FINGERABDRUCKSYSTEME	19
3.1. Grundlagen der Daktyloskopie	19
3.2. Die Aufnahmeverfahren	20
3.3. Die Vor- und Nachteile	21
4. FAQ	22
5. GRENZEN DER BIOMETRIE	23
6. ZUSAMMENFASSUNG	25
7. GLOSSAR	26
8. REFERENZEN UND WEITERFÜHRENDE LITERATUR	27

1 EINLEITUNG

Das in diesem Vortrag erzählte ist grösstenteils in meinen Artikel „Fingerzeig“ auch in prosa aufgeführt.

1.1. Definition und Begriffsklärung

In Medizin und Biologie:

Definition:

„**Biometrie**“: Wissenschaft der Körper(ver-)vermessung

In der Informationstechnologie:

Der Begriff „**Biometrie**“ steht als Synonym für „Biometrische Zutrittsverfahren“.

1.2. Inhalt und Ziele des Vortrags

- ⊗ Eine Einführung in Biometrie, deren Begriffe, Mechanismen und Möglichkeiten zu erhalten.
- ⊗ Fingerabdrucksysteme ein wenig detaillierter Betrachten.
- ⊗ Sensibilisierung auf gewisse Fragestellungen zu erlangen.
- ⊗ Die Grenzen versuchen abzustecken.
- ⊗ Den Einführungstest „bestehen“; m.a.W. Sie verstehen das Grundsätzliche einer Spezifikation eines Fingerprintsystems.
- ⊗ Sie können Zeitungsartikel über Biometrie lesen und kritisch hinterfragen.

1.3. Ein Einführungstest

Verstehen Sie die folgenden Spezifikationen eines Fingerprintsystems?

PERFORMANCE SPECIFICATIONS

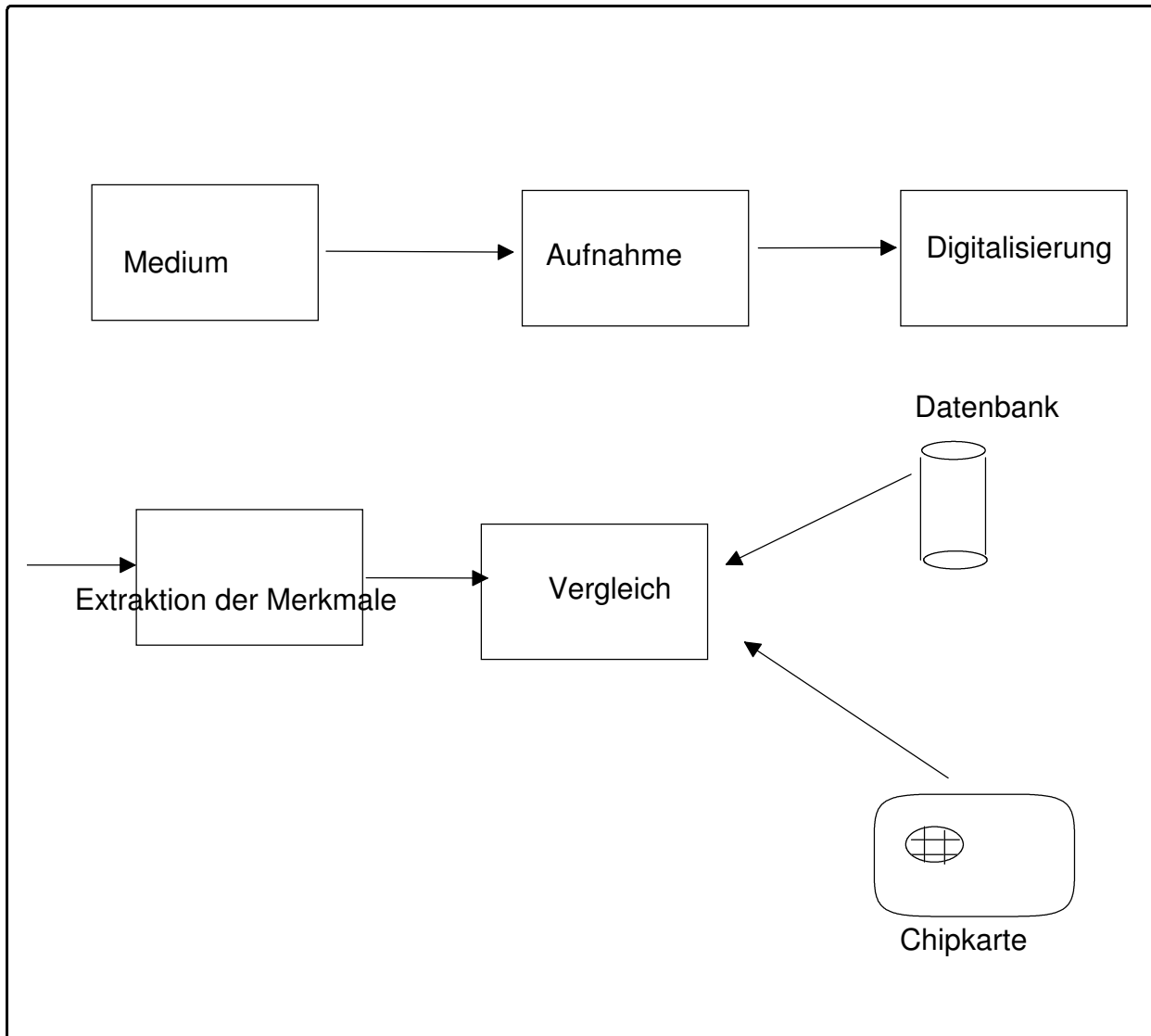
- False acceptance rate (FAR): 0.01%
- False rejection rate (FRR): 0.01%
- Equal error rate (EER): 0.1%
- Enrollment time: < 5 seconds
- Verification time: 1 second
- Allowable finger rotation: +/- 18 degrees
- Allowable finger displacement: +/- 5 mm

2 DIE BIOMETRIE

2.1. Die grundsätzliche Authentisierung

Schlüssel und ähnliches:	Überprüfen von Besitz
Unterschrift:	Überprüfen von Können
PIN- und Passwortverfahren:	Überprüfen von Wissen
Biometrie:	Überprüfen von Merkmalen (= "interner" Besitz)

2.2. Der schematische Ablauf einer Verifikation



Figur 2.1 Der grundlegende Ablauf

- Das Medium (Finger, Hand usw.) wird für die Aufnahme bereit gemacht.
- Die Aufnahme mittels Digitalkamera, Laser, kapazitiven und induktiven Sensoren usw. liefert eine Datei, die bis zu 0,5 Mbyte sein kann.
- In der Digitalisierungsphase werden die einzelnen Pixel von den ursprünglichen Grauwerten [00.. 255] in digitale Werte [0, 1] verarbeitet.
- Aus diesem Digitalbild werden die Merkmale extrahiert, damit am Schluss noch eine Datei von einigen 100 Byte bis wenige Kbyte übrigbleiben.
- Die extrahierten Merkmale werden mit den gespeicherten Merkmalen verglichen.

2.3. Die verschiedenen Verfahren, eine Übersicht

Als Medium kommen in Frage:

I) Physiologische Merkmale (statische Verfahren)

- ↳ Gesicht
- ↳ Handgeometrie
- ↳ Fingergeometrie
- ↳ Fingerabdruck
- ↳ Augenhintergrund
- ↳ Iris
- ↳ Retina
- ↳ Venenstruktur
- ↳ Geruch
- ↳ Gesichtstemperatur

II) Verhaltensorientierte Merkmale (dynamische Verfahren)

- ↳ Stimme
- ↳ Unterschrift
- ↳ Tastatureingaberythmus
- ↳ Gang- und Schritterkennung

Als Aufnahmeverfahren kommen in Frage:

- ❖ Optische Verfahren (Digital Kamera; Laser)
- ❖ Drucksensitive Verfahren
- ❖ Akkustische Verfahren
- ❖ Kapazitive Verfahren
- ❖ Chemische Analyse
- ❖ andere

Zuordnung Merkmal ↔ mögliche Verfahren:

Merkmal	mögliche Verfahren
I) Physiologische Merkmale	
☞ Gesichtsform	❖ optische
☞ Gesicht (Wärmebild)	❖ optische (Laser)
☞ Handgeometrie	❖ optische
☞ Fingergeometrie	❖ optische
☞ Fingerabdruck	❖ optische (Digitalkamera, Laser) ❖ kapazitive (Sensor) ❖ Infrarot (Sensor)
☞ Augenhintergrund	❖ optische
☞ Iris (= Muster des Gewebes um die Pupille)[*]	❖ optische (Laser)
☞ Retina (= Muster der Blutgefäße im Augenhintergrund) [*]	❖ optische (Laser)
☞ Venenstruktur	❖ optische
☞ Geruch	❖ chemische Analyse
II) Verhaltensorientierte Merkmale	
☞ Stimme	❖ akustische
☞ Unterschrift	❖ drucksensitive
☞ Tastatureingaberhythmus	❖ andere
☞ Gang- und Schritterkennung	❖ andere

[*] Siehe [RV]

2.4. Notwendige Eigenschaften biometrischer Merkmale

Einzigartigkeit

Für verschiedene Menschen muß das Merkmal hinreichend verschieden sein. Ein biometrisches Merkmal, daß nur 100 verschiedene Ausprägungen besitzt, wäre nicht sinnvoll einsetzbar.

Konstanz

Das Merkmal sollte sich im Laufe der Zeit möglichst wenig ändern. Kleinere Änderungen können durch adaptive Verfahren ausgeglichen werden.

Verbreitung

Das Merkmal muß bei möglichst vielen Personen, die das System benutzen sollen, vorhanden sein.

Gegenbeispiele:

- Die Iriserkennung ist zum Beispiel für blinde Menschen ungeeignet.
- Spracherkennung für Stumme.
- Kletterer, Putzfrauen, „Banknotenzähler“ (wegen der Abnutzung) sowie Handwerker (wegen der Verschmutzung) sind „schlechte“ Probanden für Fingerabdrucksysteme.

2.5. Einfluss auf die Benutzerakzeptanz

Die Wahl des einzusetzenden biometrischen Verfahrens hängt

- von der gegebenen Anwendung
- und von der zu erwartenden Benutzerakzeptanz ab.

Komfort bei der Benutzung

- ⊗ Zeitaufwand für eine Verifikation
- ⊗ Zeitaufwand, bei einer fehlerhaften Rückweisung.
- ⊗ Ergonomie (die Benutzerakzeptanz sinkt, falls zur Authentisierung der Finger in eine „unmögliche“ Stellung gebracht werden muss.)

Vertrautheit

Biometrische Verfahren sollten möglichst in bereits bekannte und etablierte Vorgänge integriert werden.

Hygiene

- ⊗ Ein – vermeintlich – verschmutzter Sensor kann Ekel erregen.
- ⊗ Berührungsfreie Systemen (z.B. Digitalkamera) haben da einen nicht zu unterschätzenden Vorteil.

Vorurteile und Ängste

- ⊗ Registrierungsängste (Big brother is watching you.)
- ⊗ Kriminalisierungsmanie
- ⊗ Direkte Bedrohung: abgeschnittene Finger

Beim letzten Punkt ist insbesondere zu beachten, dass

Lebendtests nicht vor dem Abschneiden von Fingern abhalten!!
Vielmehr muss mit Marketing Massnahmen breit verkündet
werden, dass das System tote Finger nicht akzeptiert.

2.6. Die wichtigsten Begriffe und Kennwerte

Biometrische Verfahren lassen sich nach mehreren Kennwerten klassifizieren:

Erkennungsraten:

FAR: „false acceptance rate“ = Zulassen von Unberechtigten. D.h. Wieviele (als Wert zwischen 0 und 1) Unberechtigte werden als Berechtigte erkannt.

FRR: „false reject rate“ = Ablehnen von Berechtigten. D.h. Wieviele (als Wert zwischen 0 und 1) Berechtigte werden als Unberechtigte erkannt. M.a.W. Wieviele Berechtigte werden (fälschlicherweise) abgewiesen.

EER: „equal error rate“: Rate, wo FAR = FRR. D.h. das System ist so eingestellt, dass die Rate der unberechtigten Zulassungen gleich hoch ist wie die Rate der falschen Abweisungen.

TAR: „true acceptance rate“ = Zulassen von Berechtigten. D.h. Wieviele (als Wert zwischen 0 und 1) Berechtigte werden wirklich auch als Berechtigte erkannt; $TAR = 1 - FAR$.

TRR: „true reject rate“ = Ablehnen von Unberechtigten. D.h. Wieviele (als Wert zwischen 0 und 1) Unberechtigte werden wirklich auch als Unberechtigte erkannt und dementsprechend abgewiesen; $TRR = 1 - FRR$.

Person	wird akzeptiert	wird abgelehnt
Berechtigte	TAR	FRR
Unberechtigte	FAR	TRR

Bemerkung: Es gibt keine genormten Angaben zur Grundgesamtheit, somit ist der Begriff „rate“ in der Regel mit Vorsicht zu geniessen.

Die 2 wichtigen (Warte-)-Zeiten:

Registrierzeit: (enrolement time); die Zeit für die Neuaufnahme einer Person.

Verifizierzeit: (verification time); die Zeit für die Erkennung einer registrierten Person.

Die 2 grundsätzlichen Überprüfungsarten:

Identifikation: Es wird die Frage beantwortet: „Wer ist es?“

Verifikation: Es wird die Frage beantwortet: „Ist es derjenige, der er vorgibt zu sein?“

Und speziell für Fingerprintsystem:

Finger rotation: Um wie viel kann der Finger um die Längsachse verdreht sein.

Finger displacement: Erlaubte Verschiebung des Fingers.

2.7. Verifikation versus Identifikation

Genau zu unterscheiden ist zwischen Verifikation und Identifikation.

Verifikation heißt der Vorgang, bei dem eine Person behauptet, XY zu sein, und dies dann mit einem biometrischen Vergleich zu beweisen hat. Dies ist eine typische Zutrittskontroll-Fragestellung, auch als One-to-one-Vergleich bezeichnet.

Verifikation: Überprüfung einer vorgegebenen (behaupteten) Identität:

Frage: „**Ist es die Person, die sie behauptet zu sein?**“

Verifikationen werden dauernd im alltäglichen Leben gemacht:

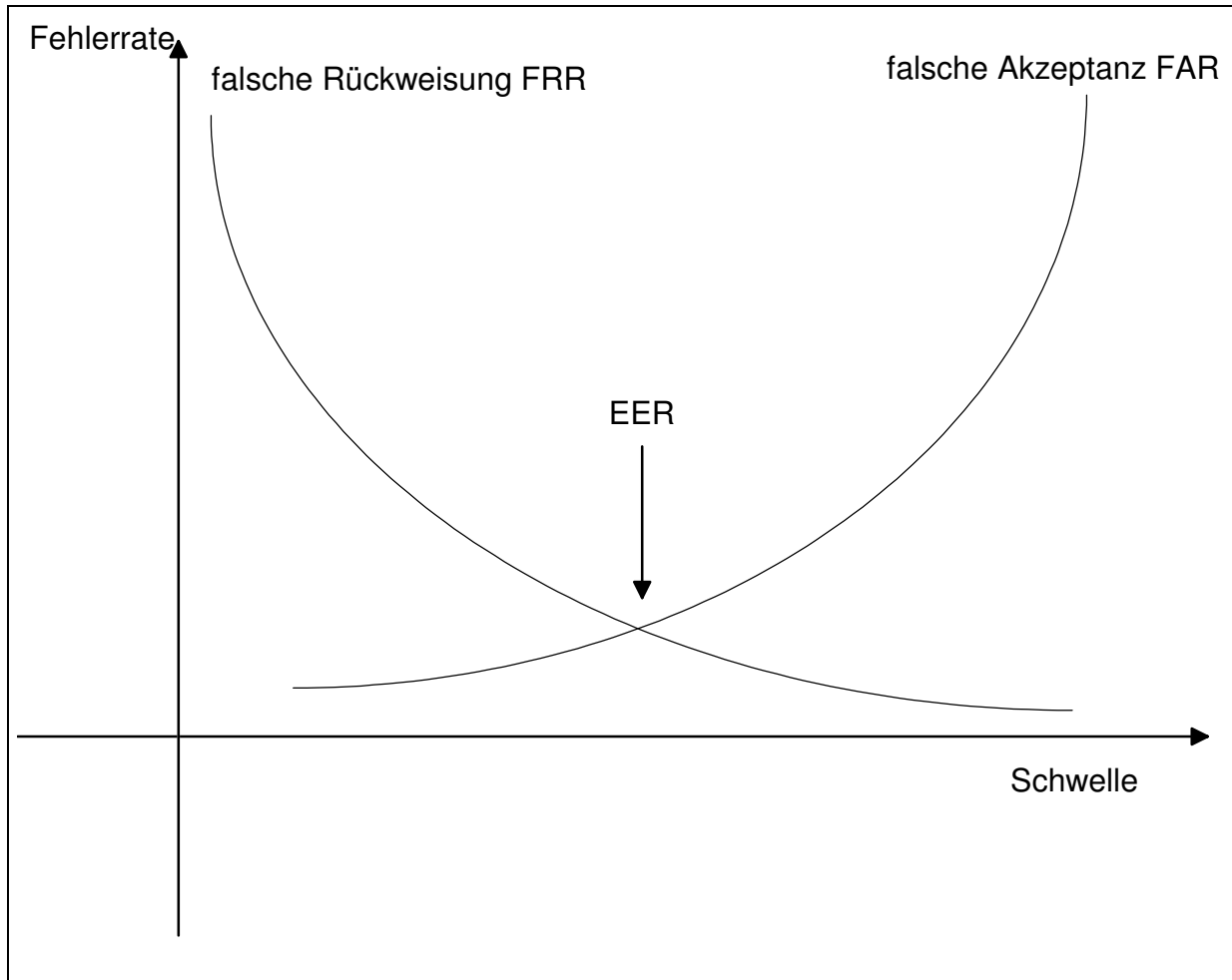
- PIN-Eingabe bei Bancomat (Überprüfen von Wissen)
- Ausweis vorlegen (Überprüfen von Besitz)
- Schloss öffnen (Überprüfen von Besitz)
- Unterschreiben (Überprüfen von Können)

Bei der Identifikation lautet die Fragestellung: Hier sind biometrische Merkmale, wer ist das? Dies bedingt eine Suche in einer zuvor angelegten Datenbank und ist eine typische Fragestellung der Polizei. Man nennt dieses Verfahren auch den One-to-many-Vergleich.

Identifikation: Feststellen bzw. Finden der Identität einer (zunächst) unbekanntem Person z.B. durch Vergleich mit gespeicherten Identitätsdaten.

Frage: „**Wer ist es, bzw. könnte es sein?**“

2.8. Erkennungssicherheit versus Fehlerwahrscheinlichkeit



Die Krux an der Sache ist, dass die FRR und die FAR sich gegenseitig „bekämpfen“: Wird die eine Rate verkleinert, so erhöht sich die andere. Somit ist es wichtig zu wissen, wie gross (oder besser: wie klein) die EER ist!!

Es ist kein Problem die $FAR = 0$ zu setzen: Ich weise einfach jeden ab!!

Folgerung: Die FRR wird 1.

Dito die $FRR = 0$ zu setzen: Ich akzeptiere einfach jeden!!

Folgerung: Die FAR wird 1.

2.9. Vor- und Nachteile

Für die Anwendung biometrischer Methoden sprechen die folgenden Vorteile:

- ☞ Die Merkmale können in der Regel weder verloren gehen, noch an andere Personen weitergegeben werden (Anmerkung: Gesichtstransplantation --> es entsteht ein neues, „drittes“ Gesicht.)
- ☞ Die meisten der verwendeten Merkmale sind verhältnismäßig unveränderlich - über die Lebensdauer einer Person gesehen.
- ☞ Je nach Art des Merkmals ist die Fälschungssicherheit relativ hoch.
- ☞ Kein Merken und Vergessen von Passwörter mehr.
- ☞ (Noch nicht vollständige) Automation der Zutrittskontrolle ohne PIN möglich.

Die Nachteile dagegen sind:

- ☞ Vorurteile gegen neue Systeme.
- ☞ Kriminalisierung des Systems (bei Fingerabdrucksystemen denkt man an die Polizei).
- ☞ Überwachungsängste (cf. biometrische Daten in neuem Pass --> amerikanische Bestimmungen).
- ☞ Angst vor Missbrauch durch den Betreiber.
- ☞ Angst vor Verlust (z.B. Finger)
- ☞ Angst, der Persönlichkeitsschutz könnte nicht mehr gewährleistet sein.
- ☞ Hygienische Bedenken spielen oft eine Rolle.
- ☞ Ohne Bedien(not-)personal noch nicht möglich.

2.10. Vergleiche

2.10.1 Vergleich der verschiedenen Biometrieverfahren

Rang	Genauigkeit	Benutzer- freundlichkeit	Kosten	MOC(*)
1	DNA	Stimme	Stimme	Finger
2	Iris	Gesicht	Unterschrift	(Stimme)
3	Retina	Unterschrift	Finger	
4	Finger	Finger	Gesicht	
5	Gesicht	Iris	Iris	
6	Unterschrift	Retina	Retina	
7	Stimme	DNA	DNA	

Quelle: Morgan Keegan&Co Report Januar 2001

(*) MOC = Match on Card, bezeichnet ein Verfahren, dass nicht nur die Referenzdaten auf der Chipkarte gespeichert hat, sondern auch der Vergleich (die Verifikation) selber geschieht auf der Chipkarte. Der Vorteil dieses Verfahrens ist, dass gewisse Manipulationen ausgeschlossen werden.

2.10.2 Vergleich Biometrie versus klassische Systeme

System	Vorteile	Nachteile
PIN/Passwort	Bei der richtigen Eingabe ist - Systemfehler ausgenommen - die FRR = 0.	Kann vergessen, gestohlen, ausgespäht oder erraten werden. D.h. FAR > 0
Ausweis	Bei vernünftigen Fotos ist die FRR klein. Ein Ausweis ist vertrauens-erweckend.	Kann gestohlen oder gefälscht werden. D.h. FAR > 0
Unterschrift	Die FRR ist nahezu 0.	Kann gefälscht werden. D.h. FAR > 0
Biometrie	Ist immer dabei und kann nicht verloren gehen. Kann nicht gestohlen werden.	Können sich durch Verletzungen, Krankheit oder Verschmutzungen ändern. FAR > 0 und FRR > 0

2.11. Marktzahlen

Ein paar Marktzahlen aus [MB].

- ☞ Weltweit gibt es 200 Anbieter von biometrischen Systemen.
- ☞ Markt volumen 1999: 100 Mio USD, davon 60% in USA.
- ☞ Geschätztes Markt volumen 2010: 1 - 2,5 Mrd. USD.

2.12. Anwendungen

Grundsätzlich gibt es „unbeschränkte“ Anwendungsfälle für biometrische Systeme. Überall da, wo die Identität einer Person zweifelsfrei festgestellt werden soll, ist es prinzipiell möglich mit Biometrischen Systemen zu arbeiten.

2.12.1 Zutrittskontrolle

- Kundenschließfächern in Banken
- Zutritt zu Banken, Gefängnissen, Kernkraftwerken, militärischen Anlagen, aber zunehmend auch in der Industrie und in weiteren Dienstleistungsbetrieben.
- Zutritt zu Computerräumen.
- Mittels Gesichtserkennung Zutritt zu Fussballspielen kontrollieren (resp. Wegweisung von Personen, die Stadionsperre haben.)
- Einchecken bei Flughäfen.
- Wegfahrsperrern bei Autos.
- Neuer resp. neuester CH-Pass.

2.12.2 Zeiterfassung

Vorteil gegenüber den herkömmlichen Systemen ist der verhinderte Betrug von nicht geleisteten Arbeitsstunden.

Man geht davon aus, dass die Betrugsrate bei herkömmlichen Zeiterfassungssystemen bei etwa einer Stunde pro Mitarbeiter und Woche liegt.

In Australien ist bei einer Supermarktkette ein solches System in Betrieb; die Amortisationsdauer der 500 Geräte umfassenden Investition wurde auf knapp sechs Monate veranschlagt [RB].

2.12.3 Computersicherheit

Von PC-Systeme über integrierte Computersysteme gibt es alles.

2.13. Evaluationskriterien

Folgende Kriterien müssen von einem biometrischen System bei der Evaluation bekannt sein.

- Welcher Typ von Merkmalen soll überprüft werden.
- Benutzerakzeptanz
- EER
- Geschwindigkeit (enrollment time und verification time)
- Das Prozedere der Erfassung (diese ist ev. umständlich!!)
- Wieviele Datensätze haben Platz
- Preis/Kosten (einmalige und laufende)
- Weitergehende Kosten (z.B. Integration in ein bestehendes Zutrittssystem)
- Grösse
- Als Outdoor geeignet oder nicht
- Muss ein Anschluss an ein bestehendes System gemacht werden oder nicht.
- Bei Systemen, die auf Verifikation beruhen, muss man wissen, welche Art von Referenzdatenträger wird eingesetzt (Chipkarte, Datenbank, PIN usw.)
- Hygiene
- Sicherheit: Resistenz gegenüber Angriffen
- Marktverbreitung/ Erfahrungspotential
- Komfort
- Ergonomie

3 FINGERABDRUCKSYSTEME

3.1. Grundlagen der Daktyloskopie

Die Fingerabdrücke werden im wesentlichen in die folgenden 3 Grundtypen aufgeteilt: Wirbel, Schleifen und Bögen.



Bemerkung:

Für jeden Typ gibt es diverse Untertypen, auf die an dieser Stelle nicht weiter eingegangen wird.

Als Merkmale werden nicht die obigen Typen und Untertypen, sondern sehr oft die sogenannten Minuzien verwendet, das sind im einzelnen Verzweigungen (Bifurkationen), Linienenden, Inseln usw.

Ein Finger enthält folgende Minuzientypen:

- Core
- Delta
- Endungen
- Gabeln (Bifurkation)
- Inseln
- usw.

3.2. Die Aufnahmeverfahren

Optisches System; Digitalkamera:

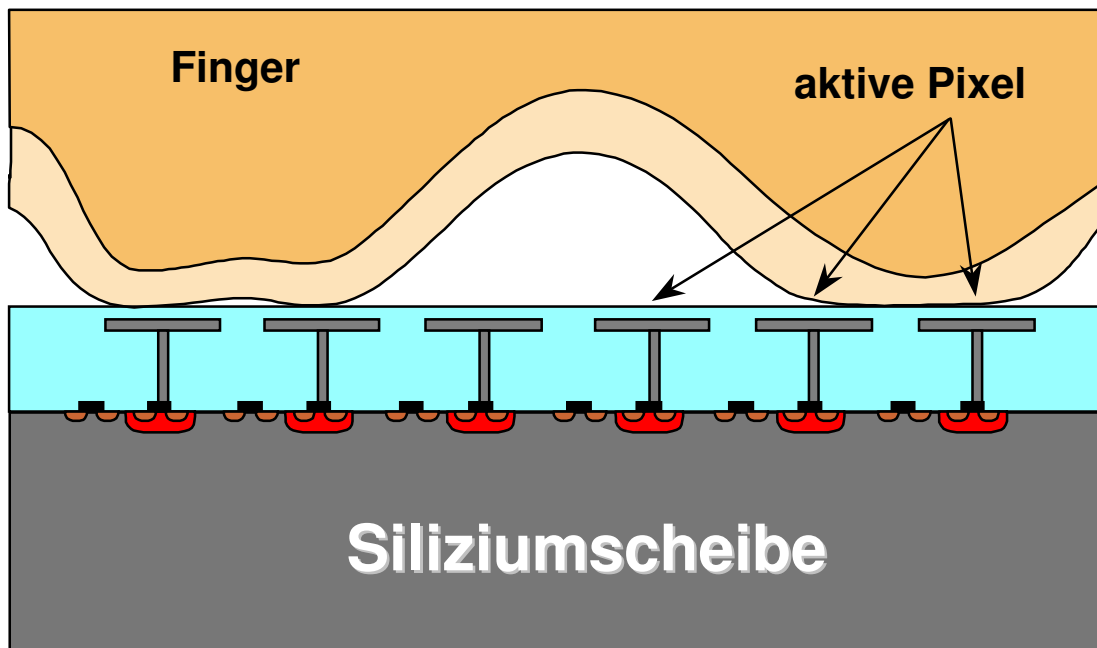
Mit einer Digitalkamera wird die Aufnahme gemacht. FingerPIN hat z.B. eine Kamera getestet, auf der die Poren, sowie der Pulsschlag ersichtlich war (es wurden 50 Bilder pro Sekunde gemacht).

Optisches System; Lasertechnik:

Der Lichtstrahl trifft in einem Winkel von 45 Grad zum aufgelegten Finger auf. Anhand der Reflexion des Lichts kann der Sensor die Linienstruktur des Fingerabdrucks erkennen.

Kapazitive Verfahren:

Kapazitive Verfahren beruhen auf der Leitfähigkeit der Haut. Überall wo ein Kontakt entsteht, entladen sich die Kondensatoren. Der Zustand der Kondensatoren - geladen oder entladen - ergibt das Bild des Fingerabdrucks.



(Z.B. Das von Siemens entwickelte Verfahren Identix resp. Fingertipp).

Infrarot Verfahren:

Infrarot-Sensoren funktionieren ähnlich wie die kapazitiven, nur daß bei dem Kontakt des Fingers mit dem Sensor keine Ladung, sondern Wärme ausgetauscht wird. Die Erhebungen geben, da sie Kontakt haben, die Wärme besser ab, als die Rillen. Die Wärmedifferenzen auf dem Sensor ergeben das Bild des Fingerabdrucks.

3.3. Die Vor- und Nachteile

3.3.1 Vor- und Nachteile gegenüber anderen Systemen

Die Vorteile der Fingerabdruckerkennung liegen in

- der langen Erfahrung auf diesem Gebiet,
- der potentiell sehr kleinen Scannergröße und
- der weiten Verbreitung des Merkmals.

Nachteile liegen in

- einem möglicherweise gestörten Hygieneempfinden der Benutzer, denn nicht jeder empfindet es als angenehm, seinen Finger auf einen Sensor zu legen, den schon viele andere Benutzer angefaßt haben. Dieses Problem tritt bei allen nicht-berührungslosen Verfahren auf.
- Möglichen Akzeptanzproblemen wegen der Assoziation von Fingerabdrücken mit einer Verbrecherkartei.

Um hohen Sicherheitsansprüchen gerecht zu werden, sollte das Verfahren eine sichere Lebenderkennung enthalten.

3.3.2 Vor- und Nachteile der verschiedenen Aufnahmeverfahren

System	Vorteile	Nachteile
Kapazitive und Infrarot Verfahren	Gewisse Fälschungsversuche (Wachsabdruck) sind u.U. einfach zu abzuwehren.	In der Regel deutlich <u>weniger</u> Anzahl Pixel per cm ² , dadurch in der Regel weniger genau.
Optische Verfahren	In der Regel deutlich <u>mehr</u> Anzahl Pixel per cm ² , dadurch in der Regel weniger genau.	Gewisse Fälschungsversuche (Wachsabdruck) sind u.U. einfach zu abzuwehren. Für Digitalkameras gilt, dass die Brennweite der Linse die Grösse des Gerätes negativ beeinflusst.

4 FAQ

Frage 1: Welche sind am weitesten und am besten akzeptiert?

- ☞ Fingerabdrucksysteme (optische und kapazitive Systeme)

Frage 2: Was sind die wesentlichen Unterschiede zwischen den beiden Aufnahmeverfahren?

- ❖ Optische Verfahren:
 - ☹ Der Lebendbeweis ist eher schwieriger zu implementieren.
- ❖ Kapazitive und Infrarot Verfahren
 - ☺ Der Lebendbeweis ist eher zu implementieren.
 - ☺ Die Geräte sind eher kompakter (keine Brennweite einer Kamera, die berücksichtigt werden muss).

Frage 3: Welche Systeme haben die besten Aussichten?

- ☞ Iris
- ☞ Retina

Grund: Ich vermute, dass dort die Veränderungen durch Verletzungen und Verschmutzungen am kleinsten sind (im Gegensatz zu den Fingerabdrücken).

Frage 4: Wohin geht der Trend?

Trend: Wegen der Hygiene, vermute ich in Richtung „berührungslos“.

Frage 5: Ist DNS schon ein Thema?

Nein

Frage 6: Welches ist das beste (Fingerprint-) System?

Alle 2 Jahre Wettbewerb mit standardisierten Daten (FVC = **Fingerprint Verification Competition**, cf. <http://biometrics.cse.msu.edu/publications.html>)

5 GRENZEN DER BIOMETRIE

Argumentation 1: Im Notfall nehmen wir die PIN!!

Diese Argumentation stimmt so nicht. Denn schlussendlich ist das System nur noch so sicher wie die PIN selber.

Grund: Der Dieb stiehlt die PIN (z.B. ec-Karte) und gibt sich biometrisch zu erkennen, er wird (hoffentlich abgewiesen), aber er kann sich mit der PIN trotzdem authentisieren.

Argumentation 2: Wir kombinieren mehrere Biometrische Systeme!!

Grundsätzlich können mehrere System mit „und“ (d.h. alle Systeme müssen „ja“ sagen.) oder mit „oder“ (d.h. mindestens ein System muss „ja“ sagen) kombiniert werden.

⊗ Bei einer „und“ Kombination, kann die FAR verkleinert werden, die FRR erhöht sich aber.

⊗ Bei einer „oder“ Kombination, kann die FRR verkleinert werden, die FAR erhöht sich aber.

Kombinationen der Art „ein bisschen von dem und ein bisschen vom anderen“ müssen gut ausgetestet und untersucht werden. Man könnte ansonsten Überraschungen erleben.

Argumentation 3: Bei PC-Systemen läuft das ganz gut!!

Das ist soweit richtig. Das System kann aber auch bez. FRR optimiert werden. D.h. a priori wird angenommen, dass die Wahrscheinlichkeit klein ist, dass ein Fremder an den PC geht. Somit kann die FRR verkleinert werden, das systembedingte Erhöhen der FAR wird kaum bemerkt.

Argumentation 4: Biometrische Verfahren sind absolut individuell!!

Das ist absolut richtig. Nur die Frage ist, ob der Computer die Einmaligkeit erkennt oder nicht.

Wunschzenarium 1: Raten von 1: 1'000'000 sind möglich!!

Ich halte eine Rate von 1:1'000'000 für die EER nicht realistisch.

Die Gründe:

- Die Verknüpfung von FRR und FAR
- Niemand weiss, wie die Kurven der FAR und FRR in Wirklichkeit aussehen.
- Was heisst EER = 1: 1'000'000? Ist das bezogen auf die Menschheit, oder nur auf diejenigen, die überhaupt erfassbar sind? Den beispielsweise gibt es Personen, die zum vorne herein ganz schlechte „Fingerprintler“ sind: Banker, die viel mit Notenzählen beschäftigt sind, Putzfrauen, die häufig scharfe Putzmittel benutzen, Kletterer, die oft ihrem Hobby frönen usw. Im weiteren gibt es Personen, die zumindestens in gewissen Zeiten schlechte „Fingerprintler“ sind: Maler, Bauarbeiter usw. während ihrer Arbeit.

Wunschzenarium 2: Bancomat und Biometrie

Die Idee, die man oft hört ist die folgende: Keine Karte und kein PIN mehr!! Wenn man Geld braucht, so geht man mit dem Finger zum Bancomat, und „That's it!“

Aber das ist es eben nicht:

- Dieses Art von Überprüfung ist eine Identifikation. Die Identifikation ist viel, viel schwieriger als eine Verifikation. Es braucht ungefähr die quadratisch bessere Rate um auf die gleiche EER wie bei der Verifikation zu kommen. D.h. um eine Rate von 1: 1'000'000 bei Identifikation zu haben ist vergleichsweise wie 1: 1'000'000'000'000 bei der Verifikation.
- Die Gefahr von falschen Belastungen wäre zu gross. In diesem Zusammenhang würde stellt sich noch eine andere Frage: Wie kann der Kunde falsche Belastungen beweisen?

6 ZUSAMMENFASSUNG

- ⌘ Genauigkeit liegt im Bereich 1: 1000 (bei Fingerabdrucksystemen) bis 1: 10' 000 (Systeme die auf Iris und Retina beruhen).
- ⌘ Beim Einsatz eines Biometrischen Überprüfungssystem muss nach wie vor ein Notfallszenarium definiert sein, um die falschen Rückweisungen zu beheben.
- ⌘ Für Einsatz in einem lokalen Umfeld (Zutrittssystem in Firmen, wo eine zentrale Stelle wie Hausdienst erreichbar ist) geeignet.
- ⌘ Als nationales, unbedientes System - wie beispielsweise ein Bancomatsystem - noch (lange) nicht geeignet.

7 GLOSSAR

Biometrie: Messen von Körpermerkmalen.

Daktyloskopie: Fingerabdruckverfahren.

Erkennungsraten:

EER: „equal error rate“: Rate, wo $FAR = FRR$. D.h. das System ist so eingestellt, dass die Rate der unberechtigten Zulassungen gleich hoch ist wie die Rate der falschen Abweisungen.

FAR: „false acceptance rate“ = Zulassen von Unberechtigten. D.h. Wieviele (als Wert zwischen 0 und 1) Unberechtigte werden als Berechtigte erkannt.

FRR: „false reject rate“ = Ablehnen von Berechtigten. D.h. Wieviele (als Wert zwischen 0 und 1) Berechtigte werden als Unberechtigte erkannt. M.a.W. Wieviele Berechtigte werden (fälschlicherweise) abgewiesen.

Finger rotation: Um wie viel kann der Finger um die Längsachse verdreht sein.

Finger displacement: Erlaubte Verschiebung des Fingers.

Minuzien: Merkmale des Fingerabdrucks.

Registrierzeit: (enrolment time); die Zeit für die Neuaufnahme einer Person.

Verifizierzeit: (verification time); die Zeit für die Erkennung einer registrierten Person.

Identifikation: Es wird die Frage beantwortet: „Wer ist es?“

Verifikation: Es wird die Frage beantwortet: „Ist es derjenige, der er vorgibt zu sein?“

8 REFERENZEN UND WEITERFÜHRENDE LITERATUR

- [AK]: Albrecht Kimmich, „Gib Deinen Finger, Dein Auge, Dein Gesicht...“, Artikel im Organisa - tor, 11/2001.
- [CC]: Clemens Cap, Vorlesungsunterlagen der Blockvorlesung über Chipkarten im WS 2002/03 an der Uni Zürich.
- [JA]: Julian Ashbourn, „Biometrics, the Complete Guide“, Springer Verlag.
- [JS]: Josef Schuler, „Fingerzeig“, im Sicherheits-Forum 5/2001 und im IT-Security-Special, 6/2002.
- [HS]: Harald Seiffert, „Hightech macht's möglich: biometrische Systeme“, Vortragsunterlagen, SSI Fachtagung 99.
- [MB]: Michael Behrens, Richard Roth, „Biometrische Identifikation“, Vieweg Verlag, 2001, ISBN 3-528-05786-6.
- [MK]: Morgam Leegam → Co Report Januar 2001.
- [NZZ]: NZZ am Sonntag, 11. Aug. 02, „Der grosse Bruder übt noch...“.
- [PO1] <http://www.protector-online.com/>
- [PO2] Norbert Pohlmann, Vortrag „Biometrie als Schlüssel zur SmartCard“
- [RB]: René Brüderlin Artikel in „Protector“, 1999
- [RV]: Roman Vögtli, Diplomarbeit NDS-INS 3, „BIOMETRISCHE VERFAHREN UND DE- REN RECHTLICHER ASPEKT“
- [SH]: Stefan Hanke „Verfahren der biometrischen Authentisierung und deren Unterstützung durch Chipkarten“, Studienarbeit, 1999, Universität Hamburg.
- [SZ]: SonntagsZeitung, 26. Mai 2002, Seite 133.