

## BIOMETRIE

Ein grundsätzliches und schwerwiegendes Sicherheitsproblem der gesamten Computertechnologie ist die Abhängigkeit in der Verwendung von Paßworten oder PIN Codes. Daher setzt sich die Biometrie mehr und mehr als Ersatz für bisher verwendeten Methoden zur Identifizierung oder Verifizierung von Personen durch.

Biometrie ist die Übertragung mathematischer Methoden auf Objekte der Biologie. Oder anders gesagt: Eine Überprüfung erfolgt nicht aufgrund eines PIN-Codes, sondern aufgrund eines BIO-Codes. Damit ist es möglich, die bisher ausschließlich ereignisbezogene Prüfung durch eine personenbezogene Prüfung zu ersetzen.

### PIN

Die Sicherheit einer PIN läßt sich im Prinzip leicht berechnen:

Falls alle Ziffern mit gleicher Wahrscheinlichkeit vorkommen (was bei der EC-Karte nicht ganz stimmt), so würde bei einer vierstelligen Zahl nur einer von 10 000 Versuchen zum Erfolg führen - die Wahrscheinlichkeit eines Zufallstreffers beträgt also  $10((E))-4$ . Falls aber andererseits jemand die Nummer kennt, so steigt seine Chance, ein fremdes Konto abzuräumen, sprunghaft auf 1. Ein einfaches Beispiel hierfür ist der verlorene Geldbeutel, in dem sich neben der EC-Karte auch die Geheimnummer befindet. Doch wie kann die Sicherheit biometrischer Verfahren festgestellt werden?

Es sind vor allem die Umfeldbedingungen entscheidend – bei wechselnden Lichtverhältnissen z.B. vor einem Tresor kann bei der Gesichtserkennung die bis zu zehnfache Fehlerrate auftreten gegenüber kontrollierten Laborbedingungen.

Ein weiteres Problemfeld sieht man in der Meßbarkeit; es gibt auf der Welt keine identischen Fingerabdrücke, aber die Wahrscheinlichkeit, daß ein Sensor zwei Abdrücke als identisch erkennt, kann durchaus im Bereich einiger Promillen liegen. Grund sind technische Beschränkungen wie verschmutzte oder trockene Finger, wodurch sich undeutliche Meßsignale und Schwierigkeiten bei der Bildverarbeitung ergeben. Das hängt auch von dem Referenzabdruck ab, der zuvor vom gleichen System aufgenommen wird. Dabei ist darauf zu achten, daß diese Referenz eine besonders hohe Qualität besitzt.

Von Vorteil sind mehrere Referenzen, um die Wahrscheinlichkeit der korrekten Identifikation zu erhöhen.

Eine weitere Schwierigkeit der Bestimmung von Fehlerraten ist die Vergleichbarkeit verschiedener Verfahren. Die Gesichtserkennung und der dynamische Unterschriftenvergleich haben mit etwa 3 % dieselbe Fehlerrate. Dabei beinhaltet jedoch das Meßverfahren dynamischer Schriftenanalyse auch trainierte Fälschung; werden, ähnlich der Gesichtserkennung, nur Tausende von zufälligen Schriftproben verglichen, sinkt die Fehlerrate beim Unterschriftenvergleich auf etwa 0.1 Prozent.

Als Ergebnis einer Untersuchung wird im allgemeinen die EER (Equal Error Rate) angegeben, bei der die Wahrscheinlichkeit, einen berechtigten Anwender abzuweisen, ebenso hoch ist, wie die, eine unberechtigte Person zuzulassen.

Über die Entscheidungsschwelle wird die Erkennungsfähigkeit eines Systems gesteuert. Über diese läßt sich das Verhältnis von FAR (False Acceptance Rate) zu FRR (False Rejection Rate) verändern. So ist z.B. eine Gesichtserkennung sicherer, wenn der Merkmalsvergleich besonders streng durchgeführt wird; damit erhöht sich auf der anderen

Seite aber die Wahrscheinlichkeit der Abweisung berechtigter Personen.

Letztendlich ist noch anzumerken, daß die Sicherheit biometrischer Identifikation keinesfalls alleine betrachtet werden kann - vielmehr ist diese Bestandteil eines Systems. Bei z.B. Chipkarten-Anwendungen muß sichergestellt sein, daß das gesamte System sicher ist - besonders in Bezug auf die Referenzdaten, deren Kopie oder Verfälschung von außen nicht möglich sein darf.

Anhand der biologischen Eigenschaften lassen sich biometrische Systeme in zwei Kategorien trennen:

a., Systeme, die auf physiologischen Merkmalen wie Gesichtszügen oder Fingerabdruck basieren. Diese Kennzeichen bleiben ein Leben lang mehr oder weniger konstant - jedoch erschweren Variationen wie unterschiedliche Finger oder andere Lage die Erkennung.

b., Systeme, die dynamische Kennzeichen wie die Bewegungen beim Schreiben oder die Stimme analysieren. Diese Merkmale variieren von Natur aus; kein Muster läßt sich exakt reproduzieren. Da aber jedes dynamische Verhalten einen physiologischen Bestandteil hat, lassen sich auch damit Personen identifizieren.

Im folgenden sind die unterschiedlichen biometrischen Merkmale mit den wichtigsten Eigenschaften aufgeführt:

### Gesichtszüge:

Aufnahme über Kameras (CCD, Video, Infrarot). Unterschiede in den Gesichtszügen infolge einer geänderten Position des Anwenders oder anderer Beleuchtung können zu Erkennungsfehlern führen. Aufgrund der "Beobachtung" ist mit Akzeptanzproblemen zu rechnen ("Big Brother is watching you"). Die Erkennung muß dreidimensional erfolgen, da nur durch die Bewertung von Reflexionen eine Abgrenzung zum Hintergrund und Kopien (z.B. Nachahmungen durch Bilder, Fernsehen, künstliche Köpfe) möglich ist.

### Fingerabdruck:

Optische, kapazitive, infrarote oder Ultraschall-Sensoren. In der praktischen Umsetzung sind z.B. Schmutz oder Kälte sowie extreme Lageabweichungen des Fingers bei der Aufnahme problematisch. Ausnahme Thermo-Zeilen Sensoren sind unempfindlich gegen verschmutzte, kalte, trockene und feuchte Finger.

### Stimmerkennung:

Mikrofon als Sensor. Problematisch ist die natürliche Schwankung der Stimmung durch z.B. Gefühle oder aber Krankheit oder bei starken Hintergrundgeräuschen. Vorteil ist, daß prinzipiell eine Identifikation auch über Telefon möglich ist. Auf der anderen Seite ist eine Vor-Ort-Erkennung notwendig, um Nachahmung z.B. mittels Aufzeichnung vorzubeugen.

### Irisabtastung:

Aufnahme über Kamera(s). Aufgrund der Einzigartigkeit von Iris-Mustern ist die Fehlerrate sehr gering. Auf der anderen Seite ist die Anwendung komplex und kann Fehler verursachen.

### Dynamische Schrifterkennung:

Erfassung über Stifte oder Schreibtablets mit Beschleunigungs- und Neigungssensoren. Die natürlichen Schwankungen der Schriftdynamik führen dazu, daß u.U. mehrere Sätze gültiger Unterschriften als Referenz dienen müssen, um die Fehlerrate geringer zu halten. Damit erhöht sich aber auch die Gefahr der Fälschung.

## BIOMETRIE AM BEISPIEL DER FINGERABDRUCK-ERKENNUNG.

Von allen biometrischen Systemen hat sich aber die Fingerabdruck-Erkennung als das universellste durchgesetzt. Die heute verwendeten Fingerprint Input Devices sind klein, kostengünstig. Sind einfach zu bedienen und können in nahezu jedem beliebigen Gerät verwendet werden. Die moderne Computerindustrie hat schon frühzeitig diese Notwendigkeit erkannt. So sind gerade in den letzten zwei Jahren zahlreiche Fingerabdruck-Erkennungssysteme namhafter Hersteller auf den Markt gekommen.

### DIE FINGERABDRUCKERKENNUNG:

Fingerabdrucke sind ein unverwechselbares Kennzeichen eines jeden Menschen. Fest verankert in der Rechtsprechung und der forensischen Medizin gilt der Fingerabdruck als eindeutiges Beweismittel.

Bei der kommerziellen Fingerabdruck-Erkennung, wie zum Beispiel der Paßwortsatz für das Logon in Computersystemen oder für die Zutrittskontrolle werden etwas vereinfachte und praxisnahe Verfahren verwendet. Sind im erkennungsdienstlichen Bereich die „gerollten“ Fingerprints (von Nagelbettkante zu Nagelbettkante) Standard, so werden im kommerziellen Bereich ausschließlich „Flat Prints“ verwendet.

### EINSATZGEBIETE DER FINGERABDRUCKERKENNUNG:

Eine typische Anwendung der Fingerabdruck-Erkennung ist das Logon in Computersystemen. Einfach den Finger auf den Scanner legen und die Anmeldung am PC oder ins Netzwerk wird ohne die Eingabe eines Paßwortes durchgeführt.

Ein weiteres Anwendungsgebiet ist die Zutrittskontrolle. Fingerabdruck-Terminals verwalten autonom oder über ein Netzwerk die Fingerabdruckdaten und geben bei positiver Überprüfung über ein eingebautes Relais eine Tür frei oder arbeiten als Zeiterfassungssystem.

Vor allem bei der Zutrittskontrolle und der Zeiterfassung werden bei Neuinstallationen vermehrt Fingerabdruck-Terminals eingesetzt. Dabei ist die Hochsicherheit, die solche Systeme bieten eher zweitrangig. Daß solche Systeme ohne Schlüssel oder Karte auskommen wird als entscheidendes Argument für die Anschaffung angeführt.

Etwas anders sieht es mit dem Anmelden an einen PC oder an ein Netzwerk (Logon) über Fingerabdruck aus. Hier sind die Paßwortüberprüfungsroutinen der Betriebssysteme, weil kostenlos, so in den Strukturen verankert, daß hier ein großer (Sicherheits-) Nachholbedarf besteht.

Ohne den Einsatz von biometrischen Systemen sind einige Bereiche mit herkömmlichen Mitteln nicht lösbar. Z.B. die Authentifizierung eines Benutzers im Dokumenten- oder Qualitäts-Management, bei digitaler Unterschrift, e-Banking, Personen-Identifikation in Haftanstalten, bei Grenzkontrollen, bei sozialen Leistungsempfänger,...

### PRAXISTAUGLICHKEIT:

Sind Fingerabdruck-Erkennungssysteme auch in der rauen Wirklichkeit des Alltags brauchbar? Die Antwort ist ein klares JA. Aber eines soll nicht unerwähnt bleiben: Es bedarf, wie es so schön heißt eines „kooperativen“ Benutzers, der einige wenige Spielregel beherzigt. Denn, ein irgendwie über das Scannerfenster gewischer verdreckter oder ein gerademal für Sekundenbruchteile hingehauchter Finger bereitet optischen Scannern, aber auch Chip Sensoren Probleme. Das nicht überraschende Ergebnis ist dann eine Ablehnung.

### DAS PRINZIP:

Das Prinzip ist denkbar einfach. Eine Scannereinheit, das kann eine opto-elektronische Einheit (CCD Kamera) oder ein kapazitiver Chip-Sensor sein, erstellen ein digitales Bild des Fingerabdrucks. Aus diesem Bild werden die Merkmale mittels eines Erkennungs-Algorithmus extrahiert (Encoding) und anschließend gespeichert (Enrollment). Das Speichermedium kann eine Festplatte, eine Chipkarte ein FlashRAM oder aber auch ein 2 dimensionale Barcode - ausgedruckt auf Papier - sein. Bei einer anschließenden Prüfung werden neuerlich die Fingerabdruck-Bilddaten extrahiert und mit den gespeicherten Daten verglichen (Matching).

Dabei werden zwei Prüfverfahren unterschieden:

#### a) Die Verifikation („one-to-one matching“- 1:1).

Es ist das derzeit am häufigsten verwendete Verfahren. Dabei werden die extrahierten Daten des zu prüfenden Fingerabdrucks nur mit einem gespeicherten Fingerabdruck verglichen. In der Praxis bedeutet das, daß bekannt sein muß, welche Daten verglichen werden sollen. Sie müssen also vorher mittels PIN oder User ID aufgerufen werden.

Eine vergleichsweise einfache Aufgabe für den Erkennungs-Algorithmus, sowohl was die Genauigkeit als auch die Zeitdauer für den Vergleich betrifft, da ja nur ein Fingerabdruck verglichen wird.

#### b) Die Identifikation ( „one-to-many matching“ - 1:N).

Dabei werden die extrahierten Daten des zu prüfenden Fingerabdrucks mit allen gespeicherten Fingerabdruck-Daten aus einer Datenbank verglichen. Dafür sind weitaus leistungsfähigere und genauere Prüfverfahren und eine hohe Rechenleistung notwendig, um akzeptable Matchingzeiten zu erreichen.

### SCHUTZ DER PERSÖNLICHEN (FINGERABDRUCK) DATEN:

In der kommerziellen Nutzung des Fingerabdrucks werden die Merkmale des Fingerabdrucks aus den Fingerprint-Bilddaten mittels mathematischer Verfahren (Encoding) extrahiert. Nur die extrahierten Daten werden für einen nachfolgenden Vergleich gespeichert. **Eine Umkehrung zu dem ursprünglichen Fingerabdruck-Bild ist dabei nicht möglich.** Deshalb ist auch ein Abgleich mit Bilddatenbanken nicht möglich.

### FINGERPRINT INPUT DEVICE:

Am Anfang der Fingerabdruck-Erkennung steht die bildgebende Einheit. Sie erstellt ein Abbild des Fingerabdrucks in digitalisierter Form. Sie teilen sich in verschiedene Gruppen.

Nachstehende Info \*

- Statisch kapazitiver
- Dynamisch kapazitiver
- Lumineszierend kapazitiver
- Optisch reflexive
- Optisch streuende
- Optisch transmissive mit Lichtleiterplatte
- Optisch kontaktlose
- Akustische (Ultraschall)
- Drucksensitive
- Thermische Zeilensensoren
- Kapazitive und optische Zeilensensoren

Alle Fingerprintsensoren versuchen ein digitales Bild der Finger Oberfläche zu erzeugen. Dieses Bild hat üblicherweise eine Auflösung von 500 dpi für die einzelnen Bildpunkte (Pixel genannt). Die Bilderzeugung selbst kann für jeden Sensortyp anders aussehen:

#### STATISCH KAPAZITIVER SENSOR

Hier steht für jedes Pixel eine Elektrode zur Verfügung, die die Kapazität zu den Nachbarelektroden/-pixeln mißt.

#### DYNAMISCH KAPAZITIVER SENSOR

Hier erfolgt die Kapazitätsmessung per Wechselspannung. Auch hier können Inter-Pixel- und Pixel-Erde-Messungen angewendet werden.

#### LUMINESZIEREND KAPAZITIVER SENSOR

Eine Elektrolumineszenzfolie mit einer durchsichtigen Rückseitenelektrode benutzt auf der Vorderseite den Finger als Gegenelektrode. Dort, wo die Fingerlinien aufliegen, sind die elektrische Feldstärke und damit das Leuchten am größten. Somit entsteht auf der Rückseite ein leuchtendes Abbild der Fingerlinien, das ähnlich wie beim optischen Sensor von einem Bildsensorchip erfaßt werden kann.

#### OPTISCH REFLEXIVER SENSOR (UNTERDRÜCKTE REFLEXION)

Der Finger liegt z. B. an einer Prismenfläche auf. Dort, wo der Finger mit seinen Linien das Glas berührt, wird eine Totalreflexion von Licht innerhalb des Glases gestört. Dies liefert z. B. auf einem Kamerachip die Abbildung der Fingerlinien.

#### OPTISCH STREUENDER SENSOR

Wie beim optisch reflexiven Sensor berührt der Finger eine Prismenfläche. Durch eine andere Lichtführung und Kamera-Chipanordnung wird jedoch erreicht, daß das Licht dort, wo die Fingerlinien die Glasoberfläche berühren, gestreut und vom Kamerachip ausgewertet wird. An den übrigen Stellen wird das Licht verschluckt statt reflektiert. Es entsteht also ein inverses Bild mit hellen Fingerlinien und dunklen Tälern.

#### OPTISCH TRANSMISSIVE SENSOREN MIT LICHTLEITERPLATTE

Hier wird der Finger von einer geeigneten Lichtquelle durchleuchtet. Der Finger liegt direkt auf einer Lichtleiterplatte auf, die wiederum direkt mit einem Kamerachip verbunden ist. Die Lichtleiterplatte sorgt dafür, daß der Finger nicht den Kamerachip berührt, das Licht aber trotzdem ohne Schärfeverlust und ohne sonstige Optik den Kamerachip erreicht.

#### OPTISCH KONTAKTLOSER SENSOR

Der Fingerabdruck wird über eine geeignete Optik direkt von einem Kamerachip ohne Berührung der Fingeroberfläche erfaßt.

#### AKUSTISCHE (ULTRASCHALL) SENSOREN

Hier erfolgt die Abbildung der auf Glas aufliegenden Fingeroberfläche durch sehr hochfrequenten Ultraschall.

#### DRUCKSENSITIVE SENSOREN

Bei Drucksensoren wird pixelweise der Druck des aufliegenden Fingers gemessen.

#### THERMISCHE ZEILENSENSOREN

Bei diesem Sensor bewegt man den Finger linear über ein zeilenförmiges Array aus Thermosensoren, wie man sie in Groß von automatischen Türöffnern kennt. Die Thermosensoren registrieren zeitliche Temperaturdifferenzänderungen, die zwischen Fingerlinien und -rillen unterschiedlich ausfallen.

#### KAPAZITIVE UND OPTISCHE ZEILENSENSOREN

Diese Sensortypen arbeiten wie die thermischen Zeilensensoren, nur daß die für jeden Bildpunkt zuständigen Einzelsensorzellen die Kapazität messen bzw. lichtempfindlich sind.

\* Quelle: <http://www.bromba.com/faq/biofaqd.htm>

#### LEBENDERKENNUNG:

Eine immer wiederkehrende Frage ist die nach der Lebenderkennung eines Fingers. Gemeint ist damit, ob ein Scanner oder Chip-Sensor auch einen künstlichen Finger akzeptiert. Sowohl

optische als auch kapazitive Systeme verfügen - sozusagen von Haus aus - über eine eingebaute Lebenderkennung. Bei den optischen Systemen erfolgt diese durch das eingespielte IR-Licht. IR-Licht wird von lebendem Gewebe reflektiert. Werkstoffe wie Papier, übliche Kunststoffe oder Wachs werden deshalb nicht erkannt. Dies trifft auch auf kapazitive Chipsensoren zu. Auch bei Chip-Sensoren wird eine signifikante Veränderung des elektrischen Feldes im Chip-Sensor durch lebendes Gewebe erzeugt.

Allerdings lassen sich Biometrik-Sensoren unter Laborbedingungen täuschen. Eine perfekte Lebenderkennung ist nach heutigem Stand der Technik nicht möglich.

#### METHODEN DER FINGERPRINT-ALGORITHMEN:

Zwei Methoden kommen derzeit zur Anwendung:

a) Die Mustererkennung (Pattern Recognition). Die Mustererkennung (wie bei OCR) benötigt lediglich ein 1-Bit monochromes Bild des Fingerabdrucks und legt geometrisch strukturierte Formen oder Vermessungen über den Fingerabdruck. Diese Methode hat den Vorteil, wenig Rechenleistung zu benötigen und wird in Systemen verwendet, in denen Scanner und Auswertung in einer Einheit verbunden sind.

b) Die minutien-basierende Erkennung. Für die minutien-basierende Erkennung wird zumeist die Grauwertdynamik eines 8-Bit Gray Scale Bildes benötigt. Aus diesen werden die Linienmuster mit seinen Verzweigungen, Inseln und Bruchstellen (Minutien) hervorgehoben und Anfang und Ende, Richtung und Lage markiert. Da diese Methode aber durch aufwendige Grafikverarbeitung eher rechenintensiv ist, wird sie nur im Zusammenhang mit leistungsfähigen CPU's oder DSP's eingesetzt.

#### FINGERPRINT-ALGORITHMEN:

Fingerprint-Algorithmen bestehen aus zwei Teilen: dem Encoding und dem Matching-Algorithmus.

Der Encoding-Algorithmus extrahiert aus den Bilddaten die Fingerprint-Merkmale, die sogenannten Minutien in ein Template. Zur Ersterfassung werden die Daten des Templates gespeichert (Enrollment).

Der Matching-Algorithmus vergleicht dann ein aktuelles Template mit einem zuvor gespeicherten Referenz-Template. Wobei dem Matching-Algorithmus eine schwere Aufgabe zukommt. Da ein Scan eines Fingers niemals den anderen gleicht, auch wenn es sich immer um denselben Finger und um die gleiche Auflageposition handelt, entscheidet nur der Matching-Algorithmus auf Übereinstimmung. Er muß in der Lage sein, bei unterschiedlicher Positionierung des Fingers am Scanfenster sowohl horizontal als auch vertikal oder Drehungen (bis zu 360°) und Verformungen durch unterschiedlichen Auflagedruck den Finger zu vergleichen.

#### IMAGE PRE-PROCESSING:

Dem Encoding ist noch die Bildbearbeitung vorgeschaltet (Image Pre-Processing). Der Bildbearbeitung kommt dabei eine besondere Stellung zu. Diese sorgt automatisch für die Eliminierung von Störungen und Unterbrechungen (Image Quality Control) und die Image-Skelettierung der Fingerabdruck. Ist das gelieferte Bild nicht einwandfrei, kann auch der beste Fingerprint-Algorithmus nichts ausrichten.

Dies ist insbesondere bei Problemfingern wichtig, die durch extreme Hauttrockenheit oder Hautfeuchtigkeit sowie physiologisch bedingte Merkmalsarmut ein klares Bild verhindern. Sind allerdings zu wenig verwertbare Merkmale vorhanden, so werden diese bereits bei der Ersterfassung von einer Speicherung ausgeschlossen.

#### GENAUIGKEIT VON BIOMETRISCHEN METHODEN:

Am Beispiel der Fingerabdruck-Erkennung. Für die Bewertung sind folgende Kenngrößen wichtig.

FAR - Die Falsche Akzeptanz Rate bezeichnet die durchschnittliche Häufigkeit, mit der ein anderer Fingerabdruck erkannt wird (Falsche Erkennung, typisch kleiner als 0.001%).

FRR - Die Falsche Reaktions- Rate bezeichnet die durchschnittliche Häufigkeit, mit der ein Fingerabdruck nicht erkannt wird (Falsche Ablehnung, typisch kleiner als 0.1%).

EER - Equal Error Rate setzt sich aus FAR und FRR (als Kurve dargestellt) zusammen und beschreibt den Punkt wo sich beide überschneiden.

Es gilt daher: Je höher die Genauigkeit (FAR), desto größer die Gefahr einer falsche Ablehnung (FRR) wobei die Wahrscheinlichkeit, einen berechtigten Anwender abzuweisen, ebenso hoch ist, wie die, eine unberechtigte Person zuzulassen.

#### ZUSAMMENFASSUNG:

Stellt der falschen Ablehnungen höchstens eine verminderte Benutzerakzeptanz dar, die zu Wutausbrüchen beim Benutzer führt und in Folge zur Ablehnung des verwendeten Systems, ist die falsche Erkennung ein ernstes Sicherheitsproblem.

Wie schon Anfangs erwähnt, hat sich die Fingerabdruck-Erkennung als die universellste von allen biometrischen Verfahren

durchgesetzt. Die heute verwendeten Fingerprint-Systeme sind klein, kostengünstig und einfach zu bedienen. Sie können in nahezu jeder beliebigen Anwendung, in der Sicherheit und Bedienungskomfort wichtig sind, verwendet werden.

---

Copyright 2000 by Biometrix Int.

Autor: Harald Griesser

Harald Griesser ist Inhaber der Firma Biometrix Int., Fingerprint Recognition Systems, Wien-Österreich