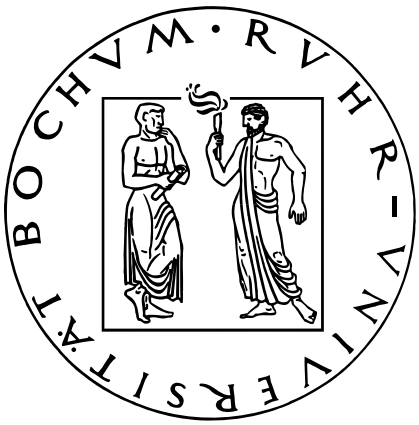
Biometrie

Ferruh Sayin

2005

Seminararbeit
Ruhr-Universität Bochum



Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

Inhaltsverzeichnis

1 Einleitung

Wenn eine ihnen bekannte Person vor ihrer Haustür steht, erkennen sie ihr Gegenüber anhand besonderer Merkmale, denn unsere Stimme, unser Verhalten, unser Gesicht sind individuell. Hier setzt die biometrische Identifikation an. Der Begriff „Biometrie“ setzt sich aus zwei griechischen Wörtern zusammen: bios - Leben und metron - Maß.
In den meisten Fällen geht es bei der Biometrie darum, eine Person zu identifizieren oder zu verifizieren, ob die Person auch wirklich die Person ist, für die sie sich ausgibt. Die Identität soll also in irgendeiner Weise nachgewiesen werden. Hier kommen bisher nur zwei Zentralbegriffe ins Spiel: Besitz und Wissen. Unter Besitz wird die tatsächliche Herrschaft über etwas (einen Ausweis oder einen Schlüssel) verstanden. Wissen bezieht sich zum Beispiel auf Kennworte, PINs, Zugangscodes und ähnliches. Damit werden gleich die Schwächen bisheriger Verfahren angesprochen. Den Ausweis können wir verlieren und das Kennwort vergessen. Außerdem sind diese Verfahren nicht uneingeschränkt und untrennbar mit einer Person verbunden. Missbrauch ist relativ unproblematisch. Biometrische Verfahren ermöglichen hingegen eine relativ eindeutige Identifikation des Betroffenen, da sie personengebundene Merkmale erfassen.
Es gibt eine Vielzahl biometrischer Verfahren, die anhand unterschiedlicher Körperteile des Menschen (z.B. Finger, Hand, Augen, Gesicht) oder anhand von Verhaltenseigenschaften (Unterschrift, Gang) versuchen, eine Person zu verifizieren oder zu identifizieren. Diese personengebundenen Eigenschaften werden unter dem Begriff biometrische Merkmale zusammengefasst.

2 Biometrische Merkmale

Biometrische Verfahren beruhen darauf, dass aus einem Merkmal einer Person ein Datenmuster abgeleitet wird, das mit einem Referenzmuster verglichen wird. Üblicherweise unterteilt man biometrische Merkmale in sogenannte aktive Merkmale, basierend auf verhaltenstypischen Merkmalen und passive Merkmale, die sich auf physiologische Merkmale beziehen.
Merkmale, die sich eine Person im Laufe des Lebens aneignet gehören zu den aktiven Merkmalen. Merkmale dieser Art werden nicht direkt sondern indirekt vom menschlichen Körper abgeleitet. Auch diese sind einzigartig, aber wesentlich schwieriger zu messen.
Merkmale, die sich in der Entwicklung eines Menschen zufällig ausbilden, gehören zu den passiven Merkmalen. Diese Merkmale werden direkt vom menschlichen Körper abgeleitet. Sie sind alle einzigartig bei jedem Menschen. Allerdings darf das Testen von bestimmte Merkmalen die Würde nicht verletzen.

Tabelle 2.1: Verhaltensbasierte und Physiologische Merkmale

Verhaltensbasierte (aktive) Merkmale	**Physiologische (passive) Merkmale**
Unterschriftendynamik	Irismuster
Lippenbewegung beim Sprechen	Fingerabdruck
Stimmerkennung	Gesichtserkennung
Bewegung (Gangartzyklus)	Retinamuster
Anschlagdynamik auf Tastaturen	Venenmuster
Sitzverhalten *	Handgeometrie
	Form des Ohres
	DNS
	Geruch *
	Hautwiderstand *

* im Forschung

3 Allgemeine Funktionsweise von biometrischen Verfahren

Im Folgenden soll die allgemeine Funktionsweise von biometrischen Verfahren erläutert werden.

3.1 Registrierung

Bei diesem Vorgang tritt der Nutzer zum ersten Mal an ein bestimmtes biometrisches System und lässt sich registrieren (*Enrollment*). Während der Registrierung werden die biometrischen Merkmale mit Hilfe von Sensoren erfasst. Die Informationen liegen damit in Form von analogen Daten vor. (vgl. Abb. 3.1)

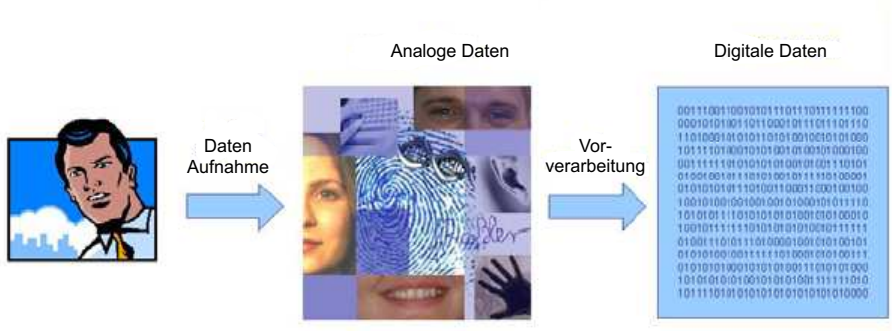


Abbildung 3.1: Datenaufnahme und Vorverarbeitung, *Quelle: [Amb03]*

Diese umfangreichen Informationen werden zu komprimierten Referenzdatensätzen (*Template*) umgewandelt, die nach einer Merkmalsextraktion die ausgewerteten Musterinformationen der Originaldaten enthalten. Wenn sich der Nutzer später gegenüber dem System identifiziert, werden seine aktuell erhobenen biometrischen Merkmale wiederum zu Datensätzen mit den ausgewerteten Musterinformationen reduziert und diese mit den Referenzdaten abgeglichen. (vgl. Abb. 3.2)

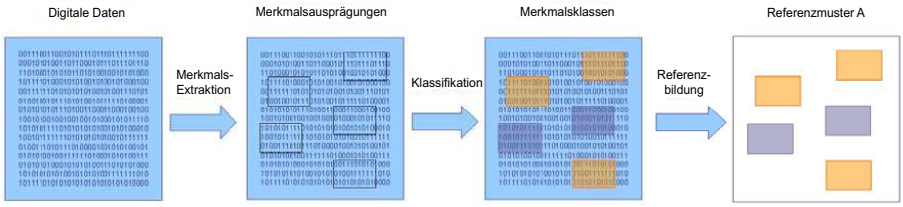


Abbildung 3.2: Merkmalsextraktion, Klassifikation und Referenzbildung, *Quelle: [Amb03]*

3.2 Identifikation und Verifikation

Bei dem Einsatz von biometrischen Systemen wird zwischen zwei Hauptverfahren, der Identifikation und der Verifikation einer Person, unterschieden. Voraussetzung in beiden Fällen ist die Registrierung.
Bei der Verifikation wird in einem 1:1 Vergleich geprüft, ob die Person, die behauptet eine bestimmte zu sein, auch den physiologischen Beweis dazu erbringen kann. Ihre aktuellen biometrischen Daten werden demnach nur mit ihren Referenzdaten verglichen. Es erfolgt also die Authentifizierung einer bekannten Person. (vgl. Abb. 3.3)

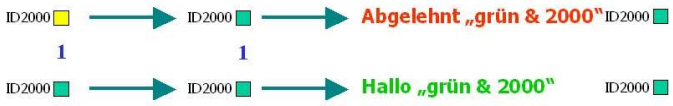


Abbildung 3.3: Verifikation, *Quelle: [Heu03]*

Bei der Identifikation wird anhand eines l:n Vergleiches die Identität des Betreffenden aus der gesamten System-Datenbank ermittelt. (vgl. Abb. 3.4). Es besteht hier also die Möglichkeit, eine zunächst unbekannte Person mit Hilfe der Datenbank zu identifizieren, sofern diese zuvor registriert wurde.

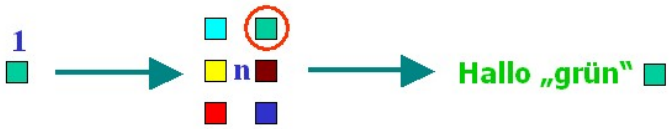


Abbildung 3.4: Identifikation, *Quelle: [Heu03]*

4 Anforderungen an biometrische Verfahren und Systeme

Biometrische Merkmale müssen unterschiedliche Anforderungen erfüllen, welche im Folgenden erläutert werden. Die Qualität biometrischer Verfahren hängt folglich stark von der Frage ab, inwieweit die körpereigenen Merkmale den folgenden Anforderungen entsprechen.

4.1 Anforderungen an biometrische Verfahren

Erfassbarkeit: Die Eigenschaften müssen in relativ kurzer Zeit messtechnisch erfassbar sein. Erst dadurch wird eine elektronische Verarbeitung möglich.
Einzigartigkeit: Die Eigenschaften sollten genügend eindeutige Merkmale beinhalten, um die Person von jeder andern zu unterscheiden. Je höher die Wahrscheinlichkeit ist, dass zwei oder mehr Menschen dieselbe Ausprägung eines Merkmals besitzen, desto unsicherer ist das biometrische Verfahren.
Permanenz: Die biometrischen Merkmale müssen zeitlich invariant sein.
Fälschungssicherheit: Wichtig ist die Lebenderkennung des Merkmals. Es sollte nicht kopiert und durch eine unechte, „nicht lebende“ Kopie ersetzt werden können.
Universalität: Jede, ausgenommen von Unfällen oder Erbkrankheiten betroffene Person, verfügt über biometrischen Merkmale. So kann garantiert werden, dass ein biometrisches System von dem Großteil aller Personen genutzt werden kann.

4.2 Toleranzschwelle

Da nicht jede Messung eines biometrischen Merkmales exakt den gleichen Wert erbringen kann, und sich einige Merkmale auch verändern können, muss dem System zur Erkennung eine gewisse Toleranzschwelle eingeräumt werden. Man spricht hier auch von skalierbaren Schwellenwerten. Die Erkennung einer Person muss auch trotz Heiserkeit, einer neuen Frisur, einem Bart, einer Schnittwunde oder etwa einer Blase am Finger hinreichend sicher erfolgen können. Insofern sollte auch bei einer nicht hundertprozentigen Übereinstimmung der Merkmale

eine Erkennung möglich sein. Im Allgemeinen stellt die Festlegung der Toleranzschwelle hohe Anforderungen an das System. Ist sie zu niedrig angesetzt, werden Personen trotz Berechtigung abgelehnt. Ist sie zu hoch angesetzt, ist keine Garantie für eine ausreichende Sicherheit mehr vorhanden. Wichtige quantitative Qualitätsmerkmale eines biometrischen Systems sind in diesem Zusammenhang die *False Acception Rate* (FAR) und die *False Rejection Rate* (FRR).

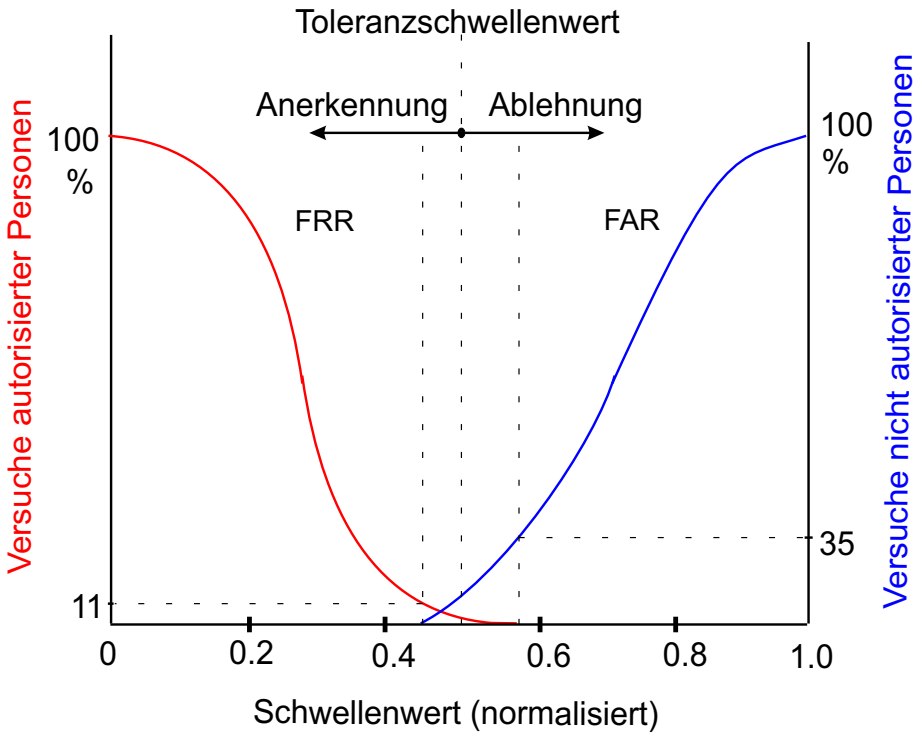


Abbildung 4.1: Toleranzschwelle, *Quelle: [Nol02]*

FAR (false acception rate): Sie gibt die Häufigkeit an, mit der nicht berechtigten Personen Zugriff gewährt wird.

FRR (false rejection rate): Sie beschreibt, wie häufig berechtigte Personen vom System zurückgewiesen werden.

Je kleiner die FAR wird, desto höher wird die FRR. Bei der Konfiguration eines Systems muss darauf geachtet werden, dass beide Werte im optimalen Verhältnis zueinander stehen. Dabei handelt es sich um einen empirischen Wert, der nur durch Tests herausgefunden werden kann.

4.3 Anforderungen an biometrische Systeme [1]

Um die Anwendung biometrischer Systeme überhaupt in Betracht zu ziehen, müssen zusätzlich zu den genannten Kriterien die folgenden Basisanforderungen erfüllt sein.

Technische Umsetzbarkeit: Das Verfahren muss die Unterscheidung einer geeignet großen Zahl von Individuen ermöglichen. Wichtige Kriterien dafür sind die einfache Erfassbarkeit des Merkmals und eine geringe Datenmenge zur Speicherung der Informationen.

Überlistungsresistenz: Das Verfahren darf durch betrügerische Techniken zumindest nur schwer beeinflussbar sein. Dieser Aspekt steht im engen Zusammenhang mit anderen Basisanforderungen, wie Akzeptanz und ökonomische Machbarkeit.

Ökonomische Machbarkeit: Die Kosten für Entwicklung und Betrieb des auf dem Verfahren aufbauenden Systems müssen in Relation zu dem Nutzen stehen. Der Nutzen ist nur gegeben, wenn das System akzeptiert wird und die Überlistungsresistenz hinreichend hoch ist.

Akzeptanz: Die Benutzer müssen sich bereit erklären, das Verfahren zu verwenden. Die Akzeptanz für Systeme, bei denen das Merkmal aktiv abgegeben wird, ist im allgemeinen höher als die Akzeptanz für Systeme, bei denen das Merkmal ohne Kenntnisnahme abgenommen wird.

[1] M. Amberg, S. Fischer, J. Rößler, 2003, S. 9

5 Klassifikation biometrischer Verfahren

Biometrische Verfahren lassen sich in physiologische (passive) und verhaltensbasierte (aktive) Verfahren unterteilen.

5.1 Physiologische Verfahren

Physiologische Verfahren basieren auf Körpermerkmalen wie z.B. der Gesichtsform, dem Handvenenmuster, dem Muster der Regenbogenhaut oder auch der DNA. Zu den physiologischen Verfahren zählen: DNA-Analyse, Analyse des Fingerabdrucks, der Fingergeometrie, der Handgeometrie, Iris-Scan, Nagelbetterkennung, Analyse des Ohrabdrucks und des Venenmusters.

5.1.1 Fingerabdruckerkennung

Biometrisches Merkmal: Fingerabdrücke werden durch reliefartig hervortretende nebeneinanderverlaufende Erhebungen der Hautleisten, den sogennanten Papillarlinien gebildet. Schleifen-, Wirbel- und Bogenmuster dienen zur Klassifikation der Struktur des Fingerabdrucks. Merkmale eines Fingerabdrucks die zur Identifikation von Personen dienen, sind: Kreuzung, Kern, Gabelung, Linienende, Insel, Delta, Pore.
Verarbeitung des biometrischen Musters: Das Bild einer Fingerkuppe wird meist mit einem Scanner aufgenommen. Diese Aufnahme kann durch optische, thermische, kapazitive, Druck- oder Ultraschallsensoren erfolgen . Aus dem Bild wird der mittlere Wert der Graustufen aller Pixel des Bildes ermittelt. Anschließend werden alle Pixel, die unterhalb des Schwellenwertes liegen, als binäre Null und die Pixel oberhalb dieses Schwellenwerts als binäre Eins dargestellt. Mit Hilfe dieses Schrittes erhält man eine Grobstruktur des Abdrucks mit Punkten, die oberhalb des Schwellenwertes liegen. Der nächste Schritt ist die Filterung der Anomalien und falsche Papillarlinien, die z.B. durch Verschmutzungen, Schweiß oder Narben hervorgerufen werden. Somit werden die Linienmuster und markanten Punkte extrahiert und in Form von Koordinaten gespeichert.

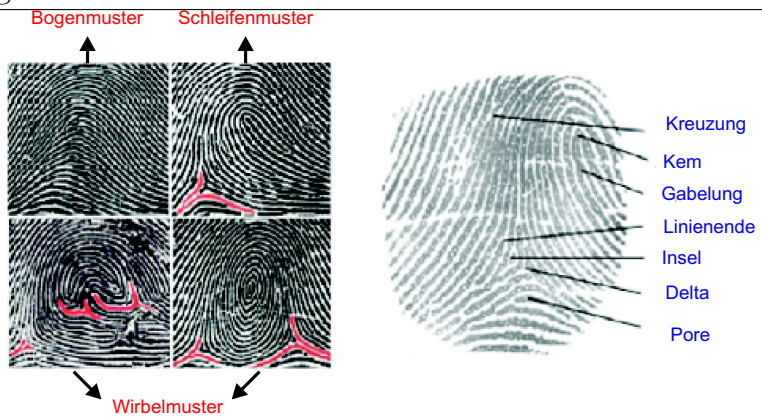


Abbildung 5.1: Grundmuster im Fingerabdruck (links) und Merkmale eines Fingerabdrucks (rechts), *Quelle: [Sch04]*

5.1.2 Gesichtserkennung

Biometrisches Merkmal: Das Gesicht umfasst die Stirn-, Augen- und Mundregion. Das Aussehen des Gesichts ist vor allem durch das Knochengerüst, die Gesichtsmuskulatur und den Haarwuchs geprägt.
Verarbeitung des biometrischen Musters: Das Gesicht wird mit Hilfe von CCD (Digitalkamera) - und Videokameras erfasst. Der Gesichtserkennungsprozess lässt sich in zwei Phasen unterteilen. In der ersten Phase muss das Gesicht im Gesamtbild gefunden und aus dem Hintergrund getrennt werden. Diese Phase wird als Face Detection bezeichnet. Die zweite Phase stellt dann die tatsächliche Erkennung des Gesichtes dar und damit die Identifikation oder Verifikation einer Person. Bei einem komplexen oder bewegten Hintergrund gestaltet sich vor allem die Gesichtsentdeckung als sehr problematisch. Für diese Aufgabe kommen mehrere Verfahren zum Einsatz. Bei der Farbanalyse werden Gesichter anhand der charakteristischen Farbe menschlicher Haut von anderen Objekten unterschieden. Die Bewegungsanalyse nutzt die Eigenschaft aus, dass sich das menschliche Gesicht immer in Bewegung befindet. Beim *Template Matching* wird nach gesichtsähnlichen Formen innerhalb des Bildes gesucht.
Nach dem Gesichtsentdeckungsprozess, wird das aufgenommene Gesichtsbild mit den Referenzbildern verglichen. Wegen unterschiedlicher Lichtbedingungen, unterschiedlichem Abstand zur Kamera, unterschiedlicher Haltung, sowie einer Reihe weiterer Faktoren (z.B. Frisur, Alterung, Brille) führen zwei zeitlich versetzte Aufnahmen eines Gesichts häufig nicht zum gleichen Ergebnis. Es gibt mehrere Methoden zum Vergleich von Gesichtern.
Ein verbreiteter Ansatz ist die Gesichtsmetrik. Dabei konzentriert sich die Erkennung auf individuelle Gesichtskennzeichen wie Augen, Nase und Mund. Es werden die Position und Größe sowie die Verhältnisse der einzelnen Kennzeichen zueinander vermessen und daraus ein Modell des Gesichts erzeugt. Beim Ver-

gleich zweier Gesichter werden die Abstände und Winkel zwischen geometrischen Punkten herangezogen.
Ein weiteres Verfahren zur Gesichtserkennung ist Eigenface. Bei diesem Verfahren geht es darum, die Unterschiede von Gesichtern zu registrieren, indem verschiedene Gesichtsbilder übereinander projiziert werden. Beim Vergleich von Gesichtsbildern ein und derselben Person lassen sich beispielsweise nur geringe Unterschiede feststellen.
Ein sehr interessantes Verfahren zur Gesichtserkennung ist *Template Matching*. Bei *Template Matching* werden die Bildsegmente der Augen, des Mundes, der Nase und des gesamten Gesichtes (Region unterhalb der Augenbrauen) verglichen. Das Verfahren Deformable Template Matching hingegen vergleicht nicht nur sondern dreht, verschiebt und verformt Bildsegmente in gewissen Grenzen. Bei einer weiteren Abwandlung dieser Methode wird mit einem Gitter gearbeitet, das über das Beispielgesicht gelegt wird. Für jeden Gitterpunkt werden dann die umgebenden Bildmerkmale aus dem Gesicht extrahiert. Bei einem Vergleich wird dieses Gitter dann so über einem Gesicht verformt, dass die größte Übereinstimmung an allen Gitterpunkten erreicht wird.

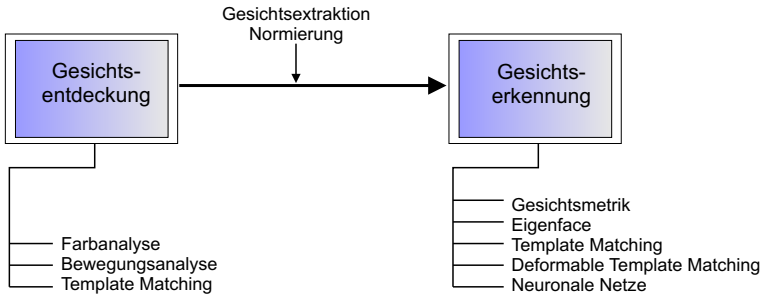


Abbildung 5.2: Prozess der Gesichtserkennung, *Quelle: [Nol02]*

5.1.3 Iriserkennung

Biometrisches Merkmal: Die Iris ist ein einzigartiges Merkmal des menschlichen Körpers. Sie enthält eine enorm komplexe Anordnung an Fasern, Flecken, Narben, radialen Furchen, Koronen und Streifen. Weiter können die räumliche Abhängigkeit und das Muster dieser Merkmale als weitere Parameter im Identifizierungsprozess verwendet werden.
Verarbeitung des biometrischen Musters: Bei der Iriserkennung wird mit einer sehr hochauflösenden Monochromkamera ein Bild der Iris aufgenommen. Nach der Aufnahme des Bildes, wird mit Hilfe eines Bildbearbeitungsalgorithmus das Auge von außen nach innen spiralförmig abgetastet. Jedesmal, wenn dabei auf ein Äderchen oder eine Pigmentkrause auftritt, wird dieser Punkt auf

der Spiralstrecke markiert. Wenn man die Spirale am Schluss der Bildbearbeitung „ausrollt“, erhält man eine Grafik ähnlich einem Barcode, welche alle Eigenarten der Iris wi derspiegelt.

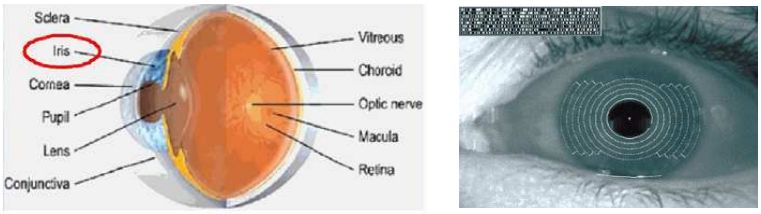


Abbildung 5.3: Lage und Struktur der Iris, *Quelle: [Gal02]*

5.1.4 Handgeometrieerkennung

Biometrisches Merkmal: Mit Hilfe der Handgeometrie kann eine Hand eindeutig identifiziert werden. Für die Bestimmung der Handgeometrie werden mehrere Merkmals-Dimensionen benötigt: Länge und Krümmung der Finger, Breite und Höhe der Finger und der Handfläche.
Verarbeitung des biometrischen Musters: Der Nutzer positioniert seine Hand auf einem Scanner. Die Hand wird mithilfe einer CCD-Kamera aufgenommen. Für die Erstanmeldung wird die Hand mehrmals aufgelegt und dreidimensional aufgenommen. Die Merkmale werden aus dem Bild extrahiert und in Form eines Merkmalsvektors gespeichert. Es werden bevorzugt Merkmale ausgewählt, die eine hohe Varianz zwischen allen Benutzern aufweisen. Für den Vergleich einer Hand mit den gespeicherten Referenzmustern wird jeweils eine Bildaufnahme angefertigt. Der Merkmalsvektor muss unabhängig von der Größe des Bildes und der Position der Finger erkannt werden.

5.1.5 Erkennung anhand eines Thermogramms

Biometrisches Merkmal: Die Thermographie ist eine Methode zur Abbildung von Objekten mittels ihrer Wärmestrahlung. Thermographie bietet eine sichere, schnelle und berührungslose Identifikationsmöglichkeit von menschlichen Gesichtern oder anderen Körperteilen. Besonders das Venenmuster der Hand ist ein einzigartiges Merkmal.
Verarbeitung des biometrischen Musters: Durch die Verteilung der Blutadern ergeben sich auf der Hand Temperaturunterschiede. Diese Temparaturunterschiede werden mit Hilfe einer Infrarotkamera erfasst. Das erfasste Bild wird zur Weiterverarbeitung digitalisiert. Nach diesem Vorgang werden aus dem vorhandenen Venenmuster die relevanten Muster extrahiert, Kreuzungs- und Ver-

zweigungspunkte identifiziert und eine persönliche Venennetzkarte generiert.

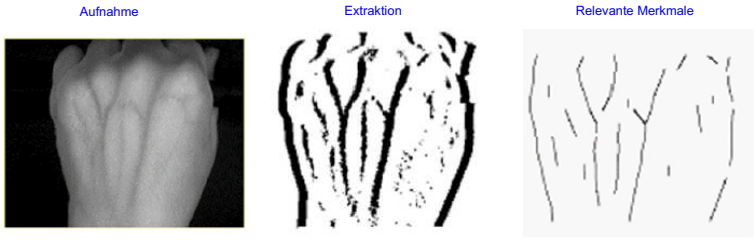


Abbildung 5.4: Erkennung eines Thermogramms, *Quelle: [Aus05]*

5.2 Verhaltensbasierte Verfahren

Verhaltensbasierte Verfahren bedienen sich bestimmter Verhaltensmerkmale. Darunter fallen u. a. die Lippenbewegung beim Sprechen, der Bewegungsablauf beim Gehen, die Stimme, der Tipprhythmus auf Computertastaturen oder die Unterschriftsdynamik.

5.2.1 Unterschriftserkennung

Biometrisches Merkmal: Jede Unterschrift besitzt ihren ganz eigenen Charakter. Bei diesem Verfahren ist sowohl das Bild der Unterschrift als auch die Dynamik bei der Erzeugung der Unterschrift wichtig.
Verarbeitung des biometrischen Musters: Bei der Unterschrifterkennung wird zwischen dem statischen (Offline-Erkennung) und dem dynamischen (Online-Erkennung) Verfahren unterschieden. Bei den statischen Verfahren erhält man die Unterschriften aus einem gespeicherten Bild und bei dem dynamischen Verfahren werden die Bilder vor Ort aufgenommen z.B. bei Notizen im PDA.

Statisches Verfahren: Bei der statischen Unterschriftsverifikation werden die geometrischen Eigenschaften der Unterschrift geprüft. Geometrische Eigenschaften sind z.B. Aufstriche, Dichten, Kreuzungen, Abzweigungen, Schleifen und Bogenformen sowie Hüllkurven. Das statische Verfahren wird folgendermaßen durchgeführt. Die Unterschrift wird mit Hilfe eines Scanners aufgenommen und als Bild im Graustufen-Format gespeichert. Zuvor wird die Schrift durch Schwellwertverfahren vom Hintergrund extrahiert. Bei diesem Verfahren geht man davon aus, dass die Schrift gegenüber dem Hintergrund dunkel ist. Das Schwellwertverfahren klassifiziert einen Pixel als Vordergrundpixel, sofern seine Intensität kleiner als der Schwellwert ist, ansonsten wird der Pixel dem Hintergrund zugeordnet. Durch

dieses Verfahren wird eine Grobstruktur der Unterschrift anhand der Pixel, die ber des Schwellenwertes liegen, dargestellt. Zur Verfeinerung der Struktur wird die Strichbreite auf ein Pixel ausgedünnt und mögliche Störpixel herausgefiltert. Das statische Verfahren ist relativ unsicher, weil es nur geometrische Eigenschaften berücksichtigt.

Abbildung 5.5: Statische Merkmale einer Unterschrift, *Quelle: [Sof03]*

Dynamisches Verfahren: Bei diesem Verfahren unterschreibt der Benutzer auf einem Tablett, das mit Sensoren ausgestattet ist. Hier werden die Unterschriftsmerkmale während des Unterschreibens ermittelt. Fr die Erkennung ist die Dynamik der Unterschrifterstellung wichtig, wobei Beschleunigung, Geschwindigkeit, Fallkurve, Länge und Unterbrechungen analysiert werden. Nach Erfassung der Referenzdaten muss ein Kennfeld aus mehreren Unterschriften erstellt werden. Die später zu erkennende Unterschrift muss in diesem Kennfeld liegen. Diese Daten werden in einer Datenbank hinterlegt und mit einer persönlichen ID versehen. ID-Informationen werden benutzt um die Referenzdaten zu extrahieren und diese mit den Werten der neueingegebenen Unterschrift zu vergleichen. Durch diesen Vergleich kann sich ein Nutzer verifizieren. Anhand eines vordefinierten Schwellwertes wird die Unterschrift anerkannt oder nicht. Dynamische Verfahren werden in der Praxis häufiger eingesetzt, da sie fälschungssicherer sind.

Abbildung 5.6: Schreibpad „Hesy Signature Pad“ (links) und dynamische Merkmale einer Unterschrift (rechts), *Quelle: http://www.hesy.de 2002*

5.2.2 Stimmerkennung

Biometrisches Merkmal: Die Stimme eines Menschen ist eine charakteristische Eigenschaft, welche in der Stimmerkennung anhand einer aktiven Sprachprobe zu Identifizierung einer Person genutzt wird. Die charakteristischen Eigenschaften der Sprache sind abhängig von der Anatomie des Stimmapparates und von den über Jahre hinweg erlernten Sprach- und Sprechgewohnheiten.
Verarbeitung des biometrischen Musters: Bei der Erfassung der Stimme durch Mikrofone wird die Schallwelle in ein analoges Signal umgesetzt. Die Methoden zur Stimmerkennung lassen sich in textabhängige und textunabhängige Stimmerkennung unterscheiden. Bei der textabhängigen Erkennung ist der gesprochene Ausdruck dem System bekannt. Das kann ein vorher festgelegtes Wort, ein Satz oder eine Serie von Zahlen sein, hierbei berücksichtigt das Stimmerkennungssytem ausschließlich den vorgegebenen Ausdruck. Dagegen akzeptiert die textunabhängige Erkennung das gesamte Vokabular. Es werden keine bestimmten Worte festgelegt. Dies erschwert die Implementierung dieses Verfahrens. Aus diesem Grund kommt hauptsächlich die textabhängige Stimmerkennung zum Einsatz. Bei der Stimmverifikation wird durch die Eingabe der Identifikationsnummer die Identität des Nutzers ermittelt. Anschließend fordert das System den Benutzer auf zu sprechen (meist nach einem Signalton). Besonders wichtig bei der textabhängigen Stimmerkennung ist die korrekte Registrierung von Anfang und Ende des aufzuzeichnenden Wortes. Erst wenn ein bestimmter Lautstärkepegel erreicht ist, wird die Stimme aufgenommen. Laute Hintergrundgeräusche führen bei diesem Vorgehen natürlich zu Problemen.

5.2.3 Erkennung anhand des Tastaturanschlags

Biometrisches Merkmal: Die Art wie eine Person Zeichenfolgen mit der Tastatur eingibt nennt man Tipprhythmus. Die Merkmale des persönlichen Tipprhythmuses sind die Schreibgeschwindigkeit, der Tastendruck, das Korrekturverhalten, das Pausenverhalten sowie die Fehlerhäufigkeit. Weitere psychometrische Merkmale sind Überholungen, Gebrauch der Shifttaste und Buchstabendreher.
Verarbeitung des biometrischen Musters: Mit einer Tastatur wird zunächst ein Referenzmuster des Tippverhaltens gespeichert. Es gibt zwei unterschiedliche Systeme. Das erste basiert auf psychometrische Merkmale wie z.B. die Art der Shifttastenbenutzung und die Registrierung von Rechts- und Linkshändern. Das zweite System basiert auf zeitabhängigen Kennzeichen wie z.B. die Haltezeiten der Tasten (Registrierung der Betätigungs- und Freigabezeitpunkte) und die Verzögerungen zwischen Tastaturanschlägen (interkey times). Zur Erkennung

einer Person anhand seines Tippverhaltens gibt es unterschiedliche Methoden. Während eine Methode den Benutzer auffordert zuvor eingelernte Worte einzugeben, muss der Benutzer bei einer anderen Methode einen Text in der Einlernphase eingeben. Für die Verarbeitung und Vergleich des biometrischen Musters werden stochastische Verfahren eingesetzt. Beispielsweise bei den zeitabhängigen Kennzeichen sind die beobachteten Zeiten in gewisser Weise zufällig verteilt, d. h. sie können als Ergebnisse eines Zufallsexperiments aufgefasst werden. Ist die dazugehörige statistische Verteilungsfunktion bekannt, lassen sich Wahrscheinlichkeitsaussagen über die Ausgänge anderer "Schreibexperimente" ableiten. Damit erkennt man, ob das aktuell aufgenommene Tippverhalten dem eingelernten ähnlich ist.

6 Sicherheit biometrischer Systeme

Die Authentisierung durch biometrische Systeme, verfolgt zwei Ziele: Während Benutzern, deren Merkmal in der Datenbank gespeichert ist, Zugang gewährt werden soll, sollen unbekannte Benutzer und Fälschungen abgewiesen werden. Zwischen diesen beiden Zielsetzungen besteht ein klarer Prioritätenkonflikt, weil sie bei allen biometrischen Verfahren voneinander abhängen. Es ist möglich die Erkennungstoleranzschwelle einzustellen. Je niedriger die Toleranzschwelle, desto besser die Erkennung bekannter Personen, da auch noch "Ausreißer" akzeptiert werden. Je höher Toleranzschwelle, desto sicherer, weil der Aufwand, eine Falsch-Positiv-Erkennung durch eine Fälschung zu erreichen, steigt. Da ein unsicheres System unbrauchbar ist, sollte Sicherheit die höchste Priorität besitzen.
Ein biomerisches System kann in vier abstrakte Teile zerlegt werden. Diese Teile bestehen aus Erfassung, Bearbeitung, Entscheidung und Speicherung (s. Abb. 6.1). Jeder dieser Teile und die Schnittstellen dazwischen knnen einzeln angegriffen werden.

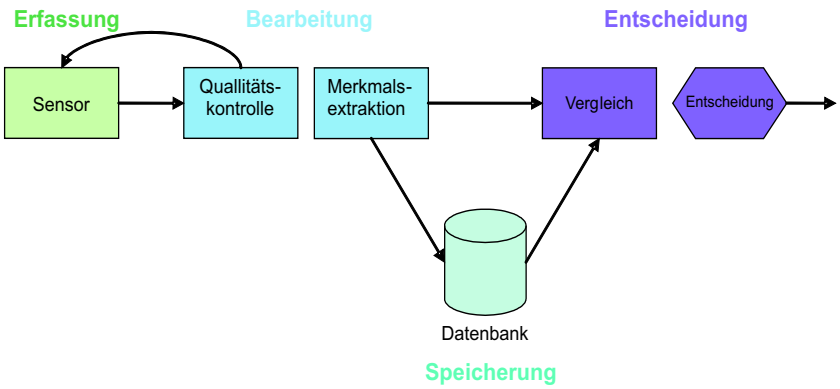


Abbildung 6.1: Generisches Aufbaumodell eines biometrischen Systems, *Quelle: [Nol02]*

Angriffe auf die Erfassung: Dies ist die häufigste Art von Angriffen auf ein biometrisches System. Es wird hier das eigentliche, biometrische Merkmal gefälscht

und dem Sensor präsentiert. Um diese Angriffe zu verhindern, werden in biometrischen Systemen zusätzliche Mechanismen integriert. Diese Mechanismen versuchen zu erkennen, ob das biometrische Merkmal zu einer lebenden Person gehört oder gefälscht ist. Bei Fingerabdrücken beispielsweise wird nach dem Puls oder Schweißdrüsen auf der Haut gesucht, bei Iris-Erkennung nach Änderung der Pupillenweitung. Das Interessante bei solchen Angriffen ist, dass sie immer möglich sind, da der Sensor immer erreichbar und offen bleiben muss.
Angriffe auf die Datenübertragung vom Sensor: Der Sensor enthält keine Logik und besteht meist nur aus einem einfachen Erfassungsmechanismus, der kontinuierlich Daten an den Rechner sendet. Bei unidirektionalen Verbindungen fällt die Erkennung von Angriffen auf dem Rechner zu. Aus Kostengründen werden Standardschnittstellen (*RS-232, FBAS-Videosignal*) verwendet, die Leitungsüberwachung nicht unterstützen. Ein klassischer Angriff ist also eine Replay-Attacke, bei der ein korrekter Authentisierungsversuch aufgezeichnet und später wieder eingespielt wird.
Um sich gegen solche Angriffe zu schützen, gibt es zwei Möglichkeiten:

- **Manipulationsüberwachung:** Beim Einschleifen von Aufzeichnungsgeräten muss die Leitung unterbrochen werden. Indem man eine solche Unterbrechung erkennt, erreicht man einen Schutz dagegen. Dies kann beispielsweise durch eine Ruhestromüberwachung erreicht werden.

- **Gesicherte Datenübertragung:** Um eine Wiedereinspielung zu verhindern, wird bei bidirektionalen Leitung, dem Sensor innerhalb einer Authentisierung spezielle zufällige Challenges zu schicken, die dann entsprechend beantwortet werden müssen. Eine wiedereingespielte Aufnahme allein kann dies nicht replizieren und wird erkannt.

Sonstige Angriffe:

- **Angriffe auf die Bearbeitung des Merkmals durch Kenntnis des Vorverarbeitungsalgorithmus:** Bei dieser Art von Angriffen wird ein entsprechendes Muster eingeschleust, das nach der Verarbeitung den gewünschten Output generiert. Alternativ kann der Algorithmus direkt so manipuliert werden, dass direkt der gewünschte Output ausgegeben wird.

- **Angriffe auf den Entscheidungsalgorithmus:** Durch Manipulation der Software auf der Festplatte oder im Speicher ("patchen") wird der Algorithmus so verändert, dass entweder immer eine Positiv-Erkennung erfolgt oder zumindest für gewünschte Identitäten.

- **Angriffe auf die Datenübertragung von der Speicherung zum Entscheidungsalgorithmus:** Bei der Übertragung wird der Merkmalsvektor vertauscht, was dann beim Vergleich mit dem „falschen“ zur positiven Erkennung führt.

- **Angriffe auf die Speicherung:** In der Datenbank wird ein Merkmalsvektor ausgetauscht, so dass der Angreifer die entsprechende Identität erlangen kann.

7 Anwendungsbeispiele

In diesem Kapitel werden zwei Beispiele für die Anwendung biometrischer Systeme vorgestellt.

7.1 Fingerabdruckerkennung mit Siemens ID-Mouse

Als Zugangsidentifikation für Computersysteme und im Mobilbereich bei Notebooks, PDAs, Handys und Autos kommt der Fingerabdruck in Frage - das am weitesten verbreitete biometrische Verfahren. In der Abb. 7.1 ist die ID-Mouse zu sehen. Sie identifiziert den Nutzer mit einem kurzen Fingertipp auf den Sensor der Maus. Die ID Mouse unterstützt nicht nur die Anmeldung am lokalen PC, sondern kann mit Hilfe einer speziellen Software auch einfach in Netzwerke eingebunden werden. Die biometrischen Referenzdaten erlauben eine automatische Freischaltung aller Ressourcen, auf die ein Anwender Zugriff hat.

Abbildung 7.1: Siemens ID-Mouse, *Quelle: [Tec03]*

7.2 Venenerkennung als Ausweis

Ein weiteres Beispiel, mit dem sich Zutrittskontrollen verbessern lassen ist die Identifizierung anhand des Adernmusters auf dem Handrücken. In der Abb. 7.2 sieht man ein Beispiel für ein Gerät welches zur Venenerkennung eingesetzt wird. Das Venenmuster wird von einer Infrarotkamera erfasst, selbst bei Händen, auf deren Handrücken das Auge kein Muster erkennt, wird die Kamera fündig. Eine

automatische Bilderkennung vergleicht die Aufnahmen mit gespeicherten Mustern. Einige Bereiche der Flughäfen von Toronto und Ottawa in Kanada, die nur Mitarbeiter betreten dürfen, sind mit der Venenerkennungstechnik gesichert.

Abbildung 7.2: Venenerkennungs Gerät, *Quelle: [Wir04]*

8 Zusammenfassung

Biometrische Verfahren basieren auf nicht kopierbaren Körper- und Verhaltensmerkmalen eines Menschen. Biometrisch auswerten lassen sich u.a. folgende Merkmale: Tippverhalten an einer Tastatur, die Handgeometrie, die Stimme, das Gesicht, die Unterschriftendynamik, das Irismuster oder der Fingerabdruck. Biometrische Erkennungssysteme sind auf dem Markt nicht weit verbreitet. Der große Vorteil biometrischer Daten liegt darin, dass sie nicht wie PINs ausgetauscht werden können. Neben dem staatlichen Sicherheitssektor sollen biometrische Systeme im wirtschaftlichen Bereich die PINs und Passwörter ersetzen und so mehr Komfort bringen . Die Kosten und hohe Fehlerquoten verhindern eine schnelle Einführung von biometrischer Verfahren. Die Fehleranfälligkeit beträgt derzeit bis zu 10 Prozent, im günstigsten Fall immer noch 1 bis 5 Prozent. Angesichts der Gelder, die derzeit in die Technologie gesteckt werden, dürfte sich diese Fehlerquote künftig aber deutlich verbessern.

Literaturverzeichnis

[Nol02] V. Nolde, L. Leger: *Biometrische Verfahren,* Lehrbuch, 2002.

[Amb03] M. Amberg, S. Fischer, J. Rößler: *Biometrische Verfahren,* Studie zum State of the Art, 2003.

[Hoh04] M. Hohensee: *Wirtschaftswoche, Ausgabe Heft 14,* Zeitschrift, 2004.

[Man01] K. Manhart: *Sicher durch Biometrie,* http://www.tecchannel.de/software/824/index.html, 2001.

[Sch02] J. Schneider: *„E-Business Prozesse authentisch und sicher“* Fraunhofer Institut fr Produktionsanlagen und Konstruktionstechnik, 2002.

[Heu03] B. Heumann: *Biometrie-online,* http://www.Biometrie-online.de, 2003.

[Tel05] TeleTrust: *Biometrische Verfahren* Wissensforum, http://www.teletrust.de /themen.asp?id=80100, 2005.

[And04] M. Anders: *Biometrische Identifikationsverfahren,* Seminararbeit, Humboldt Universität zu Berlin, 2004.

[Spe03/04] M. Speckner: *Unterschriftenerkennung,* Seminararbeit, SS 2003/04.

[Köh99] M. Köhntopp: *Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren,* Proceedings zur Arbeitskonferenz Sicherheitsinfrastrukturen, 1999.

[Lei04] H. Leitold: *Leitfaden Biometrie Überblick und stand der technik,* Secure Information Technology Center-Austria, 2004.

[Brü99] R. Brüderlin: *Was ist Biometrie?,* http://www.identix.ch/Einführung/Biometrie20deutsch.htm, 1999.

[Sch04] M. Schwan: *Biometrische Identifikationssysteme,* Seminararbeit, SS 2004.

[Aus05] austrian. security. forum: *Biometrie,* http://www.security-forum.at/index.php?id=1, 2005.

[Gal02] A. Galkin: *Iriserkennung,* http://www.ni.cs.tu-berlin.de/lehre/sembiometrie/GalkinIris.pdf, 2002.

[Sof03] Software Professional GmbH: *Bioidentifikation,* http://www.signplus.com /e/download/fachinfo-klassische-und-digitale-unterschrift.doc, 2003.

[Tec03] Tecchannel : *Sicher durch Biometrie,* http://www.tecchannel.de/software/824/index.html, 2003.

[Wir04] Wirtschaftswoche : *Wirtschaftswoche,* Zeitschrift, Ausgabe Heft 14/2004 v. 25.03.04.

[Bro04] M. Bromba : *Bioidentifikation,* http://www.bromba.com/faq/biofaqd.htm, 2004.

Abbildungsverzeichnis

Tabellenverzeichnis