Diplomarbeit:

Risikoanalyse von biometrischen Systemen

am Fachbereich Informatik der Universität Hamburg
Arbeitsbereich AGN (Anwendungen der Informatik in Geistes- und Naturwissenschaften)

Autor:
Christian Paulsen
7paulsen@informatik.uni-hamburg.de

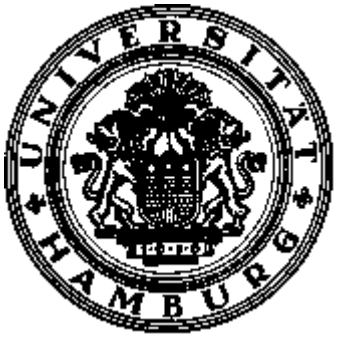
Betreuer:
Prof. Dr. Klaus Brunnstein
Dr. Hans-Joachim Mück

August 2003

Inhaltsverzeichnis:

Danksagung:

Ich möchte mich an dieser Stelle bei meinen Betreuern, Prof. Dr. Klaus Brunnstein und Dr. Hans-Joachim Mück, für die ausführliche und kompetente Betreuung bedanken. Weiterhin danke ich Samer Abdalla für hilfreiche Tipps und Dipl. Inform. Arslan Brömme für die vorbereitende Betreuung während meiner Studienarbeit.



Erklärung: Ich versichere, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe angefertigt habe und keine außer den angegebenen Quellen und Hilfsmitteln benutzt habe.

Hamburg, den 21.8.2003 Christian Paulsen

1. Einleitung

Heutzutage gehört die Verwendung von Passwörtern oder Geheimzahlen in allen Bereichen der Gesellschaft zum Alltag. Dabei wird von den Benutzern in zunehmendem Maße verlangt, dass sie sich eine Vielzahl kryptischer Codes merken, um sich für bestimmte Anwendungen legitimieren zu können. Es existieren eine Reihe von Sicherheitsrisiken, deren Relevanz durch diese „Code-Überflutung“ zunimmt und geeignete Gegenmaßnahmen erfordern: Passwörter können erraten oder erschlichen werden und sollten daher häufig gewechselt werden, möglichst lang und kompliziert sein, was teilweise dazu führt, dass der Anwender sie notiert und eine weitere Sicherheitslücke entsteht.
Eine Alternative oder Ergänzung zu den Authentisierungsverfahren, die auf Wissen (z.B. Codes), Besitz (Schlüssel, Chipkarten) oder Ort/ Zeit (Arbeitszeiten) basieren, ist die Verwendung biometrischer Authentisierungsverfahren. Biometrische Verfahren verwenden körperliche Merkmale, z.B. das Fingerabdruckmuster, um die Identität einer Person zu bestimmen oder zu verifizieren. Sie sind also *personengebunden* und nicht nur *personenbezogen* wie Passwörter oder PINs.
Die Umsätze in der Biometrik-Branche sind in den letzten Jahren stets gestiegen (siehe Abb.1 in Abschnitt 2.1), zum einen aus den eben genannten Gründen, zum anderen aufgrund der gestiegenen Leistungsfähigkeit heutiger Computersysteme, die eine benutzerfreundliche Bearbeitungsdauer ermöglicht. Trotzdem gibt es marktreife biometrische Verfahren in erster Linie für Anwendungsnischen, z.B. für die Zugangskontrolle zu Hochsicherheitsbereichen. Weltweit gibt es ca. 200 Unternehmen, die biometrische Verfahren zur Marktreife entwickeln wollen [Behrens/Roth, 2001].

Nach den Terroranschlägen in New York am 11.September 2001 wurde vielfach diskutiert, welche Sicherheitsmaßnahmen nötig sind, um weitere Attacken dieser Art zu verhindern. Unter anderem wurde vorgeschlagen, biometrische Merkmale in Personalausweisen zu integrieren (Antiterrormaßnahmen der Deutschen Bundesregierung) oder gesuchte Personen an öffentlichen Orten mittels Gesichts- oder Gangerkennung zu identifizieren. Aufgrund dieser Entwicklungen ist es sehr wichtig, dass umfangreiche Aufklärungs- und Forschungsarbeit auf diesem Gebiet durchgeführt wird. Dazu müssen sowohl technische, als auch soziale, ethische und datenschutzrechtliche Aspekte berücksichtigt werden. Entscheidend ist die Frage, welche Sicherheitsrisiken bei der Verwendung biometrischer Systeme existieren und welche Gegenmaßnahmen sinnvoll wären. Die vorliegende

Diplomarbeit befasst sich mit dieser Thematik und wird zunächst in das Thema einführen (Kapitel 2) und die Funktionsweise der gängigsten biometrischen Verfahren erläutern (Kapitel 3). Im vierten Kapitel beginnt die eigentliche Risikoanalyse mit der Aufzählung von potentiellen Schwachstellen biometrischer Systeme und einer Einschätzung, wie groß der Angriffsaufwand und die Eintrittswahrscheinlichkeit ist. Die Frage, ob und welches biometrische Verfahren für einen sinnvollen Einsatz geeignet ist, kann nur unter Berücksichtigung des Anwendungsbereiches und den spezifischen Anforderungen beantwortet werden. Daher werden im fünften Kapitel Beispielszenarien eingeführt und mögliche Sicherheitskonzepte diskutiert. In Kapitel 6 werden ethische und datenschutzrechtliche Aspekte angesprochen und die Ergebnisse zusammengefasst.

Die vorliegende Diplomarbeit richtet sich also zum einen an alle Personen, die grundlegende Informationen über Biometrik und biometrische Verfahren suchen, zum anderen an Firmen und andere Institutionen, die bereits biometrische Authentisierungsverfahren verwenden oder eine Benutzung planen. Möglicherweise kann die folgende Risikoanalyse die Herstellerfirmen von biometrischen Produkten bei der Entwicklung von sicheren und benutzerfreundlichen Produkten unterstützen.

2. Grundlagen

2.1 Biometrik

Der Begriff „Biometrik“ wird in der Öffentlichkeit häufig nicht vom Begriff „Biometrie“ unterschieden, obwohl es da Unterschiede gibt :

Definition 1: Biometrie (nach [Duden 5]) :

a) Wissenschaft von der Zählung und [Körper]messung an Lebewesen;
biologische Statistik

b) Zählung und [Körper]messung an Lebewesen [Duden 5, 1982]

Definition 2: Biometrie (nach [Lorenz 1996]) :

Unter dem Begriff der Biometrie werden die vielfältigen Anwendungen der Mathematik, insbesondere der mathematischen Statistik, in den biologischen und ihnen verwandten Wissenschaften zusammengefasst.

→ Die Vermessung des menschlichen Körpers ist hier ebenfalls enthalten!
[Lorenz, 1996]

Definition 3: Biometrik (= Biometrie + Informatik) :

Anwendungen der Biometrie in der Informatik und umgekehrt.

Häufig werden die Begriffe Biometrie und Biometrik als Kurzform für biometrische Identifikations- und Verifikationsverfahren verwendet, die wie folgt definiert sind [Brömme, 2001]:

Definition 4: Biometrische Identifikation (biometric identification) :

a) Erkennung einer Person anhand biometrischer Merkmale mit/ohne Einwilligung der Person

b) 1:n-Zugriff auf eine biometrische Datenbank (im Rahmen einer biometrischen Authentikation) [Brömme, 2001]

Es wird also anhand biometrischer Merkmale die Identität der zugehörigen Person ermittelt. Ein spezifischer Algorithmus generiert aus einem biometrischen Merkmal (z.B. dem Fingerabdruckmuster) eine vergleichbare Kenngröße („biometrische Signatur“), die gespeichert wird. Bei der biometrischen Identifikation muss die zu überprüfende Signatur gegen die gesamte Datenbank aller in Frage kommenden Signaturen getestet werden. Gesetzt den Fall, dass sie einer der gespeicherten Signaturen hinreichend ähnlich ist, werden die zugehörigen Personendaten des Trägers der gespeicherten Identität als Antwort ausgegeben. Falls keine der gespeicherten Signaturen der untersuchten ausreichend entspricht, scheitert die Identifikation [Biometric Authentication Research Group, 2002].
Die Einsatzfelder biometrischer Identifikationssysteme sind beispielsweise E-Banking- und E-Commerce-Transaktionen, sowie Zugangskontrollen zu besonders gesicherten Gebäuden, Räumen oder Gebieten (z.B. Flughafenbereiche) [Petermann/Sauter, 2002].

Fallbeispiel für eine biometrische Identifikation – das Fußballstadion:
Eine mögliche Anwendung für einen biometrischen Algorithmus, der eine Identifikation erlaubt, ist die Ermittlung der Anwesenheit von bekannten so genannten „Hooligans“ in einem Fußballstadion. Für diesen Zweck könnten mit ausreichend guter Kameratechnik die Sitzreihen des Stadions abgefilmt werden. Für die anwesenden Zuschauer werden die biometrischen Signaturen (z.B. der Gesichtsgeometrie) ermittelt. Nach diesem Schritt ist man in der Lage, diese Signaturen gegen eine Datenbank von bekannten Hooligans zu testen, um so die Anwesenheit dieser Personen festzustellen [Biometric Authentication Research Group, 2002].

Definition 5: Biometrische Verifikation (biometric authentication):

a) Überprüfung der behaupteten Identität einer Person mit zu dieser Identität gespeicherten biometrischen Daten.

b) 1:1-Zugriff auf eine biometrische Datenbank (im Rahmen einer biometrischen Authentikation) [Brömme, 2001]

Bei der biometrischen Verifikation geht es darum, eine zuvor angegebene Identität zu verifizieren oder zu falsifizieren. Man weist anhand seiner biometrischen Merkmale gegenüber einem IT-System nach, dass man tatsächlich die Person ist, die man behauptet zu sein.

Fallbeispiel für eine biometrische Verifikation – der Bankautomat:
Anstatt einem Geldautomaten gegenüber durch die Kenntnis der PIN (persönliche Identifikationsnummer) seine Identität nachzuweisen, wird sich eventuell der zukünftige Kontobevollmächtigte durch das Einscannen seines Fingerabdruckes ausweisen. Zuvor könnte dem Geldautomaten z.B. über das Einschieben einer Smartcard mitgeteilt werden, auf welches Konto zugegriffen werden soll. Neben der Kontonummer kann auf der Karte auch die biometrische Signatur des Fingerabdruckes des Kontobevollmächtigten als Vergleichswert abgelegt sein. Der Geldautomat berechnet nun aus dem eingescannten Fingerabdruck der Person, die Zugriff auf das Konto wünscht, eine biometrische Signatur und vergleicht diese mit der auf der Karte gespeicherten. Wenn der Vergleich positiv verläuft, wird der Zugriff auf das Konto gestattet [Biometric Authentication Research Group, 2002].

Definition 6: Biometrische Authentisierung

a) (im weiteren Sinne):
Der gesamte Vorgang (Prozess), mit dem eine Person konfrontiert wird, um Zugriff auf Systemressourcen zu erhalten.

Triviales Phasenmodell:

1. Phase: **Einlernen**
2. Phase: **Biometrische Authentisierung**
3. Phase: **Autorisierung**
4. Phase: **Freischaltung von Systemressourcen**

*b) (im engeren Sinne)**:***

• Phase 2 im Phasenmodell: Biometrische Authentisierung [Brömme, 2001]

Definition 7: Lebenderkennung
Alle Maßnahmen, die bei einem biometrischen Verfahren eine Überwindung durch simple Imitate oder tote Körperteile verhindern soll.

Bei allen biometrischen Verfahren werden Personen aufgrund ihrer physiologischen oder verhaltensbezogenen Merkmale identifiziert und/oder verifiziert
Diese Merkmale können u.a. sein:

- Fingerabdruck
- Handgeometrie
- Gesichtsgeometrie
- Irismuster
- Gefäßstruktur der Retina
- Stimme
- Tastaturanschlagsdynamik
- Gangart
- Ohren

Von den oben genannten Verfahren ist die Fingerabdruckerkennung die am meisten verbreitete Technologie (siehe Abb. 1). [International Biometric Group, 2001].

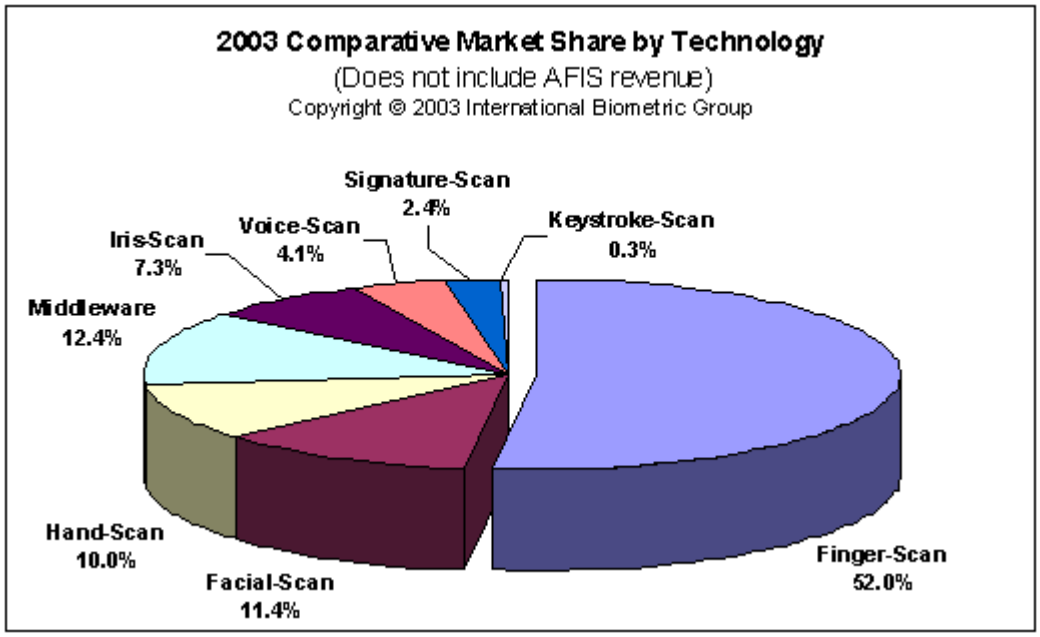


Abb.1 : Marktanteile verschiedener biometrischer Technologien in 2003

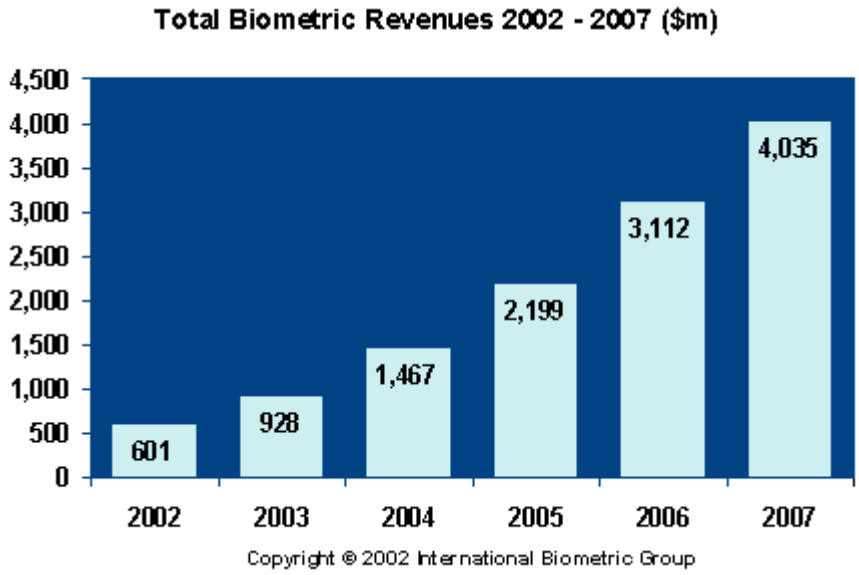


Abb.2 : Gesamteinnahmen im Biometrik-Bereich 2002 – 2007 in $m

Allgemein müssen Merkmale des Menschen, ob physiologische (passive) oder verhaltensabhängige (aktive), folgende vier Eigenschaften aufweisen, um "biometrisch optimal“ genutzt werden zu können:

- **Universalität** (bei jedem Menschen vorhanden),
- **Einzigartigkeit** (bei jedem Menschen verschieden),
- **Beständigkeit** (ohne Veränderungen über die Zeit) und
- **Erfassbarkeit** (durch ein technisches System quantitativ messbar)

[Petermann/Sauter, 2002]

2.1.1 Vorteile und Nachteile biometrischer Verfahren gegenüber herkömmlichen Authentisierungsverfahren

Biometrische Verfahren bieten folgende Vorteile:

- Biologische Merkmale gehen selten verloren und können nicht problemlos an andere Personen weitergegeben werden
- Die Gültigkeitsdauer ist vergleichsweise lang
- Sie können den Authentisierungsvorgang vereinfachen und verkürzen

Dem stehen aber auch Nachteile gegenüber:

- Die Kosten für die erstmalige Beschaffung und Einrichtung von biometrischen Systemen sind relativ hoch
- Es gibt hygienische Bedenken bei berührungssensitiven Systemen
- Einschränkungen des Persönlichkeitsrechts möglich
- Schwierigkeiten bei Veränderungen an den biologischen Merkmalen (Verletzungen, Narben)
- Die Systeme lösen bei einigen Anwendern psychische Ängste (gesundheitliche/ gesellschaftliche) aus

2.1.2 Leistungskenngrößen für biometrische Systeme: FAR, FRR, EER

Eine wichtige Phase bei der Konstruktion von Authentisierungsverfahren ist der Systemtest. Es gibt zahlreiche Datenbanken zum Testen von Fingerabdrucksystemen, beispielsweise die spezielle Datenbank Nr.9 des National Institute of Standards. Sie umfasst über 16.000 Fingerabdrücke in Form von 8-Bit Graustufenbildern der Größe 832 x 768, gescannt mit einer Auflösung von ca. 500 dpi (dots per inch).
In AFAS-Anwendungen (AFAS steht für „Automatic Fingerprint Authentication System“) gibt es vier mögliche Testergebnisse:

(1) Eine **autorisierte** Person erhält **Zugriff**
(2) Eine **autorisierte** Person wird **zurückgewiesen**
(3) Eine **nicht autorisierte** Person wird **zurückgewiesen**
(4) Eine **nicht autorisierte** Person erhält **Zugriff**

Probleme bei der Fingerabdruckerkennung, bzw. bei anderen biometrischen Methoden, treten bei (2) und (4) auf. Die hierfür herangezogenen Raten werden False Reject Rate, kurz FRR (= Fall 2) und False Acceptance Rate, kurz FAR (= Fall 4) genannt und sind Standardkenngrößen für die Qualität biometrischer Systeme [Jain et al, 1999].

Da die Ergebnisse der Anwendung eines Algorithmus auf unterschiedliche Aufnahmen des gleichen Merkmals i.a. nicht zu hundert Prozent übereinstimmen, muss ein gewisser Toleranzrahmen definiert werden („Wie groß darf der Unterschied zwischen zwei Signaturen sein?“). Die Festlegung dieses Toleranzrahmens hat entscheidenden Einfluss auf die Testergebnisse. Daraus resultiert die gegenseitige Abhängigkeit der Kenngrößen FAR und FRR. Eine Verbesserung der einen Größe hat meistens eine Verschlechterung der anderen zur Folge. Wenn beispielsweise der Toleranzrahmen eingeengt wird, führt dies zu einer niedrigeren FAR, gleichzeitig aber auch zu einer Erhöhung der FRR [Biometric Authentication Research Group, 2002]. Allgemein hängen die Ergebnisse sehr stark von der verwendeten Test-Datenbank ab. Eine zusätzliche Kenngröße ist die sogenannte „Equal Error Rate“ (EER), auch Crossover-Rate oder Gleichfehlerrate genannt. Graphisch gesehen (Abb.3) markiert die EER den Schnittpunkt von FRR und FAR. An diesem Punkt sind also FRR und FAR gleich [Jain et al, 1999].

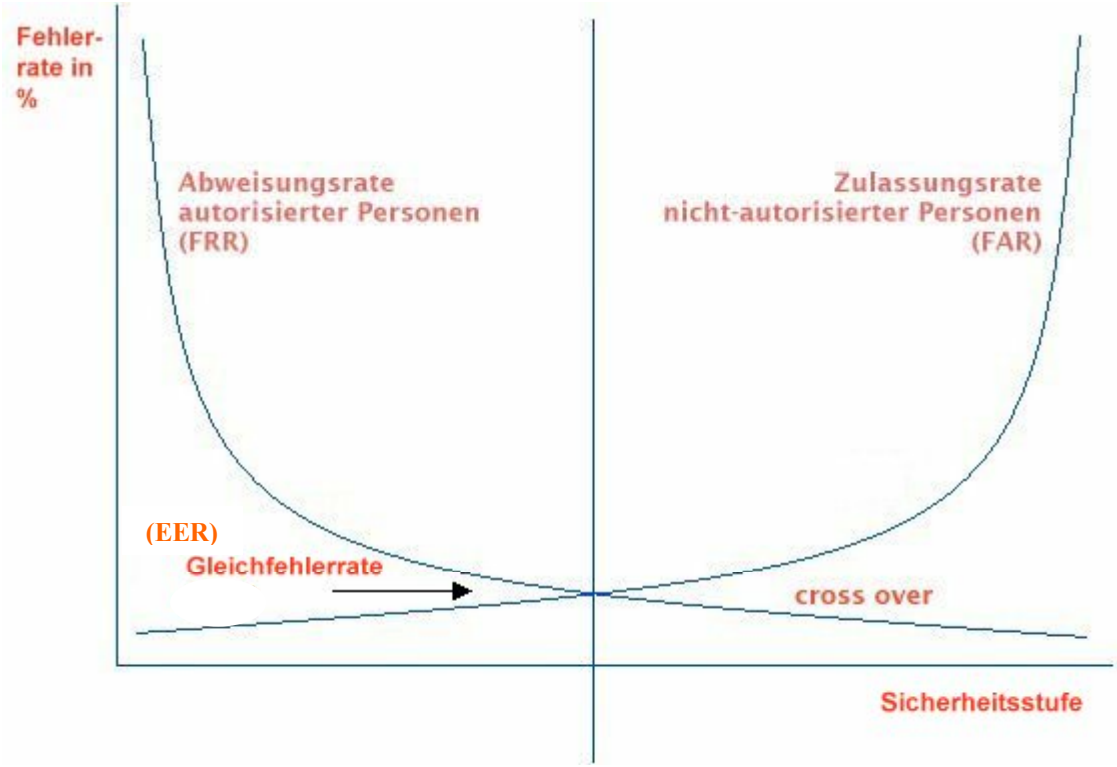


Abb.3: Biometrische Kenngrößen

2.2 Die Risikoanalyse

Risikoanalysen werden in vielen verschiedenen Bereichen (z.B. im Strahlenschutz oder in der Marktforschung) durchgeführt, um vorhandene Werte mit adäquaten Maßnahmen vor potentiellen Gefahren zu schützen oder mögliche Konsequenzen von Entscheidungen abzuschätzen. Auf dem Gebiet der Informatik sind Risikoanalysen ein wichtiger Teil der IT-Sicherheit. Udo Voges vom Institut für Angewandte Informatik des Forschungszentrums Karlsruhe hat in [Voges, 2002] einige Definitionen zum Thema Sicherheit zusammengetragen:

Definition 8: Schaden
Physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt.
[ISO/IEC Guide 51:1999, Definition 3.3]

Definition 9: Risiko
Kombination der Wahrscheinlichkeit des Auftretens eines SCHADENS und des SCHWEREGRADES dieses SCHADENS [ISO/IEC Guide 51:1999, Definition 3.2]

Definition 10: Schweregrad
Maß der möglichen Folgen einer Gefährdung [Voges, 2002]

Definition 11: Risikoanalyse
Systematische Auswertung verfügbarer Informationen, um Gefährdungen zu identifizieren und RISIKEN abzuschätzen [ISO/IEC Guide 51:1999, Definition 3.10]

Definition 12: Vertraulichkeit
Schutz von Daten gegenüber Kenntnisnahme unbefugter Dritter [Winkelmann, 2002]

Definition 13: Integrität
Unversehrtheit, Unverfälschbarkeit und Korrektheit von Daten/ Systemen [Winkelmann, 2002]

Definition 14: Verfügbarkeit
Zuverlässigkeit, Erreichbarkeit und Wartbarkeit von Daten/ Systemen [Winkelmann, 2002]

2.2.1 Risikoanalysen und Grundschutzmaßnahmen in der IT-Sicherheit

Im Bereich der Informationstechnologie, insbesondere in der IT-Sicherheit, ist das Erstellen eines Sicherheitskonzeptes empfehlenswert, um das Sicherheitsniveau eines Unternehmens bzw. einer Behörde zu erhalten oder zu erhöhen. Ein Sicherheitskonzept ist ein Plan zur Erhaltung oder Verbesserung der Sicherheit der Informationsverarbeitung in einer Organisation [BSI, 1992].
Ein wesentlicher Bestandteil des Sicherheitskonzeptes ist die Risikoanalyse. Sie dient zur Ermittlung der Risiken, die mit dem Betrieb eines IT-Systems, bestehend aus einer Vielzahl von Komponenten (Hardware, Software, Daten, Infrastruktur), einhergehen [Kassovic, 1998]. Mit der vermehrten Nutzung und Komplexität heutiger IT-Systeme und den daraus resultierenden Abhängigkeiten steigt das Risiko, dass Schwachstellen übersehen werden. IT-Systeme sind im allgemeinen drei Grundbedrohungen ausgesetzt:

- Verlust der Vertraulichkeit (loss of confidentiality)
- Verlust der Integrität (loss of integrity)
- Verlust der Verfügbarkeit (loss of availability)

Eine angemessene und ausführliche Risikoanalyse allein reicht nicht aus, diese Gefahren zu beseitigen, da erst die praktische Umsetzung geeigneter Gegenmaßnahmen im Rahmen des Risikomanagements und periodisches Überprüfen, ob nicht gegebenenfalls neue Schwachstellen entstanden sind, ein Unternehmen vor möglichen Verlusten schützen kann. [Cyranek, 1994].
Dirk Stelzer unterscheidet in [Stelzer, 2002] zwei Vorgehensweisen, wie Sicherheitskonzepte erstellt werden können:
Die Verwendung von *Grundschutzmaßnahmen* und die Durchführung von *Risikoanalysen*. Diese beiden Vorgehensweisen unterscheiden sich nicht in ihrem Ziel. Beide streben an, die Sicherheit der Informationsverarbeitung zu erhöhen oder zumindest zu erhalten. Allerdings gibt es erhebliche Unterschiede in der Art und Weise, wie dieses Ziel erreicht werden soll [Stelzer, 2002]:

a) Verwendung von Grundschutzmaßnahmen
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit dem IT-Grundschutzhandbuch eine Sammlung kontextbezogener Maßnahmen zur Erhöhung der Sicherheit in verschiedenen Bereichen der Informationstechnologie zur Verfügung.
Die Angemessenheit der ausgewählten Sicherungsmaßnahmen wird dabei nicht in erster Linie durch die Analyse bestehender Risiken und das Risikoreduzierungspotential von

Sicherungsmaßnahmen begründet, sondern durch die „übliche Praxis“ in vergleichbaren Institutionen.
Die Entwicklung von Sicherheitskonzepten auf der Basis von Grundschutzmaßnahmen beruht auf folgenden Grundgedanken: In bestimmten Bereichen sind (fast) alle Organisationen den gleichen Gefährdungen ausgesetzt. Die Mehrheit der umsichtigen und erfahrenen Sicherheitsbeauftragten verwendet in diesen Bereichen ähnliche Sicherungsmaßnahmen. Mit Hilfe dieser Sicherungsmaßnahmen kann eine ausreichende Sicherheit erzielt werden [Stelzer, 2002].
Die Frage, ob diese Grundschutzmaßnahmen für die Werte eines Unternehmens ausreichend sind, sollte im Rahmen einer Schutzbedarfsanalyse festgestellt werden. Falls der Grundschutz genügt, kann der Anwender die zu schützenden Systeme in den „Grundschutz-Baukasten“ des Handbuchs abbilden und braucht lediglich die Maßnahmeempfehlungen der verschiedenen Kataloge zu befolgen [Kassovic, 1998].
Beispiele für Sicherungsmaßnahmen, die typischerweise mit Hilfe des Grundschutzansatzes ausgewählt werden, sind Feuermelder in Rechenzentren, Virenschutzsoftware auf Arbeitsplatzrechnern oder eine unterbrechungsfreie Stromversorgung für einen Server, der geschäftskritische Anwendungen unterstützt [Stelzer, 2002].

b) Durchführung einer Risikoanalyse
Im Rahmen einer Risikoanalyse werden Gefährdungen der Informationsverarbeitung sowie ihre Ursachen und Konsequenzen detaillierter untersucht, um auf dieser Grundlage für verschiedene IT-Systeme und deren Anwendungen jeweils angemessene Sicherungsmaßnahmen auswählen zu können [Stelzer, 2002].
Im Gegensatz zur Durchführung von Grundschutzmaßnahmen ist das Erstellen einer Risikoanalyse aufwendiger und spezifischer an den vorhandenen Unternehmensstrukturen orientiert. Die Verfechter der Risikoanalyse gehen dabei von bestimmten Annahmen aus. Um beurteilen zu können, ob es sinnvoll ist, eine Risikoanalyse durchzuführen, muss man sich diese Annahmen bewusst machen:

- Struktur, Bedeutung und Umfeld der Informationsverarbeitung sowie die zu schützenden Werte sind in vielen Organisationen sehr verschieden.
- Selbst innerhalb komplexer Organisationen gibt es sehr unterschiedliche Sicherungsanforderungen.
- Deshalb gibt es für die wenigsten Bereiche, in denen Informationsverarbeitung betrieben wird, Standardvorschläge für angemessene Sicherungsmaßnahmen.

Die im folgenden dargestellte Grundstruktur aus [Stelzer, 2002] stellt eine idealtypische Vereinigungsmenge der bisher entwickelten Risikoanalyse-Methoden dar. Mit dieser Grundstruktur wird nicht etwa der Anspruch erhoben, die beste aller denkbaren Risikoanalyse-Methoden darzustellen. Die folgenden Ausführungen sollen auch nicht nahe legen, dass eine Risikoanalyse genau diesem Ablauf folgen müsste. Die Grundstruktur ist vielmehr als ein gedankliches Hilfsmittel zu verstehen, mit dem reale Risikoanalyse-Methoden eingeordnet und kategorisiert werden können:

b1) Abgrenzung und Beschreibung des Analysebereichs

Ein wichtiger Teilaspekt einer Risikoanalyse ist die Abgrenzung des zu analysierenden Bereichs. In der Regel wird eine Risikoanalyse einerseits nicht auf eine Software, einen Rechner, eine Datei, eine Anwendung oder ähnliches beschränkt bleiben können. Andererseits wird es nur selten möglich sein, sämtliche Risiken der gesamten Informationsverarbeitung einer Organisation in einer Analyse zu untersuchen und zu bewerten, da dies viel zu aufwendig wäre. Aus diesen Gründen muss ein sinnvoller Ausschnitt abgegrenzt werden. Dabei ist zu klären, welche Aspekte analysiert werden sollen und welche nicht. In diesem Zusammenhang müssen auch die Schnittstellen zu den nicht analysierten Bereichen spezifiziert werden. Ist der zu analysierende Bereich abgegrenzt, müssen die sicherheitsrelevanten Objekte identifiziert und beschrieben werden. Als sicherheitsrelevante Objekte kommen z. B. Gebäude, Etagen, Räume, organisatorische Einheiten (wie Abteilungen oder Projekte), infrastrukturelle Einrichtungen, Hardware, Daten und Software, Anwendungen der Informationsverarbeitung sowie betriebliche Funktionen in Betracht. Ferner ist die Frage zu klären, wie diese Objekte zusammenhängen, um später mögliche Ursache-Wirkungs-Beziehungen, d.h. die Fortpflanzung von Schäden in der betreffenden Organisation, ermitteln zu können.

b2) Risikoerkennung

Im Rahmen der Risikoerkennung werden die Risiken identifiziert und inhaltlich beschrieben. Zu diesem Zweck sind in einem ersten Schritt relevante Gefahren zu ermitteln. Diese Gefahren werden dann den sicherheitsrelevanten Objekten zugeordnet, um im nächsten Schritt potentielle Konsequenzen bzw. Schäden gefährdender Ereignisse einschätzen zu können.

b3) Risikobewertung

Sind die Risiken inhaltlich beschrieben, muss festgestellt werden, welche Bedeutung diese Risiken im Kontext der betreffenden Organisation haben. Das bedeutet, dass die Risiken bewertet werden müssen. Dabei sind Eintrittswahrscheinlichkeiten bzw. -häufigkeiten zu ermitteln und Schadenspotentiale zu bewerten. Zum Abschluss der Risikobewertung werden Risikokenngrößen ermittelt, indem Eintrittswahrscheinlichkeiten und Schadenspotentiale miteinander verknüpft werden.

b4) Aufbereitung und Darstellung der Ergebnisse

Da die Durchführung einer Risikoanalyse kein Selbstzweck ist, müssen die Ergebnisse der Analyse so aufbereitet und dargestellt werden, dass die Ziele, die mit der Risikoanalyse angestrebt wurden, auch sinnvoll erreicht werden können. Soll die Risikoanalyse z. B. als Entscheidungsvorlage für die Genehmigung eines Sicherheitsbudgets dienen, müssen die Ergebnisse der Risikoanalyse so aufbereitet werden, dass sie für die Entscheidungsträger verständlich sind. Das wird in der Regel bedeuten, dass die Ergebnisse nicht in Fachtermini der Informationsverarbeitung oder gar der Informationssicherheit dargestellt sind, sondern in Konzepten und Begriffen, die den Entscheidungsträgern geläufig sind. Viele Risikoanalyse-Methoden weisen besonders in diesem Punkt gravierende Schwächen auf.

Wie bereits betont, beschreibt die oben dargestellte Grundstruktur eine idealisierte Risikoanalyse. Die meisten realen Risikoanalyse-Konzepte legen ihren Schwerpunkt auf einzelne Teilaspekte dieser Struktur [Stelzer, 1994].

Daher wird im nächsten Abschnitt ein Beispiel für ein Standardverfahren beschrieben.

2.2.2 Risikoanalyse und Risikomanagement nach Moses

Robin Moses beschreibt in [Moses, 1992] ein Prozessflussmodell für die Durchführung von Risikoanalyse und Risikomanagement. Das Modell ist in drei Phasen aufgeteilt:

- Initiierung
- Risikoanalyse
- Risikomanagement

In der Initiierungsphase werden die schutzwürdigen Güter identifiziert und dementsprechend die Grenzen des Untersuchungsgegenstandes festgelegt.

Innerhalb der Risikoanalyse werden die Güter gemäß der Bedeutung, welche Vertraulichkeit, Integrität und Verfügbarkeit für sie haben und unter der Berücksichtigung

der zwischen den Gütern bestehenden Abhängigkeiten, bewertet. Anschließend werden die Bedrohungen (absichtlicher oder unabsichtlicher Natur), denen die Güter ausgesetzt sind, identifiziert und hinsichtlich ihrer Eintrittswahrscheinlichkeit abgeschätzt. Unterschieden werden Bedrohungen, die von außen auf den Untersuchungsgegenstand einwirken und solche, deren Quellen innerhalb seiner Grenzen liegen. Schließlich werden die systemimmanenten Schwachstellen ermittelt und ihre Bedenklichkeit eingeschätzt. Zusammengefasst werden diese Untersuchungen in der Einschätzung der möglichen Auswirkungen des Eintritts einer Bedrohung auf ein Gut. Daraus werden schließlich Maße für das Risiko einer Modifikation, Zerstörung, Enthüllung oder einer nicht gegebenen Verfügbarkeit eines Gutes abgeleitet.
Das Risikomanagement ist ein separater nachgeordneter Vorgang, der nochmals in zwei Subphasen unterteilt wird. Hier werden die Schutzmaßnahmen identifiziert, die durch die ermittelten Risikomaße zu rechtfertigen sind. Außerdem sind die gegebenenfalls schon existierenden Schutzmaßnahmen zu bestimmen. Innerhalb der Entscheidungsfindungsphase ist schließlich zu klären, welche Schutzmaßnahmen zu implementieren und welche Risiken unter den gegebenen Kriterien hinnehmbar sind. Ändern sich die Gegebenheiten des untersuchten Systems, erfolgt eine Rückkoppelung in die Initiierungsphase [Kassovic, 1998]; [Moses, 1992].

2.2.3 Unterscheidung von qualitativen und quantitativen Bewertungsmethoden

Nach der Art der Bewertung lassen sich Methoden der Risikoanalyse in quantitative und qualitative Methoden (auch kardinale und ordinale Methoden genannt) einteilen.
Alle quantitativen Methoden gehen auf ein Dokument namens FIPS 65 (Federal Information Processing Standards Publication Number 65) zurück, das 1979 vom „U.S. National Institute of Standards and Technology“ (NIST) herausgegeben wurde [Kassovic, 1998].
Sie haben ihre wesentliche Funktion in der Bewertung von Risiken mit berechenbaren Größen. Aus diesem Grund haben diese Methoden eine eher mathematische bzw. statistische Ausrichtung. Sie verfügen zwar häufig auch über Listen mit Gefahren, mit Kategorien potentiell gefährdeter Objekte und mit Hinweisen auf die Zuordnung von Gefahren zu Objekten. Die Identifizierung und inhaltliche Beschreibung von Risiken wird aber nur ansatzweise unterstützt. Insbesondere die Ermittlung von Folgeschäden gefährdender Ereignisse bleibt den Benutzern meist völlig selbst überlassen. Die

Methoden bieten mehr oder weniger umfangreiche statistische Funktionen an, mit denen quantitative Risikomodelle erstellt werden können.
Die Methoden unterstützen die Benutzer dabei, Risiken mittels kardinaler Größen zu ‚errechnen'. Schadenspotentiale werden in der Regel in Währungseinheiten ausgedrückt und Eintrittshäufigkeiten in Ereignissen pro Jahr. Für jedes gefährdende Ereignis werden Schaden und Häufigkeit miteinander multipliziert. Das Ergebnis der Analyse besteht aus kardinal bezifferten Risiken oder anders ausgedrückt, aus statistischen Erwartungswerten, die in anglo-amerikanischen Methoden häufig mit dem Begriff ‚Annual Loss Expectancy (ALE)' bezeichnet werden.
Die Stärken dieses Konzepts lassen sich wie folgt zusammenfassen:
Risiken werden prägnant beschrieben, nämlich in Form von Zahlen, und sie sind der Höhe nach leicht miteinander vergleichbar. Risikoanalysen, die dem quantitativen Bewertungskonzept folgen, können Anhaltspunkte für ein ökonomisch zu rechtfertigendes Sicherungsbudget liefern. Sie eignen sich deshalb als Teil einer Kosten-Nutzen-Analyse für Sicherungsmaßnahmen.
In der Praxis bereitet das Konzept aber erhebliche Probleme. Zunächst muss der Benutzer solcher Methoden die Risiken kennen und inhaltlich beschreiben können, bevor er mit der Bewertung beginnt. Die meisten quantitativen Methoden unterstützen ihn hierbei nur ansatzweise. Außerdem erzwingt das Konzept numerische Formulierungen der Risiken auch dann, wenn keine verlässlichen Angaben oder Schätzungen vorliegen. Für einige Risiken lassen sich Werte ableiten, z. B. aus Statistiken oder Erfahrungen mit ähnlichen Ereignissen in der Organisation. Insbesondere in technischen Bereichen sind diese Zahlen sinnvoll und ein Ansatz, die Sicherheit eines Systems zu verbessern. Für andere Risiken sind Schätzungen aber nur sehr schwierig oder aus prinzipiellen Gründen unmöglich. Die Analysen täuschen daher eine Exaktheit vor, die bei genauer Betrachtung nicht gegeben ist. Zudem sind die entsprechenden Methoden häufig sehr aufwendig durchzuführen [Stelzer, 1994].

Im Unterschied zu dem quantitativen bzw. kardinalen Bewertungskonzept liegt den qualitativen bzw. ordinalen Risikoanalyse-Methoden ein anderer Bewertungsmaßstab zugrunde. Sie verwenden zur Beurteilung von Schäden und Eintrittshäufigkeiten mehr oder weniger detaillierte Skalen, die nicht nach absoluten Werten, sondern nach Größenordnungen (z.B. gering/ mittel/ hoch) unterteilt sind. Schäden, deren Höhe sich finanziell ausdrücken lässt, werden zusätzlich auf eine qualitative Skala übertragen [Kassovic, 1998].

Ein Vorteil qualitativer Methoden ist, dass sie eine grobe Unterscheidung von wichtigen und weniger wichtigen Risiken ermöglichen und erste Anhaltspunkte für die Bekämpfung dieser Risiken geben. Außerdem sind sie häufig gut dokumentiert.
Allerdings haben auch die ordinalen Bewertungskonzepte eine Reihe von Schwachpunkten. Sie sind sehr arbeitsintensiv und zwingen den Benutzer, viele einzelne gefährdende Ereignisse mehr oder weniger zusammenhanglos zu betrachten und zu bewerten. Bei der Ermittlung von Folgeschäden werden die Benutzer nur schlecht unterstützt, und es ist häufig schwierig, den Gesamtüberblick zu behalten bzw. die Bedeutung eines einzelnen gefährdenden Ereignisses für die gesamte Organisation einzuschätzen. Der Zwang, auch solche Sachverhalte qualitativ bewerten zu müssen, die sich auf diese Weise nur schwer beschreiben lassen, führt häufig zu einer mangelhaften Überzeugungskraft der Ergebnisse [Stelzer, 1994].
Die Durchführung einer Risikoanalyse ist, trotz der genannten Nachteile beider Verfahren, in vielen Bereichen ein unverzichtbarer Ansatz, die vorhandenen Risiken einzuschätzen und zu minimieren.

3. Biometrische Systeme

In diesem Kapitel werden die gängigsten biometrischen Verfahren vorgestellt.

3.1 Fingerabdruckerkennung

Die Fingerabdruckerkennung ist das am meisten verbreitete biometrische Verfahren (siehe Abb.1). Dies ist hauptsächlich damit zu begründen, dass die Verwendung von Fingerabdrücken eine lange Tradition besitzt, insbesondere sind sie seit ca. 100 Jahren ein wichtiges Element der Forensik, um Spuren am Tatort zur Überführung potentieller Verbrecher zu verwenden. Die wissenschaftlichen Grundlagen für dieses Verfahren legte Ende des 19.Jahrhunderts der Engländer Sir Francis Galton [Galton, 1892].
Er formulierte zwei wichtige Schlussfolgerungen:

1. Fingerabdrücke sind **permanent**
2. Fingerabdrücke sind **einzigartig**

Selbst eineiige Zwillinge haben unterschiedliche Fingerabdrücke, die eine eindeutige Unterscheidung ermöglichen. Obwohl eineiige Zwillinge genetisch identisch sind, werden phänotypische Merkmale (u.a. die Hautstrukturen an den Fingerkuppen) während der Schwangerschaft beeinflusst und verändert [Richards, 2001] [1].
Zu Punkt 1 muss einschränkend hinzugefügt werden, dass Verletzungen, Vernarbungen und Abnutzungen zu veränderten Strukturen führen können und der Fingerabdruck möglicherweise nicht mehr für eine biometrische Authentikation verwendet werden kann.

In den 60er Jahren wurden sogenannte AFIS-Systeme (Automated Fingerprint Identification Systems) entwickelt, mit denen es erstmals möglich war, Fingerabdrücke per Computer auszuwerten und zu vergleichen. In den 80er Jahren waren Technologie und Algorithmen der optischen Fingerabdruck-Scanner so weit fortgeschritten, dass Fingerbildsensoren nicht mehr nur für kriminalistische Zwecke, sondern erstmalig auch für erste biometrische Verfahren eingesetzt werden konnten [Behrens/Roth, 2001].
Hochauflösende AFIS-Bilder sind bis zu 250 KByte groß. Bei biometrischen Fingerabdruckscans werden zwar auch die Abdrücke aufgenommen, aber nicht das gesamte Bild gespeichert. Es werden lediglich spezifische Merkmale extrahiert, die in einem 250-1000 Byte großen Template (Signatur) gespeichert werden.

[1] Ausführlicher beschrieben in [Paulsen, 2002]

Der Prozess der Datenextraktion ist nicht umkehrbar, d.h. der Fingerabdruck kann nicht aus dem Template rekonstruiert werden [International Biometric Group, 2001].
Der Vergleich selbst erfolgt bei beiden Anwendungen nach ähnlichen Prinzipien, allerdings steht für das AFIS bei der Durchsuchung einer Datenbank mit 100.000 und mehr Datensätzen erheblich mehr Zeit zur Verfügung als die zwei bis drei Sekunden tolerierbarer Wartezeit bei einem Zugangssicherungssystem [Behrens/Roth, 2001].

3.1.1 Merkmale von Fingerabdrücken

Der menschliche Fingerabdruck weist verschiedene Rillenmuster auf, die traditionell nach [Henry, 1900] in fünf Basistypen eingeteilt werden (siehe Abb.2):

1. **left loop** (linksgerichtete Schleife)
2. **right loop** (rechtsgerichtete Schleife)
3. **whorl** (Wirbel und Doppelwirbel, schneckenförmig)
4. **arch** (Bogen)
5. **tented arch** (spitzer Bogen)

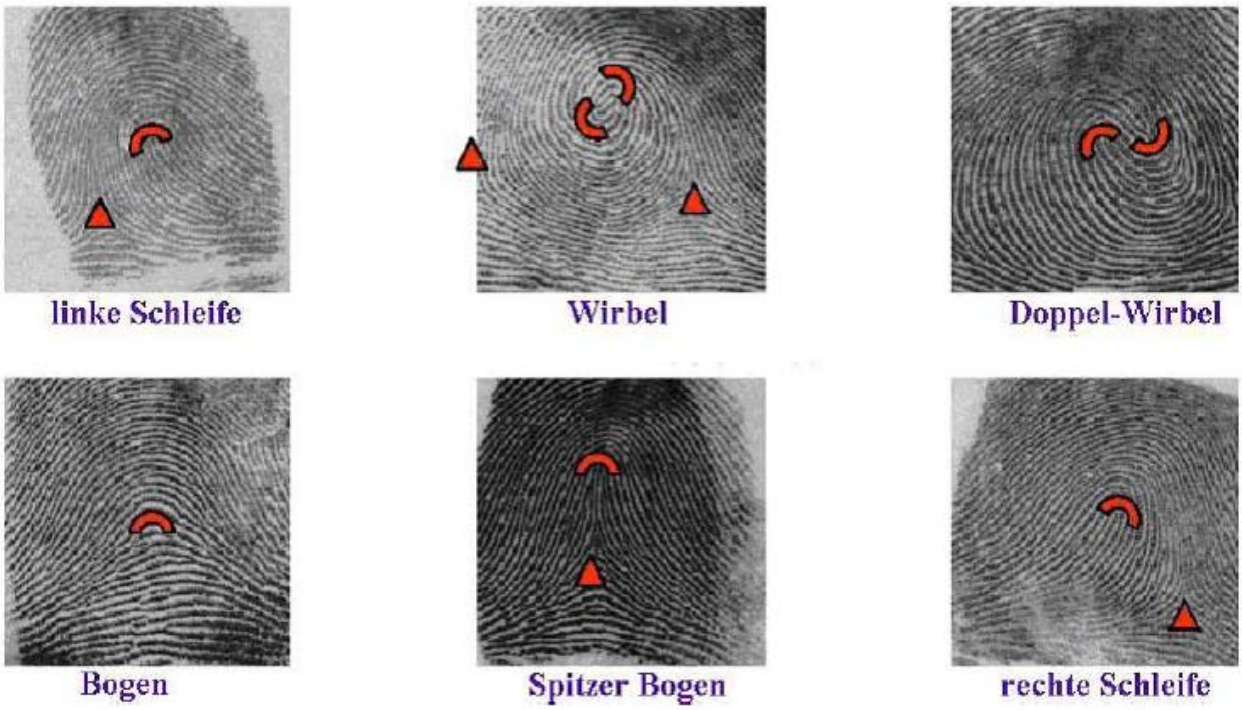


Abb.4: Die Basistypen

Core = maximale Krümmung zweier Linien (U-Turn)

Delta = zwei parallele Linien divergieren (Dreiecksform)

Charakteristische Punkte eines Fingerabdrucks, beispielsweise Verzweigungs – und Endpunkte von Linien, nennt man *Minutien*. Sie bilden die Basis für die meisten Finger-Scan-Algorithmen. [International Biometric Group, 2001]
Galton hat in seiner Arbeit [Galton, 1892] vier Minutienarten definiert. Seine Forschungen wurden fortgesetzt und die Zahl der Merkmale vergrößert.

Man unterscheidet heutzutage folgende Arten von Minutien:

- Kreuzungen
- Punkte
- Striche
- Haken
- Verzweigungen
- Poren (hohe Auflösung erforderlich)

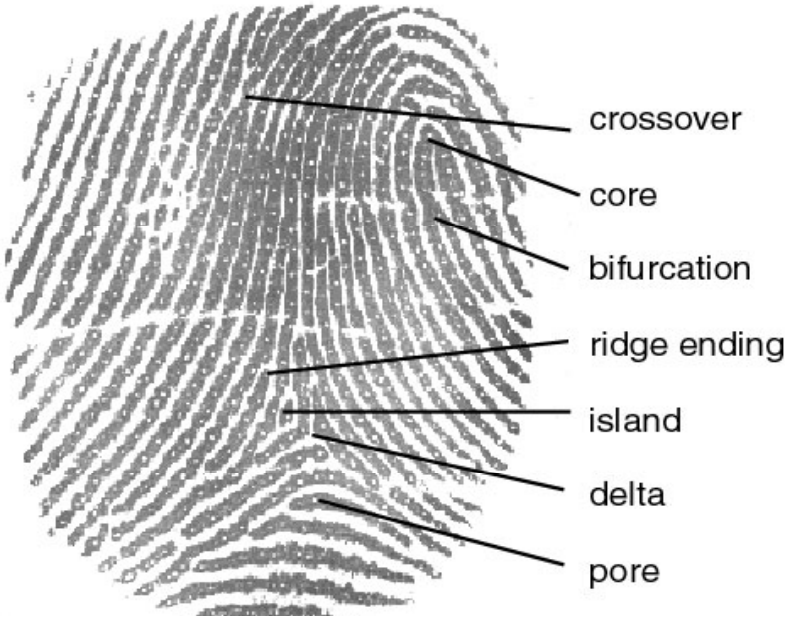


Abb.5: Ein Fingerabdruck mit einigen markierten Minutien

Neben den oben erwähnten Merkmalen sind *Core* und *Deltas* wichtige Merkmale
Als *Core* bezeichnet man den inneren Punkt, das Herzstück eines Fingerabdrucks. Es bildet das Zentrum, in dem Schleifen und Linien zusammenlaufen. Das Core ist häufig mittig gelegen (vgl. Abb.4 und 5).
Deltas nennt man die Punkte, an denen drei Serien von Erhebungen aneinander vorbeilaufen (vgl. Abb.4 und 5). Die Poren eines Fingerabdrucks können nur bei qualitativ hochwertigen Bildern zum Vergleich verwendet werden [International Biometric Group, 2001].

3.1.2 Fingerabdruck-Sensoren

Das wichtigste Ziel bei der Anwendung der Fingerabdruck-Technologien ist es, qualitativ hochwertige Aufnahmen des Rillenmusters zu bekommen.
Eine Reihe von Faktoren beeinflussen diesen Prozess nachteilig, z.B.:

- Schmutz
- Narben
- Zu trockene oder zu fettige Haut
- Alte Fingerabdrücke (Latenzabdrücke) und Fettrückstände auf der Sensorfläche

Hersteller von Fingerabdrucksystemen müssen diese Einflüsse berücksichtigen.
Heutzutage sind drei grundlegende Verfahren zur Bilderzeugung in Gebrauch:

- **Optische Verfahren**
- **Kapazitive Verfahren (Chip-Technologie)**
- **Ultraschall-Verfahren**

[International Biometric Group, 2001]

a) *Optische Verfahren*
Bei optischen Sensoren wird das Fingerbild mit einer herkömmlichen CCD-Kamera aufgenommen. Die Kamera wir dabei durch ein Prisma auf eine durchsichtige Fläche umgelenkt, auf welche der Finger aufgelegt wird (vgl. Abb.6). Die Oberfläche ist häufig durch ein spezielles gummiartiges Coating vergütet, um die Feuchtigkeit des Fingers abzuleiten. Dadurch wird gewährleistet, dass ein möglichst klares Fingerbild aufgenommen werden kann. Weiterhin ist eine Beleuchtung integriert, deren Helligkeitsregelung automatisch oder manuell durch den Benutzer geregelt wird. Das von der Kamera aufgezeichnete Bild wird über eine Frame-Grabber-Karte digitalisiert und in den PC übertragen und bearbeitet [Behrens/ Roth, 2001].

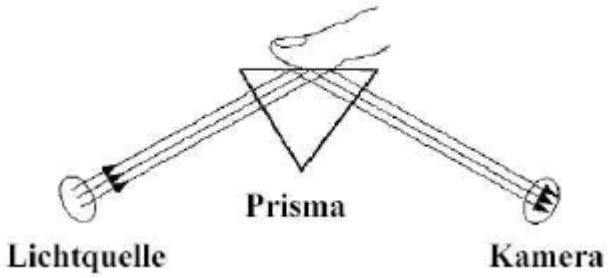


Abb.6: Prinzip eines optischen Sensors

Abb.7: Sensor Optiscan II der Firma Morphosoric©

Optische Verfahren sind im Vergleich zu den anderen Verfahren kostengünstig und temperaturunempfindlich. Allerdings muss die Sensorfläche ausreichend groß sein, für jede Art von Finger. Alte Fingerabdrücke (Latenzabdrücke) auf der Sensorfläche können das Bild des aktuellen Scanvorgangs verfälschen [International Biometric Group, 2001].

b*) Kapazitive Verfahren*

Kapazitive Sensoren zur Bilderzeugung existieren seit mehr als einer Dekade. Sie messen Kapazitäten zwischen der Fläche eines Silikon-Sensors und der Haut. Dabei bildet der Finger eine Platte des Kondensators und der Sensor die andere.
Die gemessenen Kapazitäten werden in einem 8-Bit -Graustufenbild dargestellt.
Die Bilder sind qualitativ besser als bei optischen Verfahren, trotz geringerer Messoberfläche. Genauere Angaben über die Haltbarkeit der Geräte stehen noch aus, obwohl die Hersteller behaupten, sie seien hundertmal robuster als optische Geräte. Die kleinere Sensorfläche kann allerdings auch negative Auswirkungen haben, wenn dadurch beispielsweise der Core-Punkt eines Fingers verfehlt wird [International Biometric Group, 2001]

c) *Ultraschall-Verfahren*

Die Ultraschall-Technologie ist relativ neu und noch nicht sehr verbreitet, obwohl sie als ein sehr exaktes Verfahren gilt.

Bei dieser Methode sendet das Gerät Ultraschallwellen aus mehreren Positionen aus, die von der Umgebung (Finger, Luft, Sensorfläche) unterschiedlich reflektiert werden. Diese Kontaktstreuung wird gemessen und zu einem Bild weiterverarbeitet, das nicht von Schmutz und Kratzern auf der Oberfläche negativ beeinflusst wird.

Selbst Finger mit abgewetzten Oberflächen produzieren noch ein recht gutes Bild, da ihre interne Struktur noch oberflächennah vorhanden ist. Die Größe der Sensorfläche ist beliebig.

Das Verfahren befindet sich noch in der Weiterentwicklung, könnte sich aber in Zukunft durchsetzen [International Biometric Group, 2001].

Die folgende Tabelle (Tab.1) stellt Vor- und Nachteile der einzelnen Bilderzeugungsverfahren für Fingerabdrücke gegenüber:

	Optische Methode	*Kapazitive Methode*	*Ultraschall-Methode*
Verfahren	- Finger wird auf beschichtete Oberfläche gelegt - CCD-Sensor erzeugt digitales Bild des Abdrucks	- misst Kapazitäten zwischen Silizium-sensor und Finger - Messung wird in digitales 8-bit Grau-stufenbild umgewandelt	- Ultraschallwellen werden ausgesendet und von der Umgebung unterschiedlich reflektiert - Reflektion wird gemessen und zu einem Bild verarbeitet
Vorteile	- am meisten erprobt - vergleichsweise günstig - temperaturunempfindlich	- gute Qualität - geringere Messoberfläche	- die exakteste Methode - wird bei der Abtastung nicht von Schmutz, Narben und Kratzern beeinflusst
Nachteile	- Sensoren müssen ausreichend groß sein - alte Abdrücke können Ergebnis verfälschen	-eventuell zu kleine Sensorflächen	Methode befindet sich noch in der Entwicklung

Tab.1: Vergleich der drei Methoden zur Bilderzeugung [Biometric Authentication Research Group, 2002]

3.1.3 Bildbearbeitung und Merkmalsextraktion

Nachdem ein Bild eines Fingerabdrucks aufgenommen wurde, müssen weitere Bildbearbeitungsschritte erfolgen, bevor eine verwendbare biometrische Signatur ermittelt werden kann. Dazu werden Algorithmen zur Verbesserung der Bildqualität verwendet (z.B. Hochpass- und Tiefpassfilter) und das Bild digitalisiert bzw. normiert. Schließlich werden die spezifischen Merkmale extrahiert und die Daten in einem sogenannten Template gespeichert. Die minutienbasierte Merkmalsextraktion ist die am häufigsten verwendete Methode. Sie beinhaltet folgende Verarbeitungsschritte (vgl. Abb.8):

- Gewinnung des Original-Graustufenbildes des Fingers (a)
- Berechnung des Richtungsfeldes aus dem Originalbild (b)
- Extraktion des Vordergrundanteils (c)
- Herausfilterung des Hintergrundes und Digitalisierung(d)
- Berechnung des Skelettes mit den markierten Minutien (e)
- Überlagerung der Minutien mit dem Original-Graustufenbild (f)

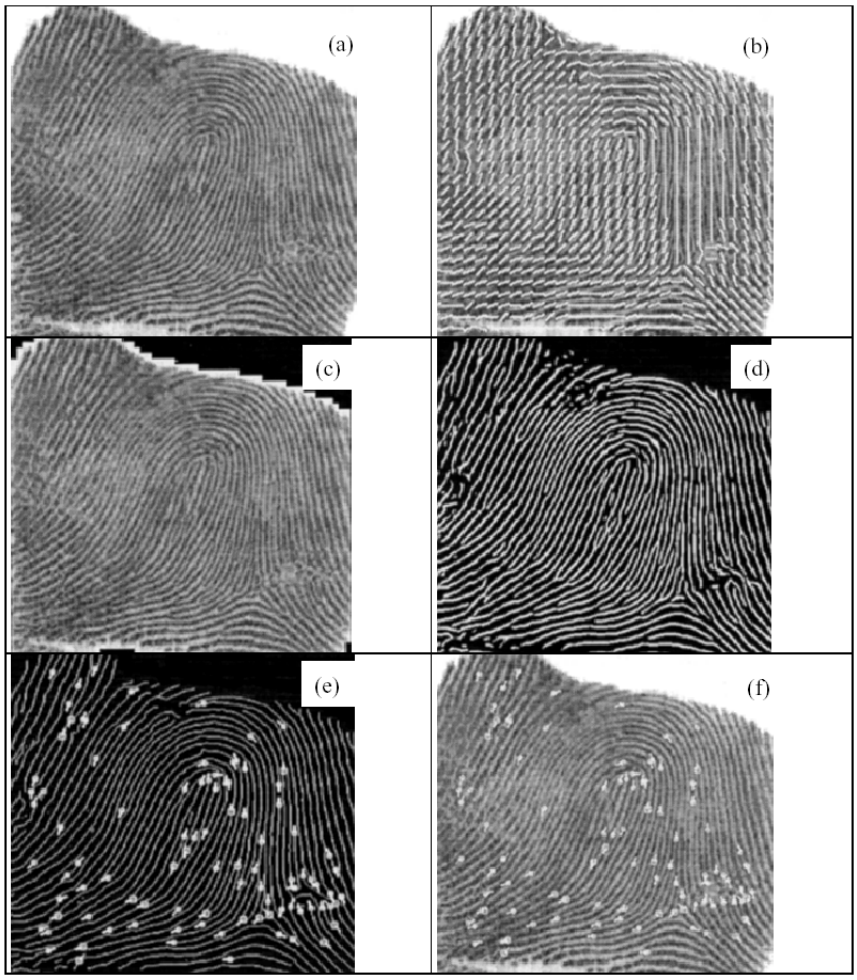


Abb.8: Minutienbasierte Merkmalsextraktion

Die minutienbasierte Merkmalsextraktion reduziert das Problem des Vergleichs zweier Fingerabdruckbilder auf einen Vergleich von Punkten oder Graphen und braucht daher erheblich weniger Rechenkapazität. Problematisch sind jedoch folgende Umstände:

1. Es gibt bisher nur wenige zuverlässige Algorithmen.
2. Es ist schwierig, festzulegen, wann zwei Minutienmengen ausreichend übereinstimmen [Jain et al, 1999]

Besonders problematisch ist es, die optimalen Schwellwerte in den Verarbeitungsschritten zu definieren (z.B. muss im Rahmen der Digitalisierung ein Grauwert als Grenze zwischen weiß und schwarz festgelegt werden).
Ein anderer Ansatz sind Fingerabdruck-Vergleiche auf der Basis von Neuronalen Netzwerken, wie sie in [Baldi/Chauvin, 1993] beschrieben werden.

3.1.4 Vergleich

Während des Verifikationsvorganges werden die abgespeicherten Referenzdaten mit den aktuellen Sensordaten verglichen. Jede Minutie lässt sich eindeutig durch ihren Abstand und ihre Ausrichtung gegenüber den benachbarten Minutien identifizieren. Außerdem werden Minutientyp und die Ausrichtung abgeglichen, also jede einzelne Minutie in bezug zu ihren Nachbarn gebracht.
Da das aufgenommene Fingerabdruckbild variiert, bedingt durch Schmutz, veränderten Druck und anderen Faktoren, kann lediglich ein Abgleich auf Ähnlichkeit, nicht auf Übereinstimmung durchgeführt werden. Daher kann bei jedem System die Abgleichschwelle eingestellt werden, wobei ein Kompromiss aus Benutzerfreundlichkeit und Sicherheit gefunden werden muss (vgl. Abschnitt 2.1.2).
Bei der Identifikation wird das Fingerbild zunächst klassifiziert, um nicht alle Referenzdatensätze für einen Vergleich heranziehen zu müssen [Behrens/ Roth, 2001].

3.1.5 Lebenderkennung

Der durchaus wichtige ‚Life-Test' wird bisher nur von wenigen Herstellern angeboten. Bekannt gewordene und teilweise realisierte Methoden sind die Erfassung der Hautfarbe, elektrische Eigenschaften und Hautreflexionen. Eine weitere Methode basiert auf der Pulsoxymetrie, d.h. es wird der Anteil des mit Sauerstoff angereicherten Hämoglobins am

Gesamthämoglobin (=Sauerstoffsättigung des Blutes) gemessen. Dies geschieht mit einer kleinen Sonde, die mit einem Clip am Finger befestigt wird und diesen mit Licht einer bestimmten Wellenlänge durchleuchtet. Das mit Sauerstoff gesättigte Hämoglobin absorbiert das Licht, während sauerstoffarmes Hämoglobin das Licht passieren lässt. Je höher die Sauerstoffsättigung, desto weniger Licht erreicht den Sensor. Bei einem lebenden und gesunden Finger liegt der Sauerstoffgehalt im Blut zwischen 96 und 98 Prozent. Einen Hinweis auf einen lebenden Finger kann auch die Temperatur- und Pulsschlagmessung geben [Behrens/Roth, 2001] .

3.2 Gesichtserkennung

Die maschinelle Gesichtserkennung hat in den letzten zehn Jahren große Fortschritte gemacht. Anfangs waren es nur wenige Forschergruppen, die sich mit dieser Aufgabe beschäftigten, die noch vor zwanzig Jahren als eine der schwierigsten auf dem Gebiet des künstlichen Sehens galt. Die Leistungssteigerung im Bereich der Computerhardware machte es möglich, komplexe Bildverarbeitungs- und Mustererkennungsverfahren zum einen mit Hilfe umfangreicher Bildsammlungen zu entwickeln und zu testen und zum anderen in Echtzeit einzusetzen. Kommerzielle Gesichtserkennungssysteme können bereits mit einem handelsüblichen PC mit einem Prozessor vom Typ Pentium II oder höher betrieben werden. Als Kamera reicht bereits eine kleine Webcam [Behrens/Roth, 2001].

3.2.1 Grundlegendes Verfahren

Im Prinzip geht es in der Gesichtserkennung darum, die markantesten Teile des Gesichts in einer biometrische Signatur zu speichern. Es werden also die Stellen gesucht, an denen sich die meisten Informationen befinden. Dazu gibt es 2 verschiedene Ansätze:

- merkmalsbasierte Gesichtserkennung
- holistischer Ansatz

Bei der merkmalsbasierten Gesichtserkennung werden markante Merkmale (engl. „features“) aus dem Rohbild eines Gesichts extrahiert und eine biometrische Signatur berechnet. Beim holistischen Ansatz wird das komplette Bild betrachtet und beispielsweise mit Hilfe der Fourier-Transformation ausgewertet. Bei dieser Methode ist bemerkenswert, dass nicht alle Frequenzen für die Erstellung der Signatur benutzt werden müssen, sondern nur die niedrigen Frequenzen, da sich hier der Großteil der Informationen befindet. Das hat wiederum zur Folge, dass die Signatur bei der Fourier-Transformation relativ klein gehalten werden kann.
Aus datenschutzrechtlicher Perspektive ist es nicht erlaubt, ganze Bilder in einer Datenbank abzuspeichern. Daher ist es notwendig, aus dem Bild eine biometrische Signatur zu erstellen, aus der das Originalbild nicht rekonstruierbar sein darf [Koleski, 2002].

Die technisch anspruchsvollsten Verarbeitungsschritte in einem Gesichtserkennungssystem sind die Gesichtsfindung in einem mit der Kamera aufgenommenen Rohbild einerseits, sowie Merkmalsextraktion und –vergleich andererseits. Ein merkmalsbasiertes Gesichtserkennungssystem verarbeitet ein digitales Bild in folgenden Schritten (siehe Abb.9):

- **Gesichtslokalisierung:** Position, Größe und eventuell Orientierung eines oder mehrerer Gesichter im Bild werden bestimmt (für die nächsten Schritte sei angenommen, dass nur ein einziges Gesicht gefunden wird).
- **Normalisierung:** Das Gesicht wird aus dem Bild ausgeschnitten und dieser Ausschnitt derart skaliert und gedreht, dass ein Bild vorgegebener Größe mit ebenfalls vorgegebener Position, Größe und Orientierung des Gesichts in diesem Bild entsteht.
- **Merkmalsextraktion:** Im normalisierten Gesichtsbild werden vorhandene Merkmale ermittelt.
- **Erzeugung der Signatur:** Bei der Registrierung werden die aus möglicherweise mehreren Bildern gewonnenen Gesichtsmerkmale einer Person in einem Referenzdatensatz (biometrische Signatur) zusammengefasst.
- **Vergleich:** Bei einer Verifikation wird der Merkmalssatz mit dem Referenzdatensatz derjenigen Person verglichen, deren Anwesenheit behauptet wird. Bei einer Identifikation findet ein Vergleich mit allen gespeicherten Referenzdatensätzen des Systems statt, die ähnlichste Person wird gewählt. In beiden Fällen gilt die Erkennung als erfolgreich, wenn die Abweichungen unter einer vorgegebenen Schwelle liegen [Behrens/Roth, 2001].

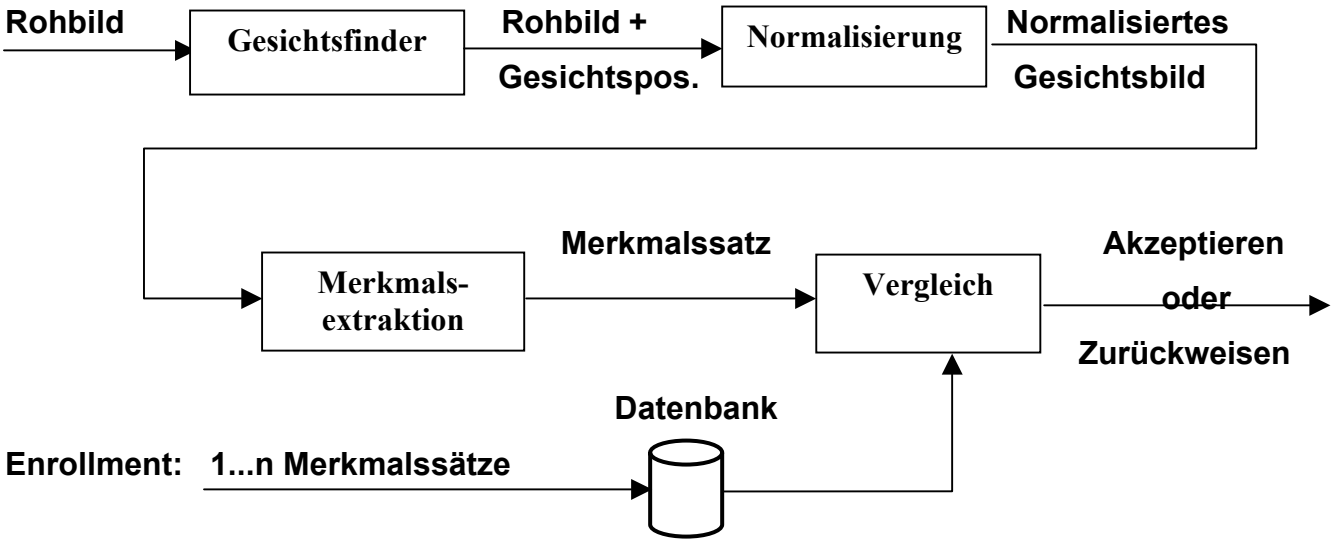


Abb.9: Verarbeitungsschritte bei der Gesichtserkennung

Viele Gesichtserkennungssysteme beinhalten eine sogenannte Lebenderkennung (engl. „live check“ oder „liveness test“). Dieser Schritt soll sicherstellen, dass das Bild von einer realen, im Moment der Aufnahme vor der Kamera stehenden lebenden Person stammt und Täuschungen erschwert werden.
Über die Zuverlässigkeit im Sinne geringer Fehlerraten lassen sich keine allgemeingültigen Aussagen treffen, da die Raten stark von den Umgebungsbedingungen am Einsatzort des Gesichtserkennungssystems abhängen und es bisher keine standardisierten und unabhängigen Vergleichstests gibt, die mit mehr als ein paar Dutzend Probanden arbeiten und verschiedene realistische Einsatzbedingungen simulieren [Behrens/Roth, 2001].

3.2.2 Merkmalsextraktion

In diesem Abschnitt werden Verfahren zur Merkmalsextraktion bei der Gesichtserkennung erläutert.

a) Template Matching

Ein sehr häufig verwendetes Verfahren der Gesichtserkennung ist das Template Matching. Dabei wird die Ähnlichkeit zwischen einem Bild und einem Template t berechnet. Ein Template ist eine vorgegebene Maske, die einem Bild oder einem Teil eines Bildes ähnlich ist (siehe Abb. 10 und 11).

Abb.10: Referenzbild und Template der Augenpartie

Abb.11: Vier Templates für Augen, Nase, Mund und das ganze Gesicht

Bei der einfachsten Form des Template Matchings wird lediglich ein Template verwendet, das Teile des Gesichts oder das ganze Gesicht darstellt. Eine verbesserte Methode des Template Matching wird in [Brunelli/Poggio, 1993] dargestellt. Dabei wird jede Person in einer Datenbank durch eine Frontalaufnahme ihres Gesichts, sowie durch vier Templates für die Augen, den Mund, die Nase und das gesamte Gesicht (Region unterhalb der Augenbrauen), dargestellt (Abb.11). Bei der Identifikation eines Gesichts wird ein Vergleich mit allen in der Datenbank gespeicherten Bildern durchgeführt. Als Ergebnis erhält man einen Vektor, der die Ähnlichkeit der jeweiligen Merkmale beschreibt. Die zu identifizierende Person wird dann als die Person mit der höchsten kumulativen Ähnlichkeit aller Merkmale identifiziert.
Die Qualität der Ergebnisse beim Template Matching hängt stark von der Qualität der verwendeten Maske ab. Die Maske muss bei möglichst vielen unterschiedlichen Personen "passen" und sollte möglichst unabhängig von Helligkeits- oder Kontraständerungen sein. Das größte Problem beim Template Matching ist jedoch, dass das Verfahren sehr viel Rechenzeit erfordert [Hofmann, 2002].
Problematisch ist, dass teilweise ganze Ausschnitte von Gesichtern abgespeichert werden müssen und es so zu datenschutzrechtlichen Problemen kommen kann [Koleski, 2002].

b) Fourier-Analyse

Die Grundidee für die Gesichtererkennung mit Hilfe der Fourier-Transformation besteht darin, das Originalbild und das Vergleichsbild in den Frequenzbereich zu transformieren, um dort die Spektren der beiden Bilder einfacher vergleichen zu können.
Bei der Fourier-Transformation handelt es sich um einen globalen Operator, also um einen Operator, der alle Pixel des Eingangsbilds benötigt, um ein Pixel des Ausgangsbilds zu berechnen. Die 1-dimensionale Fourier-Transformation wird bei der Verarbeitung 1-dimensionaler kontinuierlicher oder diskreter Zeitsignale verwendet. Dabei werden die Zeitsignale aus dem Zeitbereich in den Frequenzbereich transformiert und als Frequenzspektrum dargestellt. Für die Verarbeitung von Bildern dagegen wird die 2-dimensionale diskrete Fourier-Transformation (DFT) verwendet, da Bilder digitale (diskrete) 2-dimensionale Ortssignale sind. Die Transformation erfolgt also vom Ortsbereich in den Frequenzbereich, der häufig auch als Ortsfrequenzbereich bezeichnet wird [Hofmann, 2002]

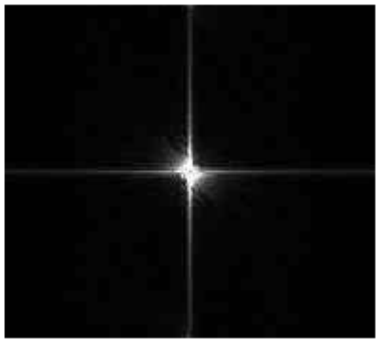


Abb.12 und 13: Bild eines Gesichts und zugehöriges Amplitudenspektrum (Transformation in den Frequenzbereich)

c) Projektion auf Eigenfaces

Der Eigenface-Ansatz geht auf Sirovich und Kirby [Sirovich/Kirby, 1987] zurück und wurde in den 90er Jahren von Pentland und seinen Mitarbeitern am Massachusetts Institute of Technology (MIT) Media Lab wesentlich erweitert [Moghaddam/Pentland, 1997].
Die Grundidee besteht darin, ein Gesichtsbild durch eine lineare Kombination von Basisgesichtern, den sogenannten Eigenfaces, zu approximieren. Die Koeffizienten dieser Linearkombination kodieren das Gesicht. Da meist nur etwa 100 Eigenfaces benutzt werden, ergibt sich ein recht kompakter Merkmalssatz. Der Vergleich zwischen zwei Gesichtern besteht in der einfachsten Version in der Berechnung des euklidischen Abstandes zwischen dem Referenzdatensatz und dem aktuellen Merkmalsansatz.
Die Eigenfaces selbst werden aus einer Menge (normalisierter) Beispielbilder gewonnen (siehe Abb.14). [...] Um mit diesem Ansatz gute Ergebnisse zu erzielen, muss die Normalisierung recht präzise sein. Es ist daher ratsam, nach der Gesichtslokalisierung auch die Position der Augen, der Nasenspitze und der Mitte des Mundes zu ermitteln, damit eine genauere und einheitlichere Normalisierung möglich ist [Behrens/Roth, 2001].

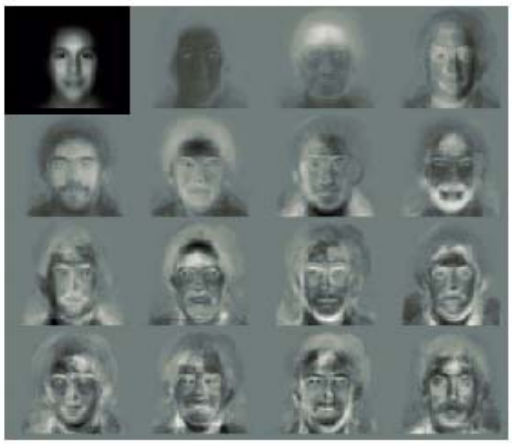


Abb.14: Eigenfaces

d) Elastic-Graph-Matching

Das Elastic-Graph-Matching wurde erstmals von Christoph von der Malsburg und seinen Mitarbeitern an der Universität Bochum und der University of Southern California auf die Gesichtserkennung angewendet [Wiskott, 1997]. Die Idee dieses Verfahrens ist, über das Gesichtsbild ein flexibles Gitter zu legen, dessen Knotenpunkten Merkmalsdetektoren zugeordnet sind, die lokal die Amplituden verschiedener räumlicher Frequenzen berechnen. Bei einem Vergleich zweier Gesichter können die Knoten in gewissen Grenzen verschoben werden, damit eine bessere Übereinstimmung der an den korrespondierenden Knoten ermittelten Merkmale erreicht wird (Abb.15). die Vergleichsfunktion ist eine gewichtete Summe aus dem Unterschied der Merkmale an den Knoten und einem topographischen Term, der die Verzerrung des Gitters quantifiziert [Behrens/Roth, 2001].

Abb.15: Elastic-Graph-Matching

3.2.3 Vor- und Nachteile der Gesichtserkennung gegenüber anderen biometrischen Verfahren

a) Vorteile

Einer der größten Vorteile der Gesichtserkennung ist ihre Natürlichkeit: Menschen sind daran gewöhnt, einen anderen Menschen am Gesicht zu erkennen und von ihm erkannt zu werden. Weiterhin ist dieses Verfahren berührungslos (ein Blick in die Kamera genügt) und unaufdringlich (engl.: non-intrusive), d.h. sie verlangt vom Benutzer eine geringe Anpassung an das System.

Ein weiterer Vorteil ist, dass häufig bereits vorhandene Infrastruktur genutzt werden kann, z.B. eine Anlage zur Videoüberwachung oder eine Webcam. Die gewonnenen Bilder können, im Gegensatz zu den meisten anderen biometrischen Verfahren, auch vom Menschen interpretiert werden, als zusätzliche Kontrolle oder im Falle eines Systemausfalls [Behrens/Roth, 2001].

b) Nachteile

Die maschinelle Gesichtserkennung hat auch Nachteile, beispielsweise können veränderte Lichtverhältnisse und Schattenwurf zu erhöhten Fehlerraten führen.
Weiterhin gibt es Probleme bei Verdeckungen des Kopfes durch Gegenstände, z.B. (Sonnen-)Brillen, Schal, Hut, Mundschutz oder durch Make-Up. Ganz natürliche Nachteile ergeben sich durch Alterung, Verletzungen, Narben, Schweiß (Reflexionen) und Schmutz. Bei einer niedrig eingestellten Toleranzgrenze können bereits Veränderungen des Gemütszustandes zu Fehlern führen, weil dadurch ein Gesicht im Aussehen stark beeinflusst werden kann. Ein bisher ungelöstes Problem ist die Unterscheidung eineiiger Zwillinge [Koleski, 2002]. Außerdem müssen die anfallenden Referenzbilder vor unbefugtem Zugriff geschützt werden [Behrens/Roth, 2001].

3.2.4 Lebenderkennung

Damit das System vor Überwindungsversuchen mit Fotos oder Videos grundlegend geschützt werden kann, muss eine Lebenderkennung integriert sein. Es kann z.B. vom Benutzer die Bewegung des Kopfes von einer Seite zur anderen verlangt werden oder es können Mund- bzw. Augenbewegungen erfasst werden. Eine Kombination mit der Sprechererkennung (siehe 3.5) ist auch eine häufig verwendete Methode der Lebenderkennung.

3.3 Iriserkennung

Der Iris-Scan gilt als eines der genauesten biometrischen Identifikationsverfahren und wird bereits vielfach bei Zugangskontrollen im Hochsicherheitsbereich verwendet, mehrere Pilotanwendungen bei Geldautomaten sind bekannt. Einem verbreiteteren Einsatz stehen derzeit noch die hohen Anschaffungskosten entgegen, die allerdings bei einer Steigerung der Produktion wohl deutlich gesenkt werden könnten. Die Nutzerakzeptanz gilt als eher verhalten, da häufig die Befürchtung von Augenschäden geäußert wird, in der fälschlichen, aber nach wie vor verbreiteten Annahme, dass ein Laser eingesetzt werde [Petermann/Sauter, 2002].

3.3.1 Aufbau des Auges

Das Auge ist ein hochempfindliches Organ, das mit höchster Präzision Lichtreize wahrnimmt, die über die Netzhaut und den Sehnerv zum Gehirn geleitet werden. Dort schließlich werden diese Reize dann zu einem Bild verarbeitet. Das gesamte Auge, oft auch Augapfel genannt, ist eine kugelförmige Struktur mit einem Durchmesser von etwa 2,5 Zentimetern und einer deutlichen Ausbuchtung auf der Vorderseite. Die äußere Hülle besteht aus drei Gewebeschichten: Ganz außen liegt die schützende Lederhaut (Sklera), die etwa fünf Sechstel der Oberfläche des Augapfels bedeckt. Auf der Vorderseite geht sie in die vorgewölbte, durchsichtige Hornhaut (Cornea) über. Die mittlere Schicht ist die Aderhaut (Choroidea), die von vielen Blutgefäßen durchzogen ist und die hinteren drei Fünftel des Augapfels umschließt (siehe Abb.16).
Sie setzt sich im Ziliarkörper und in der Regenbogenhaut (Iris) fort, die sich auf der Vorderseite des Auges befindet. Die innerste Schicht schließlich ist die lichtempfindliche Netzhaut (Retina).

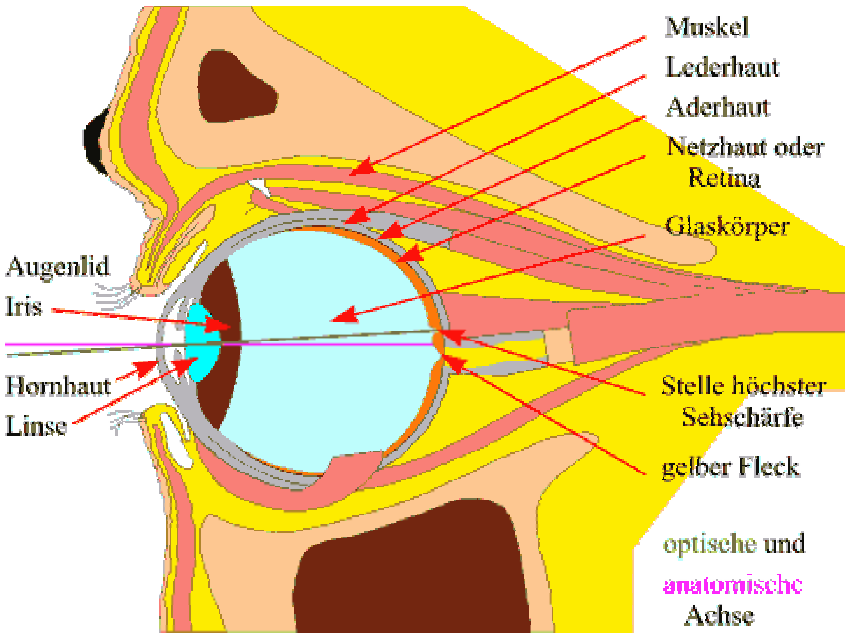


Abb.16: Aufbau des menschlichen Auges

Die farbige Regenbogenhaut (Iris), die zwischen Hornhaut und Linse liegt, hat in der Mitte eine runde Öffnung, die Pupille; ihre Größe wird von einem Muskel am Rand der Iris gesteuert. Durch Kontraktion oder Entspannung verkleinert oder vergrößert der Irismuskel die Pupille und sorgt so dafür, dass immer die richtige Lichtmenge ins Auge gelangt [DUAG, 2003].

3.3.2 Aufbau und Eigenschaften der Iris

Die Iris, auch Regenbogenhaut genannt, umgibt die Pupille und ist ein sichtbarer Bestandteil des Auges (siehe Abbildung 4). Ihre Entwicklung beginnt ab dem dritten Schwangerschaftsmonat und ist bis zum 8. Monat mit ihren Strukturen größtenteils abgeschlossen, obwohl sich die Pigmentierung in den ersten Lebensjahren noch ändern kann. Die Gestalt der Iris wird dabei nicht nur genetisch, sondern auch von Umwelteinflüssen bestimmt, so dass es sich bei der Iris um ein phänotypisches Merkmal handelt, das selbst bei eineiigen Zwillingen eine unterschiedliche Charakteristik aufweist. Nach abgeschlossener Entwicklung ändert sich das Aussehen der Iris nicht mehr und bleibt während des gesamten Lebens konstant. Vollständig ausgebildet besitzt jede Iris eine bestimmte Farbe, die von der
Anzahl von Melanin-Pigmenten bestimmt wird. Eine blaue Iris ist das Resultat fehlender Pigmente, eine hohe Pigmentanzahl führt zu einer dunklen Augenfarbe [Kronberg, 2002] ; [Daugman, 1998].

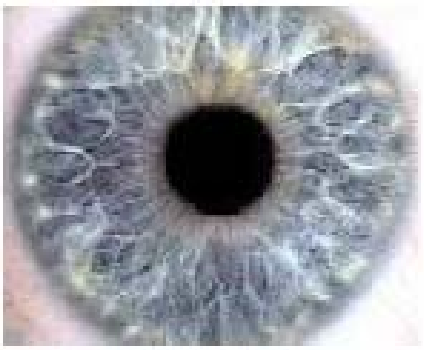


Abb.17: Iris

Weiterhin besitzt jede Iris bestimmte Muster, die ihr eine einzigartige Charakteristik verleihen und sie zur Identitätsbestimmung so interessant machen. Diese können sich aus mehreren verschiedenen Formen zusammensetzen wie bogenförmige Ränder, Furchen, Stege, Gruften, Ringe, Kronen, Tüpfel und Zackenkragen (siehe Abb.17).
Die Muster sind mit Hilfe von Digitalkameras technisch erfassbar, so dass neben Universalität, Einzigartigkeit[2] und Konstanz ebenfalls die Erfassbarkeit als Anforderung an ein biometrisches Merkmal erfüllt ist. Darüber hinaus besteht bei der Iris eine geringe Verletzungsgefahr, da sie durch die Linse und die Hornhaut geschützt wird und ein inneres Organ darstellt, das aber dennoch sichtbar ist. Durch die Fähigkeit, sich bei Helligkeitsveränderungen zusammenziehen und ausdehnen zu können, kann die Iris ebenfalls für eine Lebenderkennung genutzt werden, bei der zufällige Änderungen der Helligkeit erzeugt werden und die Reaktion der Iris beobachtet wird [Kronberg, 2002].

Geeignete Verfahren zur Abbildung und Erkennung einer Iris in Computersystemen wurden von John Daugman 1993 vorgeschlagen und 1994 patentiert [Daugman, 1994]. Die Algorithmen wurden in Form von ausführbaren Programmen auf den Markt gebracht und bilden seitdem die Grundlage für Iriserkennungssysteme, die für Versuche in der Öffentlichkeit eingesetzt werden. Projekte, bei denen der Daugman Algorithmus eingesetzt wurde, fanden bei der British Telecom, US Sandia Labs, UK International Physical Laboratory, NCR, Oki, IriScan, Iridian, Sensar und Sarnoff statt [Kronberg, 2002]; [Behrens/Roth, 2001].

[2] Diese Behauptung basiert darauf, dass bisher noch keine zwei gleichen Irismuster entdeckt wurden.

3.3.3 Das Verfahren von Daugman

Im folgenden wird der Algorithmus von John Daugman erklärt, der auch in vielen kommerziell erhältlichen Systemen eingesetzt wird. Das Verfahren teilt sich in die folgende Schritte auf:

a) Aufnahme des Auges
b) Extraktion der Iris
c) Berechnung des Iriscodes
d) Vergleich

a) Aufnahme des Auges

Wie bereits in 3.3.2 erwähnt, werden Irisbilder mit Hilfe von Digitalkameras (CCD-Kameras) erzeugt. Man unterscheidet aktive und passive Aufnahmegeräte:

- *Aktive Systeme* fordern den Benutzer dazu auf, den Kopf vor der Kamera so zu positionieren, dass ein zur Verarbeitung geeignetes Bild der Iris aufgenommen werden kann. Diese Systeme sind nicht sehr benutzerfreundlich, aber vergleichsweise kostengünstig. Ein Beispiel für ein kommerzielles aktives Aufnahmegerät ist die Authenticam™ von Panasonic (siehe Abb.18).

Abb.18: Panasonic Authenticam™ EyePicture BM-ET100US

- *Passive Systeme* sind in der Lage, mit Hilfe mehrerer Kameras Aufnahmen der Iris zu erzeugen, ohne dass der Benutzer aktiv eingreifen muss. Dabei erfassen meist zwei Kameras die Person, um Gesichtsposition und Entfernung zu berechnen, während eine dritte Kamera das Irisbild aufnimmt. Passive Aufnahmesysteme sind eher für Großunternehmen und Banken interessant, die auf Benutzerfreundlichkeit und schnelle Identifikation sehr großen Wert legen.

Alle Systeme, die auf dem Daugman-Verfahren basieren, nehmen Schwarz-Weiß-Bilder auf, da Farbinformationen bei dieser Methode irrelevant sind. Bei den meisten Aufnahmegeräten verwendet man Licht mit einer Wellenlänge, die außerhalb des von Menschen sichtbaren Bereichs liegt, um einerseits den Benutzer nicht zu blenden und andererseits dunkle Iriden kontrastreicher erfassen zu können [Arnold, 2003].
Um die reichhaltigen Einzelheiten der Irismuster zu erfassen, sollte die Auflösung des aufnehmenden Systems mindestens 50 Pixel im Irisradius entsprechen [Behrens/Roth, 2001].

b) Extraktion der Iris

Nachdem das Bild eines Auges erzeugt wurde, muss der für das Verfahren relevante Teil (der Irisring) lokalisiert und vom Restbild getrennt werden. Dann folgt eine Normalisierung der Bilddaten, um sie effizienter weiterverarbeiten zu können.
Bei der Lokalisierung werden die Kanten beim Übergang zwischen Iris und Pupille bzw. zwischen Iris und Augenweiß genutzt. Problematisch ist hierbei, dass die Pupille nicht immer genau in der Mitte der Iris liegt (sie kann leicht nach unten und zur Nase hin versetzt sein) und die Iris zusätzlich zum Teil von den Augenlidern verdeckt sein kann (vgl. Abb.19). Daher müssen also die Parameter des Pupillenkreises getrennt von den Parametern des Iriskreises bestimmt werden [Arnold, 2003].

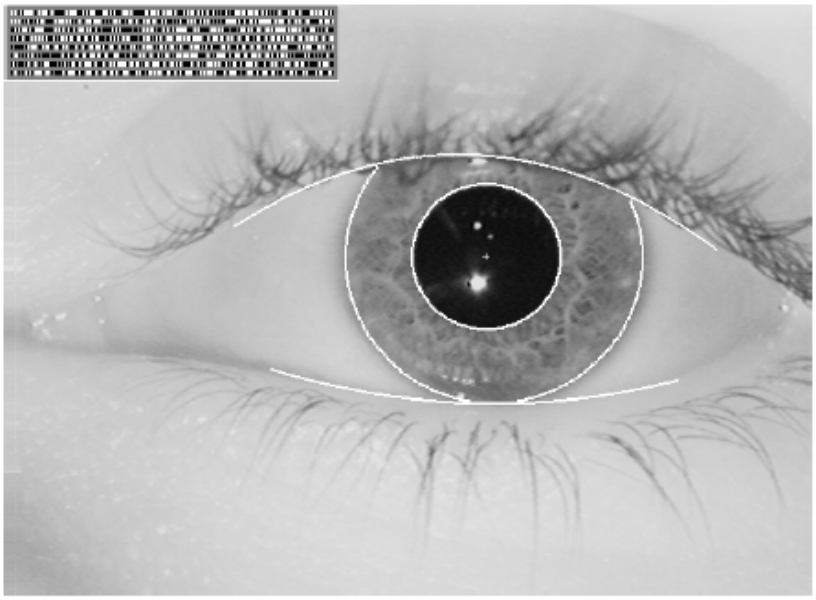


Abb.19: Beispiel eines Irismusters: die überlagerten Linien zeigen die Ergebnisse der Iris- und Pupillenortung, sowie die Erfassung der Augenlider

John Daugman verwendet folgenden Operator zur Lokalisierung der Kreiskanten:

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

wobei *I (x, y)* ein Bild wie Abb.19 ist. Der Operator sucht im Bildbereich *(x, y)* nach dem Maximum - bezüglich zunehmendem Radius *r* - der unscharfen partiellen Ableitungen, für das normierte Konturenintegral von *I(x, y)* entlang eines Kreisbogens *ds* mit Radius *r* und den Mittelpunktkoordinaten (x_0,y_0). Das Symbol $*$ steht für die Faltung und $G_\sigma(r)$ ist eine Glättungsfunktion, z.B. eine Gaußfunktion mit Skalierungsparameter σ [Behrens/Roth, 2001]. Maxima dieser Funktion entstehen an Kanten, an denen der Grauwert sich sprunghaft ändert, wie z.B. beim Übergang vom Augenweiß auf den Irisring [Arnold, 2003]. Die Tatsache, dass die Größe der Pupille durch unterschiedliche Beleuchtung variiert und sich somit auch das Irismuster dehnt oder streckt, macht es nötig, die Bilddaten für einen Vergleich zu normalisieren. Dazu wird das Irisbild vom kartesischen Koordinatensystem in ein Polarkoordinatensystem projiziert. Da somit der Radialkoordinatenbereich von der inneren Begrenzung bis zur äußeren Begrenzung der Iris ein Einheitsintervall ist ([0,1]), erfolgt hier automatisch eine Korrektur für die Musterverzerrung, die bei der Veränderung der Pupillengröße entsteht [Kronberg, 2002].

c) Berechnung des Iriscodes

Im nächsten Schritt werden die Bilddaten einer Wavelet-Transformation unterzogen.
Mit Hilfe der Wavelet-Transformation sollen die entscheidenden Merkmale in kompakter Form extrahiert werden und ein biometrisches Template erstellt werden.

Exkurs Wavelets:
Wavelets weisen eine gewisse Ähnlichkeit zur diskreten Cosinus-Transformation auf, nur dass hier zwei entscheidende Unterschiede bestehen: Es wird statt Sinus und Cosinus eine beliebige Motherwaveletfunktion benutzt und kein konstanter, sondern mit steigender Frequenz kleinerer Ausschnitt betrachtet. Bei der Wavelet-Transformation werden häufig Motherwavelets benutzt, die fraktale Eigenschaften aufweisen (Selbstähnlichkeit). Nun wird ein Bereich des Bildes mit Hilfe dieser Funktion nachgebildet (durch die Wahl der Amplitude). Dies wird rekursiv mit steigender Frequenz des Motherwavelets auf kleineren Bereichen des Bildes wiederholt, in dem der bisher angenäherte Wert zu dem des höher

frequenten addiert wird. Bei ausreichend hohen Frequenzen können so die Ursprungssignale exakt nachgebildet werden. Häufig reicht aber eine gute Näherung aus, da ab einem gewissen Detailgrad ein Rauschen ohne relevanten Informationsgehalt auftritt. Somit dient die Wavelet-Transformation gleichzeitig als Filter.
Ein interessanter Aspekt bei der Wavelet-Transformation ist die Tatsache, dass die Signalinformationen bei Vernachlässigung von Details (z. B. Rauschen) sehr kompakt dargestellt werden können. Daher ist dieses Verfahren auch zur Komprimierung von Bild-, Ton- und Videodateien geeignet.

In dem Verfahren von Daugman wird ein Gaborwavelet genutzt, um ausschließlich Musterinformation und nicht den vorhandenen Kontrast, geschweige denn die Farbwerte zu extrahieren, da sie zu stark von den Aufnahmebedingungen abhängen. Für die Datenextraktion sind daher nur die Phaseninformationen der Wavelets relevant. Für jeden Punkt im Polarkoordinatensystem wird ein Bit berechnet, welches den Wert 0 oder 1 (je nach Phaseninformation) erhält [Arnold, 2003].

d) Vergleich

In der Vergleichsphase wird das in c) erzeugte Iristemplate mit einem Referenztemplate verglichen, um festzustellen, ob diese übereinstimmen. Als Maß für die Unterschiedlichkeit verwendet Daugman den Hamming-Abstand (engl.: Hamming distance, HD), der die Anzahl unterschiedlicher Bits zweier gleichlanger Binärwerte angibt:

$$HD = \frac{\| (code\ A \otimes code\ B) \cap mask\ A \cap mask\ B \|}{\| mask\ A \cap mask\ B \|}$$

Der XOR-Operator (⊗) ermittelt hierbei die nichtübereinstimmenden Bitstellen. Der AND-Operator (∩) sorgt dafür, dass nur solche Bitstellen dem Korrelationsvergleich unterzogen werden, die nicht durch Augenbrauen, Augenlieder, Lichtreflexionen oder anderen Störungen ungültig sind.
Der normierte Hamming-Abstand entsteht aus dem Quotienten der Normen der resultierenden Bitvektoren und der in der AND-Logik kombinierten Maskenvektoren, wobei „code A“ und „code B“ die Phasenbitvektoren und „mask A“ und „mask B“ die Bitmaskenvektoren bezeichnen.

Der resultierende normierte Hamming-Abstand ist ein Maß für die Unähnlichkeit zweier Iristemplates. Ein Wert von 0 entspricht hierbei einer perfekten Übereinstimmung [Kronberg, 2002].

Das Verfahren von Daugman bietet den Vorteil sehr schnelle Vergleiche vieler Iriscodes bei sehr guter Erkennungsrate durchführen zu können, weil sie nur auf einfachen Booleschen Operatoren basieren. So kann eine 300-MHz Sun Workstation in einer Sekunde einen Iriscode mit 100.000 anderen vergleichen. Somit ist die Anwendung bei großen Datenbanken unproblematisch.
Allerdings muss einschränkend erwähnt werden, dass die Testumgebung ungenau beschrieben wurde. Aus den Quellen von John Daugman ist nicht direkt erkennbar, wie viele Personen zum Testen des Verfahrens zur Verfügung standen. Außerdem ist nicht klar, über welchen Zeitraum versetzt die Aufnahmen für gleiche Iriden gemacht wurden. Es wird auch an keiner Stelle erwähnt, wie zuverlässig der Operator zur Erkennung der Kreiskanten (siehe Abschnitt b)) ist, da eine falsch extrahierte Iris nicht richtig verglichen werden kann [Arnold, 2003].

3.3.4 Lebenderkennung

Wie bereits in 3.3.2 erwähnt, kann die Eigenschaft des Auges, sich durch Zusammenziehen oder Erweitern der Pupille den gegebenen Lichtverhältnissen anzupassen, für eine Lebenderkennung genutzt werden. Dazu muss lediglich während der Authentisierung die Helligkeit verändert und die Reaktion des Auges erfasst werden. Außerdem können Bewegungen des Auges, z.B. der Lidschlag, gemessen werden.

3.4 Handgeometrieverfahren

Die Erfassung der Handgeometrie ist eines der ältesten biometrischen Verfahren. Ab einem Alter von etwa 20 Jahren sind die Veränderungen an der menschlichen Hand meist nur noch gering. Bereits der Schatten einer Hand gilt als einzigartig. Für die biometrische Vermessung werden bis zu 90 Werte für Dicke, Länge, Breite und Fläche der Hand bzw. der Finger ermittelt. Theoretisch nutzbare Charakteristiken der Handoberfläche, wie die Verteilung der Hautporen, werden bislang nicht herangezogen [Petermann/Sauter, 2002].
Authentisierung über Handgeometrie findet heute hauptsächlich zur Arbeitszeitmessung oder als Zugangskontrolle zu Räumen oder Gebäuden Anwendung. So wird sie in etwa 50% der amerikanischen Kernkraftwerke und zur Einreisekontrolle in die USA genutzt [Maier, 2002]. Die Bedienung der Systeme ist einfach, teilweise aber unbequem (wenn z.B. für die richtige Positionierung die Hand fest an starre Anschlagstifte gedrückt werden muss, siehe Abb.20). Ein Nachteil ist sicherlich, dass der Sensor nicht berührungsfrei ist und dadurch einige Menschen das System aus Hygienegründen ablehnen. Da aufgrund der Dickenmessung dreidimensionale Aufnahmen benötigt werden, sind komplizierte Optiken erforderlich. Die Sensortechnik und mit ihr das Gesamtsystem fällt daher recht voluminös aus. Die Templategröße ist mit 10-20 Bytes klein, Angaben zur erzielbaren Genauigkeit schwanken. Eine Lebenderkennung zur Erhöhung der Überwindungssicherheit wird bislang kaum angeboten [Petermann/Sauter, 2002].

3.4.1 Der Sensor

Abb.20: HandPunch 4000™

Der Sensor eines Handreaders besteht aus einem Leuchtkörper, einer Auflagefläche für die Hand, einer Spiegelmechanik für die Seitenansicht und einer CCD-Kamera. Die Firma Recognition Systems benutzt eine CCD-Digitalkamera mit einer Auflösung von 32000 Pixel. Im Vergleich zu heutigen Digitalkameras mit 3-4 Millionen Pixel ist dies sehr gering. Um die Hand in die richtige Position zu bekommen, sind auf der Auflagefläche verschiedene Stifte angebracht. Diese stellen sicher, dass die Finger gespreizt sind und die gleiche Position wie beim Enrollment (siehe 3.4.2) einnehmen. Die Stifte sind berührungssensitiv. Sobald die Hand alle Stifte berührt, nimmt die Kamera ein Bild auf [Maier, 2002].

3.4.2 Enrollment

Beim Enrollment-Vorgang werden von der Hand des anzumeldenden Benutzers mehrere Bilder aufgenommen (siehe Abb.21). Normalerweise muss der Benutzer die Hand jedes mal komplett vom Sensor entfernen und neu auflegen, um eine „Alltagssituation“ zu simulieren. Diese Bilder werden dann vorverarbeitet (siehe 3.4.3), Merkmale extrahiert (siehe 3.4.3) und Durchschnittsvektoren erzeugt. Diese stellen nun das biometrische Template dar, mit dem sich der Benutzer zukünftig authentisieren kann [Maier, 2002].

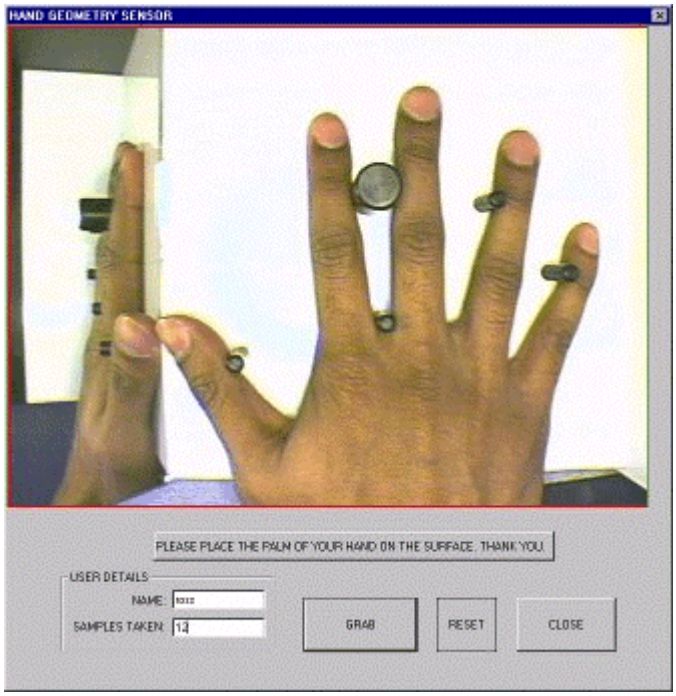


Abb.21: Graphical User Interface eines Handgometrie-Systems

3.4.3 Preprocessing und Merkmalsextraktion

Der erste Schritt bei der Vorverarbeitung ist die Konvertierung in ein Schwarz-Weiß-Bild (siehe Abb.22). Dann wird die Qualität der Aufnahme verbessert, in dem potentieller Schmutz und andere „Unreinheiten“ mit Hilfe von definierten Schwellwerten entfernt wird [Maier, 2002]

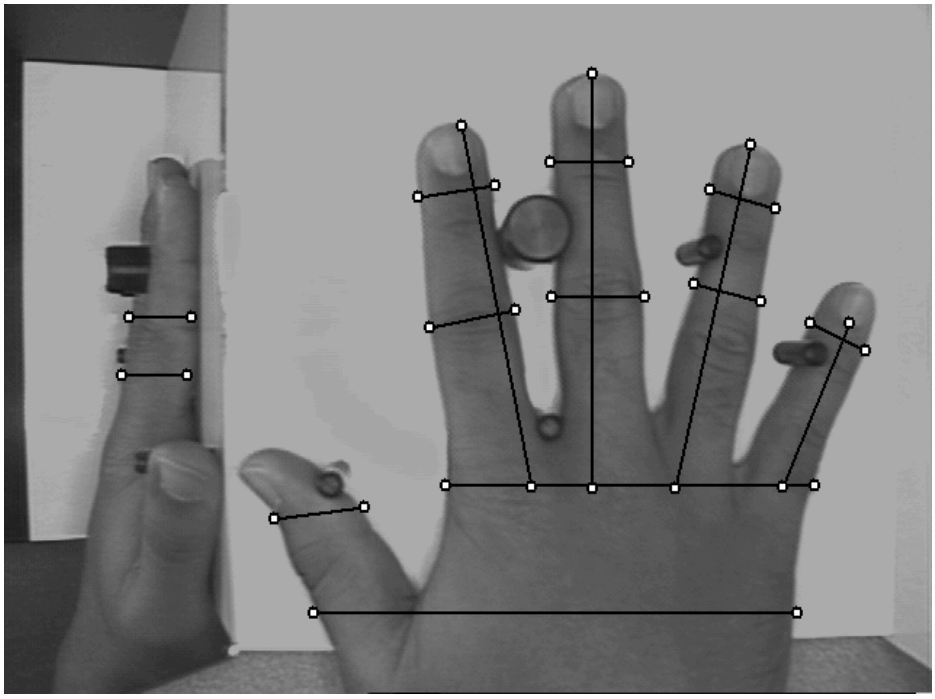


Abb.22: Aufnahme eines Handgeometrie-Sensors mit markierten relevanten Merkmalen

3.4.3.1 Relevante Merkmale

a) Längen und Breiten der einzelnen Finger

Besonders interessant in bezug auf die Länge sind der Mittelfinger als längster und der kleine Finger als der kürzeste. Manche Systeme beschränken sich daher auf diese beiden Finger, andere berücksichtigen vier (außer den Daumen, die in den Aufnahmen nicht die richtige Lage haben). Des weiteren werden die Breiten der Finger an verschiedenen Punkten und die Breite der gesamten Handfläche gemessen.

b) Dicke der Hand und der Finger

Die Höhen der Finger bzw. der Handfläche ist ebenfalls ein Merkmal, das bei biometrischen Handgeometrie-Verfahren eine Rolle spielt . Die Höhen der einzelnen Finger sind allerdings - abhängig vom verwendeten System - schwer zu ermitteln, da sie von den anderen Fingern verdeckt sein können.

c) Interfinger-Punkte

Interfinger-Punkte sind die Koordinaten zwischen den Fingern. Gemessen werden die Winkel der Interfinger-Punkte.

d) Die Krümmung der einzelnen Finger in Bezug auf ihren Mittelpunkt

3.4.3.2 Verfahren zur Feature-Extraktion

Selbst durch Ausrichten an einem Sensor mit entsprechenden Stiften ist die Lage der Hand nie ein und dieselbe. Um dies nachträglich anzupassen, existiert ein Ansatz, die Aufnahme der Hand so zu transformieren, dass die Finger auf jeder Aufnahme möglichst gleich angeordnet sind (siehe Abb.23). Die Methode nennt sich „deformable shape analysis“. Die ermittelten Handkonturen mehrerer Sensorbilder werden mittels Verschiebung auf maximale Deckungsgleichheit gebracht.

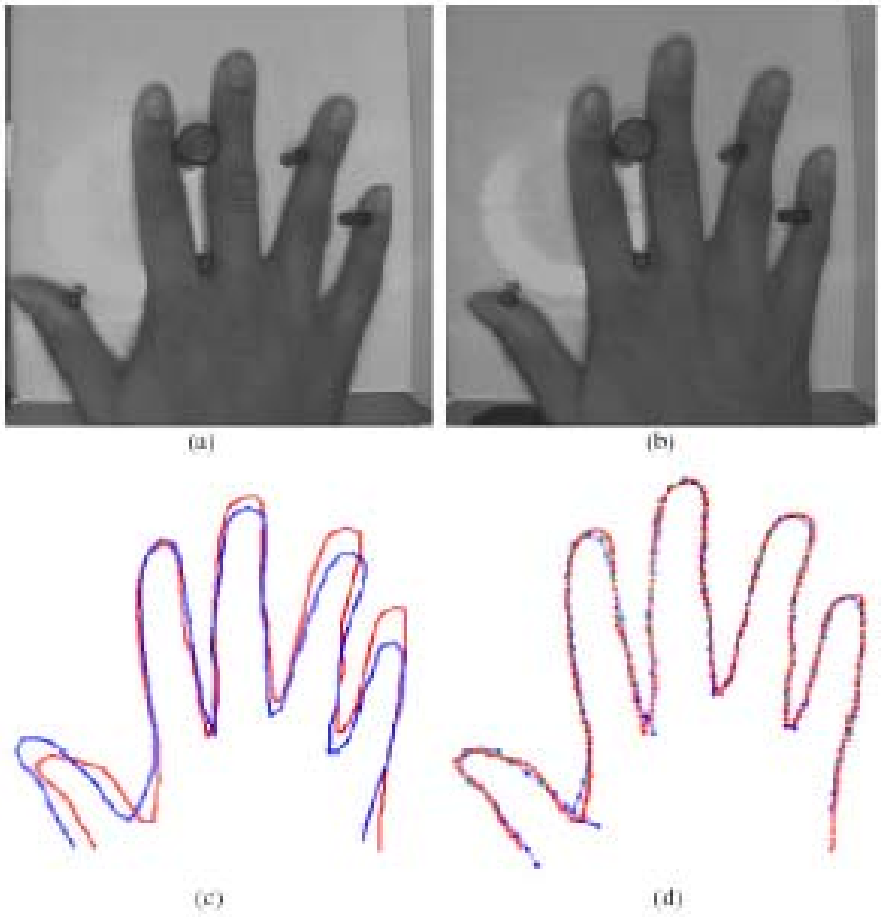


Abb.23: Deformable Shape Analysis

Den durchschnittlichen Abstand der Punkte, der bei der Verschiebung korrigiert wird, bezeichnet man als Mean Alignment Error (MAE). Dieser Wert kann auch im Template gespeichert werden. Anhand der Messlinien wird die Breite oder Länge der Finger ermittelt. Allerdings ist nicht jedes extrahierte Merkmal für eine Speicherung im Template bzw. für eine Authentisierung geeignet. Deshalb wird für jedes Merkmal die Eindeutigkeit mittels einer statistischen Methode berechnet:

$$E_i = \frac{\text{Unterschiede zwischen Bildern der gleichen Person}}{\text{Unterschiede zwischen Bildern verschiedener Personen}}$$

E_i steht für Eindeutigkeit des Merkmals i.
Wenn die Anzahl der Unterschiede eines Merkmals i zwischen den Bildern der gleichen Person relativ klein und gleichzeitig die Unterschiede zwischen den Bildern bzw. Merkmalsvektoren anderer Personen zueinander sehr groß sind, ist die Discriminability, d.h. die Unterscheidungskraft des Merkmals sehr ausgeprägt. Im Template werden nur die Features mit großer Eindeutigkeit gespeichert. Die momentane Größe eines Templates liegt je nach Anzahl der Features zwischen 9 und 25 Bytes [Maier, 2002].

3.4.4 Vergleich

Die Merkmalsvektoren (Templates) können im Rahmen einer Verifikation bzw. Identifikation verglichen werden. Es gibt verschiedene Vergleichsmethoden, z.B. die Berechnung des Hamming-Abstandes (vgl. Iriserkennung, 3.3.3). Die am häufigsten verwendete Methode ist aber die Berechnung des Euklidischen Abstandes:

$$d = \sqrt{\sum_{i=1}^{L} (x_i - t_i)^2}$$

L ist die Dimension des Feature-Vektors, x_i ist die i-te Komponente des zu testenden Vektors, t_i die i-te Komponente des Template-Vektors. Es wird also der Betrag des gesamten Abstandes berechnet. Weiterhin existieren Vergleichsmethoden auf Basis von neuronalen Netzen [Maier, 2002].

3.4.5 Lebenderkennung

Leider wird bisher bei den verbreiteten Systemen relativ selten eine Lebenderkennung angeboten. Dabei wäre es problemlos möglich, die gleichen ‚Life-Test' - Methoden wie bei der Fingerabdruckerkennung zu verwenden (siehe 3.1.5), z.B. die Messung der Pulsoxymetrie.

3.5 Sprechererkennung

Sprechererkennung ist in den USA ein sehr verbreitetes Mittel, nicht nur für hochsichere Anwendungen. Sie ist eine sehr preiswerte Methode, die durch intensive Forschung und Entwicklung in den letzten Jahren ihre anfänglichen Probleme, beispielsweise sehr lange Antwortzeiten und relativ hohe Fehlerquoten, stark minimieren konnte. Die Sprechererkennung besitzt eine sehr hohe Benutzerakzeptanz, weil Menschen es gewohnt sind, andere Personen anhand ihrer Stimme zu erkennen und weil sie täglich in das Mikrofon eines Telefons sprechen [Petermann/Sauter, 2002].
Wie bei anderen biometrischen Verfahren, muss auch bei der Sprechererkennung ein Enrollment stattfinden. Danach ist es möglich, eine Sprecherverifikation oder Sprecheridentifikation durchzuführen, wobei grundsätzlich gilt, dass eine Erkennungsaufgabe umso schwieriger wird, je mehr Muster gleichzeitig erkannt werden sollen. Für Sicherungsaufgaben wird daher überwiegend die Sprecherverifikation verwendet.
Weiterhin unterscheidet man zwischen textabhängigen und textunabhängigen Sprechererkennungsverfahren: Bei textabhängigen Systemen findet die Erkennung mittels eines bestimmten gesprochenen Textes (einem Schlüsselwort) statt, bei textunabhängigen wird der Sprecher anhand beliebiger Worte authentisiert. In bezug auf Erkennungsraten ist die Vorgabe eines Schlüsselwortes am besten geeignet. Durch Wortwahl aus einer Schlüsselwortliste lässt sich vermeiden, dass für die Erkennung ungeeignete Wörter gewählt werden. Abgesehen davon sind textabhängige Systeme einfacher zu implementieren und leichter „trainierbar“. Nachteilig ist, dass mit dem Wissen des Schlüsselwortes Einbruchversuche unberechtigter Nutzer erleichtert werden.

Bei textunabhängigen Systemen sind komplexere Verfahren notwendig, die z.B. in Diktiersystemen auf PC-Basis Anwendung finden. Dazu werden sogenannte Hidden-Markov-Modelle (HMM-Modelle) von Wortsegmenten (Phonemen) verwendet. Text-unabhängige Sprechererkennungen haben den Nachteil, dass ihr Training langwieriger und komplexer ist und die Erkennungssicherheit auch von der Länge der Sprechzeit bei der Überprüfung abhängt [Behrens/Roth, 2001].

3.5.1 Spracherzeugung

Sprache entsteht durch das Zusammenwirken von Lunge, Kehlkopf, Mund-, Nasen- und Rachenraum. Die aus der Lunge strömende Luft regt (für stimmhafte Laute) die im Kehlkopf befindlichen Stimmbänder zum Schwingen an. Für stimmlose Laute sind die Stimmbänder geöffnet. Der hindurchtretende Luftstrom bricht sich an Kanten und Ritzen des Rachenraumes. Interessanterweise dienten die Stimmbänder ursprünglich nur als Verschluss, der das Eindringen von Speiseresten in die Luftröhre verhindern sollte. Erst im Verlauf der Evolution und der Entwicklung der Sprache entwickelten sich die Stimmbänder zu einem außerordentlich komplizierten Schall-Anregungsorgan.
Die Stimmbänder produzieren das Anregungssignal für die Sprache (Phonotation). Die Frequenz des Signals bezeichnet man als *Sprachgrundfrequenz*. Sie ist maßgebend für die Intonation oder Sprechmelodie. Ihre Frequenz liegt zwischen 80 Hz (tiefe Männerstimme) und ca. 350 Hz (hohe Kinderstimme). Nach der Phonotation (Sprachanregung) erfolgt die Artikulation (Lautformung): Die Lautformung erfolgt im wesentlichen im Mund- und Nasenraum, unter Einbeziehung des Kehlkopfes.

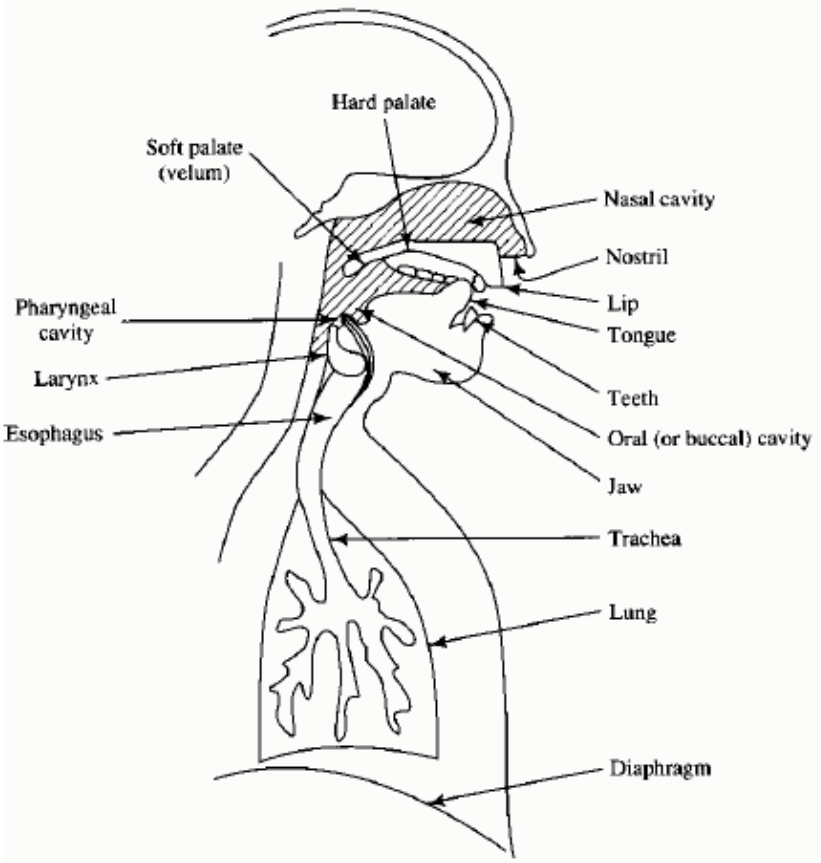


Abb.24: Das menschliche Sprachsystem

Die weitaus meisten Laute werden jedoch im Mundraum produziert. Hierbei spielt die *Zunge* eine entscheidende Rolle. Ihre Bedeutung wird z.B. dadurch unterstrichen, dass in verschiedenen Sprachen die Wörter "Zunge" und "Sprache" durch das gleiche Wort ausgedrückt werden (z.B. im Lateinischen durch "lingua"). Auch der Mundraum wirkt als Resonator. Im Gegensatz zum Nasenraum ist der Mundraum, aufgrund der Zunge, in vielfältiger Weise veränderbar [Fellbaum, 2002].

3.5.2 Mustererkennung von Sprache

Sprache ist gekennzeichnet durch ausgeprägte zeitliche Veränderungen. Diese müssen daher in den automatischen Erkennungsvorgang maßgeblich eingehen. Ein relativ einfaches Verfahren zur Erkennung von gesprochenen Schlüsselwörtern setzt die Sprachsignale (vgl. Abb.25) durch Überlagern der frequenzspezifischen Energieanteile über die Zeit in Spektrogramme um.
Anhand dieser Spektrogramme können nun die aus der optischen Mustererkennung bekannten Verfahren wie neuronale Netze eingesetzt werden. Dabei wird die Bedeutung (die Klasse) vorgegeben und das neuronale Netz so optimiert, dass beim Anlegen von Mustern dieser Klasse die geringste Abweichung auftritt, bei Anlegen anderer Klassenmuster im Training höhere Abweichungen [Behrens/Roth, 2001].

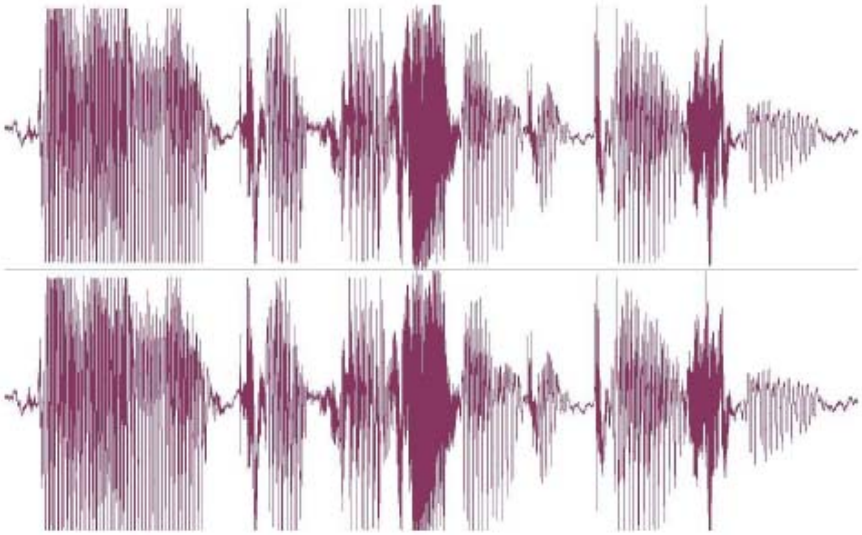


Abb.25: Darstellung der Sprachsignale beim Aussprechen der Wörter „Biometrische Authentikation“

Aufgrund der unterschiedlichen Sprechlängen sowie der zeitlichen Dehnungen und Stauchungen auch bei Äußerung des gleichen Wortes vom gleichen Sprecher, verwischen die in den Spektrogrammen sichtbaren charakteristischen Konturen. Bei neuronalen

Netzen sind somit zusätzliche Parameteraufbereitungen und eine Vielzahl von Trainingsmaterial notwendig, um stabile Erkennungen zu ermöglichen. Vorteilhaft wären Erkennungsvorgänge, die gleichzeitig mit dem frequenzmäßigen Vergleich auch eine Normierung dieser zeitlichen Verzerrungen durchführen [Behrens/Roth, 2001].

3.5.2.1 Dynamische Zeitnormierung (dynamic time warp)

Schon eine einzige Referenz und eine Testäußerung genügen, um das Verfahren der dynamischen Zeitnormierung (DTW) anzuwenden. Das DTW-Verfahren ist textabhängig. Hierbei sucht der Algorithmus entlang eines vorgeschriebenen Pfadbereiches den optimalen zeitlichen Vergleichspfad zwischen Test- und Referenzäußerung. Gleichzeitig bestimmt der Algorithmus dabei die von Anfang bis Ende aufsummierten Unterschiede der frequenzmäßigen Analyseparameter von Referenz- und Testsignal. Wird das gleiche Signal als Referenz- und als Testsignal genutzt, kommt ein Abstand von 0 heraus. Wird ein anderes Wort getestet oder spricht ein anderer Sprecher das Referenzwort, steigt dieser Abstandswert an. Im Optimalfall sollten die Abstandswerte beim Sprechen des gleichen Wortes vom gleichen Sprecher kleiner sein als in den anderen Fällen. In der Realität kommt es jedoch zu starken Streuungen dieser Werte, so dass eine Festlegung der Erkennungsschwelle erschwert wird.

3.5.2.2 Hidden-Markov-Modell (HMM)

Beim stochastischen HMM-Verfahren wird aus einer Vielzahl von Trainingsäußerungen ein Modell berechnet, das die gleichen Folgen von Merkmalsvektoren erzeugen kann, wie sie bei der Analyse der Trainingsreferenzen gefunden worden sind [Behrens/Roth, 2001].
Um ein mathematisches Modell aufzubauen, wird die Erzeugung von Sprache als stochastischer Prozess angesehen. Man geht davon aus, dass jedes Wort bzw. Phonem (kleinstes sinntragendes Sprachbestandteil) bei jedem Aussprechen anders klingt. Weiterhin kann man Worte bzw. Phoneme oder andere Sprachteile als Zustände eines Spracherzeugungsprozesses annehmen. Von einem gegebenen Zustand kann man nun verschiedene Laute erzeugen, also neue Zustände erzeugen. Es sind jedoch nicht alle Zustandsübergänge möglich. Man kann außerdem davon ausgehen, dass ein Spracherzeugungsprozess entsprechend einer Wahrscheinlichkeit bestimmte Laute erzeugt. Einige Lautübergänge erhalten höhere Wahrscheinlichkeiten (auf "e" folgt "r"), andere erhalten geringere Wahrscheinlichkeiten (auf "n" folgt "f"). Der Erzeugungsprozess

vollführt also Übergänge von einem Zustand zum nächsten.
Ein Sprachmodell besteht folglich aus Wahrscheinlichkeiten für die Lauterzeugung und für Lautübergänge. In der Trainingsphase werden bestimmte lautliche Einheiten (Phoneme oder Wortteile) als an den Sprecher angepasste Hidden-Markov-Modelle gespeichert, (auch Allophone genannt). Jedes Allophon enthält bis zu acht Zustände. Außerdem erhalten die Zustände bestimmte Anfangs- und Endwahrscheinlichkeiten, also Wahrscheinlichkeiten, dass das Modell am Anfang oder Ende steht. Die zeitliche Variation der Aussprache wird über eine Selbstreferenz hergestellt, das heißt, dass ein langgesprochener Laut (Zustand) auf sich selbst abgebildet wird und dadurch im Modell verlängert wird. Für jede Einheit (Wort) wird mit dem HMM die Wahrscheinlichkeit berechnet, dass das gespeicherte Modell (Folge aus Zuständen) das aufgenommene Signal erzeugen kann. Da die Berechnung für jedes Modell durchgeführt werden muss, kommt es zu einem hohen Rechenaufwand. Um ein HMM für ein Wort mit n Phonemen und der Länge T vollständig zu berechnen, müssen $2 \cdot T^2 \cdot n$ Berechnungen durchgeführt werden. In der Praxis kürzt man diese Berechnung durch spezielle Rechenverfahren ab. Dadurch wird die Berechnung ungenauer, aber schneller (Algorithmen: Viterbi-Algorithmus, Forward-Backward-Algorithmus, Baum-Welch-Optimierungs-Regeln). Viterbi- und F/B-Algorithmus arbeiten, ähnlich wie beim DTW, rekursiv mit Teilwahrscheinlichkeiten. Sie berechnen also erst alle Wege, um das Ziel abzubilden, dann den wahrscheinlichsten.

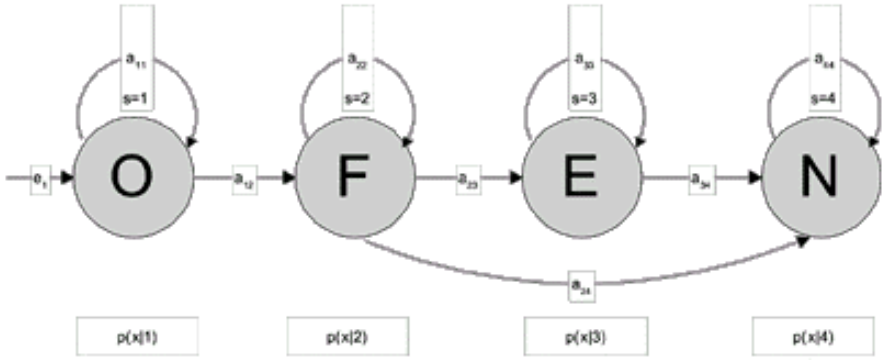


Abb.26: HMM für das Wort „Ofen“

Die Abbildung zeigt ein sehr simples HMM (nur ein Zustand pro Laut) für das Wort Ofen. Die Verlängerung der einzelnen Vokale wird durch die Selbstreferenz verdeutlicht ("Ooohfen"). Außerdem ist es möglich, aus dem "f" direkt zum "n" zu gelangen, wie es umgangssprachlich häufig vorkommt ("Ofn") [Henne, 2001].
Damit ist es möglich, mehr als nur isoliert gesprochene Schlüsselwörter wie bei DTW zu nutzen. Mit HMM kann auch natürliche Sprache analysiert werden, oder die gewonnenen

Beschreibungen der Sprachbestandteile können zur Synthese von neuen, vorher nicht gesprochenen Schlüsselwörtern dienen.
Beim HMM hängt es in starkem Maß vom Trainingsmaterial und der Organisation von Training und Erkennung ab, ob eine textabhängige Sprecherverifikation oder sogar eine textunabhängige Sprecheridentifikation realisiert werden kann [Behrens/Roth, 2001].

3.5.3 Lebenderkennung

Eine Lebenderkennung im eigentlichen Sinne ist bei der Sprechererkennung schwer realisierbar. Die Kontrolle, ob lediglich ein Tonband abgespielt wird, kann nur mit Hilfe einer Kombination mit Schlüsselwörtern oder anderen Authentisierungsmethoden realisiert werden.

3.5.4 Abschließende Bewertung

Für den praktischen Einsatz der Sprechererkennung sind einige Besonderheiten im Blick zu behalten. Abgesehen davon, dass nicht jeder Mensch sprechen kann, ist es nachteilig, dass es zu sprecher – und wortspezifischen Ausreißern in der Erkennungsleistung kommen kann. In lärmerfüllter Umgebung auftretende Hintergrundgeräusche fordern zusätzliche Verarbeitungsschritte innerhalb der Algorithmen und Implementierungen, deren Bedienoberfläche möglichst schon mit Vorergebnissen des Erkennungsalgorithmus gekoppelt sein sollte. Ungeeignete Trainingsreferenzen aufgrund zu hoher Ähnlichkeit oder Hintergrundstörungen sollten daher vermieden werden.
Die hohe Zeitinvarianz der Sprechweise und der Stimmcharakteristiken erfordert eine Anpassung, um die Erkennungsleistung nach einiger Zeit nicht zu sehr herabzusetzen. Gleichzeitig darf eine höhere Toleranz gegenüber Veränderungen der Stimme die Überwindungssicherheit nicht erheblich beeinträchtigen.
Die Sammlung umfangreicher Sprachproben beim Enrollment wird häufig als sehr lästig empfunden. Daher wird eine möglichst kurze Lernphase angestrebt, die allerdings die Variabilität der eigenen Sprechweise meist nur sehr eingeschränkt erfasst. Insgesamt erfordert die gegenüber anderen biometrischen Verfahren höhere Akzeptanz noch Kompromisse in Bezug auf die Erkennungsleistung und den Realisierungs- und Implementierungsaufwand [Behrens/ Roth, 2001].

3.6 Andere Verfahren

3.6.1 Retina-Scan

Wie das Fleckenmuster der Iris gilt auch die Anordnung der Blutgefäße in bzw. hinter der Netzhaut oder Retina, also dem lichtempfindlichen Bereich im Augeninneren, als individuell einzigartig (auch bei Zwillingen). Das Adernmuster der Netzhaut bleibt, wie das Irismuster, weitgehend konstant, es kann sich aber durch Krankheiten oder Verletzungen vorübergehend oder andauernd verändern.

Abb.27: Infrarotaufnahme einer Retina

Seit 1985 gibt es (mit dem EyeDentify 7.5) ein Gerät, das mittels Infrarot-Laser die Blutgefäße der Netzhaut scannt. Dabei werden etwa 400 charakteristische Punkte festgehalten. Relativ aufwendige Spezialtechnik ist erforderlich, um durch die Pupille hindurch die Netzhaut aufzunehmen. Das Auge muss sich sehr nahe an der Aufnahmeoptik befinden (1-2 cm) und während des Scannens ruhig gehalten werden. Der Nutzer blickt dann auf ein rotierendes grünes Licht, während das tatsächlich zum Abtasten benutzte Infrarotlicht für ihn unsichtbar ist. Die Templates sind mit 40-96 Bytes mittelgroß. Die Zeit für eine Messung beträgt ca. 1,5 Sekunden. Wie der Iris-Scan hat der Retina-Scan als sehr empfindliches Verfahren bei der Zutrittssicherung zu Hochsicherheitseinrichtungen sowohl im öffentlichen als auch im privaten Bereich Verbreitung gefunden. Eine Überlistung des Systems durch Attrappen wird kaum für möglich gehalten. Nicht nur der hohe Preis, sondern auch die bislang recht hohe Rückweisungsrate (von ca. 12 % beim ersten Versuch lt. Herstellerangabe) stellen ein Verbreitungshemmnis dar. Hinzu kommen Nutzervorbehalte, da eine Verursachung von Augenschäden durch den Laser befürchtet wird, auch wenn es hierfür bislang keinerlei Hinweise gibt. Konkrete Einschränkungen der Nutzbarkeit ergeben sich für Träger von Kontaktlinsen (ab einer bestimmten Dioptrienzahl), außerdem gibt es Probleme bei

Astigmatismus (Hornhautverkrümmung, eine recht häufige Ursache für Fehlsichtigkeit) [Petermann/Sauter, 2002].

3.6.2 Unterschriftenerkennung

Bei der Unterschrifts- bzw. Handschriftenerkennung ist nicht nur das optische Erscheinungsbild der Signatur (Schriftzug als "Offline-Parameter") entscheidend, sondern es werden Merkmale wie Druck, Geschwindigkeit, Beschleunigung, Auf- und Absetzpunkte sowie Stiftwinkelpositionen beim Schreiben (als "Online-Parameter") gemessen. Aufgenommen wird die Unterschrift/Handschrift heute meistens mit einem handelsüblichen Grafiktablett oder einem PDA bzw. Touchscreen. Alternativ sind auch Spezialstifte mit Sensoren in Verwendung, welche die Parameter bei der Leistung der Unterschrift/Handschrift aufnehmen und zur Auswertung übertragen.

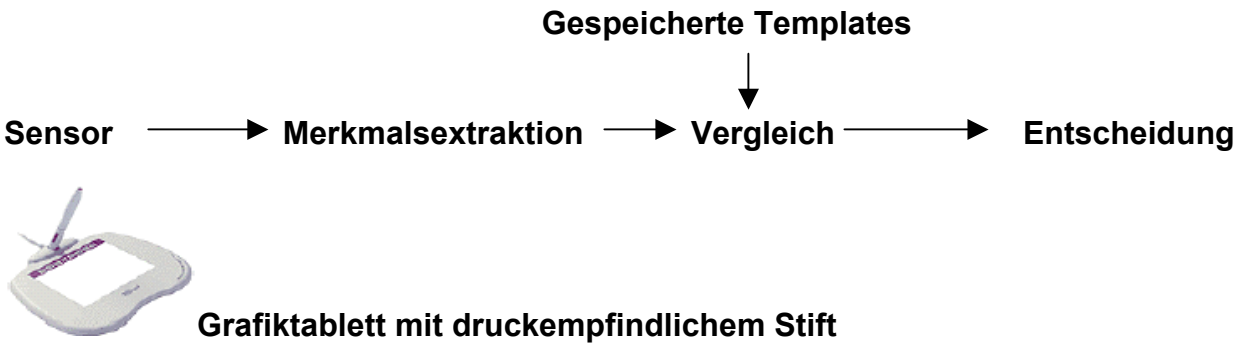


Abb.28: Schema der biometrischen Unterschriftenerkennung

Eine Erweiterung der Unterschriftanalyse liefert ein Handschriftensystem, bei welchem nicht allein die Unterschrift, sondern sog. "Semantiken" zur handschriftlichen Authentifizierung herangezogen werden. Dies können vordefinierte Wörter, ganze Sätze oder sogar kleine Zeichnungen (Sketches) sein. Ein Vorteil des Einsatzes von "Semantiken" liegt in der Anonymität - selbst bei zentral abgespeicherten Datensätzen kann diese gewahrt werden. Die Verfahren können so eingerichtet werden, dass sie vom Nutzer selbst gesteuert werden können, indem der hinterlegte Referenzdatensatz relativ kurzfristig verändert wird. Hierdurch ist eine klarere Koppelung an eine Willenserklärung möglich. Die "Beherrschbarkeit" durch den Nutzer dürfte außerdem förderlich für die Akzeptanz sein. Da die Erfassung der dynamischen

Parameter eine Lebenderkennung darstellt, ist die Fälschungssicherheit ziemlich hoch. Wegen der (noch) hohen Fehlerraten sind die Systeme bislang allerdings nur sehr eingeschränkt einsetzbar [Petermann/Sauter, 2002].

3.6.3 Messung der Tastaturanschlagsdynamik

Das Verfahren der Messung des Tastaturanschlags oder Tippverhaltens ist eine relativ neue Methode und wenig verbreitet. Sie basiert auf der Idee, dass bestimmte Verhaltensweisen beim Schreiben auf einer Tastatur typisch für eine Person sind.
Dabei wird beispielsweise die Anschlagdauer und der zeitliche Abstand zwischen den Tastenanschlägen gemessen. Ein weiteres Merkmal ist die Benutzung der Umschalt-Taste (Shift-Taste).
Mögliche Einsatzfelder sind Zugangskontrollen zu Rechnernetzen bzw. Laufwerken, Dateien und Programmen, Electronic Banking, Teleworking und Fernwartung. Die Authentisierung kann dabei unaufdringlich im Hintergrund ablaufen.
Problematisch bei diesem Verfahren ist, dass kurze Texte meistens nicht ausreichen, um eine gesicherte Erkennung durchzuführen und dass das Tippverhalten häufig von der verwendeten Tastatur oder der Tagesform abhängt. Gerade bei Handverletzungen kann es zu starken Abweichungen kommen. Ungeübte Schreiber haben meistens noch kein individuelles Tipp-Profil entwickelt und können daher nicht eindeutig identifiziert werden. Ganz abgesehen von den technischen Problemen, ermöglicht die Tastaturüberwachung Kontrolle und Spionage [Wettig, 2002]

3.6.4 DNA-Analyse

Die DNA-Analyse wird bereits in verschiedenen Bereichen angewendet, u.a.:

- Verwandschaftstests
- Archäologie
- Gerichtsmedizin und Forensik
- Medizinische Diagnostik

DNA ist die Abkürzung für „**d**esoxyribo**n**ucleic **a**cid (engl.); **D**esoxyribo**n**ukleins**ä**ure (DNS, deutsch)“. Das DNA – Molekül ist als „Bauplan des Körpers“ in jeder Zelle vorhanden und bei jedem Menschen individuell (außer bei eineiigen Zwillingen). Es besteht aus einer Doppelhelix aus komplementären Basenpaaren (Adenin-Thymin und Cytosin-Guanin):

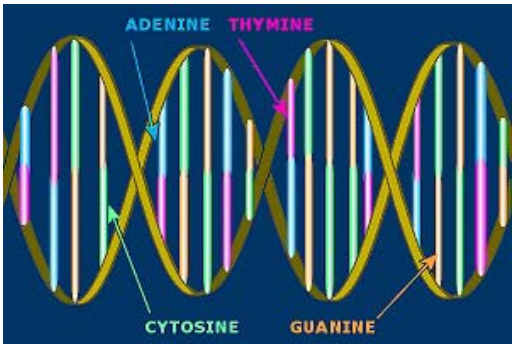


Abb.29: Das DNA-Molekül

Der Engländer Alec Jeffries entwickelte 1985 ein Verfahren, mit dem erstmals der „genetische Fingerabdruck“ des menschlichen Genmaterials festgestellt werden konnte. Die Technik wurde weiterentwickelt, so dass es möglich wurde, kleinste Proben in hoher Anzahl zu vervielfältigen und so eine genauere Analyse durchzuführen.
Bei dem Verfahren werden die Länge, Anzahl und die Position bestimmter DNA-Abschnitte ermittelt, bevor sie sortiert und sichtbar gemacht werden, um sie effektiver vergleichen zu können. Diese Methode ist seit 1990 in Deutschland vor Gericht in Form von Sachverständigengutachten als Beweismittel anerkannt (DNA-Identitätsfeststellungsgesetz; §§ 81aff., StPO).
Nachteilig ist die Tatsache, dass das Verfahren sehr komplex und zeitaufwendig ist. Es stellt hohe Anforderungen an die analysierenden Personen und Geräte und kann vertrauliche Informationen offenbaren, die missbraucht werden könnten (z.B. Informationen über Erbkrankheiten). Daher ist die DNA-Analyse für den „Normalgebrauch“ als biometrisches Verfahren noch nicht geeignet [Wettig, 2002].

3.6.5 Sonstige Verfahren

Neben den hier vorgestellten Verfahren existieren noch einige Ideen/ Techniken im Bereich der Biometrik, deren Entwicklung noch in den Anfängen stecken. Es soll daher nur kurz erläutert werden, welche Schwierigkeiten beim Einsatz dieser Verfahren entstehen können:

- Gangverhalten/ Schritterkennung und Gestik:

Bei diesen Methoden ist die Veränderlichkeit der erfassten Merkmale relativ groß und teilweise abhängig von der Tagesform. Beispielsweise haben betrunkene Personen ein verändertes Gangverhalten (Schwanken) oder eine Person hat sich am Bein verletzt und hinkt. Schwangere Frauen gehen zwangsläufig anders als vor der Schwangerschaft. Weiterhin ist es möglich, das Gangverhalten anderer Personen durch Training nachzuahmen bzw. das eigene Schrittverhalten gezielt zu verändern, um ein solches System zu täuschen.

- Gesichtswärme

Bei dieser Methode wird ein Bild erzeugt, das die Wärmeverteilung eines Gesichts dokumentiert (siehe Abb. 30).

Abb.30: Gesichtswärme-Bild

Die Kosten für die spezielle Kamera sind vergleichsweise hoch und die Gesichtstemperatur wird von äußeren Bedingungen beeinflusst. Das Gesicht kann teilweise von Haaren oder von einer Brille bedeckt sein und die Erkennung so erschwert werden.

- Ohrform

Diese Methode benutzt die Struktur des menschlichen Ohres als biometrisches Merkmal. Wie bei allen vorgestellten Verfahren, muss auch hier geklärt werden, ob die Ohrstruktur jedes Menschen wirklich einzigartig ist. Außerdem könnten Probleme durch Haarfrisuren, Kopfbedeckungen und Kopfhörern entstehen.

- Zähne

Im Bereich der Gerichtsmedizin werden Menschen bereits anhand ihrer Gebissstruktur identifiziert. Diese Methode lässt sich allerdings nicht problemlos auf lebende Menschen im Rahmen einer biometrischen Authentisierung übertragen, da noch keine schnelle und hygienisch unbedenkliche Aufnahmemethode existiert.

- Geruch

Auch der spezifische Körpergeruch eines Menschen ist schwierig messbar und wird von einer Reihe von Störfaktoren (Parfum, Umgebung) beeinflusst [Wettig, 2002].

- Gefäßmuster

Das charakteristische Venenmuster eines Menschen kann an verschiedenen Stellen des Körpers, z.B. an Handgelenk, Handrücken oder im Gesicht erfasst werden. Bei dieser ebenfalls relativ neuen Methode gestaltet sich die Messung als (noch) umständlich und teuer.

4. Risikoanalysen

4.1 Vorgehensweise

Die folgenden Risikoanalysen biometrischer Systeme beschränken sich auf die am häufigsten vorkommenden Verfahren (siehe 2.1, Abbildung 1): Fingerabdruckerkennung, Gesichtserkennung, Handgeometrieverfahren, Iriserkennung und Sprechererkennung. Viele der angesprochenen Aspekte gelten jedoch für biometrische Methoden allgemein und sollten vor ihrer Verwendung neben den spezifischen Risiken berücksichtigt werden.
Eine quantitative Risikoanalyse ist im Rahmen dieser Arbeit nicht möglich, da diese nur in der Praxis angewendet werden kann. Daher werden zunächst potentielle Risiken aufgezeigt, unterteilt in technische (4.2 und 4.3) und organisatorische Gefahren (4.4).
Die beschriebenen Angriffsarten werden hinsichtlich ihres Aufwands und den nötigen Vorkenntnissen des Angreifers qualitativ bewertet und nach [Laßmann, 2002] wie folgt unterschieden:

- **Angriffsaufwand „gering“:** Es genügt bereits geringer Aufwand des Angreifers, ohne Vorkenntnisse, mit einfachen Mitteln und ohne größeren Zeitaufwand, das System zu täuschen.
- **Angriffsaufwand „mittel“:** Der Angreifer hat beschränkte Vorkenntnisse, d.h. alle allgemein zugänglichen Informationen und einige Stunden bis Tage als Zeitaufwand.
- **Angriffsaufwand „hoch“:** Der Angreifer verfügt über sehr gute Fachkenntnisse, d.h. auch Insider-Kenntnisse über das System und einige Wochen Zeitaufwand, Gelegenheiten und Betriebsmittel.

Abschließend wird die Benutzerakzeptanz der einzelnen Methoden beleuchtet (4.5), da ein biometrisches System, das vom Benutzer abgelehnt wird, nicht zur Erhöhung der Sicherheit beitragen kann. Es wird in diesem Fall häufig auf eine benutzerfreundlichere, aber potentiell unsichere Methode ausgewichen.

4.2 Täuschen der Sensoren

Dieser und der nächste Abschnitt befassen sich mit den technischen Risiken bei der Benutzung biometrischer Systeme. Ein biometrisches System besteht aus der Sensorhardware (z.B. ein Fingerabdrucksensor) und einem Trägersystem (beispielsweise ein Personalcomputer), auf dem die Zusatzsoftware installiert ist und eventuell biometrische Daten gespeichert werden.
In 4.2 werden direkte Angriffsmöglichkeiten auf den Sensor beschrieben, in 4.3. Angriffe auf das Trägersystem.

4.2.1 Fingerabdruckerkennung

a) Latenz-Reaktivierung (Angriffsaufwand „gering“)

Ein großes Problem bei Fingerabdrucksensoren sind Rückstände auf der Sensorfläche (Latenzabdrücke). Da diese größtenteils von autorisierten Personen stammen, kann sich ein Unbefugter mit ihrer Hilfe Zutritt verschaffen. Es reicht möglicherweise aus, diese Abdrücke durch Atemluft sichtbar zu machen, indem man mit beiden Händen eine Muschel über den Sensor bildet und reinpustet.
Eine andere Möglichkeit besteht darin, eine dünnwandige Plastiktüte gefüllt mit Wasser vorsichtig auf die Sensoroberfläche zu drücken. Dabei verteilt sich die Feuchtigkeit besser als bei der Atemluft-Methode. Diese Methoden funktionieren jedoch nur bei Systemen ohne Lebenderkennung.
Bei der folgenden Methode kann ein System trotz Lebenderkennung getäuscht werden: Die Latenzabdrücke werden mit Graphitpuder eingestäubt und mit Klebefolie fixiert. Dann braucht nur noch leichter Druck ausgeübt zu werden.

b) Ausnutzen der Toleranz (Angriffsaufwand „gering“)

Ein Fingerabdrucksystem trifft die Entscheidung, ob ein Benutzer autorisiert ist oder nicht anhand des Grades der Übereinstimmung und eines definierten Schwellwertes.
Je strenger diese Vorgaben sind, umso öfter werden autorisierte Benutzer zurückgewiesen (hohe False Rejection Rate). Daher wird immer ein Kompromiss zwischen Benutzerfreundlichkeit und Sicherheit geschlossen, d.h. das System wird toleranter konfiguriert. Möglicherweise kann ein Angreifer bei einem identifizierenden System mit einer Vielzahl an eingelernten Benutzern durchaus schon Erfolg haben, indem er den Sensor wie vorgeschrieben benutzt. Bei einem sehr tolerant konfigurierten System

reicht es oftmals schon aus, den gleichen Fingerabdrucktyp (Wirbel, Schleife, etc.) eines registrierten Benutzers zu verwenden, um Zugang zu erhalten.

c) Täuschen des Sensors mit Hilfe eines Fingerabdrucks auf Papier (Angriffsaufwand „mittel“)

Im Rahmen ihrer Projektarbeit haben drei Mitglieder der Biometric Authentication Research Group der Universität Hamburg am Fachbereich Informatik[3] im Februar 2002 beschlossen, die Betrugs-Sicherheit eines kommerziellen Fingerabdruck-Sensors zu überprüfen. Getestet wurde das Fingerprint-Sensor-Keyboard F-SCAN-K001US der Firma Keytronic (siehe Abb. 31).

Abb.31 : Keyboard F-SCAN-K001US von Keytronic

Der Sensor wurde zusammen mit der Software Biologon 3.0 der Firma Identix getestet. Dies war zum Testzeitpunkt die aktuelle Version. Es wurde die Standard-Installation auf einem Windows NT 4.0 – System mit Service Pack 6a verwendet. Biologon 3.0 bietet die Möglichkeit, mehrere Benutzerprofile anzulegen. Jeder Benutzer kann seinen Fingerabdruck zur Authentisierung einlernen (Enrollment), ein Passwort und der Benutzername wird zusätzlich gespeichert. Wenn ein Benutzer das System hochfährt, wird er aufgefordert, die Tastenkombination „STRG-ALT-ENTF“ zu drücken oder einen Finger auf den Sensor zu legen. Biologon prüft, ob der Fingerabdruck dem System bereits bekannt ist, ohne dass vorher ein Benutzername eingegeben werden muss (Identifikation).

[3] Willem Fröhling, Martin Johns, Christian Paulsen

Abb.32: Screenshot von Biologon 3.0

Testablauf

Die Tester haben zunächst ein Benutzerprofil erstellt. Mehrere Testdurchläufe haben gezeigt, dass das Einlernen erfolgreich war und dass das System ordnungsgemäß identifiziert. Nur der eingelernte Benutzer erhielt Zugriff auf das System, andere Teilnehmer wurden zurückgewiesen. Dann wurde getestet, wie der Sensor auf einen Abdruck reagiert, der mit Hilfe von Klebestreifen vom eingelernten Finger abgenommen wurde. Er wurde nicht akzeptiert, die graphische Schnittstelle von Biologon (siehe Abb.32) hat kein Bild des Abdrucks angezeigt. Auch beim Auflegen einer Fingerabdruckskizze kam das gleiche Ergebnis heraus. Da beim Auflegen eines echten Fingers (auch eines nicht eingelernten) stets ein Bild angezeigt wurde, war es offensichtlich, dass eine Lebenderkennung vorhanden ist. Durch Ausprobieren wurde schnell erkannt, welche Art der Lebenderkennung eingesetzt wird: Der Sensor ist ein so genannter kapazitiver Sensor, d.h. es muss ein Strom fließen, bevor überhaupt gescannt wird. Dabei bildet der Finger die eine und die Oberfläche des Sensors die andere Leiterplatte.
Mit etwas Speichel auf der Sensoroberfläche war es möglich, diesen Zustand zu simulieren und die Lebenderkennung zu täuschen: Biologon zeigte jetzt die „gefälschten“ Fingerabdrücke an. Allerdings war die Qualität der Abbildungen nicht ausreichend, so dass immer noch kein Zutritt gewährt wurde. Das einzige, was jetzt noch benötigt wurde, war ein qualitativ hochwertiger Fingerabdruck vom Finger des eingelernten Benutzers. Druckerschwärze eines Kopierers (Toner) lieferte das beste Resultat, so dass es tatsächlich gelang, unberechtigten Zugriff zu erhalten. Es war dazu nichts weiter nötig als Klebestreifen, Papier, Toner, etwas Speichel und ein Zeitaufwand von etwa einer halben Stunde. Die Überlistung des Systems klappte mehrmals hintereinander.

d) Täuschen von Fingerabdruck-Sensoren mit Gelatine und Gummi

Dem japanischen Mathematiker Tsutomu Matsumoto ist es gelungen, mit künstlich produzierten „Gummifingern“ und Gussformen, kommerzielle Fingerabdruck-Sensoren zu täuschen. Matsumotu lehrt an der Graduate School of Environment and Information Sciences der Yokohama National University in Japan. Getestet wurden sowohl optische als auch kapazitive Sensoren [Matsumoto, 2002].
Er beschreibt zwei Wege: Die Herstellung künstlicher Finger mit Hilfe lebender Finger und die Herstellung eines künstlichen Fingers aus latenten Abdrücken :

Herstellung eines künstlichen Fingers mit Hilfe eines lebenden Fingers (Angriffsaufwand „hoch“)

Matsumoto hat bei seinen Experimenten 35g Plastikmasse und 30g Gelatine verwendet. Das Plastik wird erhitzt und zu einer Kugel geformt. Dann wird ein Finger in das weiche Plastik gedrückt und ca. 10 Minuten gewartet, bis das Material abgekühlt ist. Jetzt ist die Gussform fertig. Die Gelatine wird mit 30 ml kochendes Wasser versetzt und vermischt. Die flüssige Gelatine-Mischung wird in die Gussform gefüllt, in den Kühlschrank gelegt und nach 10 Minuten kann der künstliche „Gummifinger“ entnommen werden. Abbildung 33 zeigt Bilder eines echten und des zugehörigen Gummifingers, aufgenommen mit einem Fingerabdrucksensor.

Abb.33: Aufnahme eines Fingers und des zugehörigen Gummifingers, erstellt mit einem kapazitiven Fingerabdrucksensor der Infineon Technologies AG

Ergebnisse

Die Matsumoto-Gruppe hat insgesamt 11 verschiedene Fingerprintsensoren getestet. Jedes Gerät wurde auf vier verschiedene Arten getestet (siehe Tabelle 2). Die Versuchspersonen waren fünf 20-40 Jahre alte Personen, jede Versuchsreihe wurde genau 100mal durchgeführt und die Anzahl der erfolgreichen 1:1-Verifikationen gezählt.

Experiment	Enrollment	Verification
Type 1	Live Finger	Live Finger
Type 2	Live Finger	Gummy Finger
Type 3	Gummy Finger	Live Finger
Type 4	Gummy Finger	Gummy Finger

Tabelle 2: Die vier Experimentarten

Die Schwellwerte der Erkennung, falls Einstellungen per Software möglich waren, wurden auf den höchsten Sicherheitswert gestellt.

Die Fingerabdrucksysteme verifizierten die mit lebenden Fingern erstellten Gummifinger zu 68-100 Prozent:

X-Achse : Die getesteten Sensoren A-K

Y-Achse : Anzahl der akzeptierten Abdrücke/100 Versuche

L: Live Finger **A**: Artificial (Gummy) Finger **Enrollment - Verification**

Abb.34 : Die Versuchsergebnisse nach [Matsumoto, 2002]

Herstellung eines künstlichen Fingers mit latenten Abdrücken (Angriffsaufwand „hoch“)

Matsumoto erläutert in [Matsumoto, 2002] zusätzlich die Vorgehensweise, wie man einen hinterlassenen Fingerabdruck (Latenzabdruck) einer registrierten Person verwenden kann, um das System zu täuschen. Zunächst wird der Fingerabdruck mit Methoden der Forensik verdeutlicht (beispielsweise mit Cyanoacrylat). Dieser Abdruck wird mit Hilfe eines digitalen Mikroskops aufgenommen und am Rechner mit einem Bildbearbeitungsprogramm qualitativ verbessert. Dieses Bild wird mit einem Tintenstrahldrucker ausgedruckt und dient als Maske, die auf eine Leiterplatte mit photosensitiver Oberfläche gelegt und mit UV-Licht bestrahlt wird. Das resultierende Fingerabdruckrelief wird dann mit flüssiger Gelatine übergossen und gekühlt. Nach 10 Minuten kann dann eine Gummi-Imitation des Abdrucks abgezogen werden:

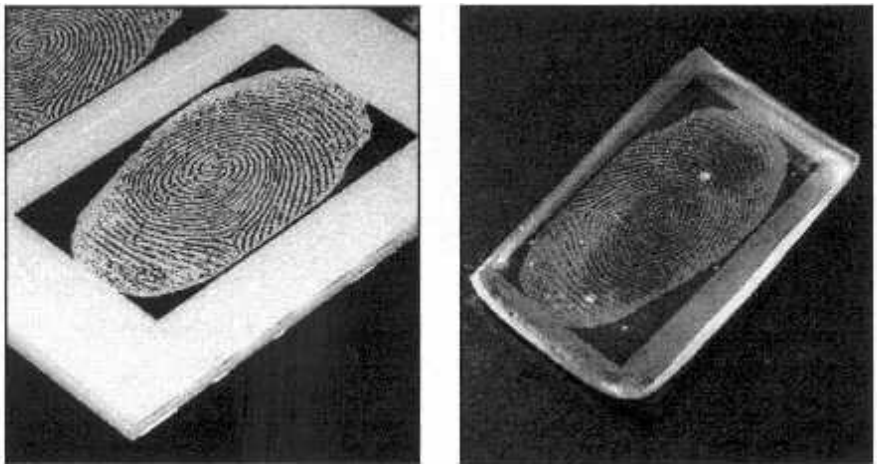


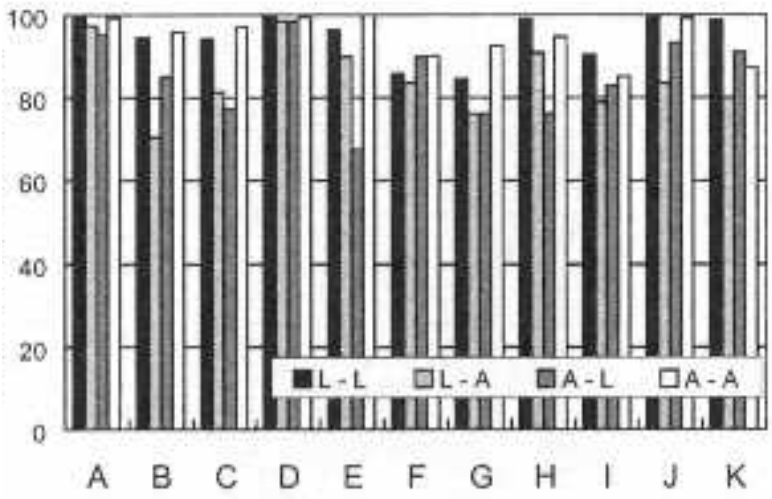
Abb.35: Aus einem hinterlassenen Fingerabdruck gewonnene Gussform und Gummifinger

Ergebnisse

Die mit latenten Fingerabdrücken erstellten Gummifinger wurden durchschnittlich zu 67 Prozent verifiziert. Zur besseren Lesbarkeit der Ergebnisse (Abb. 36) wird hier nochmals die Tabelle 2 aufgeführt:

Experiment	Enrollment	Verification
Type 1	Live Finger	Live Finger
Type 2	Live Finger	Gummy Finger
Type 3	Gummy Finger	Live Finger
Type 4	Gummy Finger	Gummy Finger

Tabelle 2: Die vier Experimentarten



X-Achse : Die getesteten Sensoren A-K

Y-Achse : Anzahl der akzeptierten Abdrücke/100 Versuche

L: Live Finger **A**: Artificial (Gummy) Finger **Enrollment - Verification**

Abb.36 : Die Versuchsergebnisse bei der Latenzabdruck-Methode [Matsumoto, 2002]

e) Amputationsangriff (Angriffsaufwand „hoch“)

Besonders skrupellose Angreifer könnten einem dem System bekannten Benutzer einen Finger amputieren und ihn auf die Sensorfläche drücken. In diesem Fall hängt das Ergebnis von der Lebenderkennung des Systems ab. Verfahren, die die Pulsoxymetrie messen, lassen sich in diesem Fall nicht täuschen. Kapazitive Sensoren können, wie bei c) erläutert, mit etwas Feuchtigkeit überwunden werden. Allerdings wird ein Angreifer diese Methode nur in Erwartung sehr wertvoller Ergebnisse anwenden. Diese wertvollen Ressourcen sollten daher auch auf anderem Wege gesichert sein, wie es in Abschnitt 4.4 („Organisatorische Risiken“) beschrieben wird.

4.2.2 Gesichtserkennung

a) Täuschen des Sensors mit Fotos (Angriffsaufwand „gering“ bis „mittel“)

Das Gesicht ist ein sogenanntes „offenes“ biometrisches Merkmal[4], das ohne großen Aufwand aufgenommen werden kann. Ein Foto eines eingelernten Benutzers, das vor die Kamera gehalten wird, kann möglicherweise ausreichend sein, ein Gesichtserkennungssystem ohne Lebenderkennung zu überwinden. Mehrere unterschiedliche Aufnahmen erhöhen die Chance des Angreifers auf eine erfolgreiche Täuschung. Wenn die Daten, die beim Enrollment gespeichert werden, nicht ausreichend gesichert werden (siehe auch 4.3.: Angriffe auf das Trägersystem) und als Rohdaten abgespeichert werden, können auch Fotos aus der Datenbank zur Überwindung verwendet werden. Die Gesichtserkennungssoftware „FaveVACS 2.1“ der Firma „Cognitec“[5] (siehe Abb.37) bietet keinen Schutz vor dieser Angriffsmethode.

Abb.37: FaceVACS Logon

b) Täuschen des Sensors mit Videoaufnahmen (Angriffsaufwand „mittel“)

Es ist, wie bei a) bereits erwähnt, prinzipiell jederzeit möglich, das biometrische Merkmal „Gesicht“ eines eingelernten Benutzers zu erfassen, auch mit einer Videokamera. Das muss nicht gezwungenermaßen heimlich geschehen. Ein freiwillig geführtes Gespräch bei laufender Kamera, beispielsweise im Rahmen einer Umfrage, kann einem Angreifer nützliche Aufnahmen liefern. Diese Aufnahmen können nun auf einem portablen Wiedergabegerät (z.B. ein Laptop) gespeichert werden und zur Täuschung des Systems

[4] [Lassmann, 2002 a)]: *Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren*, Seite 27
[5] Studienarbeit von Abdalla/ Abschinski: *Biometrische Authentikation: Verfahren und Methodenansätze unter W2K*

vor der Kamera abgespielt werden. Wenn die Lebenderkennung des Systems darin besteht, Bewegungen des Kopfes zu erfassen, kann diese Methode trotzdem erfolgreich sein. Eine statische Aufnahme (Foto) wäre in diesem Fall nicht ausreichend.

c) Täuschen des Sensors mit den registrierten Benutzern ähnlichen Personen (Angriffsaufwand „mittel“)

Bei dieser Methode muss ein Angreifer eine Person, die einem eingelernten Benutzer sehr ähnlich sieht, für seine Ziele gewinnen. Im Idealfall ist es ein Zwillingsbruder, bzw. eine Zwillingsschwester oder ein Verwandter mit großer Ähnlichkeit. In [Koleski, 2002] steht zum Thema eineiige Zwillinge: „Dies scheint bisher ein ungelöstes Problem zu sein, da sich die eineiigen Zwillinge im Gesicht normalerweise kaum bis gar nicht unterscheiden.“

d) Täuschen des Sensors mit Masken, Schminke und Perücken (Angriffsaufwand „hoch“)

Der Angreifer muss bei dieser Methode Fähigkeiten eines Maskenbildners, beispielsweise aus der Film- und Theaterbranche, und das zugehörige Material (Silikon, Gummi, Perücken, Schminke etc.) besitzen. Außerdem braucht er mindestens eine qualitativ hochwertige Aufnahme (Foto oder Videoaufnahme) eines registrierten Benutzers als Modellvorlage.
Die Person, die schließlich die Maske und Perücke beim Angriffsversuch trägt, sollte eine ähnliche Kopfgröße- und form wie der eingelernte Benutzer haben. Eine Lebenderkennung, die auf Bewegungen des Kopfes basiert, stellt bei dieser Angriffsmethode kein großes Hindernis dar.

e) Amputationsangriff (Angriffsaufwand „hoch“)

Bei der Gesichtserkennung ist diese Angriffsart relativ unwahrscheinlich und sehr makaber: Besonders skrupellose Angreifer könnten einem dem System bekannten Benutzer den Kopf abtrennen und vor die Kamera halten. Die „Erfolgsaussichten“ sind bei dieser Methode allerdings nicht besser als bei einer Videoaufnahme, eher sogar schlechter, weil einem abgetrennten Kopf die natürliche Mimik fehlt. Außerdem sollte die Systemumgebung diese Art von Angriff bereits verhindern, z.B. durch eine Person, die jene Anlage überwacht (siehe Abschnitt 4.4: „Organisatorische Risiken“).

4.2.3 Handgeometrieverfahren

a) Ausnutzen der Toleranz (Angriffsaufwand „gering“)

Ein Angreifer kann bei einem identifizierenden Handgeometriesensor bereits zufällig als registrierter Benutzer erkannt werden, obwohl er sich nie am System angemeldet hat. Das hängt zum Teil von der Anzahl der eingelernten Benutzer und von den eingestellten Toleranzwerten ab.

b) Zwillingsangriff (Angriffsaufwand „mittel“)

Die Handstrukturen von Zwillingen sind nicht identisch, aber in vielen Fällen sehr ähnlich. Ein Angreifer kann sich also bemühen, den Zwillingsbruder bzw. die Zwillingsschwester einer registrierten Person für seine Zwecke zu gewinnen und so den Handgeometriesensor zu täuschen. Die Wahrscheinlichkeit für das tatsächliche Eintreten dieses Angriffs ist allerdings sehr gering.

c) Verwenden von künstlichen Händen (Angriffsaufwand „hoch“)

Bei dieser Angriffsmethode muss ein Angreifer die Handstrukturen einer eingelernten Person (Länge, Dicke, Breite, etc.) kennen und nach diesen Daten eine künstliche Hand modellieren. Als Material kann Gummi oder Gips verwendet werden. Die größte Schwierigkeit besteht allerdings darin, unauffällig an die Handstrukturwerte zu kommen. Dabei können Fotos oder Videoaufnahmen der Person, bei denen die Hand aus mehreren Perspektiven aufgenommen wurden, ausreichend Informationen liefern, um eine geeignete Kunsthand zu entwerfen. Latente Handabdrücke auf dem Sensor können auch dazu verwendet werden, eine Kunsthand zu entwerfen.

d) Amputationsangriff (Angriffsaufwand „hoch“)

Das Abtrennen der Hand eines registrierten Benutzers ist eine grausame Methode, die nur bei entsprechenden Erfolgsaussichten und von skrupellosen Angreifern angewendet wird.

4.2.4 Iriserkennung

a) Täuschen des Sensors mit Fotos (Angriffsaufwand „gering“ bis „mittel“)
Wie bei der Gesichtserkennung kann auch bei der Iriserkennung ein qualitativ hochwertiges Foto eines Gesichts bzw. eines Auges ausreichend sein, ein System zu täuschen. Das setzt allerdings voraus, dass keine Lebenderkennung vorhanden ist. Einige Iriserkennungsalgorithmen können anhand der natürlichen Wölbung des Auges unterscheiden, ob ein Foto oder ein reales Auge vorliegt.

b) Täuschen des Sensors mit Videoaufnahmen (Angriffsaufwand „mittel“)
Videoaufnahmen eines registrierten Benutzers zu erstellen, ist normalerweise recht unproblematisch (siehe 4.2.2 b)). Wenn ein Angreifer dieses Video auf einem Laptop speichert und vor der Kamera eines Iriserkennungssystems abspielt, können selbst Systeme mit Lebenderkennung getäuscht werden, wenn es beispielsweise den Lidschlag oder andere Augenbewegungen misst. Bei Systemen, die die Reaktionen der Pupille auf unterschiedliche Lichtverhältnisse messen, wird diese Methode nicht erfolgreich sein. Außerdem fehlt auch hier, wie bei Angriffsmethode a), die natürliche Wölbung des Auges.

c) Täuschen des Sensors mit einem Glasauge (Angriffsaufwand „hoch“)
Theoretisch wäre es möglich, einen Angriff mit Hilfe eines Glasauges durchzuführen. Dazu ist allerdings eine genaue Kenntnis und Imitation des Irismusters eines registrierten Benutzers notwendig. Das Glasauge (mit natürlicher Wölbung) kann dann einfach vor die Kamera gehalten werden, wobei ein Lidschlag und eine Reaktion auf Helligkeitsveränderungen bei diesem Angriff ebenfalls nicht gegeben sind. Bei einem eingesetzten Glasauge ist zumindest der Lidschlag vorhanden, es setzt aber einen Angreifer mit fehlendem Auge voraus.

d) Täuschen des Sensors mit Kontaktlinsen (Angriffsaufwand „hoch“)
Diese Angriffsmethode kann nur dann funktionieren, wenn genaue Kenntnisse über das Irismuster einer registrierten Person und künstlerische und technische Fähigkeiten, sowie das Material für das Gestalten von Kontaktlinsen vorhanden sind. Falls es gelingt, so eine Linse herzustellen, sind die Überwindungschancen relativ groß, weil die Lebenderkennung in diesem Fall kompromittiert wäre: Die Wölbung des Auges und der Lidschlag ist vorhanden, das Auge reagiert auf Helligkeitsveränderungen und ein System sollte, um benutzerfreundlich zu sein, Kontaktlinsen akzeptieren. Allerdings stellt sich für den

Angreifer die Frage, ob der hohe Aufwand dieser Methode zum Erreichen seiner Ziele gerechtfertigt ist.

e) Amputationsangriff (Angriffsaufwand „hoch“)

Besonders skrupellose Angreifer könnten einem dem System bekannten Benutzer ein Auge entfernen und vor die Kamera halten. Diese Methode hat allerdings kaum Aussicht auf Erfolg, weil sich die Linse nach dem Abtrennen des Sehnervs sofort maximal öffnet und sich das Auge nach der Amputation unnatürlich vergrößert. Eine funktionierende Lebenderkennung („Lidschlag“, „Pupillenbewegung“, „Augenbewegung“) kann auf diesem Wege sowieso nicht überwunden werden.

4.2.5 Sprechererkennung

a) Täuschen des Sensors durch Ausnutzen der Toleranz (Angriffsaufwand „niedrig“)

Wie bei allen biometrischen Verfahren, gibt es auch bei der Sprechererkennung eine gewisse Toleranzgrenze, die durch die Festlegung von Schwellwerten definiert wird. Dabei muss immer ein Kompromiss zwischen Systemsicherheit und Benutzerfreundlichkeit geschlossen werden. Es kann also durchaus möglich sein, dass die Stimme eines Angreifers der Stimme eines eingelernten Benutzers ausreichend ähnlich ist, um unter den vorgegebenen Systemeinstellungen unberechtigten Zugriff zu erhalten. Vor allem dann, wenn das System Veränderungen der Stimme „erlernen“ kann, ist es möglich, durch mehrere Trainingsrunden die eigene Stimme dem System bekannt zu machen.

b) Täuschen des Sensors mit Tonbandaufnahmen bei textunabhängigen Systemen (Angriffsaufwand „mittel“)

Bei der Sprechererkennung ist dies die naheliegendste Angriffsmethode. Man spielt dem System Tonbandaufnahmen eines registrierten Benutzers vor. Diese Aufnahmen können jederzeit heimlich gemacht (mit Hilfe versteckter Mikrofone, „Wanzen“ im Telefon, etc.) oder im Rahmen einer öffentlichen Befragung erschlichen werden. Je besser die Qualität der Aufnahme ist, desto höher ist die Wahrscheinlichkeit der Akzeptanz.

c) Täuschen des Sensors mit Tonbandaufnahmen bei textabhängigen Systemen (Angriffsaufwand „hoch“)

Wenn das Sprechererkennungssystem eine Kombination der Sprachmerkmale mit bestimmten Schlüsselwörtern unterstützt, wird es für den Angreifer komplizierter, das System zu täuschen. Dazu müssten Tonbandaufnahmen während eines Authentisierungsvorganges erstellt werden oder die Schlüsselwörter auf anderem Wege herausgefunden werden. Diese Kodewörter sind ähnlichen Angriffsmethoden wie herkömmliche Passwörter ausgesetzt und können durch unvorsichtiges Verhalten des Benutzers (z.B. durch Notizen, Weitergeben an andere Personen) herausgefunden werden. Wenn diese Wörter einem Angreifer bekannt sind, braucht er dann noch Tonbandaufnahmen, in denen sie vorkommen, oder er verwendet die Angriffsmethode a) in Kombination mit den bekannten Schlüsselwörtern.

4.3 Angriffe auf das Trägersystem

Das Trägersystem bildet nicht nur die Schnittstelle zwischen Benutzer und dem biometrischen System, sondern ist für die Weiterverarbeitung und Datenspeicherung der vom Sensor erfassten Daten zuständig. Daher ist es für die Sicherheit des gesamten Systems unverzichtbar, das Trägersystem ausreichend vor potenziellen Gefahren zu schützen. Die Art des Trägersystems hängt wiederum vom Anwendungskontext und den Umgebungsbedingungen ab:

- Fest eingebautes, gesichertes Spezialgerät (z.B. Geldautomat)
- Gesicherte Umgebung mit Zutrittskontrolle (z.B. Rechenzentrum)
- Büroumgebung mit Zutrittskontrolle
- Zugriffs- und Zugangskontrolle zu Rechnern und Ressourcen (z.B. Login am PC)

Die in diesem Abschnitt beschriebenen Angriffsmethoden beziehen sich hauptsächlich auf den letzten Punkt (Rechnerzugriff) und sind unabhängig von der Art der biometrischen Authentisierung.
In Abschnitt 4.4 („organisatorische Risiken“) werden auch Sicherheitsaspekte der ersten drei Punkte behandelt.

4.3.1 Malware (Angriffsaufwand „niedrig“ bis „mittel“)

Der Begriff „Malware“ bezeichnet allgemein bösartige Software, wobei die „Bösartigkeit“ eines Programms eine schwer messbare Größe ist und u.a. davon abhängt, welche Erwartungen ein Benutzer an ein Programm stellt. Man unterscheidet selbstreplizierende und nicht-selbstreplizierende, sowie sich in Netzen ausbreitende und einzelne Rechner befallende Malware. Abbildung 38 zeigt eine Übersicht der existierenden Malware-Arten. Es muss hierbei erwähnt werden, dass sich Viren und Trojaner durchaus auch über Computer-Netzwerke verbreiten können, aber diese Eigenschaft nicht charakteristisch ist. Im Gegensatz zu den Würmern benötigen Viren kein Netzwerk zur Verbreitung [Kittel/Ticak 2002].

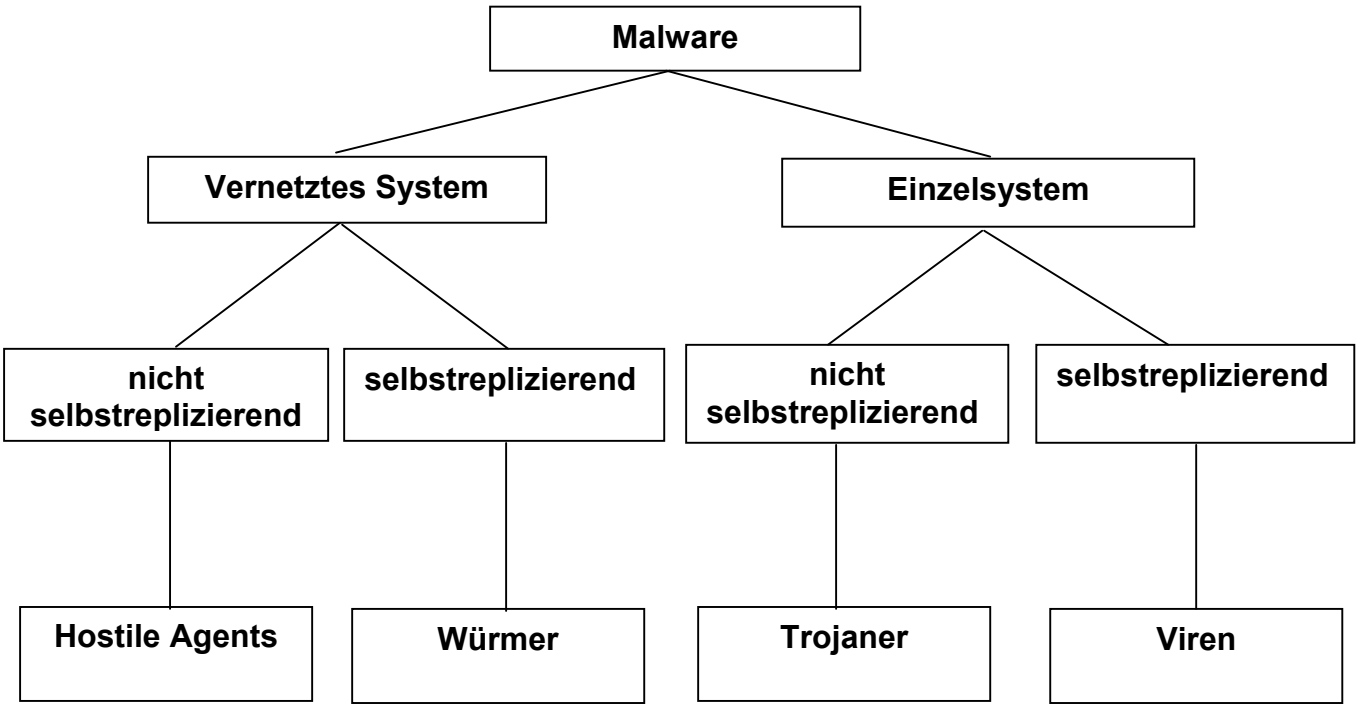


Abb.38: Übersicht Malware

Ein Angreifer kann Malware dazu verwenden, das Trägersystem auszuspionieren oder funktionsuntüchtig zu machen. Die in Abb.38 erwähnten Malware-Arten werden daher genauer erläutert:

a) Viren

Definition 15: Computervirus

Ein Computervirus ist ein in ein Wirtsprogramm eingebettetes oder mit einem Wirtsprogramm verbundenes, sich selbst reproduzierendes Computerprogramm bzw. Stück ausführbarer Programmcode.

Ein Virus besteht aus einem Installationsteil und einem Reproduktionsteil. Der Installationsteil sorgt für die Ausführung, der Reproduktionsteil enthält die Anweisungen zum Kopieren und damit zur Vermehrung des Virus. Einige Viren beinhalten zusätzlich einen Schadensteil („Payload“) (siehe 4.3.1.2), der verschiedene Auswirkungen haben kann. Meistens ist die Ausführung der Schadfunktion an eine Bedingung verknüpft, damit der Virus nicht sofort bemerkt wird und sich besser verbreiten kann. Es existieren verschiedene Grundtypen von Viren, u.A.:

- Systemviren (Bootviren): Diese Virenart benutzt als Wirt keine Anwendungsprogramme, sondern das System selbst. Sie werden somit beim Booten des Systems zur Ausführung gebracht.

- Dateiviren (Fileviren): Dateiviren infizieren ausführbare Programme.
- Makroviren: Einige moderne Anwendungsprogramme (z.B. Word™ oder Excel™ von Microsoft™) besitzen Dateiformate, die nicht nur Texte oder Daten enthalten, sondern auch ausführbaren Code, sogenannte Makros. Makroviren sind in einer entsprechenden Makro-Programmiersprache geschrieben und infizieren Dokumentdateien der entsprechenden Anwendung.

b) Trojanische Pferde (Trojaner)

Definition 16: Trojanische Pferde (Trojaner)

Als Trojaner bezeichnet man Programme, die neben einer vom Benutzer erwarteten und gewünschten Funktionalität noch weitere, verborgene und u.U. unerwünschte Funktionen enthalten. Sie sind nicht selbstreplizierend und können eigenständige Programme sein.

c) Würmer

Definition 17: Würmer

Würmer sind Programme, die sich ausbreiten, indem sie sich selbst über Netze kopieren. Sie befallen dabei das Netz als Gesamtheit und keine isolierten Rechner.
Sie sind dabei, anders als Viren, nicht an ein Wirtsprogramm gebunden und bewegen sich selbständig im Netz fort, indem sie in den Speicher eines Rechners eindringen, dort weitere Netzwerkadressen von anderen Computern ermitteln und Kopien ihrer selbst dorthin schicken. Die besondere Gefährlichkeit liegt in ihrer hohen Ausbreitungsgeschwindigkeit. So können sie sich, bevor sie bemerkt werden, bereits auf zahlreiche andere Rechner kopiert haben [Kittel/Ticak, 2002].

d) Hostile Agents

Hostile Agents („feindseligen Agenten“) sind eine vergleichsweise neue Art der Malware, die sich über das Internet verbreitet. Die Technik der Agents (Applets und Controls) soll das Design von Multi-Media-Web-Seiten ermöglichen. Es wurde dabei Wert auf die Übertragung geringer Datenmengen gelegt: Elemente wie Animationen oder Laufschriften werden nicht als komplette Bilder-Sequenzen übertragen werden, sondern durch die Applets lokal errechnet, teilweise unter Verwendung nachträglich übertragener, aktueller Daten. Die Applets enthalten also Instruktionen zum Aufbau der zu übertragenen Web-Seite. „Hostile“ wird ein Applet genannt, das Handlungen ausführt, die nicht im Sinne des Benutzers liegen oder das den Benutzer dazu bringt, diese auszuführen.

4.3.1.1 Übertragungswege

Malware kann auf allen Datenträgern (z.B. CDs, DVDs, Disketten oder Bänder) enthalten sein. Sogar mit Original-Software wurde bereits Malware und speziell Viren verbreitet. Der Hauptübertragungsweg ist heutzutage allerdings die E-Mail. Eine Übertragung kann ebenfalls über Netzwerke stattfinden. Dabei sind die verwendeten Übertragungsdienste, wie z. B. WWW, FTP, E-Mail, News usw., nur das Transportmedium.

4.3.1.2 Schadenspotential

Der Schaden (auch „Payload“ genannt) reicht von einfachen Bildschirmmeldungen bis zur Zerstörung aller Programme und Daten auf allen beschreibbaren Datenträgern. Einige Viren überschreiben das BIOS („Basic-Input-Output-System“), oder aktivieren BIOS-Passwörter, sofern es nicht mit einem entsprechenden Schreibschutz versehen ist. Einige Trojaner sind in der Lage, Passwörter auszuspähen oder in Texten nach interessanten Schlüsselwörtern zu suchen und diese Texte dann an eine vorgegebene Adresse zu senden. Auch die Fernsteuerung befallener Rechner ist möglich. Es gilt: Was sich programmieren und als Schadensfunktion nutzen lässt, wird früher oder später auch realisiert werden [Kittel/Ticak, 2002].

Deshalb muss allen Beteiligten vor der Verwendung biometrischer Systeme auf herkömmlichen PCs bewusst sein, dass Malware den sicheren und störungsfreien Betrieb empfindlich stören oder sogar vorübergehend beenden kann. In Kapitel 5 werden geeignete Gegenmaßnahmen beschrieben.

4.3.2 Netzwerkangriffe (Angriffsaufwand „mittel“ bis „hoch“)

Wenn ein Personalcomputer, der als biometrisches Trägersystem fungiert, Teil eines Netzwerkes ist, gibt es neben Malware noch weitere Risiken, die beachtet werden müssen. Insbesondere dann, wenn dieses Netzwerk einen Zugang zum Internet besitzt, bestehen für einen Angreifer eine Reihe von Möglichkeiten. Dieser Angreifer („man in the middle“) kann von einem entfernten Standort aus agieren und dabei weitgehend unbeobachtet bleiben. Angriffe über Netzwerke bleiben nach Schätzungen des Bundesamtes für Sicherheit in der Informationstechnik zu ca. 95 Prozent unerkannt. Manipulationen können außerdem zum Einbau von Hintertüren für spätere Angriffe verwendet werden.

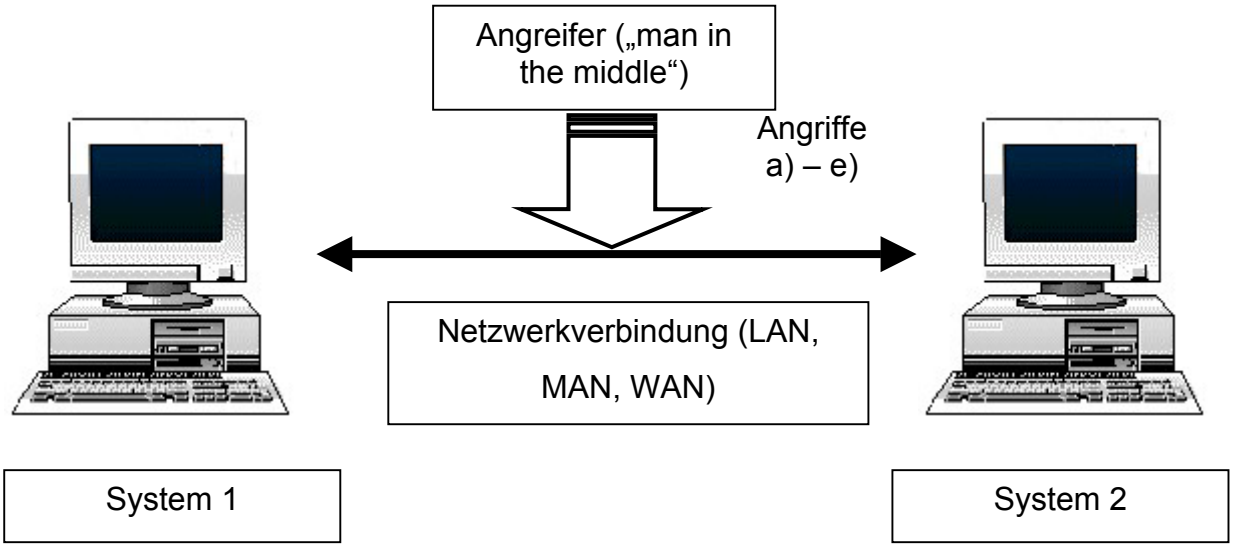


Abb.39: Schema Netzwerkverbindung mit Angreifer

Abb.39 zeigt schematisch eine Netzwerkverbindung zwischen zwei Rechnern. System 1 könnte beispielsweise einen Fingerabdrucksensor beinhalten, System 2 kann ein beliebiger Server sein, der z.B. biometrische Daten speichert. In [Winkelmann, 2000] werden die gängigsten Angriffsmethoden auf Netzwerkverbindungen wie folgt erläutert:

a) Sniffing

Als Sniffing wird das unberechtigte Abhören des Datenverkehrs anderer Netzteilnehmer bezeichnet. Der Angreifer fängt Datenpakete, die zwischen zwei Adressen versendet werden, gezielt oder ungezielt ab und analysiert dann den Datenverkehr mit dem Motiv, die dabei gewonnenen Informationen (z.B. Passwörter, Protokollarten und biometrische Daten) für seine Zwecke zu missbrauchen. Oft dient Sniffing als Vorbereitung für weitere Netzwerkangriffe unterschiedlicher Art.

b) Replay-Attacken und Masquerading

Das Wiedereinspielen von Daten, die zuvor durch Sniffing erworben wurden, nennt man Replay-Attacke. Das erneute Einspielen von abgefangenen (biometrischen) Anmeldesequenzen beispielsweise kann einem Angreifer unberechtigten Zugang zum System ermöglichen. Um bei diesen Angriffen nicht erkannt zu werden oder um sich als ein anderer Teilnehmer des Netzwerkes auszugeben, kann es für Angreifer nützlich sein, eine andere Identität vorzuspielen. Dieses unberechtigte Vorgeben einer fremden Identität wird als Masquerading bezeichnet. Das IP-Protokoll ermöglicht durch seine Spezifikation eine Form des Masquerading, das sogenannte IP-Spoofing: Unter IP-Spoofing wird das Fälschen der Senderadresse in einem IP-Paket verstanden.

c) Umleiten von Datenverkehr

Ein Angreifer kann gezielt Datenverkehr umleiten, um diesen abzuhören (Sniffing) oder zu manipulieren. Es ist auch möglich, nicht nur die Route des Datenverkehrs zu ändern, sondern auch zu verhindern, dass die Daten zum eigentlichen Zielsystem gelangen und stattdessen an eine Adresse gelangen, die sich für das Zielsystem ausgibt.

d) Denial-of-Service-Attacken

Bei DoS- und DDoS-Angriffen („Distributed Denial-of-Service“) verfolgt der Angreifer das Ziel, die Verfügbarkeit von Systemen oder einzelne Dienste dieser Systeme zu stören. Dazu wird gezielt die Auslastung der vorhandenen Systemressourcen herbeigeführt. Dies kann vor allem bei kommerziellen Dienstleistungsunternehmen zu hohen finanziellen Schäden und Unzufriedenheit bei den Kunden führen.

e) Hijacking

Hijacking ist eine Angriffsmethode, die das Ziel verfolgt, die Anmeldungsmechanismen am Zielsystem zu umgehen. Dazu beobachtet der Angreifer den Netzverkehr solange, bis er festgestellt hat, dass sich ein Dritter erfolgreich beim Opferrechner angemeldet hat. Er blockiert dann den Dritten, z.B. mittels einer DoS-Attacke, und übernimmt die bestehende Verbindung.

4.4 Organisatorische Risiken

In diesem Kapitel werden Risiken erläutert, die den einwandfreien und sicheren Betrieb eines biometrischen Systems gefährden, aber weder als Täuschung des Sensors, noch als Angriff auf das Trägersystem eingestuft werden können. Es sind vielmehr Gefährdungen, die durch eine gesicherte und organisatorisch durchdachte Arbeitsumgebung und Benutzerschulungen vermieden oder eingeschränkt werden können. Daher werden die einzelnen Risiken nicht wie bisher nach ihrem Aufwand für den Angreifer bewertet, sondern nach ihrer Eintrittswahrscheinlichkeit, bezogen auf eine durchschnittliche Betriebslaufzeit von fünf Jahren:

- **Eintrittswahrscheinlichkeit „gering“:** Dieses Ereignis tritt während der Betriebslaufzeit eines Systems höchstens einmal oder gar nicht ein.
- **Eintrittswahrscheinlichkeit „mittel“:** Dieses Ereignis tritt während der Betriebslaufzeit eines Systems schätzungsweise zwei- bis fünfmal ein.
- **Eintrittswahrscheinlichkeit „hoch“:** Dieses Ereignis tritt während der Betriebslaufzeit eines Systems öfter als fünfmal ein.

Diese Einteilung ist rein subjektiv und nicht berechenbar, genauso wie die Betriebslaufzeit eines Systems nicht vorhersehbar ist. Sie ermöglicht aber eine gewisse qualitative Einschätzung, wie groß die Gefährdung ist. Die Art und der Umfang der spezifischen Gegenmaßnahmen hängt neben der Eintrittswahrscheinlichkeit auch von den zu schützenden Werten ab (siehe Kapitel 5).
Die organisatorischen Risiken werden unterteilt in Risiken, bei denen die Benutzer des biometrischen Systems eine Rolle spielen und Umgebungsrisiken, bei denen die örtlichen Bedingungen entscheidend sind. Sie beziehen sich auch auf Anlagen, die im Freien betrieben werden (z.B. Geldautomaten).

4.4.1 Benutzerbezogene Risiken

a) Erpressung (Eintrittswahrscheinlichkeit „gering“ - „mittel“)

Ein Angreifer kann einen registrierten Benutzer eines biometrischen Systems unter Androhung von (Waffen-)Gewalt dazu zwingen, sich am System anzumelden und den Zugang dann für seine Zwecke missbrauchen. Diese Angriffsmethode funktioniert bei allen biometrischen Verfahren. Die Eintrittswahrscheinlichkeit bei Systemen, die in Gebäuden betrieben werden ist allerdings gering, weil es ein sehr riskanter Angriff ist und nur bei entsprechend hoher Motivation (z.B. hohe Geldsummen) und Skrupellosigkeit durchgeführt wird. Die Gefahr eines solchen Angriffs ist bei frei zugänglichen Geldautomaten größer.

b) Insiderangriffe (Eintrittswahrscheinlichkeit „mittel“)

Wenn sich ein registrierter Benutzer am System anmeldet, um die zu schützenden Werte (Geld, Daten, etc.) zu stehlen oder zu manipulieren und zu seinem eigenen Vorteil zu verwenden, dann spricht man von einem „Insiderangriff“. Diese Methode bietet viele Möglichkeiten, diese Angriffe zu verschleiern und z.B. einen imaginären Diebstahl von außerhalb vorzuschieben. Der Insider selber ist möglicherweise mit einer gewissen Geldsumme bestochen worden. Allerdings bezeichnet man bereits kleine beabsichtigte Manipulationen eines internen Benutzers, die eventuell aus Frust oder Rachegefühlen durchgeführt werden, als Insiderangriffe.

c) Fehlverhalten von Benutzern (Eintrittswahrscheinlichkeit „hoch“)

Ein System, das von Menschen erstellt, eingerichtet, administriert und benutzt wird, kann niemals fehlerfrei funktionieren. Es existiert daher ein ständiges Risiko, dass menschliches Versagen dazu führt, dass das biometrische System nicht im Sinne der Spezifikation oder der Benutzererwartungen funktioniert. Bei der Komplexität heutiger Systeme ist es für einen Menschen unmöglich, sämtliche elektrotechnischen und programmiertechnischen Aspekte zu durchschauen bzw. alle Eventualitäten bei der Herstellung und beim Gebrauch zu berücksichtigen.

4.4.2 Umgebungsrisiken

a) Diebstahl (Eintrittswahrscheinlichkeit „gering“)

Diese Gefahr geht nicht nur von gewöhnlichen Dieben aus, die Wertgegenstände aller Art erbeuten wollen, sondern auch von Angreifern, die gezielt das biometrische System stehlen, um es an einem anderen Ort ungestört umgehen zu können.

b) Vandalismus (Eintrittswahrscheinlichkeit: stark kontextabhängig)

Als Vandalismus bezeichnet man sinnlose und meistens nicht zielgerichtete Zerstörungswut, die an Gegenständen aller Art ausgelassen wird. Insbesondere öffentlich zugängliche Anlagen sind häufig Opfer von Vandalismus. Daher ist die Wahrscheinlichkeit relativ hoch, dass beispielsweise ein Geldautomat, der mittels eines biometrischen Verfahrens nutzungsberechtigte Personen authentisiert, Vandalismusschäden davonträgt. Die Auswirkungen von Vandalismus reichen von harmlosen Kratzern bis zum kompletten Systemausfall. Bei internen Anlagen, die durch Gebäude geschützt werden, ist Vandalismus eher selten.

c) Physikalische Risiken (Eintrittswahrscheinlichkeit „gering“)

Zu den physikalischen Risiken gehören Zerstörung, Systembeeinträchtigungen oder –ausfälle verursacht durch Feuer, Wasser, Blitzeinschlag, Explosionen oder Stromausfällen. Diesen Risiken kann durch geeignete Gegenmaßnahmen (z.B. Brandschutzmaßnahmen, Blitzableiter, Sicherungen, Notstromaggregate) effektiv (bis auf ein gewisses Restrisiko) entgegengewirkt werden.

d) Altersbedingte Defekte (Eintrittswahrscheinlichkeit „hoch“)

Alle hardwaretechnischen Elemente eines biometrischen Systems sind natürlichen Alterungs- und Abnutzungsprozessen ausgesetzt. Bei jedem System gibt es neben den Trägersystemen besondere funktionsrelevante Abnutzungspunkte, die oft ausgetauscht und gezielt gewartet werden müssen:

- Fingerabdrucksensoren: Sensoroberfläche, Beleuchtung
- Gesichtserkennung: Kamera
- Sprechererkennung: Mikrofon
- Iriserkennung: Kamera, Beleuchtung
- Handgeometrie: Sensoroberfläche
- Unterschriftenanalyse: Grafiktablett

4.5 Benutzerakzeptanz

Die Benutzerakzeptanz ist ein wesentlicher Faktor bei der Bewertung von biometrischen Authentisierungsmethoden. Neben der generellen Handhabung der Systeme spielen vor allem psychologische Faktoren eine Rolle. Da bei der biometrischen Erkennung körperliche Merkmale einer Person erfasst und verarbeitet werden, wird die biometrische Erfassung nach bisherigen Untersuchungen als intimer und persönlicher aufgefasst als z.B. die Eingabe eines Passwortes. Bisher durchgeführte Befragungen sind zumeist unter Personen durchgeführt worden, die sich freiwillig zur Verfügung gestellt haben. Dieser Personenkreis steht allerdings technischen Neuerungen allgemein positiver gegenüber. Daher besteht ein großer Bedarf an Studien mit Nichtfreiwilligen, da eine breite Einführung biometrischer Authentisierungsmethoden auch diese Benutzer betrifft [Laßmann, 2002 b)].

4.5.1 Erwartungen und Vorkenntnisse von Benutzern

Ein weitreichendes Basiswissen über Biometrik existiert heutzutage in der Bevölkerung (noch) nicht. Der überwiegende Anteil befragter Personen verbindet keinerlei Vorstellung mit dem Begriffen Biometrie/ Biometrik. Nach der erstmaligen Nutzung eines biometrischen Verfahrens äußerten sich die bisher befragten Nutzer grundsätzlich positiv. Sie würden gerne auf ihre PINs / Passwörter verzichten und sehen hier eine bequeme Alternative. Andererseits herrscht jedoch Skepsis vor, insbesondere im privaten Bereich ist bisher kaum jemand bereit, biometrische Verfahren einzusetzen [Laßmann, 2002 a)].
Es haben sich laut [Laßmann, 2002 b)] durch gezielte Befragungen folgende Benutzererwartungen herauskristallisiert:

- Eine deutliche Mehrheit erwartet durch biometrische Systeme zusätzliche Sicherheit
- Eine deutliche Mehrheit erwartet einen Komfortgewinn durch den Einsatz biometrischer Verfahren

Folgende Bedenken wurden geäußert:

- Eine Mehrheit hat Bedenken in bezug auf Datenschutz und Datenmissbrauch
- Eine Minderheit hat Bedenken bezüglich Gesundheitsgefährdungen und Hygiene
- Einer kleinen Minderheit ist die Benutzung biometrischer Systeme in der Öffentlichkeit peinlich (z.B. Stimme)
- Eine kleine Minderheit lehnt biometrische Verfahren grundsätzlich ab

Wenn bereits längere Zeit mit einer biometrischen Methode gearbeitet wurde, bekamen die Kriterien Bedienbarkeit, Geschwindigkeit und Zuverlässigkeit eine zentrale Rolle bei der Beurteilung der Nutzerakzeptanz zugesprochen. Die Systeme sollten daher

- eine einfache Benutzerführung besitzen
- kurze Reaktionszeiten haben
- möglichst kleine FRR- und FAR-Werte[6] haben [Laßmann, 2002 b)]

Die umfassende Aufklärung und Information über biometrische Authentisierungsverfahren sowohl hinsichtlich der Chancen als auch der Risiken sind entscheidende Akzeptanzfaktoren. Kurze, übersichtliche Informationsschriften und Informationsveranstaltungen erscheinen hierfür sinnvoll. Das konkrete Verfahren muss zudem ausführlich erläutert werden. Hierzu zählen Informationen über Ort und Umfang der Datenspeicherung und die Templateverwaltung, Maßnahmen zur Verhinderung von Missbrauch, Zugriffsrechte beim Betreiber, schriftliche Einwilligung in die Erhebung und Verarbeitung der biometrischen Datensätze, Einstellung der (individuellen) Toleranzschwelle und die erreichbare Sicherheit [Laßmann, 2002 a)].

4.5.2 Einlernphase

Die Qualität der ersten Aufnahmen in der Einlernphase (Enrollment) bildet die Grundlage für ein reibungsloses Authentisieren im Alltag. Deshalb sollte das Enrollment von geschultem und erfahrenem Personal, das die Qualität des aufgenommenen Templates hinreichend beurteilen kann, durchgeführt werden. Unmittelbar im Anschluss sollte ein erster Probelauf erfolgen, um die Qualität des erstellten Templates zu überprüfen und ggf. eine neue Erfassung vorzunehmen.
Aufgrund der allein schon aus Datenschutzsicht zu fordernden aktiven Kooperation des Nutzers ist eine genaue Einweisung in den Umgang mit dem Verfahren erforderlich. Dazu zählt auch die Handhabung des Endgeräts. Zusätzlich sollte eine schriftliche Kurzanleitung am Gerät mit den wichtigsten Verhaltensregeln sowie ein permanenter Ansprechpartner etwa über eine Telefon-Hotline bereitgestellt werden. Hilfreich sind z.B. auch FAQs („frequently asked questions“), anhand derer sich der Nutzer jederzeit aktuell informieren kann [Laßmann, 2002 a)].

4.5.3 Diskriminierungsfreier Einsatz

Unabhängig davon, welche biometrische Methode zur Authentisierung verwendet wird, gibt es immer Personen, denen das spezifische Merkmal komplett oder teilweise fehlt bzw. es nur eingeschränkt erfasst werden kann. Beispiele hierfür sind fehlende Gliedmaßen, Blindheit, Taubheit, Stummheit, aber auch Sehhilfen (Brillen, Kontaktlinsen) und Analphabetismus. Ein weiterer Aspekt in bezug auf einen nichtdiskriminierenden Einsatz und die Nutzerakzeptanz stellen die entstehenden Kosten für die Anschaffung, Inbetriebnahme, Betrieb und Wartung eines biometrischen Systems dar.
Aufgrund dieser Umstände ist dem Nutzer stets ein Ersatzverfahren anzubieten. Das ist auch deshalb notwendig, um neben der ungewollten auch die gewollte Nichtnutzung biometrischer Verfahren zu berücksichtigen: die Nutzung muss stets freiwillig erfolgen können. Allen Personen, die ein biometrisches Verfahren nicht nutzen möchten, sollten keine Nachteile entstehen. Neben der (parallelen) Beibehaltung des herkömmlichen Verfahrens kommt hier auch ein weiteres biometrisches Verfahren in Betracht, das mit einem anderen Merkmal arbeitet. Bei einem Systemausfall sollte generell ein Ersatzverfahren zur Identifikation zur Verfügung stehen [Laßmann, 2002 a)].

4.5.4 Akzeptanz der einzelnen Verfahren

Neben den bisher erwähnten allgemeinen Gesichtspunkten gibt es bei allen Verfahren spezielle Faktoren, die zu berücksichtigen sind. In diesem Abschnitt werden daher die bisher in Kapitel 4 behandelten Authentisierungsmethoden hinsichtlich der Benutzerakzeptanz untersucht. Dabei werden sowohl positive als auch negative Aspekte aufgezählt, die zu Zustimmung oder Ablehnung der Methoden durch den Benutzer beitragen können.

a) Fingerabdruckerkennung

Die grundsätzliche Methode, den Fingerabdruck zur Identifikation zu verwenden, existiert bereits seit über 100 Jahren (siehe 3.1). Daher sind die Berührungsängste gegenüber diesem Verfahren nicht so groß wie bei vergleichsweise neuen biometrischen Methoden. Allgemein ist die Fingerabdruckerkennung das am längsten erprobte Verfahren und wurde bisher am häufigsten praktisch angewendet.
Nachteilig für die Benutzerakzeptanz ist die Assoziation mit der forensischen

[6] False Rejection Rate (FRR), False Acceptance Rate (FAR), siehe 2.1.2

Fingerabdruckanalyse zur Verbrecheridentifikation[7]. Weiterhin existieren (außer bei berührungsfreien Sensoren) hygienische Bedenken hinsichtlich der vielfach benutzten Sensoroberfläche. Da die Hände bei einigen Menschen sehr stark beansprucht werden (z.B. bei Bauarbeitern) können diese Benutzer Probleme beim Authentisieren haben und das Verfahren ablehnen. Weitere Schwierigkeiten entstehen bei zu breiten Fingern (bzw. zu kleinen Sensorflächen), Verletzungen, Schmutz, Narben und fehlenden oder verstümmelten Fingern.

b) Gesichtserkennung

Die biometrische Gesichtserkennung ist ein berührungsloses und relativ bequemes Verfahren, bei dem der Benutzer lediglich in eine Kamera blicken muss, um sich zu authentisieren. Es ist ein natürliches Verfahren, da Menschen es gewohnt sind, andere Personen anhand ihres Aussehens zu identifizieren und selbst erkannt zu werden. Mittlerweile ist der Gebrauch von Überwachungskameras an vielen Orten der Welt zum Alltag geworden. Genau diese Tatsache ist aber auch eines der Nachteile bezüglich der Benutzerakzeptanz, da es teilweise als Einschränkung der persönlichen Freiheit empfunden wird, unter ständiger Beobachtung zu stehen. Es besteht die Möglichkeit, dass die Aufnahmen für andere Bereiche (Verfolgungen, Spionage, Veröffentlichungen) missbraucht werden. Viele der bisher entwickelten Gesichtserkennungssysteme haben noch Probleme mit unterschiedlichen Lichtverhältnissen und weisen höhere Fehlerkennungsraten auf als z.B. die Iriserkennung. Die Authentisierung kann auch durch Kopfbedeckungen, Brillen, veränderten Frisuren, Verletzungen, Narben und Stimmungsschwankungen beeinträchtigt sein und der Anwender unnötigerweise aufgehalten werden. Daher sollten regelmäßig Erneuerungen der Templatedateien durchgeführt werden.

Wie bereits in 4.2.2 erläutert, können die Systeme mit relativ geringem Aufwand (Masken, Schminken) getäuscht werden, bei eineiigen Zwillingen ist eine Unterscheidung nicht möglich. Das führt unter Umständen dazu, dass die Benutzer den Gesichtserkennungssystemen nicht vertrauen. Außerdem gibt es Menschen, die vor dem Blick in eine Kamera eine gewisse Scheu empfinden.

[7] Anmerkung: Fingerabdrücke werden vor Gericht nicht als Beweismittel anerkannt.

c) Iriserkennung

Die Iriserkennung gilt bisher als das genaueste und zuverlässigste Verfahren und eine Sensortäuschung ist vergleichsweise umständlich (siehe Abschnitt 4.2.3). Trotzdem ist die Benutzerakzeptanz bei diesem Verfahren eher als verhalten einzustufen, da häufig Augenschäden befürchtet werden [Petermann/ Sauter, 2002]. Die Iriserkennung ist für den Benutzer (bisher noch) umständlicher als z.B. die Gesichtserkennung, weil das Auge so positioniert werden muss, dass eine für den Vergleich qualitativ ausreichende Aufnahme gemacht werden kann. Brillen und Kontaktlinsen können den Vorgang erschweren. Es besteht zusätzlich die Möglichkeit, dass anhand der Aufnahmen des Auges Krankheiten (z.B. Gelbsucht) oder andere personenbezogene Informationen erkannt und missbraucht werden können. Auch hier muss beachtet werden, dass Personen, die ihre Augen nicht öffnen können oder keine Pupillen besitzen, durch den Einsatz der Iriserkennung nicht diskriminiert werden.

d) Sprechererkennung

Die Sprechererkennung ist ein berührungsloses Verfahren, das ebenso wie die Gesichtserkennung als ein natürliches Verfahren bezeichnet werden kann, da auch der Mensch dazu in der Lage ist, andere Personen anhand ihrer Stimmen zu identifizieren. Da dieses Verfahren z.B. durch geeignete Tonbandaufnahmen kompromittiert werden kann (siehe Abschnitt 4.2.4), ist das allgemeine Vertrauen der Benutzer bei der Sprechererkennung eher zurückhaltender: Es kommt bei den heutigen Systemen laut [Behrens/ Roth, 2001] relativ häufig zu sprecher – und wortspezifischen Ausreißern in der Erkennungsleistung und einer erhöhten False-Rejection-Rate. Weiterhin gibt es Probleme durch Hintergrundgeräusche in lärmerfüllten Umgebungen, die hohe Ansprüche an die Erkennungsalgorithmen stellen. Dabei darf allerdings die Toleranzgrenze nicht zu hoch eingestellt sein, um Einbruchsversuche effektiv abwehren zu können. Häufig wird die Sammlung umfangreicher Sprachproben in der Trainingsphase als lästig empfunden und die Benutzerakzeptanz negativ beeinflusst. Abgesehen davon, dass nicht jeder Mensch sprechen kann, muss bei dieser Methode verstärkt auf temporäre Veränderungen (Stimmbruch, Erkältungen, etc.) eingegangen werden.

5. Ergebnisse

In Kapitel 4 wurde zunächst der Analysebereich abgegrenzt (siehe 2.2.1 b1) und anschließend potentielle Risiken, die bei der Anwendung biometrischer Verfahren bestehen, erläutert (siehe 2.2.1 b2). In diesem Kapitel werden die bestehenden Risiken im Kontext von Beispielszenarien bewertet (siehe 2.2.1 b3), weil nur dann eine vernünftige Bewertung erfolgen kann. Dazu gehört auch die Beschreibung möglicher Gegenmaßnahmen. Die Ergebnisse werden in 5.3 noch einmal zusammenfassend dargestellt (siehe 2.2.1. b4).

5.1 Beispielszenarien

Es werden zunächst vier Beispielszenarien eingeführt, in denen jeweils Werte mit unterschiedlich großem Schutzbedarf existieren. Es sind bereits nicht-biometrische Sicherheitsbarrieren (z.B. Passwörter) vorhanden, die eventuell durch biometrische Methoden ersetzt (oder ergänzt) werden sollen. Deshalb werden Vorschläge gemacht, welche Methoden geeignet wären, auch hinsichtlich der Benutzerakzeptanz.
In 5.2 wird dann erläutert, welche Risiken aus Kapitel 4 für das jeweilige Szenario relevant sind und welche Gegenmaßnahmen ergriffen werden können. Es sollen dabei sowohl die technischen als auch die organisatorischen Risiken berücksichtigt werden.

5.1.1 Geringer Schutzbedarf: Privater Personal-Computer (Szenario A)

Persönliche Dokumente und Dateien, die auf einem privaten PC abgespeichert sind, haben vor allem einen ideellen Wert, den nur der Eigentümer selbst festlegen kann. Im Vergleich zu den Werten eines Unternehmens (z.B. Server und Kundendaten) ist der Schutzbedarf geringer, da der Verlust der Privatdateien selten zu größeren finanziellen Schäden oder Imageverlusten führt. Daher soll das folgende Szenario als Beispiel für einen Bereich mit geringem Schutzbedarf dienen:
Szenario A:
Herr Müller verwendet seinen privaten PC, der in seinem Arbeitszimmer steht, um dort persönliche Dokumente (z.B. Briefe und Abrechnungen) anzufertigen und zu speichern. Außerdem speichert Herr Müller digitale Fotos und surft gelegentlich im Internet.
Zum Schutz dieser Werte ist der Zugang zum Rechner passwortgeschützt.

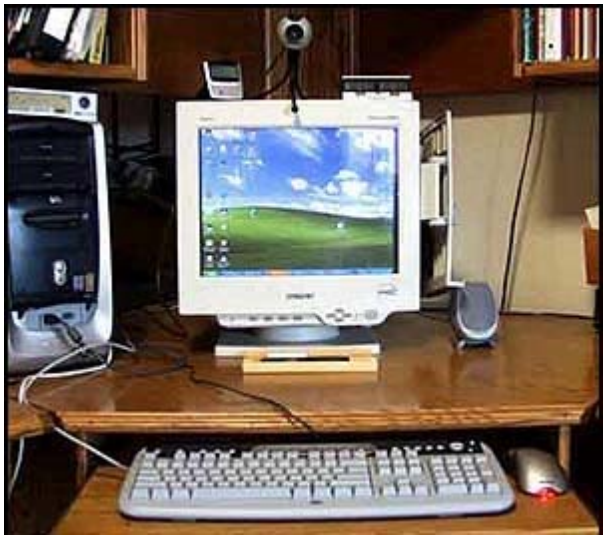


Abb.40: Privater PC

Herr Müller überlegt, ob er sich einen Fingerabdrucksensor zulegen soll, der eventuell in der Maus oder der Tastatur integriert ist. Auch die Gesichtserkennung (per Webcam) wäre für ihn eine denkbare Alternative.

5.1.2 Mittlerer Schutzbedarf, wenig Benutzer: Unternehmen (Szenario B)

Diese Kategorie repräsentiert die Wertebereiche, die ein höheres Maß an Schutzmaßnahmen erfordern, da das Eintreten eines Schadens finanzielle und personelle Konsequenzen bedeuten könnte. Dazu zählen z.B. Werte eines Unternehmens, dessen Existenz zu einem großen Teil vom reibungslosen und sicheren Betrieb einer informationstechnologischen Infrastruktur abhängt.
Die folgenden Szenarien B und C sollen für diesen Bereich als Beispiel dienen:

Szenario B:
Das Unternehmen „WebShopper“ vertreibt Waren aller Art über ein Internetportal. Der Firmensitz besteht aus einem Lager, Büroräumen und einem Serverraum, in dem mehrere Server (Webserver, Mailserver, Applikationsserver) betrieben werden. In einigen Büroräumen und im Lager stehen Rechner mit Zugang zu den Kundendaten und den aktuellen Bestellungen. Es bestehen bereits Standardschutzmaßnahmen für den IT-Bereich: Passwortgeschützte Rechnerzugänge, Firewalls und Antivirensoftware.
Folgende gebäudetechnische Schutzmaßnahmen sind vorhanden: Überwachungskameras, Alarmanlage, unterbrechungsfreie Stromversorgung, Feuerlöscher, Notausgänge, Rauchmelder und Blitzableiter.

Abb.41: Büroräume des Unternehmens „WebShopper“

Die Unternehmensleitung erwägt die Einführung biometrischer Methoden in einigen Bereichen:

- Die Zugänge zum Serverraum und zum Lager sollen durch ein Gesichtserkennungssystem, eventuell in Kombination mit einer Sprechererkennung geschützt werden
- Die Rechner in den Büroräumen sollen mit Fingerabdrucksensoren ausgestattet werden

5.1.3 Mittlerer Schutzbedarf, viele Benutzer: Geldautomaten (Szenario C)

Szenario C:
Eine städtische Bank hat ihren Kunden bei mehreren Filialen frei zugängliche Geldautomaten als Serviceleistung zur Verfügung gestellt. Die registrierten Kontoinhaber besitzen eine Kontokarte mit vierstelliger Geheimzahl, andere Kunden verwenden ihre EC-Karte um an diesen Automaten (gebührenpflichtig) Geld abzuheben.

Abb.42: Geldautomat

Der Vorstand der Bank möchte überprüfen, inwieweit die Einführung biometrischer Authentisierungsverfahren den Benutzerkomfort und die Sicherheit erhöht. Es kommt immer wieder vor, dass Kontoinhaber ihre Geheimzahl vergessen und diese teilweise auf der Karte notieren. Bei Verlust oder Diebstahl der Karten kann der finanzielle Schaden relativ hoch ausfallen. Da Geldautomaten öffentlich zugänglich sind und von vielen Benutzern aufgesucht werden, können keine maximalen Sicherheitsbarrieren aufgebaut werden. Es muss also ein geeigneter Kompromiss zwischen Benutzerkomfort und Sicherheit gefunden werden.

5.1.4 Hoher Schutzbedarf: Tresorraum einer Bank (Szenario D)

Im Hochsicherheitsbereich sind die vorhandenen Werte (Geld, Edelmetalle, geheime Daten, etc.) mit größtmöglichem Aufwand zu schützen, da potentielle Angreifer mit entsprechendem Aufwand versuchen werden, die Sicherheitsvorkehrungen zu umgehen. Beispielszenario D :

Der Tresorraum einer großen Zentralbank ist durch eine Panzertür abgeriegelt, die bei Eingabe eines korrekten sechsstelligen Codes geöffnet werden kann. Der Vorraum ist videoüberwacht. Der Zugang zum Vorraum wird von einem Sicherheitsbeamten beaufsichtigt, der den Schlüssel zur Tür besitzt. Das Gebäude selbst ist nur zu den Öffnungszeiten der Bank zugänglich, die Standardschutzmaßnahmen sind vorhanden: Überwachungskameras, Alarmanlage, unterbrechungsfreie Stromversorgung, Feuerlöscher, Notausgänge, Rauchmelder und Blitzableiter.

Abb.43: Tresor

Die Bank prüft die Einführung folgender biometrischer Verfahren:

- Der Sicherheitsbeamte soll durch ein Gesichtserkennungssystem ersetzt werden, um so den Zugang zum Vorraum zu schützen.
- Der Zugang zum Tresorraum soll durch eine Kombination eines Iriserkennungssystems mit einem Handgeometriesensor nur autorisierten Personen ermöglicht werden.

5.2 Risiken und Gegenmaßnahmen

Die im vorigen Abschnitt dargestellten Szenarien und die formulierten Fragestellungen sollen nun anhand der Erkenntnisse aus Kapitel 3 und den Risiken aus Kapitel 4 diskutiert werden: Welche Gefahren sind für das jeweilige Szenario relevant und welche Maßnahmen können ergriffen werden, um das Risiko zu minimieren? Letztendlich wird immer ein Restrisiko bestehen bleiben. Daher sollte ein Notfallplan existieren, damit im Schadensfall mit geeigneten Mitteln die Konsequenzen so klein wie möglich ausfallen.

5.2.1 Szenario A

5.2.1.1 Täuschen der Sensoren

a) Fingerabdruckmethode

Bei der Verwendung der Fingerabdruckmethode in diesem Szenario ist die Eintrittswahrscheinlichkeit der Angriffsmethoden, die einen mittleren bis hohen Angriffsaufwand erfordern, sehr gering. Daher werden die relevanten Risiken und Gegenmaßnahmen beschrieben (vgl. Kapitel 4.2.1):

- *Latenzreaktivierung*: Diese Art von Angriffen können durch regelmäßiges Säubern der Sensorfläche durch den Administrator vereitelt werden. In diesem Szenario ist bereits das Vorhandensein einer Lebenderkennung eine geeignete Gegenmaßnahme.

- *Ausnutzen der Toleranz:* Diese Methode sollte bei ausgereiften Sensoren mit guten FRR- und FAR- Werten nicht erfolgreich sein. Bei der Einstellung des Systems sollte darauf geachtet werden, die Erkennungsschwellwerte nicht zu tolerant einzustellen. Ein Restrisiko besteht allerdings bei allen Systemen.

b) Gesichtserkennung

Auch bei der Gesichtserkennung sind in diesem Szenario die Angriffsmethoden mit mittlerem und hohem Aufwand vernachlässigbar (vgl. 4.2.2):

- *Täuschen des Sensors mit Fotos:* Es sollte generell eine Lebenderkennung bei dem verwendeten Gesichtserkennungssystem vorhanden sein, so dass diese Methode nicht zu einem Angriffserfolg führen kann.

5.2.1.2 Angriffe auf das Trägersystem

Die Risiken bezüglich des Trägersystems (vgl. Kapitel 4.3) sind dagegen weitaus ernster zu nehmen. Da der Rechner von Herrn Müller Zugang zum Internet hat, sind alle aufgezählten Gefahren relevant. Es ist also empfehlenswert, dass Herr Müller ein Antivirenprogramm und eine Firewall installiert, um dieses Risiko zu minimieren. Wenn die Performanz des Rechners es zulässt, kann zusätzlich ein Intrusion-Detection-System eingerichtet werden, um Netzwerkattacken zu lokalisieren.

5.2.1.3 Organisatorische Risiken

In diesem Szenario ist es ausreichend, bei den organisatorischen Risiken die Gefahren mit einer hohen Eintrittswahrscheinlichkeit zu betrachten (vgl. 4.4):

- *Fehlverhalten von Benutzern:* Herr Müller sollte sich vor dem Gebrauch einer biometrischen Methode ausreichend informieren und beigefügte Informationen dringend lesen und den Anweisungen folgen. Das Restrisiko besteht aus Fehlern, die bei der Planung, der Herstellung oder beim Transport entstehen können.

- *Altersbedingte Defekte:* Defekte treten nach längerem Gebrauch der Systeme auf. Wichtig ist, dass die Komponenten des biometrischen Systems in regelmäßigen Abständen gepflegt, überprüft und ggf. gewartet werden

5.2.1.4 Benutzerakzeptanz

Beide Verfahren, die Herr Müller als mögliche Alternativen in Betracht zieht, haben eine relativ einfache Handhabung. Bei der Fingerabdruckmethode gibt es die Möglichkeit, den

Sensor in der Maus oder der Tastatur integriert zu erwerben. Wenn die Haut an den Fingerkuppen von Herrn Müller stark abgenutzt oder die Finger sehr dick sind, gibt es eventuell Probleme bei der Erkennung, ebenso bei Narben oder Verletzungen. Vorteilhaft ist die Tatsache, dass viele Geräte mit unterschiedlichen Eigenschaften auf dem Markt erhältlich sind. Bei der Gesichtserkennung könnte es Probleme bei kurzzeitigen Veränderungen (Bart, Brille, Verletzungen) oder unterschiedlichen Lichtverhältnissen geben. Positiv ist die Tatsache, dass eine vorhandene Webcam genutzt werden kann.

5.2.2 Szenario B

5.2.2.1 Täuschen der Sensoren

a) Fingerabdruckmethode

Die Fingerabdrucksensoren bei „WebShopper“ würden an den Einzelplatzrechnern in den Büroräumen zur Authentisierung der Mitarbeiter installiert werden. In dieser Umgebung sollten die Systeme leistungsfähiger sein als in Szenario A, da bei den dort vorhandenen Werten alle Angriffe mit niedrigem und mittlerem Aufwand relevant sind (vgl. 4.2.1):

- *Latenzreaktivierung*: Diese Art von Angriffen können durch regelmäßiges Säubern der Sensorfläche durch den Administrator vereitelt werden. In diesem Szenario sollte aber auch erwogen werden, berührungslose Sensoren zu verwenden.
- *Ausnutzen der Toleranz:* Diese Methoden sollten bei ausgereiften Systemen mit guten FRR- und FAR- Werten nicht erfolgreich sein. Bei der Einstellung des Systems sollte darauf geachtet werden, die Erkennungsschwellwerte nicht zu tolerant einzustellen. Ein Restrisiko besteht allerdings immer.
- *Täuschen des Sensors mit Hilfe eines Fingerabdrucks auf Papier:* Der Angriff, der in 4.2.1 beschrieben wird, bezieht sich auf ein Modell der Firma Keytronic™. Der Beweis, dass diese Methode auch bei anderen kapazitiven Sensoren funktioniert, steht noch aus. Trotzdem sollte in diesem Szenario eher ein nicht-kapazitiver Sensor mit einer ausgereifteren Lebenderkennung (eventuell berührungsfrei) verwendet werden.

b) Gesichtserkennung

Die Zugänge zum Serverraum und zum Lager werden bereits mittels Videokameras überwacht. Ein Gesichtserkennungssystem könnte also bereits vorhandene Ressourcen verwenden und nur den Administratoren Zutritt zum Serverraum gewähren. Relevant für diesen Bereich mit mittlerem Schutzbedarf sind die Angriffe mit niedrigem und mittlerem Aufwand (vgl. 4.2.2):

- *Täuschen des Sensors mit Fotos:* Es sollte generell eine Lebenderkennung bei dem verwendeten Gesichtserkennungssystem vorhanden sein, so dass diese Methode nicht zu einem Angriffserfolg führen kann.
- *Täuschen des Sensors mit Videoaufnahmen:* Diese Angriffsmethode kann durch organisatorische Maßnahmen verhindert oder zumindest eingeschränkt werden. Eine zweite Kamera könnte den Eingang zum Serverraum überwachen. Die Kombination der Gesichtserkennung z.B. mit einer textabhängigen Sprechererkennung macht es für einen Angreifer sehr umständlich, die Barriere zu überwinden. Der Aufwand wäre in diesem Szenario sehr hoch.
- *Täuschen des Sensors mit den registrierten Benutzern ähnlichen Personen:* Ein Angreifer muss in diesem Fall zumindest eine Person mit Zugangsberechtigung kennen und eine ihr ähnliche Person überzeugen, das System zu überwinden. Noch günstiger wäre es, einen Zwilling eines zugangsberechtigten Mitarbeiters zum Angriff zu verwenden, da in diesem Fall sogar eine Kombination mit der Sprechererkennung kein Hindernis wäre. Die Eintrittswahrscheinlichkeit dieser Konstellation ist allerdings ziemlich gering.

c) Sprechererkennung

Die Risiken dieses Verfahrens (siehe 4.2.4) haben gezeigt, das diese Methode noch nicht ausgereift ist. In diesem Beispielszenario ist eine Kombination mit der Gesichtserkennung trotzdem eine Möglichkeit, den Zugang zum Serverraum zu sichern. Folgende Gefahren bestehen:

- *Täuschen der Sprechererkennung durch Ausnutzen der Toleranz:* Sollte ein Angreifer probieren, die Toleranz des Systems auszunutzen, kommt es in diesem Fall auf die eingestellte Toleranzgrenze an, ob er zufällig erkannt wird. Die Kombination mit der Gesichtserkennung vereitelt diesen

Versuch allerdings.

- *Täuschen der textunabhängigen Sprechererkennung mit Hilfe von Tonbandaufnahmen:* Da es bei der textunabhängigen Methode nur auf den Klang der Stimme ankommt, stellt sie nur ein relativ kleines Hindernis dar. In diesem Szenario braucht dann lediglich eine Videoaufnahme mit Ton für den Angriff erzeugt werden und mit einem Laptop vor der Kamera und Mikrofon gestartet werden. Es sollte also in diesem Szenario von einer textunabhängigen Sprechererkennung abgesehen werden, weil sie keinen großen Sicherheitsgewinn darstellt.

5.2.2.2 Angriffe auf das Trägersystem

Die Einzelplatzrechner in den Büroräumen der Firma und die Server sollten durch Standardmaßnahmen zur Netzwerksicherheit (Firewall(s), Antivirensoftware, Intrusion-Detection-Systeme) vor Malware und Netzwerkangriffen geschützt werden (vgl. 4.3). Das biometrische System zur Überprüfung der Zugangsberechtigung zum Serverraum sollte nicht vernetzt sein und eine Antivirensoftware verwenden.

5.2.2.3 Organisatorische Risiken

In diesem Beispielszenario sind die organisatorischen Risiken mit mittlerer und hoher Eintrittswahrscheinlichkeit zu betrachten (vgl. 4.4):

- *Erpressung:* Ein Angreifer, der mit Waffengewalt einen oder mehrere Firmenmitarbeiter dazu zwingt, sich am System anzumelden, umgeht auf diesem Wege die biometrischen Schranken. Dieser Angriff kann erschwert werden, indem die Tür zu den Büroräumen nur angemeldeten Personen gestattet wird. Ein wirklich skrupelloser Angreifer lässt sich allerdings nur schwer aufhalten.
- *Insiderangriffe:* Diese Angriffsform ist sehr viel wahrscheinlicher als Erpressung, da es immer wieder vorkommt, dass interne Mitarbeiter das in sie gesetzte Vertrauen und ihre Kenntnisse missbrauchen. Dieses Risiko lässt sich dadurch minimieren, dass für eine zufriedene Belegschaft gesorgt wird. Eine Überwachung und Protokollierung der Authentisierungsvorgänge kann die Täter im Nachhinein überführen.

- *Fehlverhalten von Benutzern:* Fehler von Benutzern wird es immer geben, allerdings kann die Fehlerquote durch ausreichende Schulungen und Aufklärungen minimiert werden. Es sollte außerdem vermieden werden, dass die gegebenen Arbeitsbedingungen (erhöhter Stress beispielsweise) Fehler provozieren.
- *Altersbedingte Defekte:* Defekte treten nach längerem Gebrauch der Systeme auf. Wichtig ist, das die Komponenten des biometrischen Systems in regelmäßigen Abständen gepflegt, überprüft und ggf. gewartet werden.

5.2.2.4 Benutzerakzeptanz

Die Verfahren Fingerabdruckerkennung und Gesichtserkennung sind vergleichsweise benutzerfreundliche Verfahren (Finger auf den Sensor legen oder in die Kamera schauen genügt), die trotzdem im privaten Bereich selten angewendet werden, im Unternehmensbereich aber häufiger vorkommen. Es ist wichtig, dass die Mitarbeiter gut auf den Gebrauch dieser Anlagen vorbereitet und geschult werden und dass mögliche Probleme in den ersten Monaten angesprochen und berücksichtigt werden. Außerdem sollte es im Notfall immer die Möglichkeit geben, kurzfristig auf alternative Methoden umzusteigen.

5.2.3 Szenario C

Ein Geldautomat steht einer Vielzahl von Benutzern zur Verfügung und sollte daher schnell und komfortabel bedient werden können. Dem gegenüber steht der hohe Sicherheitsbedarf, der allerdings nur durch Maßnahmen, die den Benutzerkomfort maßvoll einschränken, gedeckt werden kann. Daher sollte die Bank bei der Wahl der(s) geeigneten biometrischen Verfahren(s) den Aspekt Benutzerakzeptanz ausführlich beleuchten. Aus diesem Grund wird dieser Abschnitt entgegen der bisherigen Reihenfolge als erstes behandelt.

5.2.3.1. Benutzerakzeptanz/ Wahl der geeigneten Verfahren

Aus Sicherheitsgründen sollte eine biometrische Methode die Verifikation über Besitz nicht ersetzen, sondern den Benutzern lediglich das Merken einer PIN-Nummer ersparen, da dies häufig als sehr lästig empfunden wird. Allerdings sollte die Umstellung freiwillig sein, damit niemand diskriminiert wird und immer eine Alternative (der Rückfall auf die Geheimzahl) verfügbar ist. Mit diesem Wissen wären viele Kunden eher dazu bereit, die neuen Verfahren zu testen und zu akzeptieren.
Am komfortabelsten hinsichtlich der Benutzung und Dauer der Gewöhnungsphase wäre die Gesichtserkennung, weil alle Automaten bereits Kameras besitzen, das Verfahren berührungslos ist und der Benutzer nicht außergewöhnlich aktiv sein muss. Es wäre ausreichend, die Chipkarte zu verwenden und dabei automatisch erfasst zu werden, eventuell aus mehreren Blickrichtungen. Nachteilig ist der Umstand, dass die Lichtverhältnisse störenden Einfluss haben könnten und die Benutzer regelmäßig neu eingelernt werden sollten, um Veränderungen zu berücksichtigen.
Die Sprechererkennung ist in diesem Szenario nicht empfehlenswert, da unter Umständen die Umgebungsgeräusche zu hohen Falschabweisungsraten (FRR) und häufigen Wiederholungsversuchen führen könnten.
Denkbar wäre es, auch hinsichtlich der Überwindungssicherheit, Iriserkennungsverfahren einzusetzen. Aufgrund der Benutzerakzeptanz ist die Iriserkennung jedoch (noch) nicht für die Benutzung am Geldautomaten empfehlenswert, da viele Menschen Augenschäden befürchten. Außerdem muss der Benutzer sein registriertes Auge so positionieren, dass eine geeignete Aufnahme gemacht werden kann. Retina-Verfahren sind in diesem Bereich ebenfalls zu aufwändig. Bei der Gesichtserkennung ist die Positionierung nicht ganz so umfangreich, wie bei der Iriserkennung.

Eine weitere Möglichkeit wäre die Fingerabdruckerkennung: Bei dieser Authentisierungsmethode kann die Assoziation mit der Verbrecheridentifikation zu einer geringen Nutzerakzeptanz führen.
Eine Ablehnung des Verfahrens kann auch aus hygienischen Gründen erfolgen, da die Sensoroberfläche von vielen Benutzern berührt wird. Diese Methode wird unter Umständen nicht als komfortabel empfunden, wenn die Sensoroberfläche zu klein ist oder mehrere Versuche nötig sind, aufgrund zu geringen Drucks, fettigen oder zu trockenen Fingerkuppen etc. Ähnliche Nachteile existieren bei Handgeometrieverfahren. Allerdings gibt es hier keine Assoziation mit einer Verbrecherfahndung und kaum Probleme mit der Größe der Sensorflächen. Geldautomten mit Handgeometriesensoren werden bereits getestet.
Allerdings ist aufgrund der Benutzerakzeptanz die Gesichtserkennung in Kombination mit Besitz einer Chipkarte die Authentisierungsmethode, die in diesem Szenario am ehesten in Frage kommt. Daher sollen die Risiken und Gegenmaßnahmen dieser Kombination im folgenden Abschnitt erläutert werden.

5.2.3.2 Täuschen der Sensoren

In diesem Szenario sind die Risiken mit niedrigem und mittlerem Aufwand zu berücksichtigen. Der maximale Ertrag (Geldbetrag), den ein Angreifer erbeuten könnte, ist durch die organisatorische Maßnahme eingeschränkt, dass pro Tag und Kontoinhaber nur ein begrenzter Geldbetrag (z.B. 500 Euro) abgehoben werden darf und der Angreifer die Chipkarte besitzen muss. Daher sind die Angriffsmethoden mit hohem Aufwand vernachlässigbar (vgl. 4.2.4):

- *Täuschen des Sensors mit Fotos:* Es sollte generell eine Lebenderkennung bei dem verwendeten Gesichtserkennungssystem vorhanden sein, so dass diese Methode nicht zu einem Angriffserfolg führen kann.
- *Täuschen des Sensors mit Videoaufnahmen:* Diese Angriffsmethode kann durch bereits bestehende organisatorische Maßnahmen verhindert oder eingeschränkt werden, z.B. durch die Kombination mit einer Chipkarte und Videoüberwachung. Bei Automaten, die im Freien stehen, ist die Möglichkeit, von Passanten beobachtet zu werden, ein abschreckender Aspekt.
- *Täuschen des Sensors mit den registrierten Benutzern ähnlichen Personen:* Ein Angreifer muss in diesem Fall zumindest eine Person mit

Zugangsberechtigung kennen und eine ihr ähnliche Person überzeugen, das System zu überwinden. Noch günstiger wäre es, einen Zwilling eines zugangsberechtigten Mitarbeiters zum Angriff zu verwenden. Dazu wäre allerdings noch der Besitz einer Chipkarte der betreffenden Person nötig. Die Eintrittswahrscheinlichkeit dieser Konstellation ist allerdings ziemlich gering.

5.2.3.3 Angriffe auf das Trägersystem

Da ein Geldautomat ein Gerät ist, das nicht von außerhalb (z.B. über das Internet) angreifbar ist, stellen Malware und Netzwerkangriffe in diesem Fall keine Risiken dar, die in diesem Szenario näher betrachtet werden müssen.

5.2.3.4 Organisatorische Risiken

In diesem Beispielszenario sind die organisatorischen Risiken mit mittlerer und hoher Eintrittswahrscheinlichkeit zu betrachten (vgl. 4.4):

- *Erpressung:* Ein Angreifer kann einen registrierten Bankkunden dazu zwingen, Geld abzuheben und ihn anschließend berauben. Ein Einsatz biometrischer Verfahren hat keinen Einfluss auf die Eintrittswahrscheinlichkeit dieser Attacke. Die Bank hat aber die Möglichkeit, das Risiko zu vermindern, in dem die Standorte der Automaten geschickt gewählt werden (keine unübersichtlichen oder dunklen Plätze, Videoüberwachung).
- *Insiderangriffe:* Mitarbeiter der Bank können das in sie gesetzte Vertrauen und ihre Kenntnisse missbrauchen und die biometrischen Daten entwenden. Dieses Risiko lässt sich dadurch minimieren, dass für eine zufriedene Belegschaft gesorgt wird und jeder Angestellter nur so viele Rechte bekommt, wie es für seine Tätigkeiten nötig ist („minimum privileges“). Eine Überwachung und Protokollierung der Zugriffe auf die sicherheitsrelevanten Daten kann im Nachhinein für Aufklärung sorgen und potentielle Täter abschrecken.
- *Fehlverhalten von Benutzern:* Der Gebrauch der Geldautomaten sollte so einfach wie möglich gestaltet und erklärt werden. Mögliches Fehlverhalten (z.B. Abstand zum Automaten, falsche Blickrichtung, etc.) sollte durch freundliche und gezielte Fehlermeldungen angezeigt werden. Die Konsequenzen eines Fehlverhaltens sollten abschätzbar und wie bei den heute verwendeten Systemen, möglichst geringfügig sein. Bei den heutigen Geldautomaten führt

das dreimalige Eingeben einer nicht korrekten PIN-Nummer zum Einzug der Chipkarte.

- *Vandalismus:* Die mutwillige Zerstörung von öffentlichen Anlagen jeglicher Art ist ein großes Problem. Dies geschieht häufig aus Frust (z.B. nachdem der Automat die Geldausgabe aufgrund eines überzogenen Kontos verweigert hat) oder aus Langeweile und Aggressivität. Das Design der Automaten sollte daher sowenig Angriffsfläche wie möglich bieten und der Standort gut sichtbar sein. Kameraüberwachung kann helfen, Täter zu überführen und abzuschrecken.
- *Altersbedingte Defekte:* Defekte treten nach längerem Gebrauch der Systeme auf. Wichtig ist, dass die Automaten in regelmäßigen Abständen gepflegt, überprüft und ggf. gewartet werden und den Benutzern sichtbare Meldemöglichkeiten (Filialen, Telefonnummern) von Defekten zur Verfügung gestellt werden.

5.2.4 Szenario D

Im Hochsicherheitsbereich sind alle aufgezählten Risiken relevant, weil ein Angreifer keine Kosten und Mühen scheuen wird, um an die geschützten Ressourcen zu gelangen. In diesem Beispielszenario geht es um den Inhalt des Tresorraums einer Bank. Der Vorraum soll durch ein Gesichtserkennungssystem geschützt werden, der Tresor durch Iriserkennung und Handgeometrie-Erkennung. Die Systeme sollten (und können) auf die maximale Sicherheitsstufe gestellt werden, da der Benutzerkomfort bei wenigen registrierten Personen nicht so relevant ist.

5.2.4.1 Täuschen der Sensoren

a) Gesichtserkennung

- *Täuschen des Sensors mit Fotos:* Es sollte generell eine Lebenderkennung bei dem verwendeten Gesichtserkennungssystem vorhanden sein, so dass diese Methode nicht zu einem Angriffserfolg führen kann.
- *Täuschen des Sensors mit Videoaufnahmen:* In diesem Szenario soll der Zugang zum Vorraum mit einem Gesichtserkennungssystem geschützt werden, das einen Sicherheitsbeamten ersetzen würde. Dieser Täuschungsversuch wird erst durch diese Ersetzung ermöglicht und kann nur durch verbesserte Erkennungsmethoden und Algorithmen vereitelt werden: Beispielsweise könnten mehrere Kameras ein dreidimensionales Bild einer Person aufnehmen und analysieren. Dadurch erhöht sich allerdings die Komplexität und Fehleranfälligkeit.
- *Täuschen des Sensors mit den registrierten Benutzern ähnlichen Personen:* Ein Angreifer muss in diesem Fall zumindest eine Person mit Zugangsberechtigung kennen und eine ihr ähnliche Person überzeugen, das System zu überwinden. Noch günstiger wäre es, einen Zwilling eines zugangsberechtigten Mitarbeiters zum Angriff zu verwenden. Die Eintrittswahrscheinlichkeit dieser Konstellation ist allerdings ziemlich gering.
- *Täuschen des Sensors mit Masken, Schminke und Perücken:* Heutzutage ist es durchaus möglich, realistische Masken zu gestalten, die so real wirken, dass das System und sogar ein Sicherheitsbeamter Probleme hätte, dies zu bemerken. Daher gibt es nur die Möglichkeit, den Zugang mit einer weiteren beliebigen Authentisierungsmethode zu sichern.

- *Amputationsangriff:* Amputationsangriffe, um ein Gesichtserkennungssystem zu täuschen sind höchst unwahrscheinlich und makaber. Trotzdem sollte diese Methode nicht völlig unbeachtet bleiben, da es immer wieder skrupellose Menschen gibt, die bei ausreichender Motivation auch vor dem Abtrennen eines Kopfes nicht zurückschrecken. In diesem Szenario sollte die Bank deshalb erwägen, den Sicherheitsbeamten nicht zu ersetzen, um einem potentiellen Angreifer eine weitere Hürde in den Weg zu stellen.

b) Iriserkennung

- *Täuschen des Sensors mit Fotos:* Das verwendete Iriserkennungssystem sollte grundsätzlich eine Lebenderkennung besitzen, um diese Angriffe zu verhindern.
- *Täuschen des Sensors mit Videoaufnahmen:* Im Hochsicherheitsbereich sollte das Iriserkennungssystem mit einer Lebenderkennung ausgestattet sein, die die Wölbung des Auges und die Reaktionen der Pupille auf unterschiedliche Lichtverhältnisse registrieren kann.
- *Täuschen des Sensors mit einem Glasauge:* Die Eintrittswahrscheinlichkeit dieser Angriffsmethode ist relativ gering. Sie kann durch eine Lebenderkennung, bei der das System die Pupillenreaktionen misst, verhindert werden.
- *Täuschen des Sensors mit Kontaktlinsen:* Diese Attacke ist sehr unwahrscheinlich, sollte aber in diesem Szenario trotzdem berücksichtigt werden. Das Iriserkennungssystem selbst kann den Angriff nur erschweren, in dem die Erkennungsgenauigkeit so hoch wie möglich gesetzt wird.
- *Amputationsangriff:* Ein Amputationsangriff kann nicht erfolgreich durchgeführt werden, weil sich die Pupille nach dem Durchtrennen des Sehnervs unnatürlich vergrößert.

c) Handgeometrie-Verfahren

- *Ausnutzen der Toleranz:* In diesem Szenario sollten nur wenige Mitarbeiter der Bank Zugang zum Tresorbereich haben und der Toleranzwert nicht zu niedrig eingestellt werden. Dieser Angriff kann daher kaum erfolgreich sein.
- *Zwillingsangriff:* Bei der geringen Anzahl zugangsberechtigter Personen ist es sehr unwahrscheinlich, dass einer von ihnen einen Zwilling hat, der zu

einer Täuschungsaktion bereit ist. Trotzdem besteht diese Möglichkeit und sollte daher berücksichtigt werden. Bei einer Kombination mit der Iriserkennung würde ein Zwilling ohne gezielte Täuschungsaktionen (siehe 5.2.4.1 b) nur den Handgeometrie-Sensor überwinden können.

- *Verwenden von künstlichen Händen:* Eine Lebenderkennung, z.B. das Messen der Pulsoxymetrie, kann Angriffe dieser Art abwehren. Auch hier erhöht sich die Überwindungssicherheit bei einer Kombination mit einer zusätzlichen Authentisierungsmethode. Zusätzlich kann der gesamte Tresorraum mit einer Kamera überwacht werden.
- *Amputationsangriff:* Eine Lebenderkennung und eine Kombination mit der Iriserkennung sind in diesem Fall geeignete Gegenmaßnahmen.

5.2.4.2 Angriffe auf das Trägersystem

Die Bank sollte bei der Planung und Installation der biometrischen Systeme darauf achten, dass sie möglichst nicht vernetzt werden und auf allen Trägersystemen eine Antivirensoftware mit aktuellen Signaturen verwendet wird. Alle Dateien, die der Systemverwalter aufspielt, sollten auf Viren überprüft werden. Es sollten höchstens zwei Systemadministratoren für die Instandhaltung der biometrischen Anlagen verantwortlich sein, um die Gefahr von Insiderangriffen (siehe 5.2.4.3) nicht unnötig zu erhöhen.

5.2.4.3 Organisatorische Risiken

In diesem Szenario müssen alle in 4.4 genannten Risiken berücksichtigt werden, da von ihnen die größte Gefahr ausgeht, insbesondere durch Erpressung und Insiderangriffe:

- *Erpressung:* Im Rahmen eines Überfalls können Mitarbeiter der Bank unter Androhung von Gewalt dazu gezwungen werden, die biometrischen Zugangsbarrieren zu öffnen. Bei dieser Angriffsart kann kein biometrisches System etwas ausrichten. Daher muss die Bank einen Notfallplan entwerfen und die Mitarbeiter durch Übungen auf diese Situationen vorbereitet werden. Eventuell gibt es die Möglichkeit, heimlich einen stummen Alarm auszulösen und so die Polizei zu benachrichtigen. Videoaufnahmen können bei der nachträglichen Fahndung hilfreich sein.

- *Insiderangriffe:* Diese Angriffe sind ebenfalls nicht durch biometrische Methoden zu verhindern. Das Risiko kann nur dadurch verringert werden, dass möglichst wenige und vertrauensvolle Mitarbeiter die Zugangsberechtigung zum Tresorraum erhalten. Die Einschätzung, wer dieses Vertrauen verdient hat, ist natürlich rein subjektiv. Wichtig ist auch, dass die Mitarbeiter zufrieden sind, um die Hemmschwelle bezüglich Insiderangriffe möglichst hoch zu halten, und Bestechungsversuche abgelehnt werden. Eine mögliche Gegenmaßnahme wäre, dass für das Betreten des Tresorraums zwei Mitarbeiter erfolgreich authentisiert werden müssen.
- *Fehlverhalten von Benutzern:* Die zugangsberechtigten Mitarbeiter müssen intensiv geschult werden und sich mit den Systemen vertraut machen. Es muss jeder Mitarbeiter genau wissen, was in Ausnahmesituationen (z.B. Systemabstürzen) gemäß eines Notfallplans zu tun ist.
- *Diebstahl und Vandalismus:* Die biometrischen Systeme sollten so eingerichtet werden, dass ein Diebstahl nur sehr schwer möglich ist. Wie bereits erwähnt, sollte die Bank erwägen, den Sicherheitsbeamten nicht durch den Einsatz der biometrischen Verfahren zu ersetzen, sondern lediglich ergänzen. So kann der gesamte Zutrittsvorgang vernünftig überwacht werden und Manipulationsversuche, Diebstahl und Vandalismus erschwert werden.
- *Physikalische Risiken:* Die Bank setzt in diesem Szenario bereits alle Gegenmaßnahmen ein, die dem Schutz vor Feuer, Wasser, Blitzen und Stromausfällen dienen.
- *Altersbedingte Defekte:* Defekte treten nach längerem Gebrauch der Systeme auf. Daher müssen sämtliche Komponenten der Zugangsicherung in regelmäßigen Abständen überprüft und ggf. erneuert werden.

5.2.4.4 Benutzerakzeptanz

Die Mitarbeiter der Bank, die Zutritt zum Tresorraum besitzen, sollten auf jeden Fall ein Mitspracherecht bei der Wahl der Zugangssicherungsmethoden haben. Dadurch ist die Bereitschaft, sich mit den Funktionsweisen zu beschäftigen (die Benutzerakzeptanz), größer. Im Rahmen der Schulungen sollte darauf hingewiesen werden, dass es im Hochsicherheitsbereich nicht möglich ist, die Schwellwerte tolerant zu konfigurieren und daher die Falschabweisungsraten steigen. In einer ausführlichen Testphase sollten die letzten Fragen weitestgehend geklärt werden.

5.3 Tabellarische Übersicht

Angriff	Aufwand	Relevanz in Szenario			
		A	B	C	D
Fingerabdruckerkennung					
Latenz-Reaktivierung	gering	X	X		
Ausnutzen der Toleranz	gering	X	X		
Papier-Abdruck	mittel		X		
Matsumoto-Methode	hoch				
Amputationsangriff	hoch				
Gesichtserkennung					
Foto-Methode	gering bis mittel		X	X	X
Video-Methode	mittel		X	X	X
Ähnliche Person	mittel		X	X	X
Maske, Schminke, Perücke	hoch				X
Amputationsangriff	hoch				X
Handgeometrie-Verfahren					
Ausnutzen der Toleranz	gering				X
Zwillingsangriff	mittel				X
Künstliche Hände	hoch				X
Amputationsangriff	hoch				X

Angriff	Aufwand	Relevanz in Szenario			
		A	B	C	D
Iriserkennung					
Foto-Methode	gering bis mittel		X		X
Video-Methode	mittel		X		X
Glasauge	hoch				X
Kontaktlinsen	hoch				X
Amputationsangriff	hoch				X
Sprechererkennung					
Ausnutzen der Toleranz	niedrig		X		
Tonbandaufnahmen	mittel		X		
Tonbandaufn. (textabhängig)	hoch				
Angriffe auf das Trägersystem					
Malware	gering bis mittel	X	X		X
Netzwerkangriffe	mittel	X	X		

Tabelle 3: Täuschen des Sensors und Angriffe auf das Trägersystem

Risiko	Eintrittswahrscheinlichkeit	Relevanz in Szenario			
		A	B	C	D
Benutzerbezogene Risiken					
Erpressung	gering bis mittel		X	X	X
Insiderangriffe	mittel		X	X	X
Fehlverhalten v. Benutzern	hoch	X	X	X	X
Umgebungsrisiken					
Diebstahl	gering				X
Vandalismus	kontextabhängig			X	X
Physikalische Risiken	gering				X
Altersbedingte Defekte	hoch	X	X	X	X

Tabelle 4: Organisatorische Risiken

6. Zusammenfassung und Diskussion

6.1 Ethische und datenschutzrechtliche Aspekte

Biometrische Verfahren verwenden spezifische körperliche Merkmale, die bestimmten Personen zugeordnet werden und daher grundsätzlich als personenbezogene Daten bezeichnet werden. Damit unterliegen sie in aller Regel dem Schutz des informationellen Selbstbestimmungsrechts, das 1983 vom Bundesverfassungsgericht im sogenannten „Volkszählungsurteil“ aus dem verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrecht entwickelt wurde.
Das informationelle Selbstbestimmungsrecht beinhaltet für jeden Betroffenen die Befugnis, grundsätzlich selbst über Preisgabe und Verwendung persönlicher Daten zu bestimmen.[8] Daher muss vor einer flächendeckenden Verwendung biometrischer Systeme im staatlichen Bereich ein neues Gesetz unter der Beachtung des Verhältnismäßigkeitsgrundsatzes verabschiedet werden, im privaten Bereich gelten die entsprechenden Vorschriften des Bundesdatenschutzgesetzes über nicht-öffentliche Stellen. Das Bundesdatenschutzgesetz (BDSG) von 2001 sieht Datenvermeidung und Datensparsamkeit als allgemeine Grundsätze vor, die bei der Auswahl von Datenverarbeitungsanlagen berücksichtigt werden müssen. Bezüglich des Einsatzes biometrischer Systeme bedeutet dies, dass immer die datenschutzfreundlichste Methode gewählt werden muss, was eventuell auch die Wahl eines nicht-biometrischen Verfahrens bedeuten kann [Lassmann, 2002 a)]. Während der Einsatzphase eines biometrischen Systems müssen laut des TeleTrust-Dokuments „Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren“ folgende Aspekte besonders beachtet werden:

- Datenvermeidung - und Sparsamkeit:
  Paragraph 3 des BDSG schreibt vor, bei der Datenerfassung und -speicherung deren Erforderlichkeit genau zu beachten (d.h., sich sparsam zu verhalten). Wird von vornherein darauf verzichtet, Daten zu erheben und zu speichern, entstehen keine Datenbestände, die eventuell missbraucht werden könnten. Sollte dennoch eine Datenerhebung nötig sein, muss sich diese auf den angemessenen Umfang beschränken. Dies beinhaltet auch die Dauer der Datenspeicherung.

[8] Sie kann allerdings durch Gesetze in einigen Bereichen (z.B. im Gesundheitswesen, bei Wahlen und bei der Strafverfolgung) eingeschränkt werden.

- Keine heimliche Erhebung biometrischer Daten:

Es sollte grundsätzlich ausgeschlossen sein, dass biometrische Merkmale von Personen erfasst werden, ohne dass diese darüber in Kenntnis gesetzt wurden. Es sollte außerdem die Erlaubnis der betroffenen Nutzer sowohl in der Enrollment- als auch in der Vergleichsphase eingeholt werden, da ein aktives Mitwirken der Benutzer das gesamte Verfahren durchschaubarer macht und möglicherweise vorhandene Berührungsängste abbaut. Daher sollten solche Installationen abgelehnt werden, bei denen beim bloßen Passieren einer bestimmten Stelle, heimlich biometrische Daten erfasst werden. Das folgende Beispiel aus den USA ist ein Beweis dafür, dass diese Befürchtungen nicht aus der Luft gegriffen sind, auch wenn dort ein anderes Datenschutzgesetz gilt:
In Tampa, USA wurde beim SuperBowl-Finale 2001 ein Gesichtserkennungssystem verwendet. Dort wurden alle Besucher per Video erfasst und die Gesichter mit denen von gesuchten Straftätern verglichen. In diesem Fall sollte man neben den datenschutzrechtlichen Aspekten die folgende Frage diskutieren: Ist es überhaupt moralisch vertretbar, grundsätzlich alle Menschen ohne konkrete Hinweise zu verdächtigen, möglicherweise gegen das Gesetz verstoßen zu haben?

- Informationsgehalt biometrischer Daten:

Es sollten nur die Verfahren verwendet werden, bei denen sich aus den biometrischen Daten kein Informationsgehalt ergibt, der für den eigentlichen Zweck der Authentisierung unnötig ist. Rückschlüsse auf den Gesundheitszustand des betroffenen Nutzers sollten technisch nicht möglich sein oder zumindest nicht ausgewertet werden. Daher sollte auf die Speicherung von unbearbeiteten, biometrischen Rohdaten ganz verzichtet werden.

- Rückschließbarkeit auf die hinter den biometrischen Daten stehende Person:

Es sollte ausgeschlossen oder zumindest nur sehr schwer möglich sein, aus den biometrischen Identifikationsdaten die zugehörige natürliche Person zu ermitteln. Insbesondere Gesichtsbilder können auch manuell identifiziert werden und sollten daher nicht in Rohform gespeichert werden. Es könnte beispielsweise ein Verfahren verwendet werden, bei dem erst der Besitz einer Chipkarte den Vergleich mit verschlüsselten Referenzdaten ermöglicht.

- Dauerhaftigkeit der Bindung zwischen biometrischen Daten und Personen:

Bei biometrischen Datenbeständen muss bedacht werden, dass die Bindung zwischen den Daten und der Person in den meisten Fällen auf natürliche Weise gegeben ist und vor allem dauerhaft anhält. Dadurch besteht über einen langen Zeitraum eine Missbrauchsgefahr der Daten. Als Gegenmaßnahmen können Verfahren verwendet werden, die bei der Berechnung der Referenzdaten noch weitere, veränderbare Daten mit einbeziehen (z.B. Zufallszahlen).

- Ort der Speicherung der biometrischen Daten:

Grundsätzlich sollte von einer zentralen Datenhaltung abgesehen werden, da diese viele Gefahren für das informationelle Selbstbestimmungsrecht beinhaltet. Die biometrischen Daten sollten beim Nutzer (z.B. auf einer Chipkarte, einem Token oder einen anderen mobilen Speichereinheit) gespeichert werden, damit dieser die Kontrolle über seine Daten behält. Je mehr Daten zentral abgelegt werden und auf diese zumindest theoretisch zugegriffen werden kann, umso größer sind die Begehrlichkeiten, die bei Behörden und privaten Stellen entstehen könnten. Falls auf eine zentrale Speicherung der Referenzdaten auch nach sorgfältiger Abwägung nicht verzichtet werden kann, so müssen insbesondere die Zugriffsbefugnisse genau definiert sein.
Ein weiteres Problem besteht darin, dass zentrale Datenbestände üblicherweise ohne Wissen (und Zutun) des Benutzers ausgewertet werden können, was ebenso dessen Selbstbestimmungsrecht einschränkt [Lassmann, 2002 a)].

6.2 Zusammenfassung und Fazit

Im Grundlagenteil (Kapitel 2) dieser Diplomarbeit wurde zunächst in das Thema Biometrik anhand grundlegender Definitionen eingeführt. Außerdem wurde erläutert, welche Konzepte, Möglichkeiten und Grenzen für die Durchführung von Risikoanalysen existieren und wie sich quantitative und qualitative Verfahren unterscheiden.
Im dritten Kapitel wurden dann die gängigsten biometrischen Verfahren ausführlicher erläutert und die Probleme weniger verbreiteter Systeme, die noch in der Experimentierphase stecken, aufgezählt. Bei allen Verfahren wurde auf das Thema „Lebenderkennung“ eingegangen. Lebenderkennung ist, wie auch in den Folgekapiteln deutlich wurde, eine effektive Maßnahme, um viele Arten von Sensormanipulationen zu vereiteln. Leider wird sie bei der Konstruktion biometrischer Systeme noch zu selten oder nicht qualitativ ausreichend integriert.
Zu Beginn des vierten Kapitels wurde zunächst die Vorgehensweise für die dann folgende Risikoanalyse festgelegt. Dabei wurde deutlich, dass im Rahmen dieser Arbeit nur eine qualitative Bewertung der Schwachstellen möglich war, da eine konkrete Anwendungsumgebung nicht vorlag. Die Risiken wurden unterschieden in Sensorangriffe, Angriffe auf das Trägersystem und organisatorische Risiken. Insbesondere die Ergebnisse des Japaners Matsumoto bezüglich der Überwindungssicherheit von Fingerabdrucksensoren haben deutlich gemacht, dass noch viele Systemschwächen existieren, die vor einem flächendeckenden Einsatz der Biometrik weitestgehend behoben werden sollten. Weiterhin gibt es noch organisatorische Probleme, z.B. Erpressung oder Insiderangriffe, die durch die Einführung von biometrischen Verfahren nicht gelöst werden können, sondern weiterhin einkalkuliert werden müssen. Auch Malware, Netzwerkattacken und andere Sicherheitsprobleme, die durch die gestiegene Komplexität heutiger Systeme immer mehr in den Vordergrund getreten sind, können durch Biometrik kaum eingeschränkt werden. Genauso wichtig wie die Systemsicherheit ist die Benutzerakzeptanz: Erst wenn ein Verfahren von den Anwendern akzeptiert wird, erhöht es möglicherweise den Sicherheitslevel, während es bei Ablehnung zur Sicherheitslücke werden kann.
In Kapitel 5 wurden die zuvor aufgezählten Risiken im Rahmen von vier Beispielszenarien hinsichtlich ihrer Relevanz bewertet und Gegenmaßnahmen vorgeschlagen. Die Beispielszenarien unterscheiden sich hinsichtlich der Werte, die jeweils durch biometrische Verfahren geschützt werden sollen. Abschließend wurden die Ergebnisse in Tabellenform zusammengefasst.

Fazit und Ausblick:

Die Biometrik ist ein Fachgebiet der Informatik, in dem noch viel Forschungsbedarf besteht, sowohl auf technischer, rechtlicher, organisatorischer und sozialer Ebene. Besonders wichtig ist es, dass die Akzeptanz der Techniken und das Vertrauen in die Systeme verbessert wird. Dies kann nur durch geeignete Aufklärungsmaßnahmen und durch die Beurteilung biometrischer Produkte durch unabhängige Zertifizierungsstellen erfolgen.
Bevor eine dritte, unabhängige Partei einem System das Vertrauen in Form eines Zertifikates aussprechen kann, müssen die Richtlinien und Anforderungen klar definiert werden. Wichtig ist dabei die Unterscheidung in Systeme, die von einer großen Anzahl von Benutzern verwendet wird (z.B. Fingerabdrücke in Personalausweisen oder biometrische Authentisierung bei Geldautomaten) und sogenannten Anwendungsnischen (z.B. im Hochsicherheitsbereich). Die Richtlinien für Zertifikate sollten hinsichtlich Benutzerkomfort, Sicherheit und rechtlichen Aspekten den Anwendungsbereichen angepasst sein. Es müssen Testmethoden entwickelt werden, die stärker als bisher den Praxisbezug berücksichtigen, da viele Hersteller biometrischer Systeme ihre Produkte mit einer zu geringen Zahl von Probanden unter Laborbedingungen überprüfen. Eine Lebenderkennung sollte als Mindestvoraussetzung für den Erhalt eines Zertifikats gelten.

Zukünftige Arbeiten in diesem Bereich könnten sich beispielsweise mit dem praktischen Testen von biometrischen Produkten beschäftigen. Dazu sollte, wie bereits erwähnt, eine adäquate Testmethodik mit klar definierten Bewertungskriterien entwickelt werden.
Im Verlauf dieser Arbeit wurde auch deutlich, dass die einzelnen Verfahren ausreichend Entwicklungs- und Forschungspotential für weitere Arbeiten besitzen.

Anhang

A: Literaturverzeichnis

[Arnold, 2003]
Arnold, Claus:
Iriserkennung
Seminararbeit im Rahmen des Seminars „Biometrics“ am Fachbereich Informatik der Westfälischen Wilhelms-Universität Münster, 2003
http://wwwmath.uni-muenster.de/u/xjiang/lectures/WS02/Biometrics-Ausarbeitung-Iris.pdf

[Behrens/Roth, 2001]
Behrens, Michael/ Roth, Peter:
Biometrische Identifikation – Grundlagen, Verfahren, Perspektiven
Vieweg-Verlag Braunschweig/ Wiesbaden, 2001

[Biometric Authentication Research Group, 2002]
Biometrik in der Gesellschaft
Biometric Authentication Research Group, University of Hamburg
Januar 2002, http://agn-www.informatik.uni-hamburg.de/hct/biomtrie.pdf

[Brömme, 2001]
Brömme, Arslan:
Politik-gewollte Anwendungen der Biometrik: Fahndung, Ausweise, Terrorbekämpfung: Eine Diskussion unter Berücksichtigung des Datenschutzes,
Vorlesungsfolien, Universität Hamburg, November 2001,
http://agn-www.informatik.uni-hamburg.de/papers/pub2001.htm

[Brunelli/Poggio, 1993]
Brunelli, R./ Poggio, T.:
Face Recognition: Features versus Templates
IEEE Trans on Pattern Analysis and Machine Intellegence, 1993
http://hera.itc.it:3003/~brunelli/Papers/FR.ps.gz

[BSI, 2002]
IT-Grundschutzhandbuch 2002
hrsgg. vom BSI, 2002
http://www.bsi.de/gshb/deutsch/menue.htm

[Cyranek et al, 1994]
Günter Cyranek u. Kurt Bauknecht:
Sicherheitsrisiko Informationstechnik – Analysen, Empfehlungen, Maßnahmen in Staat und Wirtschaft,
Vieweg-Verlag 1994

[Daugman, 1994]
Daugman, John:
Biometric Personal Identification System Based on Iris Analysis
US Patent No.: 5.291.560, 1994

[Daugman, 1998]
Daugman, John:
How Iris Recognition Works
University of Cambridge CB2 3QG, UK, 1998

[DUAG, 2003]
Homepage der Deutschen Uvaitis Arbeitsgemeinschaft e.V. (DUAG e.V.):
Informationen zum Aufbau des Auges
http://212.80.228.147/duag.org/auge.asp?mid=0&uid=0&iid=53

[Duden 5, 1982]
Drosdowski/ Köster/Müller/Scholze-Stubenrecht (hrsg.):
Duden, Fremdwörterbuch, 4. Aufl., Mannheim, 1982

[Fellbaum, 2002]
Fellbaum, Klaus-Rüdiger:
Ausgewählte Gebiete der Sprachsignalverarbeitung
Online-Vorlesung an der BTU Cottbus, 2002
http://www.kt.tu-cottbus.de/teleteaching/vcbook/vcbook1.html

[Galton, 1892]
Galton, F.:
Fingerprints
Macmillan, London, 1892

[Henne, 2001]
Henne, Sebastian:
Grundlagen der Spracherkennung
Ausarbeitung an der Fachhochschule Wedel, 2001
http://www.fh-wedel.de/~si/seminare/ss01/Ausarbeitung/a.sprache/gdlgsprerk34.htm

[Hofmann, 2002]
Grundsätzliche Untersuchung von Bildverarbeitungsalgorithmen zur Gesichtererkennung
Diplomarbeit, Fachhochschule Regensburg, 2002
http://www.markus-hofmann.de/

[International Biometric Group, 2001]

- *„Biometric Market Report 2000-2005"*
  International Biometric Group
  http://www.biometricgroup.com/e/biometric_market_report.htm
- *„Biometric Technology Overview"*
  International Biometric Group
  http://www.biometricgroup.com/a_biometrics_42/biometric_technology_overview.asp
  (Registrierung erforderlich)

[Jain et al, 1999]
Jain, Halici, Hayashi, Lee und Tsutsui:
Intelligent Biometric Techniques in Fingerprint and Face Recognition
CRC Press, New York, 1999

[Kassovic, 1998]
Diplomarbeit
Kassovic, Marian:
Risikoanalyse des Homebanking-Standards HBCI, 1998

[Kittel/ Ticak, 2002]
Kittel, Martin/ Ticak, Mario:
Viren und Malware: Eine Einführung
Broschüre für die Hamburger Computertage, 2002
http://agn-www.informatik.uni-hamburg.de/hct/vtc.pdf

[Koleski, 2002]
Koleski, Aleksander:
Praktische Anwendbarkeit künstlicher neuronaler Netze für die Gesichtserkennung in der biometrischen Authentikation
Studienarbeit, Fachbereich Informatik an der Universität Hamburg, Dezember 2002

[Kronberg, 2002]
Kronberg, Marcel:
Implementierung einer Iris-Biometrik in ein „Client-Server-Authentisierungssystem“
Diplomarbeit, Fachbereich Informatik an der Universität Hamburg, 2002

[Laßmann, 2002 a)]
Laßmann, Gunter:
Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren
Kriterienkatalog von TeleTrust Deutschland e.V., 2002
http://www.teletrust.de/publikat.asp?id=40600

[Laßmann, 2002 b)]
Laßmann, Gunter:
Test und Erprobung der Alltagstauglichkeit von biometrischen Systemen
12. SIT-SmartCard-Workshop, Fraunhofer Institut, 2002
http://www.sit.fraunhofer.de/smartcard-ws/WS_02/Beitrag_Lassmann.pdf

[Lorenz, 1996]
Lorenz, Rolf J.:
Grundbegriffe der Biometrie
Gustav Fischer Verlag, Stuttgart/Jena/Lübeck/Ulm, 1996

[Maier, 2002]
Maier, Alexander:
Identifikation durch Handgeometrie
Ausarbeitung am Institut für Neuroinformatik, der Universität Ulm, 2002
http://www.informatik.uni-ulm.de/ni/Lehre/WS02/HS-Biometrische-Systeme/ausarbeitungen/Handgeometrie.pdf

[Matsumoto, 2002]
Matsumoto, Tsutomu:
Impact of Artificial "Gummy" Fingers on Fingerprint Systems
Yokohama National University, 2002
http://cryptome.org/gummy.htm

[Moghaddam/Pentland, 1997]
Moghaddam, B./ Pentland, A.:
Probalistic Visual Learning for Object Representation
IEEE Trans on Pattern Analysis an Machine Intelligence, 1997

[Moses, 1992]
Moses, Robin H.:
Risk Analysis and Management
In: Jackson, K.M./Hruska, J.:
Computer Security Reference Book, 1992

[Paulsen, 2002]
Paulsen, Christian:
Merkmalsanalyse von Fingerabdrücken zur biometrischen Authentikation im Windows-Logon
Studienarbeit, Fachbereich Informatik an der Universität Hamburg, August 2002

[Petermann/Sauter, 2002]
Petermann, Thomas/ Sauter, Arnold:
Biometrische Identifikationssysteme-Sachstandsbericht, Arbeitsbericht Nr.76
Büro für Technikfolgenabschätzung beim Deutschen Bundestag, 2002
http://www.tab.fzk.de/de/projekt/zusammenfassung/Ab-76.pdf

[Richards, 2001]
Edward P. Richards, J.D., M.P.H., Professor of Law, UMKC School of Law:
Phenotype VS Genotype: Why Identical Twins Have Different Fingerprints
http://www.forensic-evidence.com/site/ID_Twins.html

[Sirovich/Kirby, 1987]
Sirovich, L./ Kirby, M.:
Low-Dimensional Procedure for the Characterizations of human face
Journal of the Optical Society of America, 1987

[Stelzer, 1994]
Stelzer, Dirk:
Risikoanalyse – Konzepte, Methoden und Werkzeuge
Publiziert in: Kurt Bauknecht, Stephanie Teufel (Hrsg.): Sicherheit
in Informationssysteme. Proceedings der Fachtagung SIS '94. Universität Zürich-Irchel, Zürich 1994, S. 185-200
http://www.wirtschaft.tu-ilmenau.de/im/infothek/documents/Stelzer_Risikoanalyse_Konzepte_Methoden_Werkzeuge_1994.pdf

[Stelzer, 2002]
Stelzer, Dirk:
Risikoanalysen als Hilfsmittel
Publiziert in: Peter Roßbach, Hermann Locarek-Junge (Hrsg.): IT-Sicherheitsmanagement in Banken. Frankfurt am Main 2002, S. 37-54
http://www.wirtschaft.tu-ilmenau.de/deutsch/institute/wi/wi3/infothek/documents/Stelzer_Risikoanalysen_als_Hilfsmittel.pdf

[Voges, 2002]
Voges, Udo:
Definitionen von Begriffen im Kontext ‚Sicherheit (safety)'
Forschungszentrum Karlsruhe, Institut für Angewandte Informatik, 2002
http://www.m-lehrstuhl.de/veranstaltung/GI_WS_07_02/Voges.doc

[Wettig, 2002]
Wettig, Steffen:
Biometrie: Verfahren und ausgewählte Rechtsprobleme
Präsentation im Rahmen des Seminars „Biometrie" an der Universität Jena, 2002
http://www2.informatik.uni-jena.de/~wettig/sem_biometrie_ss_2002/biometrie_uni_jena-xl-Dateien/frame.htm

[Winkelmann, 2000]
Winkelmann, Tobias:
Systemsicherheit - Angriffspunkte eines Rechners
Ruhr-Universität Bochum, Lehrstuhl für Datenverarbeitung, 2000
http://www.etdv.ruhr-uni-bochum.de/dv/lehre/seminar/syssec-apr/syssec-apr.pdf

[Wiskott, 1997]
Wiskott, L. et al:
Face Recognition by Elastic Bunch Graph Matching
IEEE Trans on Pattern Analysis and Machine Intelligence

B: Abbildungs-und Tabellenverzeichnis