Studienarbeit:

„Merkmalsanalyse von Fingerabdrücken zur biometrischen Authentikation im Windows-Logon“

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

Autor:
Christian Paulsen

Matrikelnummer: 501 56 05
Lottestrasse 43
22529 Hamburg
E-mail: 7paulsen@informatik.uni-hamburg.de

Betreuer:
Dipl.-Inf. B.Sc. Arslan Brömme

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich AGN

6.8.2002

Inhaltsverzeichnis:

1. Einleitung

1.1. Vorwort

Ein grundsätzliches und schwerwiegendes Sicherheitsproblem der gesamten Computertechnologie ist der Einsatz von Passwörtern für die Kontrolle berechtigter Systemzugriffe. Passwörter stellen einen Kompromiss zwischen Zugangskontrolle und Benutzerfreundlichkeit dar und dienen scheinbar dem Schutz vor unberechtigten Zugriffen.
Aufgrund der leichten Übertragbarkeit von Passwörtern (Wissen) sind biometrische Verfahren auf Basis von Fingerabdrücken (Merkmal) ein Zugewinn an Personalisierung bei der Zugriffskontrolle und Benutzerkomfort. Durch den Einsatz moderner Elektronik ist die Identitätsprüfung per Fingerabdruck recht einfach geworden – und bietet eine Alternative zur Verwendung von Schlüsseln, Passwörtern, PINs oder Chipkarten (Token).
Im Rahmen des Biometrik-Projekts am Fachbereich Informatik der Universität Hamburg setzen sich Studierende der Informatik bereits seit dem Wintersemester 1999/2000 im Hauptstudium mit Konzepten und Techniken biometrischer Algorithmen und Authentikationsysteme auseinander. Hierbei wurden von Anfang an nicht nur die technische Machbarkeit von biometrischen (Überwachungs-/ Authentikations-) Systemen betrachtet, sondern auch kritisch die gesellschaftlichen Auswirkungen des Einsatzes biometrischer Systeme im Sinne des Datenschutzes und des generellen Schutzes der Privatsphäre diskutiert [Biometric Authentication Research Group, 2002 a].

Aufgrund der Aktualität und der Gefahren, die dieses Themengebiet mit sich trägt, ist es besonders wichtig, dass die verschiedenen Aspekte der Biometrik ausreichend untersucht und analysiert werden.

Diese Studienarbeit zum Thema Authentikation per Fingerabdruck soll dazu ihren Beitrag leisten.

1.2. Motivation

Ich bin seit 1998 bei einem Hamburger Verlag tätig und erstelle dort einen Newsletter zum Thema IT-Sicherheit. Diese Arbeit hat mein Interesse an dem Vertiefungsgebiet IT-Sicherheit geweckt und mein Nebenfach Medizin führte zur Entscheidung, sich genauer mit der Biometrik zu befassen. Zu dem Zeitpunkt, als ich der Biometrikgruppe beitrat, wurde gerade über Maßnahmen zur Terrorbekämpfung und besonders über die Integration von Fingerabdrücken in Personalausweisen diskutiert. Weiterhin gab es auf diesem Gebiet noch Forschungsbedarf, weil kein weiteres Mitglied der Gruppe diesen Bereich ausführlich behandelte.

1.3. Überblick

Diese Studienarbeit untersucht die biometrische Authentikation mittels Fingerabdrücken. Dafür werden die Vorgehensweisen zur Merkmalsanalyse und die Integration von Algorithmen für die Fingerabdruckanalyse und -erkennung in das Logon-System von Windows beschrieben.

Es existieren bereits mehrere Verfahren, die auch schon in der Praxis verwendet werden, doch um sie hinsichtlich ihrer Eignung und Effizienz bewerten und verbessern zu können, ist es wichtig, den Aufbau dieser Systeme genauer kennen zu lernen. So können auch mögliche Probleme bei der Authentikation per Fingerabdruck besser nachvollzogen werden.

Zum Einstieg in das Thema erläutere ich zunächst die Grundlagen (Kapitel 2). Dazu gehören Definitionen der Begriffe „Biometrik“ und „biometrische Authentikation“, sowie die Beschreibung, wie Fingerabdruckerkennung generell funktioniert. Dann gehe ich auf den schematischen Aufbau der Sicherheitsarchitektur von Windows und der Schnittstelle zur Netzwerk-Authentikation (Kerberos) ein, insbesondere auf die Struktur des Logon-Systems. (Kapitel 3)

Kapitel 4 beschreibt den Test eines fertigen, kommerziellen Fingerabdrucksensors von Keytronic und die Versuchsreihe eines japanischen Mathematikers, der mit Hilfe von künstlichen Fingern die Sicherheit mehrerer Fingerprint-Sensoren überprüft hat.

In Kapitel 5 wird ein Konzept zur Integration der Fingerabdruckerkennung in ein Test-Rahmenwerk vorgestellt. Die Hamburger Biometrikgruppe hat dieses Rahmenwerk entwickelt, um biometrische Verfahren gezielter testen zu können.

In Kapitel 6 diskutiere ich Risiken und Chancen der Fingerabdruckerkennung und der Biometrik allgemein.

Kapitel 7 fasst noch mal alle Ergebnisse zusammen und zeigt mit dem Ausblick auf, was über diese Studienarbeit hinaus untersucht werden kann und welche neuen Arbeitsansätze sich hieraus ergeben.

Mit dieser Studienarbeit beabsichtige ich, interessierte Leser über das Thema zu informieren und darüber hinaus zu weiteren Betrachtungen zu motivieren.

Christian Paulsen

2. Grundlagen der Fingerabdruckerkennung

2.1 Was ist „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 b]:

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 b]

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.

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 a].

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 b]

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 a].

Definition 6: Biometrische Authentikation

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 Authenti(fiz|s)ierung
3. Phase: Autorisation
4. Phase: Zugriff auf Systemressourcen

b) (im engeren Sinne):

• Phase 2 im Phasenmodell
• Biometrische Authenti(fiz|s)ierung [Brömme, 2001 b]

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 biometrische Authentikation per Fingerabdruck die am meisten verbreitete Technologie (siehe Abbildung 1).
Sie beruht auf der Einzigartigkeit von Fingerabdruckmustern.
Dabei wird zunächst ein Bild eines Fingerabdrucks aufgenommen, bestimmte Merkmale extrahiert und in einer Fingerabdruckschablone (Template) gespeichert.
Mit Hilfe dieser Daten können Personen identifiziert bzw. verifiziert werden [International Biometric Group, 2001].

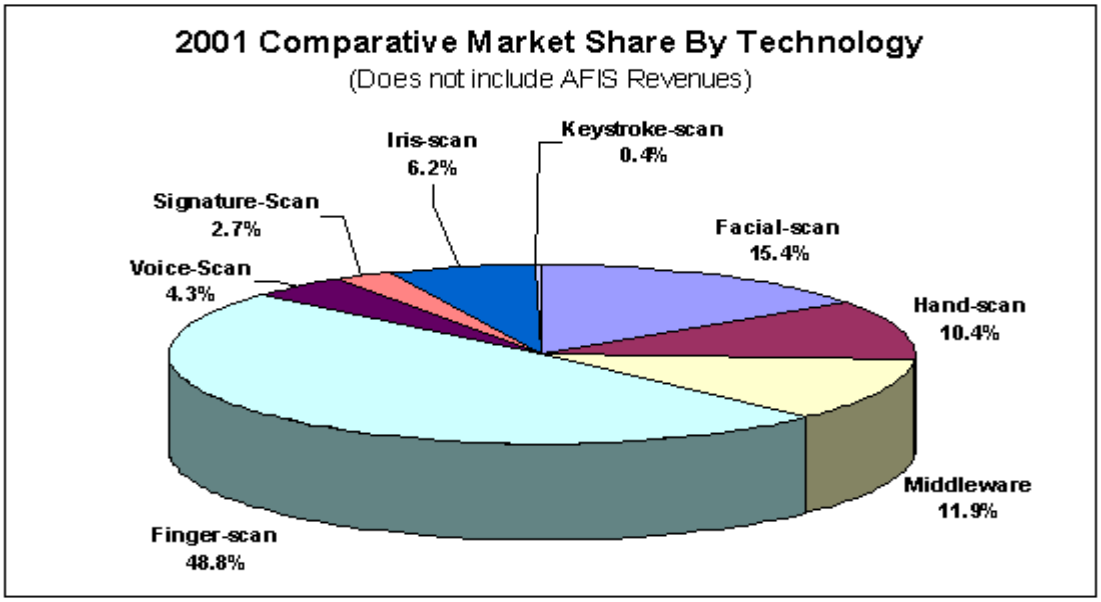


Abb.1 : Marktanteile verschiedener biometrischer Technologien in 2001

2.1.1 Vorteile und Nachteile biometrischer Verfahren gegenüber herkömmlichen Authentikationsverfahren

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 Authentikationsvorgang 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)

2.2 Fingerabdruckerkennung

2.2.1 Grundsätzlicher Unterschied zwischen klassischen Fingerabdrücken (Forensik) und Fingerabdruck-Scans (Biometrik)

Die Forensik bedient sich seit ca. 100 Jahren der Identifikation per Fingerabdruck. Die Abdrücke werden in großen Datenbanken gespeichert und weltweit zur Verbrechensbekämpfung eingesetzt. Dafür verwendet man mittlerweile so genannte *Live- Scans*, die die veraltete Tintenabdruck-Methode als Standard ablösten. Hochauflösende Bilder sind bis zu 250 KByte groß.

Bei Fingerabdruckscans werden zwar auch die Abdrücke aufgenommen, aber nicht das gesamte Bild gespeichert. Es werden nur spezifische Merkmale extrahiert, die in einem 250-1000 Byte großen Template (Signatur) gespeichert werden.
Der Prozess der Datenextraktion ist nicht umkehrbar, d.h. der Fingerabdruck kann nicht aus dem Template rekonstruiert werden [International Biometric Group, 2001].

2.2.2 Merkmale von Fingerabdrücken

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

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

Zwei Drittel aller Fingerabdrücke sind Schleifen (Typ 1 oder 2), ca. 25 % sind Wirbel (Typ 3). Die Bögen (Typ 4 und 5) kommen mit 5-10 % am wenigsten vor. [International Biometric Group, 2001]

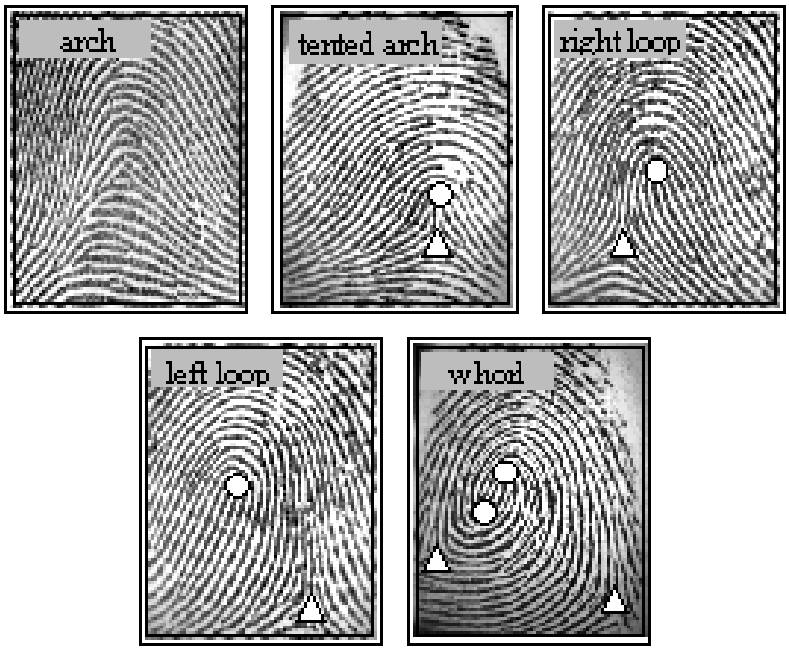


Abb.2: Die fünf Basistypen, Einteilung nach [Henry, 1900]. Kreise markieren Corepunkte, Dreiecke markieren Deltas

Neben Henry hat sich auch Sir Francis Galton Ende des 19.Jahrhunderts intensiv mit Fingerabdrücken beschäftigt und zwei Schlussfolgerungen formuliert, die die Grundlage für weitere Forschungsarbeiten auf diesem Gebiet gelegt haben [Galton, 1892] :

1. Fingerabdrücke sind permanent
2. Fingerabdrücke sind einzigartig

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)

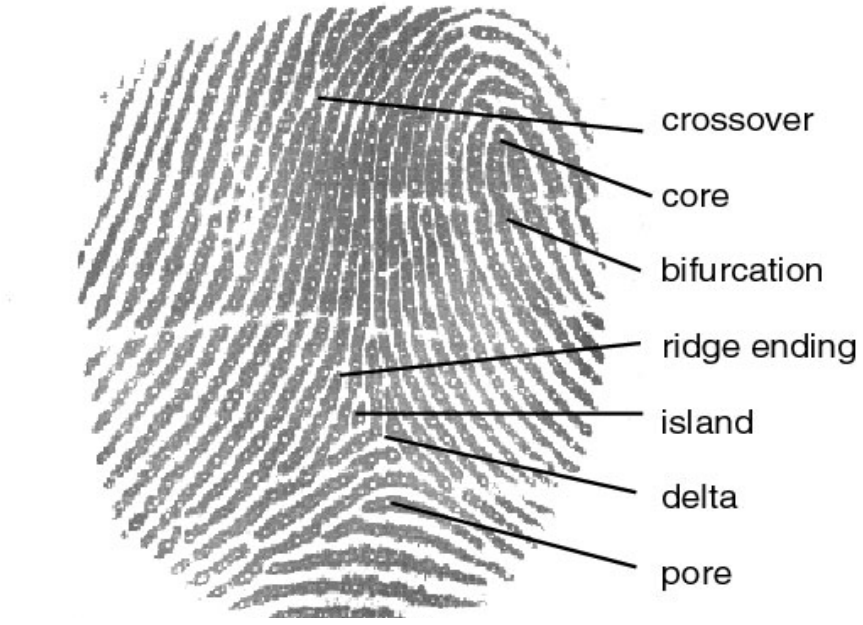


Abb.3: Ein Fingerabdruck mit einigen markierten Minutien

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.3).
Deltas nennt man die Punkte, an denen drei Serien von Erhebungen aneinander vorbeilaufen (vgl. Abb.3) [International Biometric Group, 2001]. Bei Fingerabdrücken vom Typ Bogen sind weder Cores noch Deltas vorhanden, bei Abdrücken vom Typ Wirbel gibt es zwei Cores und zwei Deltas (vgl. Abb.2).

2.2.3 Der Fingerabdruck – ein genotypisches oder phänotypisches Merkmal?

Während der Projektarbeit hat sich die Frage ergeben, ob der Fingerabdruck eines Menschen ein genotypisches oder ein phänotypisches Merkmal ist.

Definition Genotyp:
Die Gesamtheit der Erbfaktoren eines Lebewesens. [Duden 5, 1982]

Definition Phänotyp:
Das Erscheinungsbild eines Organismus, das durch Erbanlagen und Umwelteinflüsse geprägt wird. [Duden 5, 1982]

Edward P. Richards, Professor of Law an der UMKC School of Law, hat sich in [Richards, 2001] ausführlich mit diesem Thema beschäftigt und den folgenden Artikel verfasst:[1]

„*Phenotype vs Genotype: Why Identical Twins Have Different Fingerprints*" nach [Richards, 2001]
Im letzten Jahrzehnt konzentrierten sich die Forschungen im Gebiet der Forensik hauptsächlich auf die genetische Analyse. Vor Gericht werden immer häufiger die Ergebnisse von DNA-Tests verwendet, um Schuld oder Unschuld von Angeklagten zu beweisen. Sie ergänzen traditionelle Techniken wie die Fingerabdruckanalyse, die dazu verwendet werden kann, ein Schlüsselproblem der genetischen Analyse zu lösen: Die Unterscheidung eineiiger Zwillinge.
Eineiige Zwillinge haben ihren Ursprung, wie der Name schon sagt, in einer gemeinsamen Eizelle, aus der zwei Embryonen entstanden sind. Da beide

[1] Siehe auch [Cavanaugh, 2000]

Embryonen der gleichen Kombination von Eizelle und Spermium entspringen, haben sie identische Erbanlagen, abgesehen von den allgemein nicht messbaren Mikromutationen die sofort ab der ersten Zellteilung auftreten können. Mit einer Standard-DNA-Analyse ist kein Unterschied feststellbar. Trotzdem sind Eltern von identischen Zwillingen in der Lage, diese anhand geringer visueller Merkmale zu unterscheiden Auch die Fingerabdrücke sind ähnlich, aber nicht identisch. Fingerabdrücke und das physische Erscheinungsbild sind im allgemeinen Teil des Phänotyps eines Menschen. Der Phänotyp entsteht aus dem Zusammenspiel der Gene und der prägenden Einflüsse der Gebärmutter. Im Falle der Fingerabdrücke prägen die Gene die allgemeine Charakteristik des Musters, die bei der Einteilung nach Henry verwendet wird (siehe 2.2.2). Haut ist aber ein Oberflächengewebe und hat daher Kontakt zur Gebärmutterflüssigkeit. Außerdem berühren die Fingerspitzen weitere Teile des Fötus und der Gebärmutter und verändern ständig ihren Standort aufgrund eigener Bewegungen und die der Mutter.

Dies führt dazu, dass die nahe Umgebung der wachsenden Zellen an den Fingerspitzen ständig wechselt und leichte Unterschiede von Hand zu Hand und von Finger zu Finger aufweist. Es ist diese Mikroumgebung, die die feinen Details der Fingerabdrücke prägen. Obwohl die Unterschiede in der Mikroumgebung der einzelnen Finger eher klein sind, werden ihre Effekte durch die Zellteilung verstärkt und bilden so die makroskopischen Unterschiede, die es ermöglichen, Fingerabdrücke eineiiger Zwillinge zu unterscheiden.
Allgemein gesprochen hat die Umgebung in der Gebärmutter nicht nur Einfluss auf die Entwicklung der Fingerabdrücke, sondern auch auf die Entstehung des gesamten Phänotyps der eineiigen Zwillinge. Daher zeigt eine Untersuchung anderer Merkmale, dass Zwillinge trotz identischer DNA-Struktur unterscheidbar sind, auch wenn die Unterschiede auf dem ersten Blick nicht erkennbar sind. Der Prozess der unterschiedlichen Entwicklung setzt sich im Laufe des Lebens weiter fort, so dass ältere eineiige Zwillingspaare sehr viel einfacher auseinander gehalten werden können [Richards, 2001].

2.2.4 Methoden zur Bilderzeugung

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 sollten diese Einflüsse berücksichtigen.

Heutzutage sind drei grundlegende Verfahren zur Bilderzeugung in Gebrauch:

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

a) *Optische Verfahren*
Optische Verfahren sind die ältesten und am meisten verbreitet. Bei dieser Methode wird der Finger auf eine beschichtete Hartplastik-Sensor-Oberfläche gelegt. Eine CCD- Kamera (charged coupled device) nimmt ein Bild des Abdrucks auf. Dabei werden die Erhebungen dunkel und die Täler hell dargestellt. Unter Umständen muss die Helligkeit verändert werden, um ein für die Weiterverarbeitung ausreichendes Bild zu erfassen. Die Änderung der Helligkeit kann entweder automatisch oder manuell vorgenommen werden.
Optische Verfahren sind laut [International Biometric Group, 2001] 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.

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 das Zentrum (Core) bei einer Aufnahme nicht getroffen wird.

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, die von der Umgebung (Finger, Luft, Sensorfläche) unterschiedlich reflektiert werden. Diese Kontaktstreuung wird gemessen und zu einem Bild weiterverarbeitet, dass 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 a]

2.2.5 Minutienbasierte Merkmalsextraktion

Nachdem das Bild eines Fingerabdrucks erzeugt wurde (vgl. 2.2.4), müssen weitere Bearbeitungsschritte erfolgen, um eine Authentikation bzw. Identifikation zu ermöglichen.
Es besteht die Möglichkeit, das gesamte Rillenmuster zu kodieren und das resultierende Graustufen-Bild zum Vergleich zu verwenden. Diese Methode benötigt aber sehr viel Rechenkapazität und ist fehleranfällig.
Daher wurden andere Methoden, wie z.B. die minutienbasierte Merkmalsextraktion, entwickelt. Sie reduziert das Problem auf einen Vergleich von Punkten oder Graphen. Problematisch sind dabei folgende Umstände:

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

Ein anderer Ansatz sind Fingerabdruck-Vergleiche auf der Basis von Neuronalen Netzwerken, wie sie in [Baldi/Chauvin, 1993] beschrieben werden.

Die drei grundlegenden Schritte der minutienbasierten Merkmalsextraktion sind:

1. Bearbeitung/ Vorbereitung eines Fingerabdruckbildes
2. Extraktion/ Codierung der Minutien
3. Erstellen einer Liste oder eines Graphen (Template)

Das folgende Blockdiagramm (Abb.4) beschreibt die Vorgehensweise ausführlicher:

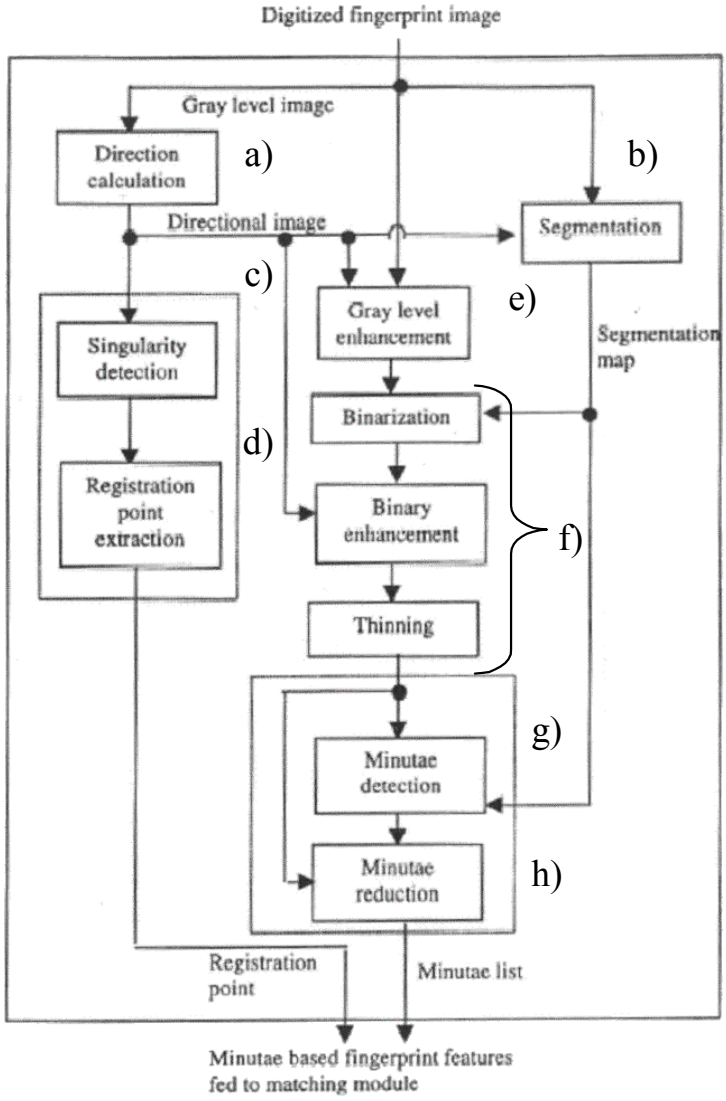


Abb.4: Blockdiagramm der minutienbasierten Merkmalsextraktion nach [Jain et al, 1999]

a) Richtungsberechnung (direction calculation)

Die Richtungsberechnung dient dazu, den grundsätzlichen Verlauf des Linienmusters eines Fingerabdrucks mit Hilfe einer Richtungskarte (direction map) darzustellen (siehe Abb.5). Die Richtungskarte ist eine aus mehreren Richtungsvektoren bestehende Matrix. Da es sehr viel Rechenkapazität kostet, die Richtungsberechnung pixelweise durchzuführen, wird nur die durchschnittliche Orientierung in gleich großen quadratischen Blöcken berechnet.
Die resultierende Richtungskarte ist eine Darstellung des Abdrucks mit niedriger Auflösung. Sie wird während der gesamten Bildbearbeitung häufiger verwendet [Jain et al, 1999].

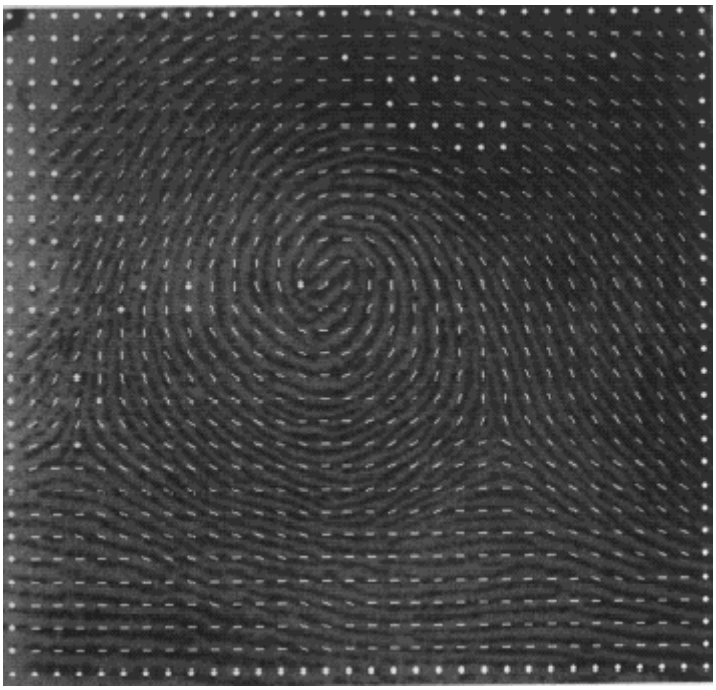


Abb.5: Richtungskarte (direction map)

b) Segmentierung (Unterscheidung Hintergrund/ Fingerabdruck)

Bei der Segmentierung (segmentation) wird der Teil des Bildes, der den Fingerabdruck darstellt, ausgeschnitten. Das Bild hat meistens einen uniformen Hintergrund, der ausgeblendet werden muss. Wie bei a) wird das Bild dafür in Blöcke gleicher Größe aufgeteilt. Jeder Block erhält dann die Zuordnung „Hintergrund“ oder „Fingerabdruck“ [Jain et al, 1999].

c) Markierung von Sonderpunkten (singularity points)

Sonderpunkte, wie z.B. das Core oder die Deltas (siehe 2.2.2) werden hierbei mit Hilfe der Richtungskarte aus a) lokalisiert. Dafür benutzt man entweder strukturelle Heuristiken oder es wird der so genannte *Poincaré Index* der Richtungskarte verwendet. Als Poincaré Index bezeichnet man das Integral der Richtungswechselgröße einer geschlossenen Struktur. Gewöhnliche Punkte des Richtungsfeldes haben einen Index von 0. Core und Deltas haben einen Index von 0,5 bzw. –0,5. Problematisch ist diese Methode bei Abdrücken vom Typ Bogen (arch type), so dass hier strukturelle Heuristiken nötig sind [Jain et al, 1999].

d) Bestimmen eines Registrierungspunktes (registration point extraction)

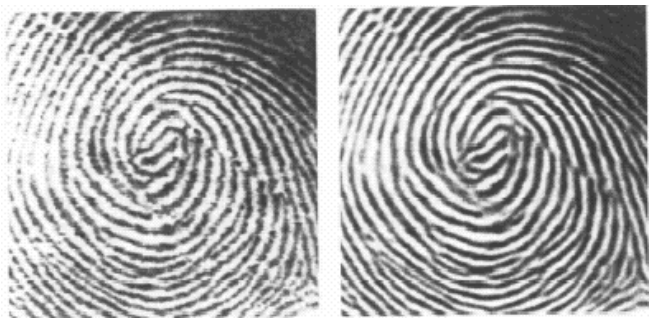
Der Registrierungspunkt wird bei der Normalisierung der Fingerabdruckposition beim Vergleich benötigt und daher für jeden Fingerabdruck bestimmt. Die in c) erwähnten Sonderpunkte sind potentielle Registrierungspunkte.

e) Verbesserung des Graustufenbildes (gray- level enhancement)

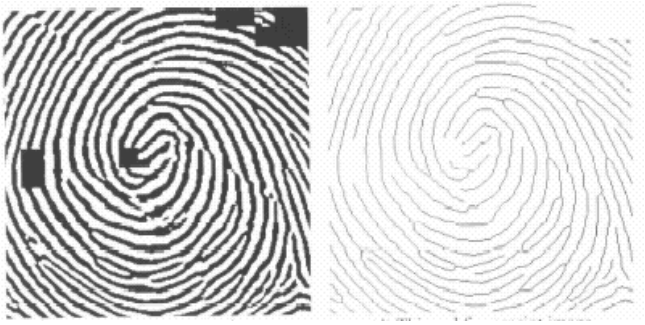
Eine Möglichkeit, die Qualität eines Bildes zu verbessern, ist das Anwenden einer Low-Pass-Filterung, um unerwünschtes Rauschen (störende Bildelemente) zu entfernen. Da die Qualitätsverbesserung des Fingerabdruckbildes großen Einfluss auf die Performanz des Gesamtsystems hat, werden inzwischen komplexere Algorithmen angewendet. O'Gorman und Nickeron beschreiben in [Nickeron und O'Gorman, 1989] die Verwendung von gerichteten Filtermasken.
Die Parameter der Masken sind zum einen die durchschnittlichen Breiten der Erhebungen und der Täler, zum anderen deren Ausrichtung. Der Fingerabdruck und die Masken werden überlagert, wobei die Form der Masken ständig der Richtungskarte angepasst wird (Abb.6 b) [Jain et al, 1999]. Einen ähnlichen Ansatz beschreibt Erol in [Erol, 1998]. Die Richtungsfilter werden mit Hilfe von *Gabor-Filtern* konstruiert. Der Gabor Filter ist eine Auswertungstechnik, die ursprünglich aus der Signalverarbeitung kommt und auf zeitkontinuierliche Daten angewendet wird. Sie liefert eine Frequenzanalyse, allerdings im Unterschied zur Fourier -Transformation nur von den Daten in der unmittelbaren Umgebung eines vorgegebenen Zeitpunktes. In den letzten Jahren hat der Gabor Filter wachsendes Interesse in der Bildverarbeitung gefunden, wo er statt eindimensional mit der Zeit als Parameter zweidimensional mit dem (Bild-)Ort als Parameter angewandt wird. Ein Grund hierfür

ist, dass sich herausgestellt hat, dass in der unteren Ebene des menschlichen visuellen Cortex Informationsverarbeitung durchgeführt wird, die analog zum Gabor Filter ist [DLR/Institute of Robotics and Mechatronics, 2002].

f) Erstellen eines Binärbildes und Ausdünnung der Linien (binarization/ thinning)
Zum Erstellen eines Binärbildes ist die in e) beschriebene Qualitätsverbesserung zwingende Voraussetzung. Eine mögliche Methode wird in [Wilson, 1993] beschrieben: Hierbei wird über kleine Linienabschnitte unterschiedlicher Ausrichtung integriert, um die Breite der Linien einzubeziehen. Der Binärwert berechnet sich dann aus dem minimalen und maximalen Integralwert, sowie dem Graustufenwert des zugehörigen Pixels. Dann erfolgt erneut eine Bildverbesserung. Moaver und Fu schlagen in [Fu/Moaver, 1986] die wiederholte Anwendung eines Laplace-Operators vor. Meistens weist das resultierende Binärbild Löcher oder Risse in der Rillenstruktur auf, die entdeckt und gefüllt werden müssen. Dafür kann jeder Algorithmus zur Bildverbesserung angewendet werden, auch mit Hilfe der Richtungskarte (siehe Abb.6 c). Falls bei qualitativ schlechten Teilgebieten keine klare Zuordnung (weißes oder schwarzes Pixel) erfolgen kann, wird lediglich der schwarze Hintergund angezeigt. Schließlich werden die Linien des Binärbildes ausgedünnt (siehe Abb.6 d) [Jain et al, 1999].



(a) Original Fingerabdruck (b) Verbessertes Bild



(c) Binäres Bild (d) Ausgedünntes Binärbild

Abb.6: Einige Zwischenstufen der Bildverarbeitung

g) Auffinden von Minutien (minutiae detection)

Das aus f) resultierende Bild wird pixelweise nach Verzweigungen und Endungen durchsucht. Zu diesem Zeitpunkt werden auch einige Eigenschaften (Attribute), die später beim Vergleich benutzt werden, berechnet, z.B.:

a. Ort der Minutie in Bezug zum Registrierungspunkt
b. Minutienart
c. Die Steigung der Linie (Tangente), die Minutie und Registrierungspunkt verbindet

Maio und Hanson sprechen sich in [Hanson/Maio, 1997] dafür aus, die Minutien direkt im Graustufenbild zu suchen. Der Anlass für diese Studie war der Informationsverlust, der bei f) auftritt und die schlechten Ergebnisse bei qualitativ minderwertigen Fingerabdruckbildern. [Jain et al, 1999]

h) Minutien-Reduzierung (minutiae reduction)

Eine unvermeidbare Fehlerquelle bei der Fingerabdruckerkennung sind falsche Minutien. Mögliche Ursachen sind (siehe 2.2.4) Narben, trockene Haut, Fett oder Schweiß. Daher wird die in der Entdeckungsphase g) entstandene Minutienliste auf falsche Minutien untersucht. Die Reduzierung basiert auf intuitiven Heuristiken. Es werden z.B. Minutien gestrichen, die zu dicht beisammen oder zu nah am Rand liegen. Problematisch ist, dass bei Anwendung dieser intuitiven Regeln auch echte Minutien versehentlich gelöscht werden können. Daher schlägt Hung in [Hung, 1993] einen angepassteren Algorithmus vor. Er teilt die Ursachen von falschen Minutien in die Kategorien Ausläufer, Löcher, Brücken und Unterbrechungen ein. Jede dieser Strukturen wird entdeckt und korrigiert [Jain et al, 1999].

2.2.6 Vergleich von Minutien-Codes (minutiae-based matching)

Der minutienbasierte Vergleich ist, wie bereits erwähnt, die gebräuchlichste Matching- Methode. Es gibt zwei Hauptansätze: Punktvergleich (point matching) und Strukturvergleich (structural matching).

Beim Punktvergleich werden zwei Minutien- Code- Mengen nach Lage der Minutien ausgerichtet und die Ähnlichkeit überlappender Merkmale mit Hilfe der Attribute aus 2.2.5. g) berechnet. Die Ausrichtung ist das Hauptproblem beim Punktvergleich, während dies beim Strukturvergleich nicht notwendig ist. Bei dieser Methode werden Strukturgraphen, die die relative Verteilung der Minutien repräsentieren, verglichen.

Ein Beispiel für einen Punktvergleichsalgorithmus wird in [Ratha/Karu/Shayon/Jain, 1996] erläutert: Alle möglichen Minutienpaare werden auf Übereinstimmungen untersucht und dabei verschiedene Rotationen getestet. Der Winkel mit der größten Übereinstimmungsquote wird für die Ausrichtung verwendet.
Isenor und Zaky verwenden in [Isenor/Zaky, 1986] Strukturgraphen und schlagen einen passenden Vergleichsalgorithmus vor. Diese Methode ist flexibler gegenüber möglichen Störfaktoren (Strukturvergleich) [Jain et al, 1999].

2.3 Leistungskenngrößen für biometrische Systeme: FAR, FRR, EER

Ein wichtiger Abschnitt bei der Konstruktion von Authentikationsverfahren 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.
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 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 a]. 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.7) markiert die EER den Schnittpunkt von FRR und FAR. An diesem Punkt sind also FRR und FAR gleich [Jain et al, 1999].

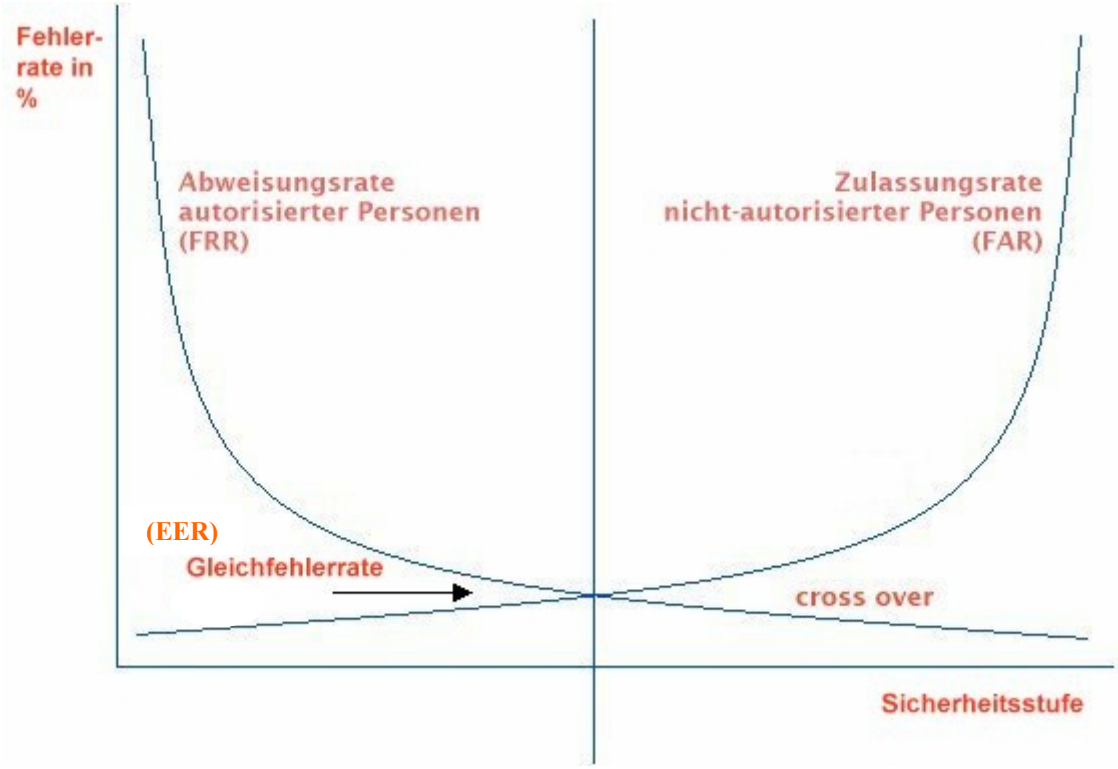


Abb.7: Biometrische Kenngrößen

3. Schematischer Aufbau des Logon-Systems von Windows NT/2k/XP

3.1 Übersicht

Dieses Kapitel befasst sich mit der Sicherheitsarchitektur, insbesondere mit dem Logon-System der Betriebssysteme Windows NT/2k/XP, da dieser Bereich bei der biometrischen Authentikation eine wichtige Rolle spielt.
Microsoft dokumentiert den Aufbau dieser und anderer Komponenten in der Microsoft Developer's Library (MSDN Library) [Microsoft Developer's Libary, 2001] und im Microsoft Platform Software Development Kit (Platform SDK) [Microsoft Platform SDK, 2001].
Dort findet man nicht nur Beschreibungen, sondern auch Codebeispiele, Import Libraries und technische Artikel, die Entwicklern als Referenzen bei der Verwendung von Microsoft Technologie dienen sollen.
Die Authentikation in Windows NT/2k/XP basiert auf der Passwort-Verifikation von registrierten Benutzern. Eine spezielle Einheit des Betriebssystems, das sogenannte „security subsystem" stellt die für den Logon-Prozess benötigten Authentikationsdienste zur Verfügung, neben weiteren Sicherheitskomponenten wie Zugangskontrolle und Auditing [Brömme et al, 2002].

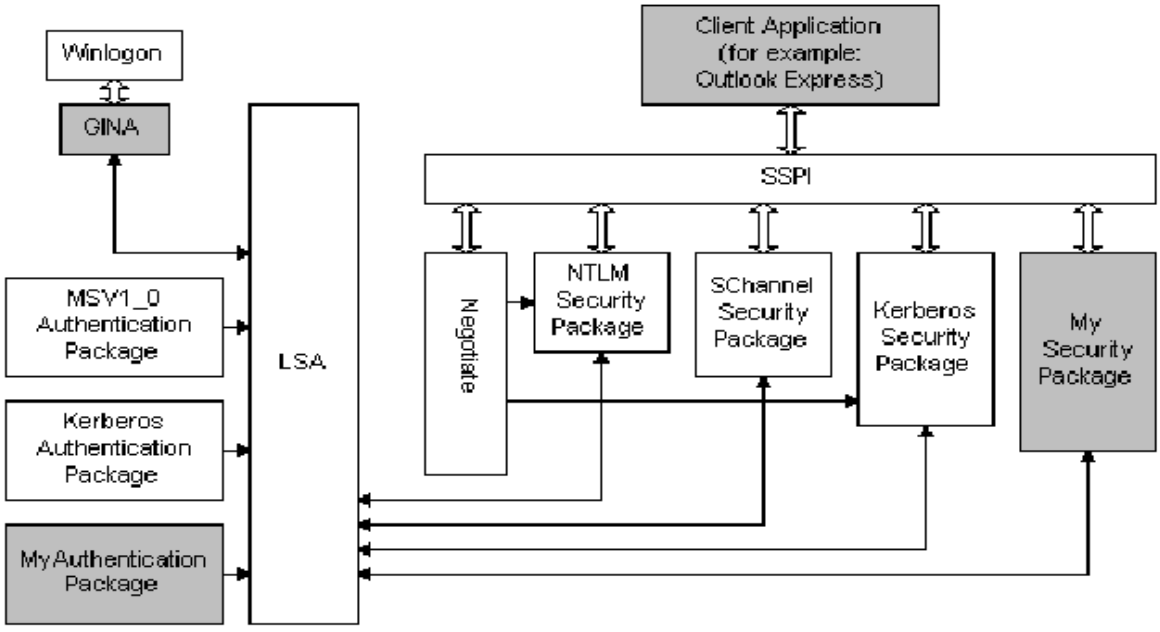


Abb.8: Schematischer Aufbau der Windows NT/2k/XP – Sicherheitsarchitektur

Abbildung 8 zeigt den schematischen Aufbau der Windows-Sicherheitsarchitektur. Die dunkel hervor gehobenen Komponenten können Entwickler selbst einbinden bzw. umgestalten.

3.2 Beschreibung der Komponenten des lokalen Logons

3.2.1 Winlogon

Winlogon ist der Prozess in Windows NT/2k/XP, der das interaktive Ein- und Ausloggen von Benutzern regelt. Neben der Hauptkomponente „WINLOGON.EXE“ beinhaltet das interaktive Logon-Modell zwei weitere Komponenten:
Eine sogenannte „GINA.DLL“ („Graphical Identification and Authentication dynamic-link library, siehe 3.2.2) und beliebig viele „network providers“. WINLOGON.EXE bildet die Schnittstelle zwischen diesen Komponenten und ist dabei unabhängig von der Art der Authentikation [Microsoft Platform SDK, 2001].

3.2.2 GINA.DLL

Diese logisch ersetzbare DLL-Datei wird von der Winlogon-Komponente gestartet und regelt die Interaktionen mit dem Benutzer in Bezug auf Identifikation und Authentikation. Statt der standardmäßigen Benutzerkennung- und Passwortabfrage kann also eine biometrische Gina.dll verwendet werden, die den Benutzer beispielsweise auffordert, den Finger auf einen Sensor zu legen [Microsoft Platform SDK, 2001].

3.2.3 Local Security Authority (LSA)

Die LSA ist ein geschütztes Untersystem von Windows NT/2k/XP, das Benutzer authentisiert und einloggt, bzw. den Zugriff verweigert. Für die Verifikation der Benutzerdaten greift die LSA auf „authentication packages“ zu, beispielsweise KERBEROS.DLL für *Kerberos* Authentikation (siehe Abb.8). [Microsoft Platform SDK; Brömme et al, 2001]

Ein Authentication Package ist eine DLL-Datei, die die Regeln beinhaltet, nach denen einem Benutzer das Logon erlaubt oder verweigert wird. Sie erhält die zu analysierenden Anfragedaten von der LSA. Außerdem startet sie eine neue Logon-Session und erstellt einen einmaligen Logon-Identifier für den erfolgreich angemeldeten Teilnehmer.
Ein anderes Beispiel für ein Authentication Package ist MSV1_0.DLL. Dieses Paket erwartet einen Benutzernamen mit gehashtem Passwort und vergleicht dieses Tupel mit den Daten aus der SAM (Security Accounts Manager) Datenbank. Stimmen die Daten überein, wird der Zugang gewährt. Die SAM enthält Informationen über alle Benutzer- und Gruppenkonten.
Wie bei der GINA.DLL ist es auch an dieser Stelle möglich, eigene biometrische Authentication Packages zu definieren („My_Authentication Package, Abb.8) [Microsoft Platform SDK, 2001].

3.2.4 SSP/ SSPI

Ein Security Support Provider (SSP) ist eine DLL-Datei, die Anwendungen das Benutzen eines oder mehrerer Sicherheitspakete (Security Packages) ermöglicht. Security Packages sind Softwareimplementationen von Sicherheitsprotokollen.
Die Schnittstelle zum SSP, das so genannte Security Support Provider Interface (SSPI), bietet Transport-Level-Anwendungen, wie beispielsweise Microsoft Remote Procedure Call (RPC), die Möglichkeit über die Sicherheitsprotokolle eine authentisierte Verbindung aufzubauen [Microsoft Platform SDK, 2001].
Negotiate ist ein spezieller Security Support Provider, der als Anwendungsschicht zwischen der SSPI und den anderen SSPs fungiert. Wenn eine Anwendung sich mittels SSPI in ein Netzwerk einloggen möchte, dann kann sie das SSP, das die Anfrage bearbeiten soll, bestimmen oder Negotiate wählen. Negotiate analysiert dann die Anfrage und wählt dann den geeigneten SSP für die Bearbeitung aus [Microsoft Platform SDK, 2001].

3.3 Authentisierung über ein Netzwerk

3.3.1 Das Kerberos-Protokoll

Kerberos ist ein Protokoll für die Netzwerkauthentifizierung, das in den 80er Jahren am Massachusetts Institute of Technology (MIT) entwickelt wurde. Das Projekt wurde als *Project Athena* bezeichnet und das wichtigste Ziel bestand darin, Fähigkeiten zur Administration von verteilten Systemen zu entwickeln, zu implementieren und zur Verfügung zu stellen. Mit diesem Ziel im Visier musste das Entwicklerteam für eine starke Authentisierungsmethode im Umfeld von Client/Server-Applikationen sorgen. Um die Authentisierung für diese Art von Umgebungen durchzuführen, wurde eine symmetrische Verschlüsselung auf Basis gemeinsamer geheimer Schlüssel benutzt. Der Name Kerberos stammt aus der griechischen Mythologie. Kerberos war der dreiköpfige Hund, der den Ausgang des Hades bewachte.

In der Computerwelt könnten diese drei Köpfe die drei Komponenten des Protokolls darstellen: den Client/die Applikation, die Netzwerkressource und das Key Distribution Center (KDC). Kerberos ist eine dreiteilige Methode, die für Sicherheit in einem Netzwerk und den Zugriff auf Netzwerkressourcen sorgen soll [Schmidt, 2001].

3.3.2 Das Key Distribution Center

Das Key Distribution Center (KDC) ist als Domänendienst auf allen Domänen-Controllern implementiert und verwendet das Active-Directory als Datenbank für Netzwerkbenutzer sowie den globalen Katalog. Das KDC ist ein Prozess, der zwei Dienste zur Verfügung stellt:

- *Authentication Service:* Dieser Dienst stellt so genannte Ticket-Granting Tickets aus und wird in diesem Kapitel noch näher erläutert.
- *Ticket-Granting Service:* Dieser Dienst stellt Sitzungstickets aus, die den Zugriff auf Netzwerkressourcen auf Basis der für den Benutzer geltenden Rechte und Berechtigungen ermöglichen. Er wird ebenfalls später in diesem Kapitel detailliert dargestellt.

Der KDC-Dienst wird auf allen Domänen-Controllern installiert. Er wird automatisch von der Local Security Authority (LSA) (siehe 3.2.3) auf dem Domänen-Controller gestartet und läuft im Prozessbereich der LSA. Dieser Dienst kann nicht beendet werden, es sei denn, der Contoller fällt aus [Schmidt, 2001].

3.3.3 Kerberos Security Support Provider

Kerberos wird als ein Security Support Provider (SSP) (siehe 3.2.4) implementiert, der als Dynamic Link Library von Windows zur Verfügung gestellt wird. Windows 2000 enthält außerdem einen SSP für die NT-LAN-Manager(NTLM)-Authentisierung, der abwärtskompatible Clients und das Einloggen in einen eigenständigen Windows-2000-Rechner unterstützt. Die LSA startet beim Booten des Systems sowohl den Kerberos- als auch den NTLM-SSP und ein Benutzer kann von jedem der beiden SSPs authentisiert werden. Dies hängt von der Konfiguration des Computers ab, jedoch ist der Kerberos-SSP stets die erste Wahl.

Systemdienste greifen über das Microsoft Security Support Provider Interface (SSPI) auf die SSPs zu. Alle verteilten Dienste unter Windows 2000 benutzen SSPI für den Zugriff auf den Kerberos-SSP. Beispiele:

- Dienste der Druckwarteschlange
- Remote-Dateizugriff
- Systemmanagement und Weiterleitungen für verteilte Dateisysteme
- Intranet-Authentisierung gegenüber Internet-Information-Server [Schmidt, 2001]

3.3.4 Namensauflösung über DNS

Microsoft hat sich bei der Implementation der Version 5 des Kerberos-Protokolls an die Spezifikation der Internet Engineering Task Force (IETF) gehalten (RFC 1510/1964). RFC 1510 spezifiziert, dass für alle Nachrichten zwischen dem Client und dem KDC IP-Transportmechanismen verwendet werden sollen. Wenn der Kerberos-SSP auf einem Client eine erste Dienstanforderung übertragen will, muss er eine Adresse für das KDC in der Domäne des Benutzers finden. Dafür benötigt der

Client den Namen des Servers, auf dem der KDC-Dienst läuft. Wenn der DNS-Name in eine IP-Adresse aufgelöst werden kann, sendet der Kerberos-SSP eine Fehlermeldung, in der er informiert, dass er die verlangte Domäne nicht finden konnte.

Beispiel: Nehmen wir an, eine Person hat sich bereits angemeldet (siehe Abb.9; 1.), wurde im Netzwerk authentifiziert und hat ihr Ticket-Granting-Ticket (TGT) erhalten (2.). Im Laufe des Tages muss dieser Benutzer auf eine Netzwerkressource (Drucker) zugreifen. An diesem Punkt präsentiert die Benutzersitzung (Session) dem KDC ein TGT und verlangt ein Sitzungsticket (ST) für den Zugriff auf die Netzwerkressource (3.). Das Sitzungsticket (ST) wird vom KDC auf Basis der Benutzer-Rechte und Berechtigungen für den Drucker ausgestellt (4.). Der Druckserver wird nun das vom KDC ausgestellte ST verwenden, um dem Benutzer Zugriff auf die Ressource (Drucker) zu gewähren (5.) (siehe Abb.9) [Schmidt, 2001].

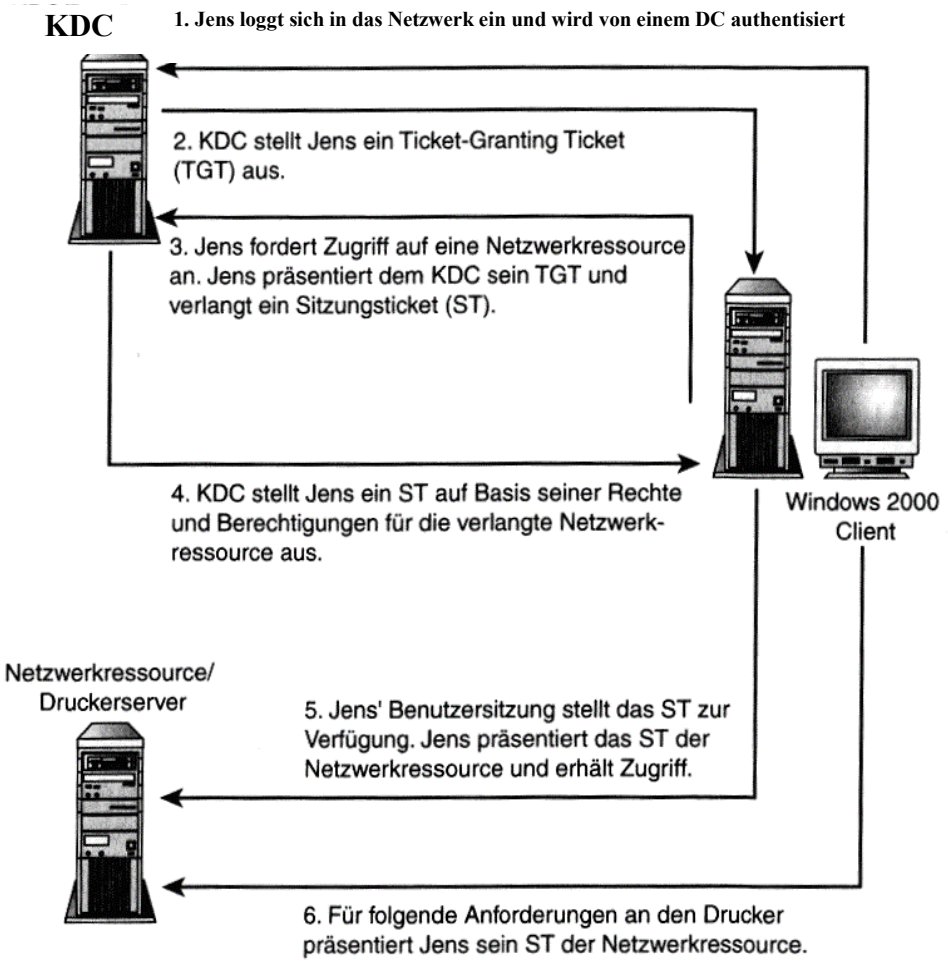


Abb.9: Anmeldung und Zugriff auf eine Netzwerkressource unter Windows 2000 am Beispiel des Benutzers „Jens“

Ein Ticket enthält folgende Informationen:

- Name des Servers
- Name des Client
- Internetadresse des Client
- Zeitstempel
- Zeitdauer der Gültigkeit
- Session Key [Bindrich, 1995]

3.3.5 Sicherheit

Ein entscheidender Punkt für die Sicherheit von Kerberos ist die Sicherheit der Kerberos Datenbank. Ein schreibender Zugang zu dieser ist nur durch einen administrativen Service, dem Kerberos Database Management Service (KDMS) möglich. Jede Änderung ist nur auf der Master Datenbank, auf der das KDMS läuft, möglich. KDMS hat zwei Hauptaufgaben:

- Bearbeitung von Anfragen zur Passwortänderung
- Hinzufügen neuer Nutzer [Bindrich, 1995]

Kerberos verwendet Verschlüsselungsverfahren, um die Authentizität der miteinander kommunizierenden Elemente zu gewährleisten. Es soll sowohl dem Benutzer als auch der Ressource garantiert werden, dass sie nicht mit einem Betrüger im Netzwerk kommunizieren. In 3.3.4 wurde aufgelistet, welche Informationen ein Ticket enthält. Zur Sicherung dieser Informationen sind Teile des Tickets mit einem geheimen Schlüssel verschlüsselt, den nur der Benutzer und der Domänen-Controller teilen. Die anderen Informationen im Ticket werden mit einem geheimen Schlüssel verschlüsselt, den nur die Netzwerkressource und der Domänen-Controller teilen. Da jede Identität seinen bestimmten Teil des Tickets lesen kann, wird angenommen, dass jeder derjenige ist, der er zu sein vorgibt [Schmidt, 2001]. Diese Art zu verschlüsseln nennt man symmetrische Verschlüsselung. Symmetrische Verschlüsselung ist auch unter dem Namen Secret Key-Verschlüsselung bekannt. „Symmetrisch“, weil beide an der Verschlüsselung

beteiligten Parteien den selben Schlüssel teilen und „secret“, weil dieser Schlüssel unbedingt geheim gehalten werden muss. Bei der asymmetrischen Verschlüsselung (auch Public-Key-Verschlüsselung genannt), werden zwei Schlüssel verwendet. Ein Prozess generiert hierfür zwei Schlüssel für jeden Benutzer. Eine Nachricht, die mit dem einen Schlüssel verschlüsselt wird, kann nur mit dem anderen entschlüsselt werden. Der erste Schlüssel ist der Private Key, der zweite Schlüssel ist der Public Key. Der Public Key darf jedem bekannt sein, der Private Key muss aber unbedingt geheim gehalten werden [Ferrari/Schmid, 1998].

3.3.6 Gültigkeitsdauer der Tickets

Jedes vom KDC ausgestellte Ticket besitzt eine Start- und eine Ablaufzeit. Zu jeder Zeit, in der das Ticket gültig ist, kann ein Client, der Zugriff zu einer Ressource verlangt, das Sitzungsticket präsentieren und die Ressource verwenden. Der Client kann mit dem gleichen Ticket den Dienst immer wieder anfordern, unabhängig davon, wie oft er das Ticket schon benutzt hat. Um aber die Wahrscheinlichkeit zu minimieren, dass Tickets oder die entsprechenden Dienste beeinträchtigt werden, kann ein Administrator die maximale Gültigkeitsdauer für Tickets einrichten. Wenn ein Client ein Sitzungsticket für eine Ressource vom KDC verlangt, bestimmt das KDC den Wert für das Feld mit der Ablaufzeit, indem es die maximale Gültigkeitsdauer für das Ticket, die von den Kerberos-Richtlinien festgelegt ist, zum Wert für das Startfeld addiert. An diesem Punkt vergleicht das KDC das Ergebnis mit der verlangten Gültigkeitsdauer. Der frühere Zeitpunkt wird zur Ablaufzeit für das Ticket. Kerberos benachrichtigt den Client nicht, wenn ein Ticket abgelaufen ist, um die Netzwerk- und Server-Performanz nicht zu beeinträchtigen. Abgesehen von kurzfristigen Einträgen, die zur Verhinderung von Wiederholungsangriffen (Replay-Attacken) benötigt werden, macht Kerberos tatsächlich keinen Versuch, Transaktionen mit Clients zu verfolgen. Wenn Kerberos alle Clients, denen Tickets ausgestellt werden, benachrichtigen müsste, wäre das nachteilig für die Performanz des Netzwerks.
Zwei typische Situationen im Zusammenhang mit abgelaufenen Tickets sind:

- Das TGT des Clients ist abgelaufen und der Client fordert ein Sitzungsticket für eine Netzwerkressource an. Der KDC antwortet mit einer Fehlermeldung. Der Client muss ein neues TGT vom KDC anfordern.
- Der Client versucht mit einem abgelaufenen Sitzungsticket auf eine Netzwerkressource zuzugreifen. Der Server antwortet mit einer Fehlermeldung. Der Client muss vom KDC ein neues Sitzungsticket verlangen. Wenn er authentisiert ist, kann der Client auf die Ressource zugreifen. Läuft das Sitzungsticket ab, während ein Benutzer mit einer Ressource verbunden ist, wird die Verbindung nicht beendet. Wenn der Client aber beim nächsten Mal die Ressource verlangt, werden die oben aufgeführten Aktionen durchlaufen [Schmidt, 2001].

Im Rahmen dieser Arbeit wird auf das lokale Windows-Logon Bezug genommen. Die Einbettung der lokalen biometrischen Anmeldung befindet sich bei Windows jedoch in der generellen Authentisierungsarchitektur, die Netzwerkanmeldungen umfasst.

Eine mögliche Anwendung für die biometrische Authentikation im Netzwerk, bei der das Kerberos-Protokoll verwendet werden kann, ist ein Biometrischer Authentikationsserver, der Benutzerzugänge zum System per biometrischer Authentikation überwacht und die dafür benötigten Daten speichert (Signaturen, Benutzerkennungen, etc.).

4. Testen kommerzieller Fingerprint-Sensoren

4.1 Test eines Fingerabdruck-Sensors von Keytronic

In anbetracht der zunehmenden Relevanz der Biometrik in unserer Gesellschaft, ist es besonders wichtig, die bereits vorhandenen Lösungen gründlich zu testen. Daher haben mehrere Mitglieder der Biometric Authentication Research Group der Universität Hamburg am Fachbereich Informatik beschlossen, die Betrugs-Sicherheit eines kommerziellen Fingerabdruck-Sensors zu überprüfen.[2]

4.1.1 Verwendete Hard- und Software

Getestet wurde das Fingerprint-Sensor-Keyboard F-SCAN-K001US der Firma Keytronic (siehe Abb.10).

Abb.10 : 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 (siehe Abb.11).

[2] Willem Fröhling, Martin Johns, Christian Paulsen im Februar 2002
[Biometric Authentication Research Group, 2002 b]

Biologon 3.0 bietet die Möglichkeit, mehrere Benutzerprofile anzulegen. Jeder Benutzer kann seinen Fingerabdruck zur Authentikation einlernen (Enrollment), ein Passwort und Benutzername wird ebenfalls gespeichert.
Wenn ein Benutzer das System hochfährt, wird er aufgefordert, die Secure Attention Sequence „STRG-ALT-ENTF“ zu aktivieren, oder einen Finger auf den Sensor zu legen.
Legt dann ein Benutzer seinen Finger auf den Sensor, prüft Biologon automatisch, ob dies ein eingelernter Abdruck ist, ohne dass man vorher einen Benutzernamen eingeben muss. Es findet also keine Verifikation, sondern eine Identifikation statt.

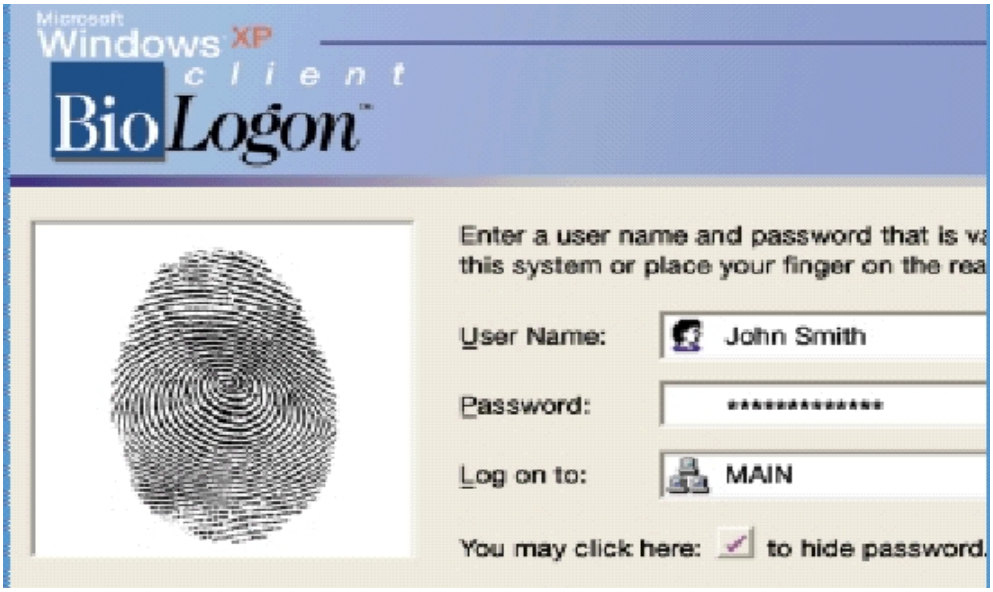


Abb.11: Screenshot von Biologon 3.0

4.1.2 Durchführung des Tests und Testergebnis

Zunächst wurde ein Benutzerprofil erstellt. Dafür hat ein Student den Fingerabdruck seines linken Zeigefingers eingelernt (Enrollment). Mehrere Testversuche 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 erwartungsgemäß 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 hat nicht mal ein Bild des Abdrucks angezeigt, genauso beim Auflegen einer Fingerabdruckskizze.
Da beim Auflegen eines echten Fingers (auch eines nicht eingelernten) stets ein Bild angezeigt wurde, war es offensichtlich, dass eine Lebenderkennung vorhanden ist. Sie soll unter anderem verhindern, dass beispielsweise ein toter Finger oder Wachsabdrücke verwendet werden können, um einen unbefugten Zugriff zu erhalten. Durch Ausprobieren wurde schnell erkannt, welche Lebenderkennung eingesetzt wird: Der Sensor ist ein so genannter kapazitiver Sensor, d.h. es muss ein Strom fließen, bevor ein Scan stattfindet. Dabei bildet der Finger die eine und die Oberfläche des Sensors die andere Leiterplatte (siehe Kapitel 2, Abschnitt 2.2.4). Mit etwas Speichel auf der Sensoroberfläche war es möglich, diesen Zustand zu simulieren und die Lebenderkennung zu täuschen, denn jetzt zeigte Biologon 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.

4.2 Täuschen von Fingerabdruck-Sensoren mit Gelatine und Gummi

In diesem Abschnitt wird beschrieben, wie es dem japanischen Mathematiker Tsutomu Matsumoto und ein paar seiner Studenten gelungen ist, 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 dabei sowohl optische als auch kapazitive Sensoren. Matsumoto möchte mit seiner Arbeit darauf hinweisen, dass Hersteller von Fingerabdruck-Sensoren nicht ausreichend überprüft haben, wie ihre Systeme getäuscht werden können.
Häufig fehlen Herstellerangaben, die den Umgang ihres Systems mit künstlichen Fingern dokumentieren [Matsumoto, 2002].

4.2.1 Risikoanalyse für Fingerabdruck-Systeme

Matsumoto führt in [Matsumoto, 2002] eine Risikoanalyse in Bezug auf die Gefahren bei der Nutzung von Fingerabdruck-Systemen durch. Es wird vorausgesetzt, dass mindestens ein Benutzer in einem Enrollment-Prozess registriert wurde. Matsumoto nennt mehrere Möglichkeiten, ein System zu täuschen. Dafür muss ein Angreifer eines der folgenden Elemente verwenden:

(a) *Den registrierten Finger:* Eine eingelernte Person kann dazu gezwungen werden, den registrierten Finger auf den Sensor zu legen. Ebenso kann diese Person vorher betäubt werden. Die Anwendung dieser Methoden kann laut [Matsumoto, 2002] verhindert werden, indem mehrere Authentikationsmethoden miteinander verknüpft werden, z.B. Passwort, PIN und Fingerabdruck.

(b) *Einen unregistrierten Finger:* Ein Angreifer kann versuchen, Zugriff zu erhalten, indem er einen nicht-registrierten Finger verwendet. Dazu ist es nötig, dass der Typ des Abdrucks (Schleife, Wirbel, etc., vgl. Kapitel 2) bekannt ist. Dann ist es möglich, dass die False Acceptance Rate höher liegt als der Durchschnittswert. Matsumoto empfiehlt daher, dass zusätzlich die FARs bei der Verwendung derselben Henry-Kategorie ermittelt werden sollten (vgl. 2.2.2).
Möglicherweise kann der Angreifer seinen Finger auch gezielt verändern, beispielsweise bemalen oder verletzen. Allgemein führen diese Methoden aber sehr selten zu gelungenen Täuschungsaktionen.

(c) *Eine abgetrennte Fingerspitze des registrierten Fingers:* Eine „grausame“ Methode ist es, den registrierten Finger einer Person abzuschneiden und auf den Sensor zu legen. Dagegen hilft die sogenannte Lebenderkennung („Live-Check“) und die Kombination von verschiedenen Authentikationsmethoden.

(d) *Ein genetischer Klon des registrierten Fingers:* Wie bereits in Kapitel 2.2.3 erläutert wurde, haben selbst eineiige Zwillinge keine identischen Fingerabdrücke, das gleiche würde daher auch für Klone gelten. Trotzdem ist die Ähnlichkeit sehr groß und möglicherweise reicht dies aus, um den Sensor zu überlisten. Daher ist es

wichtig, die zukünftigen Forschungsergebnisse und Bemühungen der Genforscher genauestens und kritisch zu beobachten.

(e) *Eine künstliche Kopie des registrierten Fingers:* Die Verwendung von künstlichen Fingern ist eine weitaus häufigere Angriffsmethode, als die bisher aufgezählten. Darauf geht Matsumoto in [Matsumoto, 2002] genauer ein, indem er beschreibt, wie künstliche Gummifinger mit oder ohne Gussformen hergestellt werden können. Dagegen hilft wieder einmal ein funktionstüchtiger Live-Check oder die Kontrolle durch eine zweite Person.

(f) *Andere Möglichkeiten:* Einige Sensoren können während des Authentikationsprozesses irritiert werden, beispielsweise durch Lichtblitze, erhitzen, abkühlen, stoßen oder rütteln. Diese Angriffe werden „fault based attacks“ genannt und können in Kombination mit den Methoden (a) – (e) ausgeführt werden. Weiterhin können latente Fingerabdrücke auf der Sensoroberfläche mit Hilfe eines Sprays sichtbar gemacht werden und zum Täuschen verwendet werden. Es braucht dann nur noch irgendein Finger auf die Fläche gedrückt werden.

Matsumoto hat sich in [Matsumoto, 2002] auf den Fall (e) konzentriert, das Herstellen eines künstlichen Fingerabdrucks.

4.2.2 Herstellung von künstlichen Fingern

Es gibt mehrere Wege, künstliche Finger herzustellen. 4.2.2.1 beschreibt die Herstellung eines „Gummifingers“ mit Hilfe eines lebendigen Fingers, 4.2.2.2 erläutert die Vorgehensweise bei zurückgebliebenen, latenten Fingerabdrücken oder künstlich generierten Bildern. Bei beiden Methoden verwendete die Forschergruppe Gelatine, die in eine Plastikform gefüllt wird.

4.2.2.1 Herstellung eines künstlichen Fingers mit Hilfe eines lebenden Fingers

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 12 zeigt Bilder eines echten und des zugehörigen Gummifingers, aufgenommen mit einem Fingerabdrucksensor.

a) echter Finger b) Gummifinger

Abb.12: Aufnahme eines echten Fingers und eines Gummifingers, aufgenommen mit einem kapazitiven Fingerabdrucksensor „FingerTIP“ der Infineon Technologies AG, nach [Matsumoto, 2002]

4.2.2.2 Herstellung eines künstlichen Fingers mit latenten Abdrücken

Matsumoto erläutert in [Matsumoto, 2002] die Vorgehensweise, wie man einen hinterlassenen Fingerabdruck 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 wie bei 4.2.2.1 mit flüssiger Gelatine übergossen und gekühlt. Nach 10 Minuten kann dann eine Gummi-Imitation des Abdrucks abgezogen werden (vgl. Abb.13).

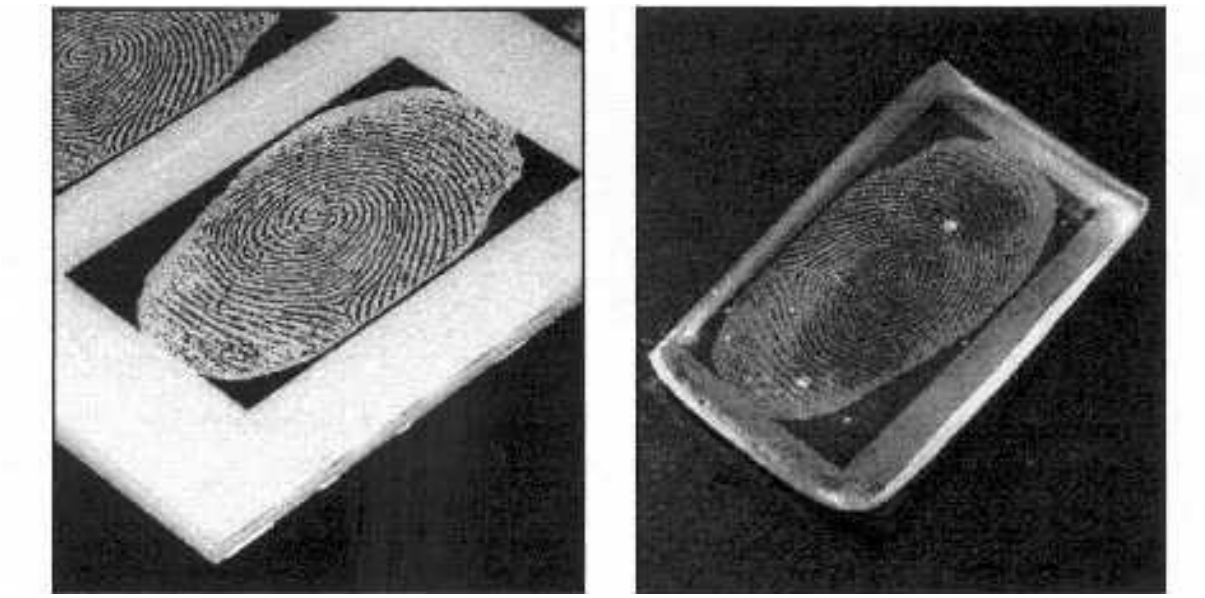


Abb.13: Aus einem hinterlassenen Fingerabdruck gewonnene Gussform und Gummifinger

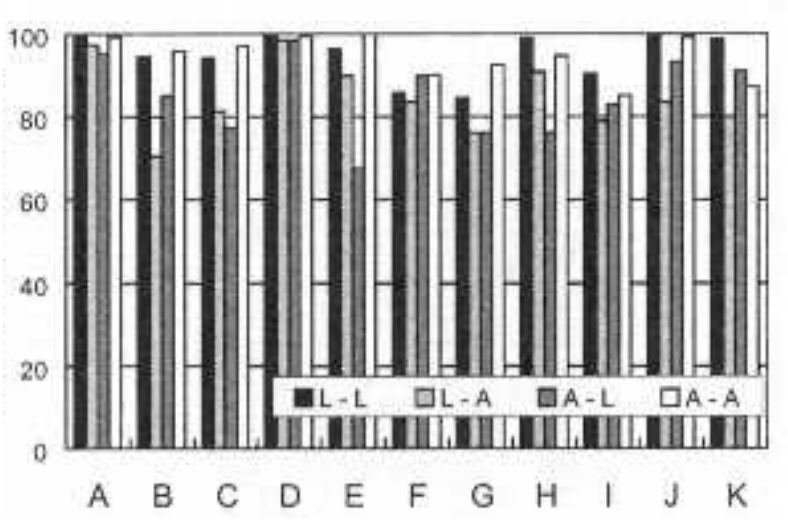
4.2.3 Versuchsreihe und Ergebnisse

Die Matsumoto-Gruppe hat insgesamt 11 verschiedene Fingerprintsensoren getestet. Jedes Gerät wurde auf vier verschiedene Arten getestet (vgl.Tabelle 2) und es wurden jeweils Gummifinger nach 4.2.2.1 und 4.2.2.2 verwendet. 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

Matsumoto hat die Schwellwerte der Erkennung, falls Einstellungen per Software möglich waren, auf den höchsten Sicherheitswert gestellt.
Die folgenden Abbildungen 14 und 15 dokumentieren die Ergebnisse der Experimente: Die Fingerabdrucksysteme verifizierten die mit lebenden Fingern erstellten Gummifinger zu 68-100 Prozent, die mit latenten Fingerabdrücken erstellten Gummifinger durchschnittlich zu 67 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.14 : Die Versuchsergebnisse bei Gummifingern nach 4.2.2.1

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.15 : Die Versuchsergebnisse bei Gummifingern nach 4.2.2.2

5. Konzept zur Integration der biometrischen Fingerabdruckerkennung in ein Rahmenwerk zum Testen biometrischer Algorithmen

5.1 Ein konzeptuelles Rahmenwerk zum Testen biometrischer Verfahren

Die Entwicklung biometrischer Algorithmen für die Authentikation erfordert ausführliches Testen unter realen Bedingungen, um mit Hilfe der gewonnenen Testdaten die Robustheit, Performanz und Brauchbarkeit einordnen und bewerten zu können.
Die Biometrik-Gruppe des Fachbereichs Informatik an der Universität Hamburg hat daher ein konzeptuelles Rahmenwerk zum Testen biometrischer Algorithmen entwickelt, das in diesem Abschnitt vorgestellt wird.
Ein Data Logging Modul soll spezifische Daten, die während des Authentikationsprozesses anfallen, speichern. Dies sind hauptsächlich quantitative Daten, beispielsweise Zeitstempel, biometrische Rohdaten und andere Zwischenergebnisse. Ein weiteres Modul enthält den biometrischen Algorithmus (z.B. für die Authentikation per Fingerabdruck), das wiederum aus vier Modulen besteht, deren Funktionen in diesem Kapitel näher erläutert werden.
Alle personenbezogenen biometrischen Daten und Signaturen müssen in einer sicheren Datenbank gespeichert werden. Schutzbedarf besteht auch für die Kommunikationswege zwischen den Modulen und den Datenbanken.
Da es nicht möglich ist, qualitative Bewertungen (beispielsweise die Benutzerfreundlichkeit eines Systems) zu automatisieren, ist eine menschliche Aufsichtsperson während der Testdurchführung erforderlich. Die abschließende Auswertung kombiniert die Erkenntnisse aus den quantitativen und qualitativen Tests, die unter Labor- und Realbedingungen gewonnen wurden [Brömme et al, 2002].

5.1.1 Biometrische Authentikation mit Data Logging

Der Prozess der biometrischen Authentikation beginnt mit dem Login-Vorgang, durch den der Benutzer vom Login-Dialog geleitet wird. Der Login-Dialog fordert den Benutzer dazu auf, sein/e biologisches/n Merkmal/e für die Datenerfassung zur

Verfügung zu stellen. Bei der Fingerabdruckerkennung könnte der Dialog wie folgt beginnen: „Legen Sie bitte Ihren Finger auf die Sensorfläche“.
Dann werden die biologischen Merkmale erfasst/gescannt, beispielsweise das Bild eines Fingerabdrucks. Die erfassten Merkmale werden einem biometrischen Algorithmus als Eingangsdaten übergeben, wenn die bisherigen Schritte erfolgreich verlaufen sind. Der Algorithmus verarbeitet die Eingangsdaten und gibt als Resultat entweder „akzeptiert (accept)“, „nicht akzeptiert (reject)“ oder eine Fehlermeldung aus. Für einen erfolgreichen Login-Vorgang wird vorausgesetzt, dass der Benutzer bereits korrekt eingelernt ist (→Enrollment) (vgl. Abb.16)

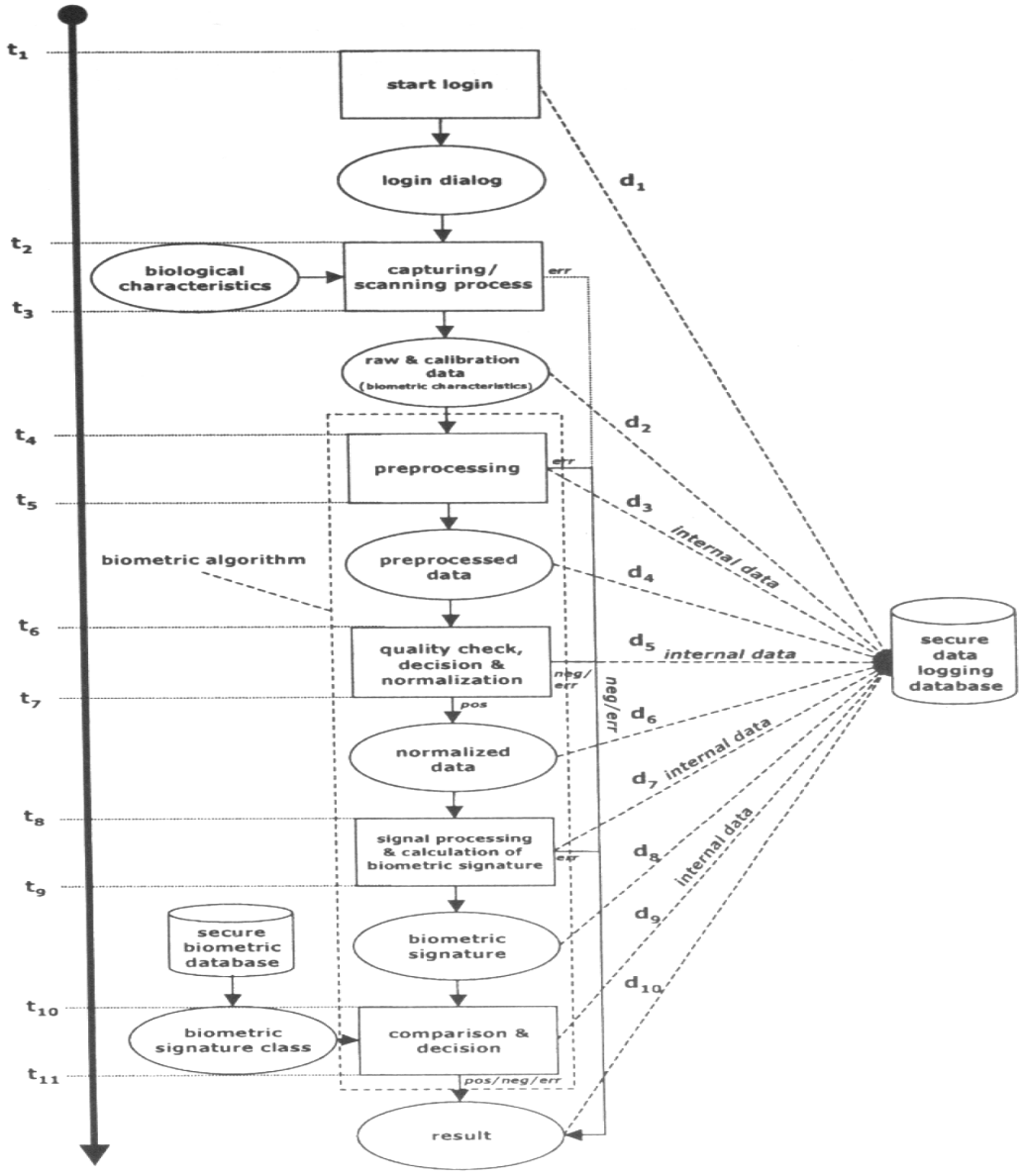


Abb.16: Prozess der Biometrischen Authentikation mit Data Logging

Der biometrische Algorithmus besteht aus vier Modulen:

1. **P**: **P**reprocessing (Vorverarbeitung)
2. **Q**: **Q**uality Check, Decision, Normalization (Qualitätsüberprüfung, Entscheidung und Normalisierung)
3. **S**: **S**ignal Processing, Calculation of Biometric **S**ignature (Signalverarbeitung und Berechnung der biometrischen Signatur)
4. **D**: Comparison and **D**ecision (Vergleich und Entscheidung)
   → Verifikation (1:1) und Identifikation (1:n)

Die Module Q und D können den Authentikationsprozess mit einer negativen Entscheidung beenden bzw. alle vier Module und der Scan-Prozess können Fehlermeldungen ausgeben und damit den Vorgang stoppen.
Während eines Authentikationsversuchs können die Zeitstempel t_1 - t_{11} (vgl. Abb.16) und die Zwischendaten d_1 - d_{10} über verschlüsselte Kommunkationswege („secure biometric channels“) an eine gesicherte Logging-Datenbank übermittelt und dort gespeichert werden [Brömme et al, 2002].

5.1.2 Windows NT/2000-Komponenten für die biometrische Authentikation

Der Aufbau des Logon-Systems von Windows NT/2000 wurde bereits in Kapitel 3 behandelt. Abb.17 zeigt noch einmal eine grobe Übersicht der Authentikationskomponenten:

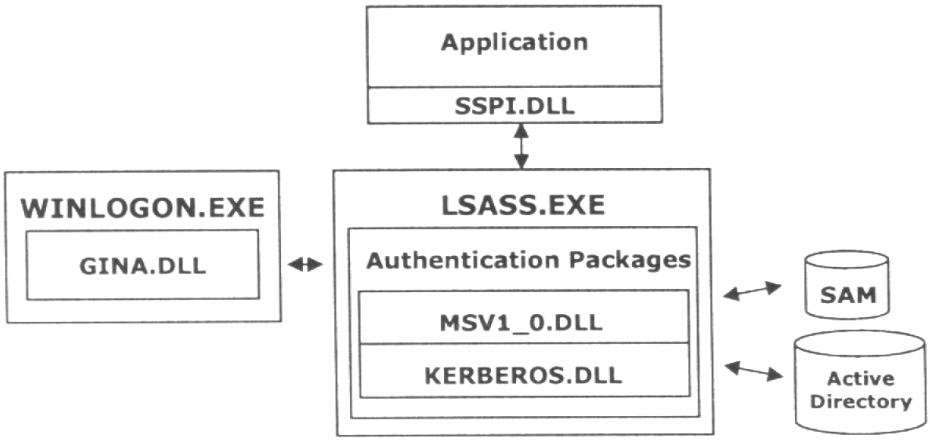


Abb.17: Authentikationskomponenten in Windows NT/2000

In Kapitel 3 wurde auch erwähnt, dass die Komponenten ersetzbar bzw. erweiterbar sind, um eine Integration alternativer Authentikationsverfahren zu ermöglichen. Für die biometrische Authentikation muss eine neue biometrische GINA.DLL eingesetzt werden. Sie regelt die Benutzer-Interaktion für die Erfassung der biometrischen Login-Daten. Die Module P und Q des biometrischen Algorithmus können ebenfalls in die GINA.DLL integriert werden. Die Module S und D sind in einem biometrischen Authentikationspaket integriert (biometric authentikation package, vgl. Abb.18).

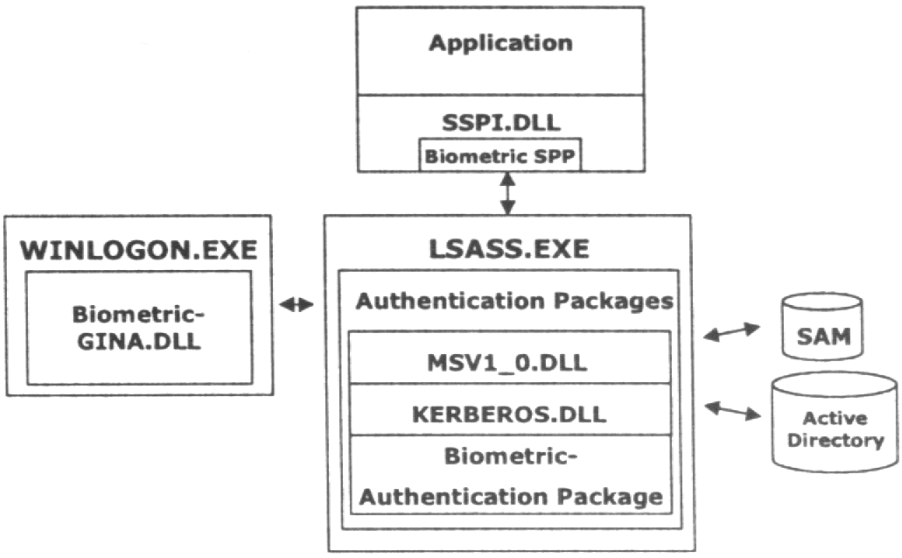


Abb.18: Windows NT/2000 Komponenten für die biometrische Authentikation

Ein neuer biometrischer Security Service Provider (SSP) kann eine einheitliche Schnittstelle für Anwendungen, die Dienste des Authentikationspaketes aufrufen, zur Verfügung stellen. In diesem Fall sollte das P-Modul eher im biometrischen Authentikationspaket enthalten sein, statt in der GINA.DLL.
Die biometrische GINA.DLL und das biometrische Authentikationspaket können auf das Data-Logging Modul zugreifen, um dort die in 5.1.1 genannten Testdaten zu speichern [Brömme et al, 2002].

5.1.3 Aufbau des Testrahmenwerks

Da es nicht ausreicht, die Qualität eines biometrischen Systems unter Laborbedingungen zu testen, hat die Hamburger Biometrikgruppe in ihrem konzeptuellen Rahmenwerk [Brömme et al, 2002] verankert, dass zusätzlich ein Test am geplanten Einsatzort unter realen Bedingungen durchgeführt werden muss.
Als erstes sollten die Anwendungsbedingungen ausgewählt werden, d.h. das Betriebssystem und das biometrische Verfahren (siehe Abb.19):

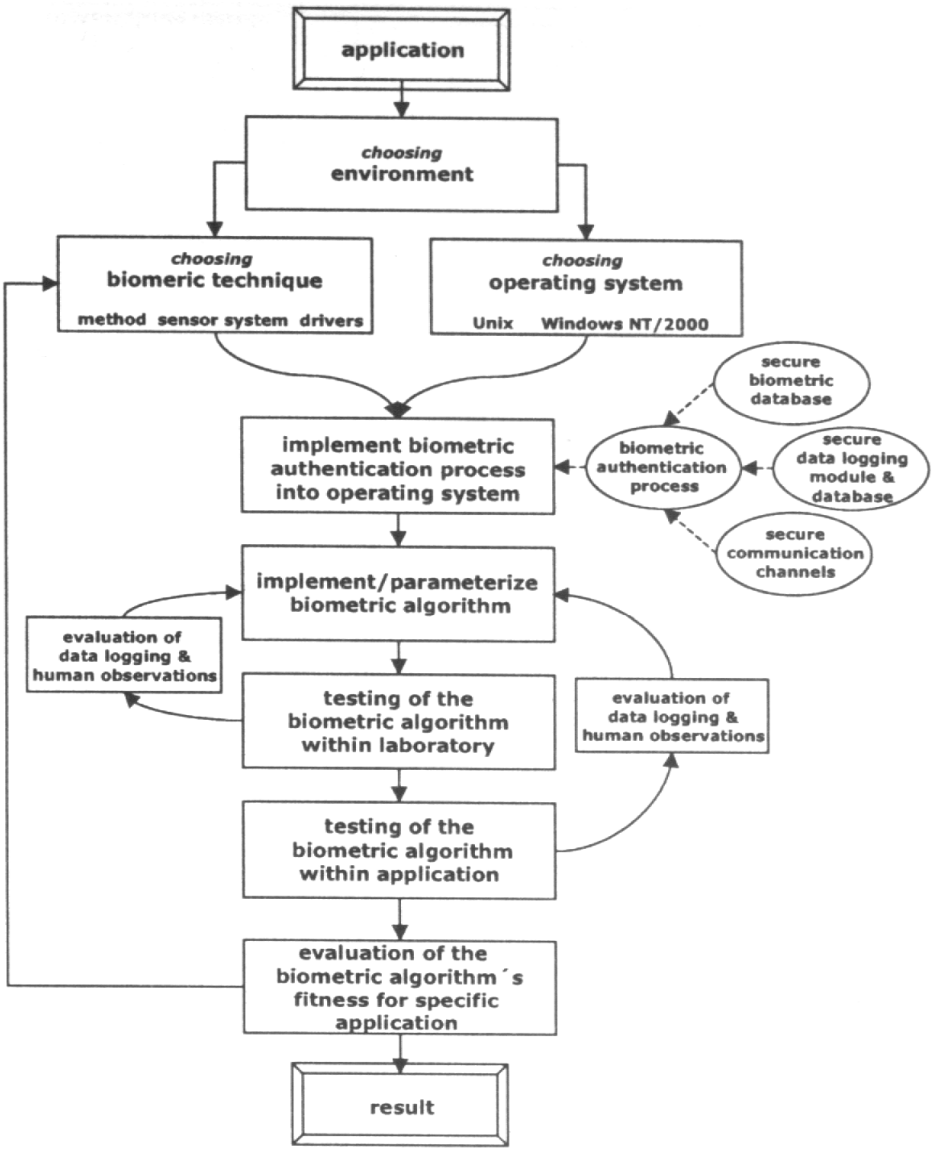


Abb.19: Konzeptuelles Rahmenwerk zum Testen biometrischer Verfahren

Im nächsten Schritt werden die in 5.1.1 und 5.1.2 genannten Elemente in das gewählte Betriebssystem integriert: Das Data Logging Modul, die sichere biometrische Datenbank, die sicheren Kommunikationskanäle und der ausgesuchte biometrische Algorithmus. Die ersten Tests und Auswertungen finden unter Laborbedingungen statt, mögliche Änderungen an der Implementierung werden durchgeführt.
Dann folgen Tests unter Realbedingungen, deren Ergebnisse wiederum zu Änderungen am Algorithmus oder an der Parametrisierung führen können. Nach mehreren Durchläufen wird ein endgültiges Testergebnis evaluiert und möglicherweise der gleiche Vorgang mit einer alternativen biometrischen Technik wiederholt, um bessere Ergebnisse zu erzielen. [Brömme et al, 2002]

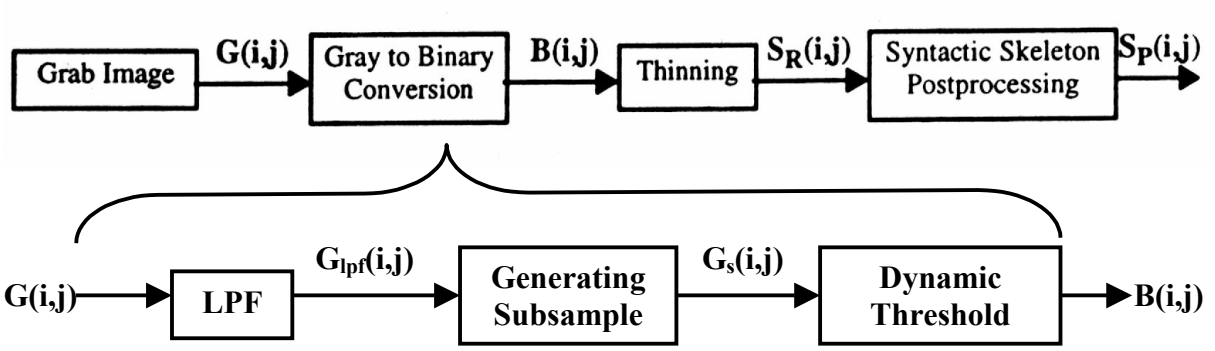
5.2 Einbindung der Verarbeitungsschritte bei der Fingerabdruckerkennung in die Testmodule

In diesem Abschnitt werden die in Kapitel 2 beschriebenen Methoden zur Fingerabdruckanalyse detaillierter dargestellt und in die Testmodule P, Q, S, D aus 5.1 eingeordnet. Die Module P, Q, S werden sowohl beim Einlernen (Enrollment), als auch bei jeder Identifikation und Verifikation durchlaufen, während das D-Modul zum Einlernen nichts beiträgt.

5.2.1 Preprocessing (P-Modul)

Das P-Modul erhält ein Graustufenbild als Eingabe. Dieses Bild muss vorverarbeitet werden, bevor eine Merkmalsextraktion durchgeführt werden kann. Das sogenannte Preprocessing umfasst laut [Jain et al, 1999] folgende Zwischenschritte (siehe Abb.20):

1. Bild aufzeichnen (Grab Image)
2. Umwandlung Graustufenbild → Binärbild (Gray to Binary Conversion)
3. Skelettierung (Thinning)
4. Nachbearbeitung (Syntactic Skeleton Postprocessing)



- **G(i,j) = Graustufenbild der Größe i x j**
- **G_{lpf}(i,j) = Graustufenbild nach Low-Pass-Filterung**
- **G_s(i,j) = Teilregion (Subsample) des Graustufenbildes**
- **B(i,j) = Binärbild**
- **S_R(i,j) = Skeleton Raw (skelettiertes Binärbild, nicht nachbearbeitet)**
- **S_P(i,j) = Skeleton Postprocessed (skelettiertes Binärbild, nachbearbeitet)**

Abb.20: Preprocessing

Der 4.Punkt (Nachbearbeitung) gehört bereits zum Q-Modul und wird daher erst in 5.2.2 erläutert [Jain et al, 1999].

5.2.1.1 Umwandlung eines Graustufenbildes in ein Binärbild

Hierbei wird zunächst eine Low-Pass-Filterung des Graustufenbildes G(i, j) durchgeführt. Das resultierende Bild G_{lpf}(i, j) enthält weniger Rauschen, ist dafür aber kontrastärmer geworden. Dann wird ein Bildausschnitt G_s(i, j) (Subsample) erstellt, um die sensorabhängigen Unterschiede in den Auflösungen auf eine normierte Größe (Anzahl der horizontalen und vertikalen Pixel) zu reduzieren:

$$G(i, j) \rightarrow G_{lpf}(i, j), \text{ wobei } 0 \leq i \leq X \text{ und } 0 \leq j \leq Y$$

$$G_{s,lpf}(i, j) = G_{lpf}(\alpha i, ß j), \text{ wobei } 0 \leq i \leq X/\alpha \text{ und } 0 < \alpha \leq 1$$

$$\text{sowie } 0 \leq j \leq Y/ß \text{ und } 0 < ß \leq 1$$

wobei X+1 und Y+1 für die Größe des Bildes stehen und α, ß die Faktoren sind, mit denen die gewünschte Normierungsgröße erlangt wird. Anschließend wird das Bild einer Schwellwert-Berechnung (Dynamic Thresholding) unterzogen. Das daraus entstehende Binärbild B(i, j) besteht dann nur aus schwarzen und weißen

Bildpunkten. Die Schwellwert-Routine teilt G_s in A x B große Teilstücke auf, die einzeln bearbeitet werden, wobei $1 \leq A \leq X$ und $1 \leq B \leq Y$ gilt.
Zunächst wird der durchschnittliche Pixelwert μ einer Subregion ermittelt und alle Pixel mit einem Grauwert > μ werden auf eins (schwarz) gesetzt und alle anderen auf 0 (weiß):

$$\mu_{mn} = \left(\sum_{j=nB}^{(n+1)B-1} \sum_{i=mA}^{(m+1)A-1} G_S(i,j) \right) / (AB) \quad \begin{array}{l} \text{, für m = 0,1,...,(X/A) – 1} \\ \text{, für n = 0,1,…,(Y/A) – 1} \end{array}$$

Beispiel: Ein 640 x 480 großes Bild G_S soll in Subregionen der Größe 160 X 120 (A x B) unterteilt werden. Das bedeutet, dass m und n die Werte 0, 1, 2, 3 durchlaufen und G_S in 16 Subregionen unterteilt wird:

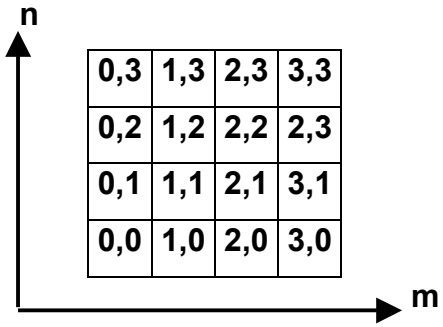


Abb.21: Beispiel für eine Aufteilung eines Bildes G_S in Subregionen

Der Durchschnittswert $\mu_{0,0}$ für die erste Subregion berechnet sich dann folgendermaßen:
Die äußere Summe geht von 0 bis 159 (j), die innere Summe von 0 bis 119 (i). Die Gesamtsumme aller 19200 Pixel wird dann durch 19200 (160 x 120) geteilt, um den Durchschnittswert $\mu_{0,0}$ zu erhalten.

Ein Binärbild repräsentiert das Originalbild meist sehr gut und bietet den Vorteil, dass es einfacher bearbeitet werden kann [Jain et al, 1999].

5.2.1.2 Skelettierung (thinning) des Binärbildes

Ein skelettiertes Bild entsteht durch Verkleinerung der Objekte eines Binärbildes bis sie nur noch ein Pixel breit sind. Es ist wichtig, dass dabei Verbindungen nicht unterbrochen werden und dass die morphologische Struktur des Originalobjekts erhalten bleibt. Die Merkmale eines ausgedünnten Bildes sind einfacher zu extrahieren als bei einem nicht skelettierten Binärbild. Im Binärbild eines Fingerabdrucks stellen die weißen Linien die Fingerabdruck-Täler und die Poren dar, die schwarzen Bereiche repräsentieren die Erhebungen. Wenn die Poren als Merkmal verwendet werden sollen, werden beim Thinning die weißen Strukturen vor einem schwarzen Hintergrund bearbeitet. Definierte Thinning-Bedingungen, die mehrfach auf alle Pixel angewendet werden müssen, führen schließlich zu einem skelettierten Bild S_R. Nach folgendem Schema werden dafür die Nachbarpixel p_1-p_8 eines zentralen Pixels p_0 definiert:

p_8	p_7	p_6
p_1	p_0	p_5
p_2	p_3	p_4

Abb.22: Das zentrale Pixel P_0 und seine Nachbarpixel P_1-P_8

Die Thinning-Bedingungen nach [Jain et al, 1999] lauten:

$$1)\ 1 < \Sigma(p_0) < 7$$
$$2)\ \tau(p_0) = 2$$
$$3)\ p_0 p_5 p_7 = 0 \text{ or } \tau(p_7) \neq 2$$
$$4)\ p_3 p_5 p_7 = 0 \text{ or } \tau(p_5) \neq 2,$$

Wobei Σ (p_0) die Summe der von 0 verschiedenen Nachbarn von p_0 und τ (p_0) die Anzahl der Pixelübergänge (Transitionen) der Nachbarn von p_0 darstellt (Summe der $0 \Leftrightarrow 1$ Übergänge in der geordneten Menge {p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_1} :

$$\Sigma(p_0) = \sum_{n=1}^{8} S(p_n)$$

$S(p_n)$ steht für den Wert des Pixels p_n im skelettierten Bild S.

$$\tau(p_0) = \left(\sum_{n=1}^{7} S(p_n) - S(p_{(n+1)})\right) + \left(S(p_8) - S(p_1)\right)$$

S wird anfangs mit dem Binärbild B gleichgesetzt. Dann werden mehrere Iterationen durchlaufen, bis sich trotz Anwendung der Thinning-Bedingungen keine Veränderungen mehr ergeben. Bei einem final ausgedünnten Bild sind die Strukturen genau ein Pixel breit und in der Mitte der Täler und Poren gelegen. Natürlich ist auch der umgekehrte Vorgang möglich: Thinning der dunkel dargestellten Erhebungen. Jedoch können dann die Poren nicht als Merkmale verwendet werden.

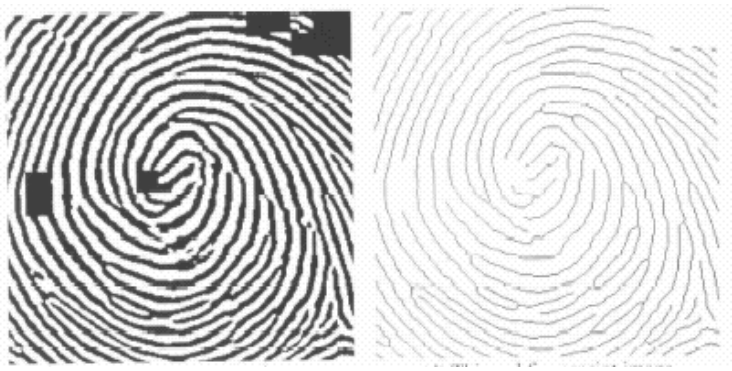


Abb.23: Thinning

In beiden Fällen gibt das P-Modul das skelettierte Bild S aus, das dann dem Q-Modul zur Qualitätsanalyse und Normalisierung übergeben wird. Je nachdem, ob die Täler oder die Erhebungen ausgedünnt werden, ergibt sich z.B. ein Endpunkt oder aber eine Verzweigung und umgekehrt (siehe Abb.24).

Abb.24: Endpunkt und Verzweigung

Die Skelettierung kann auch als Normalisierung aufgefasst werden. In diesem Fall gehört sie zum Q-Modul.

5.2.2 Qualitätsüberprüfung und Normalisierung (Q-Modul)

Das Q-Modul soll die Qualität des vorverarbeiteten Bildes analysieren und nach definierten Regeln eventuelle Fehler beseitigen, die bei der Bildaufnahme und dem Preprocessing entstehen können. Wenn zu viele störende Strukturen erkannt werden, kann das Modul den Authentikationsvorgang mit einer Zurückweisung oder Fehlermeldung abbrechen. Bei einem Fingerabdruck können Störungen durch Narben, Risse, zu trockene oder zu fettige Haut entstehen (vgl. 2.2.4).
Die folgende Abbildung 25 zeigt einige häufig auftretende Strukturen bei skelettierten Fingerabdruckbildern:

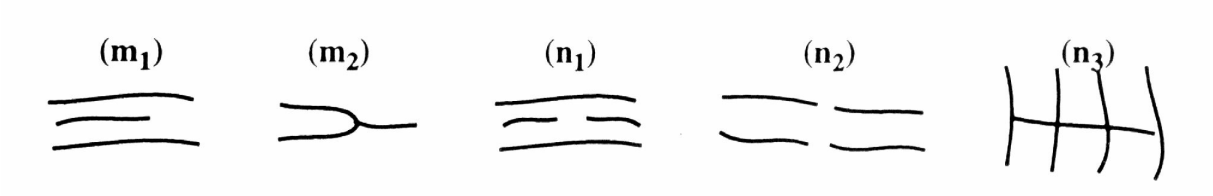


Abb.25: Typische Merkmalsstrukturen

Hinweis: Die Linien repräsentieren in diesem Fall Täler (nicht Erhebungen)!

m_1 und m_2 sind Minutienstrukturen (Verzweigung und Endpunkt), n_1-n_3 sind Problemstrukturen: n_1 ist ein Bruch in der Tallinie, der meistens durch Schmutz oder bei schlecht gewählten Schwellwerten entsteht. Bei n_2 scheint die Tallinie völlig verschwunden zu sein, ein typischer Effekt bei sehr fettigen oder feuchten Fingern. n_3 zeigt drei parallel verlaufende Erhebungen, die von einem Riss durchkreuzt werden, möglicherweise von einer Narbe oder einer Verletzung.
Um feststellen zu können, ob eine gegebene Struktur korrekt ist bzw. für eine Normalisierung repariert werden sollte, muss die nähere Umgebung jedes Endpunkts und jeder Verzweigung untersucht und ihre genaue Position und Ausrichtung bestimmt werden.

a) Reparatur unterbrochener Linienstrukturen
   Unter folgenden Voraussetzungen erfolgt eine Reparatur (Verbindung der Linien, Healing) :
   1. Der Abstand zwischen zwei Endpunkten e_0 und e_1 liegt unter einem definierten Schwellwert.

2. Die Endpunkte e_0 und e_1 laufen aufeinander zu, d.h. die Linienelemente, die zur Richtungsbestimmung eingesetzt wurden, haben die gleiche Ausrichtung. Wie bei 1. wird hierbei ein Schwellwert definiert (die tolerierte Winkelabweichung).

b) Entfernen von Rissen/Linien
   Die Linie in Abbildung 25 (n_3) stellt einen Riss dar, der die weitere Bearbeitung des Fingerabdrucks, insbesondere die Merkmalsextraktion stören würde und daher vom Q-Modul entfernt werden muss. Sie kann aber nur entfernt werden, wenn die folgenden Bedingungen erfüllt sind:

   1. Ein Verzweigungspunkt b_0 hat mindestens zwei benachbarte Verzweigungspunkte b_1 und b_2, welche beide nicht weiter von b_0 entfernt sind, als ein maximaler Abstandsschwellwert vorschreibt.
   2. Der Winkel eines Zweiges von b_1 muss 180 Grad (+/ - einem Schwellwert) betragen und muss sich in der Ausrichtung her von einem der beiden Punkte b_0 und b_1 unterscheiden.
   3. Die Verzweigungen müssen jeweils aufeinander zeigen oder nahe beisammen sein [Jain et al, 1999]

Es wäre sinnvoll, wenn das Q-Modul die Fingerabdruckbilder verschiedenen Qualitätsklassen zuordnet, da die unterschiedlichen Methoden, Merkmale zu extrahieren (siehe 5.2.3) und zu vergleichen (5.2.4), andere Qualitätsansprüche an das zu verarbeitende Bild stellen. Das zugeordnete und normalisierte Bild gibt das Q-Modul dann zur Signalverarbeitung an das S-Modul weiter.

5.2.3 Signalverarbeitung und Templateberechnung (S-Modul)

Das S-Modul extrahiert die für die Authentikation relevanten biometrischen Daten aus den vorverarbeiteten und normalisierten Signalen und berechnet das sogenannte „Template“ (biometrische Signatur). Im Falle der Fingerabdruckerkennung bezieht sich dieses auf die Extraktion der Minutien und/oder Poren und die Speicherung ihres Typs und ihrer Positionen im Template.

5.2.3.1 Techniken zur Extraktion von Minutien und Poren

Die Techniken zur Minutienextraktion unterscheiden sich nicht wesentlich von denen zur Extraktion von Poren. Hierbei ist der Ort eines Merkmals in einem gegebenen Fingerabdruck-Bild eine relevantere Information als Minutientyp/-ausrichtung oder Porengröße/-form.

Abbildung 26 a) zeigt einige Minutienarten:

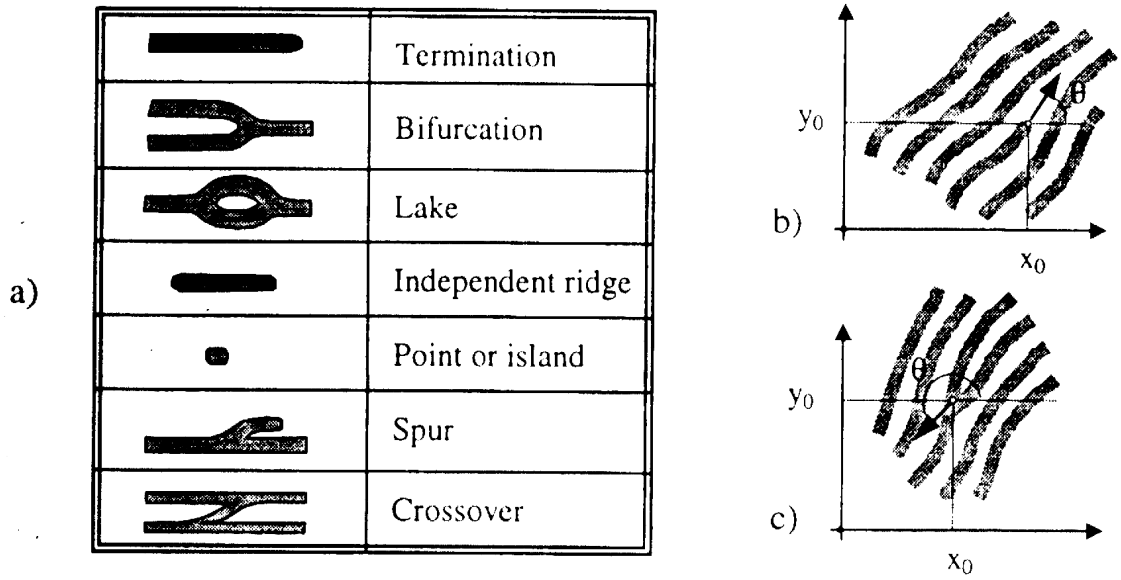


Abb.26: a) Minutienarten, b) Endpunkt, c) Verzweigung

In b) und c) markiert (x_0,y_0) die Position und θ bezeichnet den Winkel zwischen Minutien-Tangente und der X-Achse bei einem Endpunkt und einer Verzweigung. Bei einem gegebenen skelettierten Fingerabdruckbild werden zunächst einmal alle End- und Verzweigungspunkte bestimmt und gespeichert. Ein Endpunkt ist dabei definiert als ein weißes Pixel mit entweder einem oder keinem Nachbarn, ein Verzweigungspunkt hat genau drei Nachbarn. Alle anderen Skelettkomponenten

haben genau zwei Nachbarn und werden daher als Verbindungspunkte bezeichnet. Die Anzahl der gefundenen Endpunkte N_E und ihre Positionen $(x_{E,i}, Y_{E,i})$ für i=0,1,..., N_{E-1} sowie die Anzahl der Verzweigungspunkte N_B mit ihren Positionen $(x_{B,i}, Y_{B,i})$ für i=0,1,..., N_{B-1} werden zum Erstellen einer Minutienkarte gespeichert, die beim Vergleich verwendet wird.
Eine Möglichkeit, potentielle Minutien in einem ausgedünnten Bild zu entdecken, ist das so genannte „Tracking“. Bei dieser Methode wird jeder Endpunkt als Start eines Pfades verwendet, der entlang eines Liniensegments verläuft, bis eine der unten aufgeführten Abbruchbedingungen eintritt. Die Position der untersuchten Elemente (x_i, y_i) wird in einer Pfadvariablen P gespeichert. Die Abbruchbedingungen für das *Endpoint-Tracking* lauten:

(1) ein anderer Endpunkt wird erreicht
(2) ein Verzweigungspunkt wird erreicht
(3) die Pfadlänge L_{path} übersteigt eine definierte maximale Länge

Die Bedingungen (1) und (2) bedeuten, dass der untersuchte Abschnitt eine Pore ist. Wenn (1) die erfüllte Abbruchbedingung ist, dann wird die Position der Pore (x_p, y_p) durch folgende Gleichung berechnet:

$$x_p = \left(\sum_{i=0}^{L_{Path}-1} P(x_i) \right) / L_{Path} \qquad y_p = \left(\sum_{i=0}^{L_{Path}-1} P(y_i) \right) / L_{Path}$$

Es werden die durchschnittlichen Koordinaten der untersuchten Pfadelemente zur Positionsbestimmung verwendet.
Wenn (2) die erfüllte Abbruchbedingung ist, dann ist die Position der Pore gleich den Koordinaten des ersten Pfadelements (Endpunkt):

$$x_p = P(x_0) \qquad y_p = P(y_0)$$

Bedingung (3) bedeutet, dass der untersuchte Bereich einen gültigen Endpunkt des Fingerabdruck-Skeletts darstellt. In diesem Fall sind die Koordinaten des Punktes $P(x_0, y_0)$ bereits bekannt. Die Orientierung wird folgendermaßen berechnet:

$$\theta = \arctan\left(\frac{y_P - P(y_0)}{x_P - P(x_0)}\right)$$

wobei x_p und y_p wie bei Bedingung (1) berechnet werden.

Das Tracking wird mit allen Endpunkten durchgeführt und die gefundenen Poren in einer Porenkarte (poremap) gespeichert. Eine ähnliche Prozedur wird mit den Verzweigungspunkten durchgeführt, das Branchpoint-Tracking.
Die Abbruchbedingungen beim Branchpoint-Tracking sind:

(4) ein anderer Verzweigungspunkt wird erreicht
(5) ein Endpunkt wird erreicht
(6) die Pfadlänge der untersuchten Verzweigungen überschreitet einen Schwellwert

Wenn (4) die erfüllte Abbruchbedingung ist, wird der Abschnitt als Pore gespeichert. Es werden wiederum die Durchschnittskoordinaten des Abschnittes berechnet, der die Verzweigungen miteinander verbindet. Bedingung (5) sollte bereits durch das Endpoint-Tracking abgedeckt worden sein und Bedingung (6) heißt, dass ein validierter Verzweigungspunkt gespeichert wird. Die Position ist bekannt, für die Orientierung θ wird der Winkel des Zweiges verwendet, der sich am meisten von dem Winkel der anderen beiden Verzweigungen unterscheidet (Berechnung des Winkels θ wie bei Bedingung (3)).
Die gefundenen Poren werden nach dem Speichern entfernt (weiße Pixel des Porensegments werden zu schwarzen Pixeln konvertiert). Abbildung 27 zeigt ein Beispiel eines Fingerabdruckskeletts, dass von Poren befreit wurde:

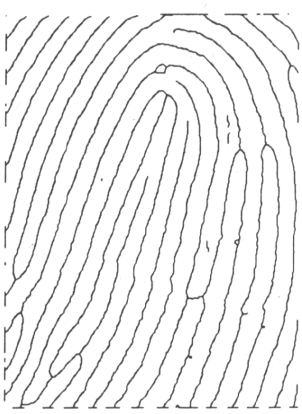


Abb.27: Fingerabdruckbild nach Branchpoint-Tracking und Entfernen der Poren

5.2.3.2 Segment-Extraktion für Korrelationsvergleich (correlation matching)

Ein Problem bei der Fingerabdruckerkennung ist die Tatsache, dass die Position ein und des selben Fingers bei jedem Scan unterschiedlich ist und die Plastizität des Fingers in einem zweidimensionalen Bild nicht dargestellt wird. Daher wurde der Korrelationsvergleich entwickelt, bei dem eine Menge von kleinen Bildabschnitten (Segmenten) extrahiert wird. Dabei werden nicht nur die Abschnitte selbst, sondern auch ihre relative Position zueinander gespeichert. Beim Vergleich werden dann die beim Enrollment gespeicherten Segmente mit dem Gesamtbild verglichen und die beste Übereinstimmung verwendet. Dafür sollten möglichst nur Segmente mit einzigartigen Linienmustern verwendet werden. Die Segmente sollten groß genug sein, um genügend Strukturen aufzuweisen, jedoch sollten sie nicht zu groß sein, damit die Plastizität des Fingers keinen negativen Einfluss auf das Ergebnis hat (siehe auch 5.2.4.1) [Jain et al, 1999].

Zusammenfassend kann man sagen, dass das S-Modul bei der Verwendung der hier beschriebenen Vorgehensweisen eine Minutienkarte, eine Porenkarte und die eben beschriebenen Segmente mit relativer Position zueinander berechnet und im Template speichert. Dieses Template, das während des Enrollment-Vorgangs erstellt wird, referenziert das D-Modul im Rahmen einer Authentikation (siehe Abb.28).

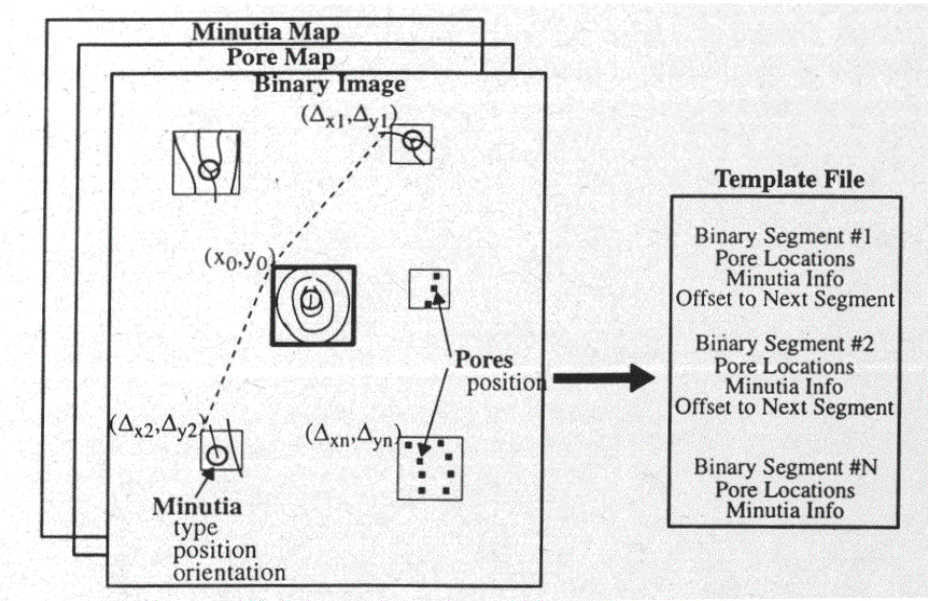


Abb.28 : Berechnung des Template-Files

5.2.4 Vergleich (D-Modul)

Das D-Modul kommt im Rahmen einer Identifikation bzw. Verifikation zum Einsatz. Das folgende Schema (Abbildung 29) zeigt eine Übersicht der Verarbeitungsschritte bei der Fingerabdruckerkennung:

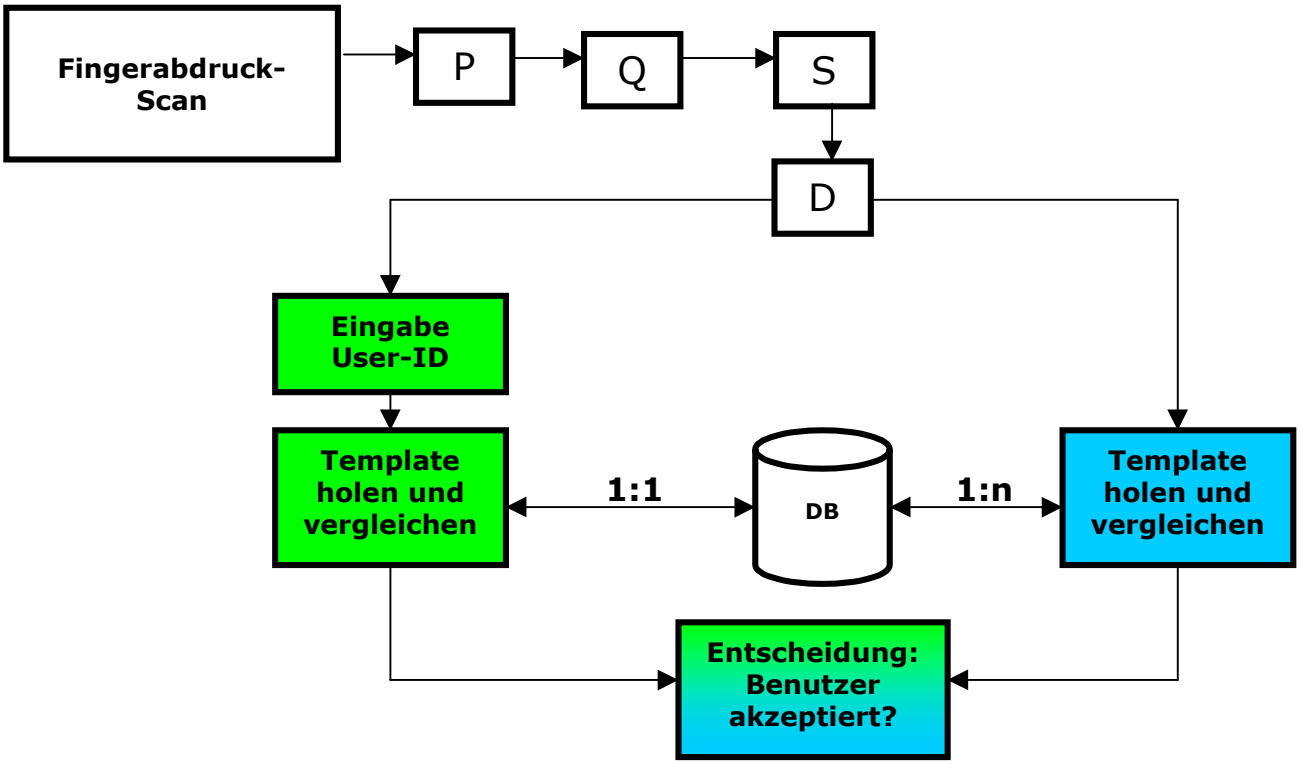


Abb.29: Verarbeitungsschritte bei der Fingerabdruckerkennung

Die farbig markierten Kästen gehören zum D-Modul, wobei grün für die Verifikation und blau für die Identifikation steht. Der Merkmalsvergleich kann beispielsweise ein Korrelationsvergleich (correlation matching) sein (5.2.4.1), oder ein Vergleich von Poren und/oder Minutien (5.2.4.2) oder eine Kombination aus Segment-, Poren- , und Minutienvergleich (multilevel verification, 5.2.4.3).
Der Vergleichs-Algorithmus, der angewendet wird, kann von der im Q-Modul bestimmten Qualitätsklasse des Fingerabdruckbildes abhängen, um die größtmögliche Performanz zu gewährleisten. Bei sehr guten Fingerabdruckbildern reicht es aus, ein Minutienvergleich durchzuführen. Sehr schlechte Bilder sollten einen Korrelationsvergleich durchlaufen, und Bilder, die einige qualitativ gute Abschnitte aufweisen, sollten mit einer Kombination der Möglichkeiten bearbeitet werden (multilevel verification) [Jain et al, 1999].

5.2.4.1 Korrelationsvergleich (correlation matching)

Beim korrelationsbasierten Vergleich wird ein Vergleichsergebnis $S_{S,i}$ (segment matching score) für jedes im Template abgespeicherte Segment i berechnet. Das Ergebnis $S_{S,i}$ wird nach der Qualität des Segments und des Live-Scans gewichtet. Schließlich wird ein Gesamtergebnis S_S ermittelt, das die einzelnen Ergebnisse des Segment-Vergleichs kombiniert und für die Entscheidung verwendet wird:

$$S_S = \left(\sum_{i=0}^{N_S - 1} S_{S,i} \right) / N_S$$

wobei N_S die Anzahl der verwendeten Bildsegmente ist. S_S liegt im Intervall [0,1]. 1 bedeutet perfekte Übereinstimmung. S_S repräsentiert einen durchschnittlichen Messwert dafür, wie gut die Template-Segmente mit den Segmenten des Live-Scans übereinstimmen und ist dabei nicht von vorhandenen Minutien abhängig und fast unabhängig von Poren. Ein weiteres und wichtigeres Ergebnis des Korrelationsvergleichs ist die Positions-Information. Kleine Segmente können schrittweise mit dem gesamten Live-Scan verglichen werden, wobei die Position mit der größten Übereinstimmung gespeichert wird. Diese Konstellation kann dann für den Vergleich verwendet und ein Positionsvergleichs-Ergebnis S_L errechnet werden. Je größer der Wert für S_L, desto akkurater ist die Übereinstimmung zwischen den Template-Informationen und dem Live-Scan [Jain et al, 1999].

5.2.4.2 Poren- und Minutienvergleich (pore and minutia matching)

Wie bereits erwähnt werden Typ, Position und Ausrichtung der Minutien, sowie die Position von Poren (relativ gesehen zu Minutien oder Korrelationssegmenten) beim Enrollment im Template gespeichert. Beim Porenvergleich werden diese gespeicherten Segmente oder Minutien als Ursprung für die Ausrichtung verwendet und mit dem Live-Scan verglichen. Nach der Ausrichtung wird überprüft, ob die Poren des Live-Scans an den im Template registrierten Positionen existieren oder nicht. Das Porenvergleichs-Ergebnis S_P ist das Verhältnis von Anzahl der bestätigten Poren zur Anzahl der beim Enrollment gespeicherten Poren:

$$S_P = \left(\sum_{\mathrm{i}=0}^{N_S - 1} N_{MP,\mathrm{i}} \right) \Big/ \left(\sum_{i=0}^{N_S - 1} N_{P,i} \right)$$

wobei $N_{P,i}$ die Anzahl der Poren des Template-Segments i ist und $N_{MP,i}$ die Anzahl der Übereinstimmungen in i. Abbildung 30 zeigt ein Beispiel für poren- und minutienbasierten Vergleich zwischen zwei Segmenten von unterschiedlichen Fingern und zwei Segmenten des selben Fingers:

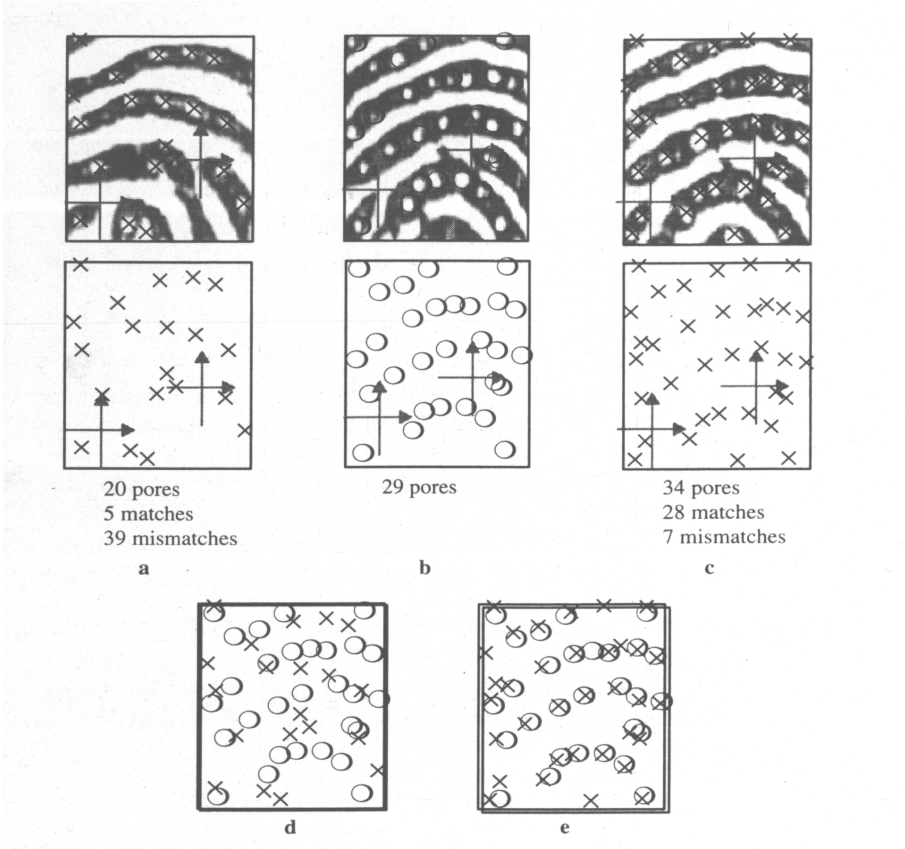


Abb.30: Poren– und minutienbasierter Vergleich von Fingerabdrucksegmenten

Die Segmente b und c sind vom selben Finger, a ist von einem anderen Finger. In a und b sind zwei sehr ähnliche Endpunkt-Minutien vorhanden, die bei ausschließlicher Verwendung von minutienbasiertem Vergleich als übereinstimmend bewertet werden. Wenn aber die Minutien nur zur Ausrichtung der Segmente verwendet und die Poren verglichen werden, stimmen nur b und c überein (siehe e) und nicht a und b (siehe d).
Der Minutienvergleich ähnelt im Prinzip dem eben beschriebenen Porenvergleich. Der Typvergleich ist eine binäre Entscheidung (Endpunkt oder Verzweigung), der Ort und die Ausrichtung dagegen erlauben geringe Abweichungen. Zwingend bezüglich des Ortes kann es beispielsweise sein, dass ein Minutienpunkt des Live-Scans innerhalb des Bildbereichs liegen muss, der mit dem abgespeicherten Segment korrespondiert.
Die Richtungsvorschrift beim Vergleich könnte lauten, dass der Rotationswinkel innerhalb von 45 Grad des abgespeicherten Minutienwinkels liegen muss, um eine Übereinstimmung zu erzielen. Das Minutienvergleichs-Ergebnis S_M ist das Verhältnis aus übereinstimmenden Minutienpunkten $N_{MM,i}$ des Segments i zur Gesamtzahl der Minutien $N_{M,i}$ des im Template gespeicherten Segments i:

$$S_M = \left(\sum_{i=0}^{N_S - 1} N_{MM,i} \right) / \left(\sum_{i=0}^{N_S - 1} N_{M,i} \right)$$

Diese Merkmale und Ergebnisse können zusätzlich nach Qualität und Einzigartigkeit gewichtet werden [Jain et al, 1999].

5.2.4.3 Multilevel-Verifikation (multilevel verification)

Multilevel-Verifikation steht für eine Kombination mehrerer Vergleichstechniken, aus der eine Menge von Vergleichsergebnissen resultiert:

- Ein Ergebnis S_S des Segmentsvergleichs
- Ein Ergebnis S_L des Segmentpositionsvergleichs
- Ein Ergebnis S_M des Minutienvergleichs
- Ein Ergebnis S_P des Porenvergleichs

Für jedes Ergebnis wird ein Schwellwert T_X definiert:

- $S_S >= T_S$
- $S_L >= T_L$
- $S_M >= T_M$
- $S_P >= T_P$

Außerdem kann definiert werden, wie viele und welche Resultate über dem Schwellwert liegen müssen, damit ein Benutzer akzeptiert wird oder nicht. Die Schwellwerte können verändert werden, um die Fehlerraten bzw. die Performanz des Systems anzupassen [Jain et al, 1999].

Als Ergebnis gibt das D-Modul aus, ob der Fingerabdruck des Benutzers akzeptiert oder zurückgewiesen wird.

6. Diskussion

Diese Studienarbeit hat gezeigt, welche Aufgaben bei der Merkmalsanalyse von Fingerabdrücken gelöst werden mussten und welche Probleme noch immer vorhanden sind. Viele Hersteller kommerzieller Fingerabdrucksensoren preisen ihre Produkte als fälschungssicher an und garantieren, dass die Benutzung zu einer Erhöhung der Sicherheit und des Bedienskomforts führt. Dies trifft hinsichtlich der Sicherheit nur teilweise zu, denn die in Kapitel 4 beschriebenen Experimente mit dem Fingerabdruckscanner und die Ergebnisse von Matsumoto haben ganz deutlich gezeigt, dass nicht alle Produkte so sicher sind, wie ihre Hersteller behaupten. Es zeigt sich vielmehr, dass bisher versäumt worden ist, geeignete Tests durchzuführen. Das in dieser Arbeit auf die Fingerabdruckerkennung angewendete Testrahmenwerk für biometrische Algorithmen könnte hierfür einen Beitrag leisten.
Die Anwendung des Rahmenwerks ermöglicht es, anhand der gespeicherten Logdaten die Verarbeitungsschritte genauer zu verfolgen und bei problematischen Fingerabdrücken sehen zu können, in welcher Phase der Algorithmus nicht die geplante Leistung erbringt. Dadurch wird es möglich, gezielt Veränderungen vorzunehmen, deren Auswirkungen wiederum getestet werden können. In welcher Phase gehen wichtige Informationen (beispielsweise Minutien) verloren bzw. hinzugefügt?
Insbesondere Matsumotos Ergebnisse machen deutlich, wie wenig Aufwand nötig ist, um ein System zu täuschen. Die Anwendung des Testrahmenwerks kann dabei helfen, robustere Verfahren zu entwickeln. Beispielsweise kann so analysiert werden, ob die künstlichen Finger Poren aufweisen. Das könnte im Q-Modul untersucht werden. Wenn ein Live-Scan zu detailliert und kontrastreich ist, so dass kaum noch Vorverarbeitung nötig ist, deutet dies ebenfalls darauf hin, dass kein echter Finger verwendet wurde. In diesem Fall könnte bereits dass P-Modul den Authentikationsvorgang beenden. Bei dem in 4.1 beschriebenen Test eines Fingerprint-Sensors wäre die Toner-Kopie des registrierten Abdrucks eventuell zurückgewiesen worden. Weiterhin lassen sich mit Hife des Rahmenwerks feststellen, welche Auswirkungen Schäden (z.B. Verletzungen, Narben oder extrem trockene oder fettige Haut) auf die FAR/FRR eines biometrischen Algorithmusses haben. Eventuell wird dabei sogar deutlich, dass der Algorithmus nicht weiter verbessert werden kann.

Da Fingerabdrücke beinahe überall entnommen und zur unberechtigten Authentisierung eingesetzt werden können, ist es für einen Angreifer kein Problem, auf diesem Wege Datenspionage zu betreiben oder andere Schäden anzurichten. Das Design identifizierender biometrischer Systeme (vgl. Kapitel 4) erleichert dem Angreifer den Zugriff, da die Verifikationsinformation nicht erforderlich ist.
Allgemein ist es erforderlich, eine ausführliche Risikoanalyse durchzuführen, um u.a. zu klären:

- Was möchte ich sichern?
- Wie groß wäre der Schaden bei einem Missbrauch?
- Welche Schutz-Maßnahmen sind für mich geeignet?
- Wie groß ist das Restrisiko?
- Welche Notfallprogramme muss ich vorbereiten?

Eine Kombination mehrerer Sicherheitsverfahren kann in vielen Fällen eine adäquate Lösung sein, um das Restrisiko so klein wie möglich zu halten. Es könnten beispielsweise mehrere biometrische Authentikationsmethoden gleichzeitig oder hintereinander ausgeführt werden: Gesichtserkennung mit Sprecherkennung, Iriserkennung und Fingerabdruck, nachdem ein sich dem System nähernder Mensch zusätzlich am Gang identifiziert wurde. Das scheint auf dem ersten Blick übertrieben zu sein, die Benutzerfreundlichkeit wird dabei aber kaum eingeschränkt, da dies ein Vorgang ohne große Unterbrechungen wäre: Auf die Kamera zugehen, hineinschauen und gleichzeitig den Finger auf einen Sensor legen. Möglich ist auch eine Kombination von biometrischen Authentikationsverfahren mit anderen bekannten Verfahren (Wissen, Besitz, Ort und Zeit): Die biometrische Signatur eines Fingerabdrucks auf einer Chipkarte, die in einen Kartenleser geschoben wird und mit den Daten des Live-Scans verglichen wird.
Viele Fingerabdruck-Verfahren vernachlässigen die Charakteristik der Poren, obwohl diese, wie in Kapitel 5 beschrieben, durchaus zur Fehlervermeidung (FAR/FRR) beitragen können. Allerdings müssen bei dieser Methode qualitativ gute, hochauflösende Bilder erzeugt werden, um ausreichend viele Poren aufnehmen zu können.

Die Biometrik hat in den letzten Jahren immer mehr an Bedeutung gewonnen (siehe Kapitel 1). Abbildung 31 zeigt, dass die Umsätze in der Branche stark gewachsen sind und in Zukunft weiter ansteigen werden.

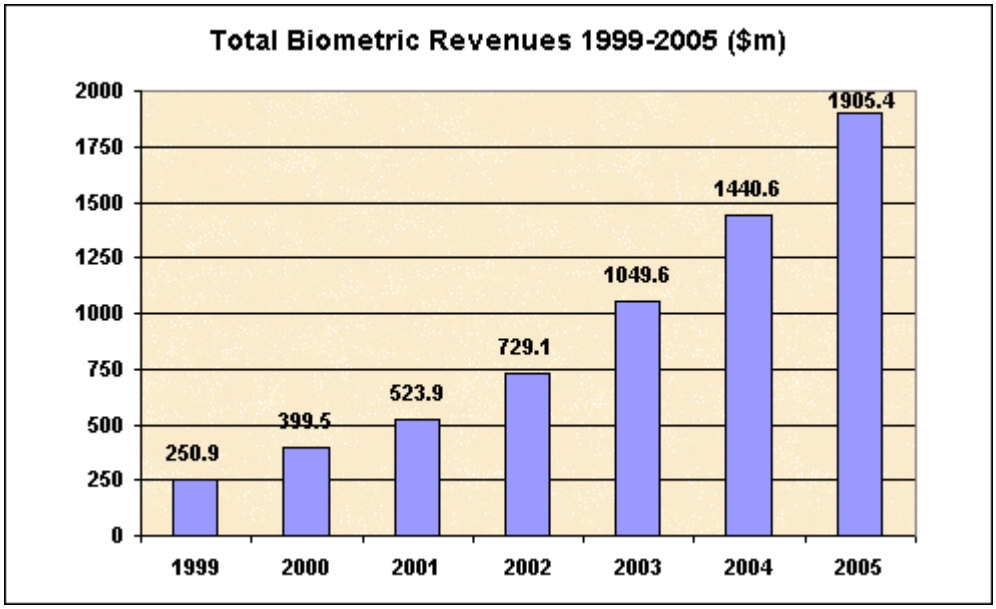


Abb.31: Umsätze in der Biometrik-Branche in US-Dollarmillionen von 1999-2005

Mit der wachsenden Verbreitung steigen auch die Anforderungen sowohl an Benutzerfreundlichkeit, Performanz als auch an die Fälschungssicherheit.

7. Zusammenfassung und Ausblick

Ich habe in dieser Studienarbeit die Grundlagen der Fingerabdruckerkennung und Grundbegriffe der Biometrik erläutert, sowie den schematischen Aufbau des Logon-Systems der Betriebssysteme Windows NT/2000/XP beschrieben (Kapitel 2 und 3). In Kapitel 4 habe ich anhand eines persönlich durchgeführten Versuchs und anhand der Versuche des Japaners Matsumoto gezeigt, dass die meisten kommerziellen Fingerabdruck-Sensoren angreifbar sind. In Kapitel 5 habe ich ein konzeptuelles Rahmenwerk zum Testen biometrischer Verfahren beschrieben, das von Mitgliedern der Biometric Authentication Research Group an der Universität Hamburg erarbeitet wurde. Ich zeigte dann, wie die Fingerabdruckerkennung in dieses Rahmenwerk integriert werden kann. In Kapitel 6 wird deutlich, dass die meisten Hersteller von Fingerabdrucksystemen die Sicherheit und die Testverfahren deutlich verbessern müssen.

Zum Schluss möchte ich einen Ausblick auf weitere Arbeitsmöglichkeiten im Themenbereich Fingerabdruckerkennung geben und erläutern, was ich im Laufe der Arbeit aus Zeitgründen weggelassen habe und möglicherweise in meiner Diplomarbeit ausführlicher behandeln werde.
Es bietet sich an, die in Kapitel 2 und 5 beschriebenen Verfahren zur Merkmalsanalyse von Fingerabdrücken im Rahmen einer Diplomarbeit zu implementieren. Dazu wird es nötig sein, eine ausreichend große Anzahl von Fingerabdruckbildern in einer Datenbank zu speichern, um die implementierten Verarbeitungsschritte ausreichend testen zu können. Die Aufnahmen müssen nicht unbedingt durch aufwendiges Scannen gesammelt werden, sondern können auch mit Hilfe von bereits existierenden Programmen generiert werden. An der Universität von Bologna wurde das Programm „SfinGe (Synthetic FINgerprint Generator)“ entwickelt, bei dem man mehrere Parameter einstellen kann, mit deren Hilfe eine Aufnahme eines Abdrucks erzeugt wird. Es können auch bewusst „Fehler“ (Narben, fettige Finger, etc.) eingebaut werden (siehe Abbildung 32).

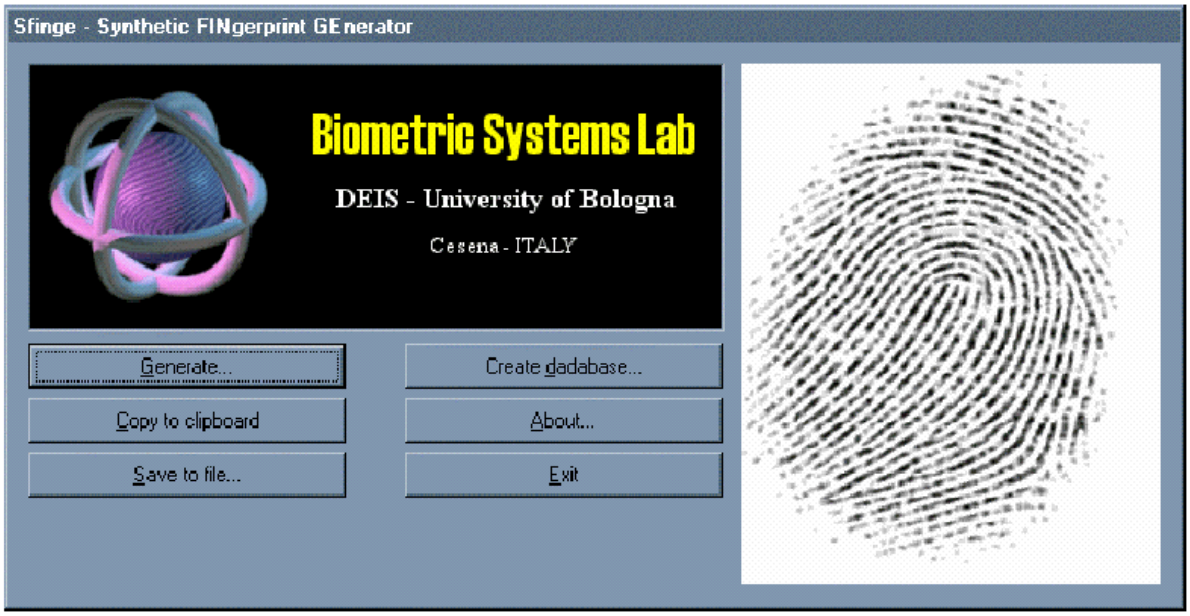


Abb.32: Screenshot von „SfinGe“

Das Testen sollte mit Hilfe des Rahmenwerks zum Testen biometrischer Algorithmen durchgeführt werden. Dabei wäre eine Aufteilung des Programms in Module, wie sie beispielsweise in Kapitel 5 vorgenommen wurde, sinnvoll.

Weiterhin konnte ich das Thema „Gabor-Filter“ und „Wavelets“ nur grundsätzlich erwähnen, da eine tiefergehende Behandlung des Themas zu weit geführt hätte. Das gleiche gilt für den in Kapitel 2 genannten Ansatz, die Merkmalsanalyse mit Hilfe von Neuronalen Netzen zu gestalten. Die Anwendbarkeit von Wavelets und Neuronalen Netzen für biometrische Algorithmen wird gegenwärtig von Mitgliedern der Biometric Authentication Research Group in Studien-, Diplomarbeiten und einer Dissertation behandelt.
Allgemein bietet die Biometrik noch viele Forschungsmöglichkeiten, da sie ein sehr junges Forschungsgebiet ist und die zunehmende Verbreitung das Interesse an neuen Ergebnissen steigern wird.

A: Literaturverzeichnis

[Baldi/Chauvin, 1993]
Baldi, P., Chauvin, Y.
„Neural Networks for Fingerprint Recognition“
1993

[Bindrich, 1995]
Vortrag
„Kerberos Authentifikation“
Anja Bindrich, 1995
http://wwwbs.informatik.htw-dresden.de/svortrag/ai95/Bindrich/kerberos.html

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

[Biometric Authentication Research Group, 2002 b]
Biometric Authentication Research Group, University of Hamburg
http://agn-www.informatik.uni-hamburg.de/people/broemme/arslan.htm

[Biometrika, 2001]
„Introduction To Fingerprints“
Biometrika, Italien
http://www.biometrika.it/eng/wp_fingintro.html

[Brömme et al, 2002]
SAC 2002, Madrid:
„A Conceptual Framework for Testing Biometric Algorithms within Operating Systems' Authentication“
Arslan Brömme, Marcel Kronberg, Oliver Ellenbeck, Oliver Kasch
Universität Hamburg, 2002
http://agn-www.informatik.uni-hamburg.de/people/broemme/arslan.htm

[Brömme, 2001 a]
Vorlesungsfolien
„Biometrische Logons für Windows NT/2k/XP“
Arslan Brömme, Dezember 2001, Universität Hamburg, Fachbereich Informatik
http://agn-www.informatik.uni-hamburg.de/people/broemme/arslan.htm

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

[Cavanaugh, 2000]
Homepage von John Cavanaugh, M.D.
„Chapter18: Forensic Medicine And Molecular Biology"
Bioengineering Center, Wayne State University Detroit
http://ttb.eng.wayne.edu/~cavanau/ch18lec5030w2000.html

[DLR/Institute of Robotics and Mechatronics, 2002]
Praktikumsarbeit:
„Erkennung natürlicher Landmarken durch Vergleich von Gaborspektren",
DLR-Institute of Robotics and Mechatronics
http://www.robotic.dlr.de/MOBILE/gabor1.html

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

[Erol, 1998]
Erol, A.
„Automated Fingerprint Recognition"
Ph.D. Thesis Proposal Report, Dept. of Electrical and Electronics Eng.,
Middle East Technical University, Ankara, 1998

[Ferrari/Schmid, 1998]
Homepage des Instituts für Internet Technologien und Anwendungen der Hochschule Rapperswil, Schweiz
Tutorial Netzwerksicherheit (Wintersemester 1998)
http://www.ita.hsr.ch/studienarbeiten/arbeiten/WS98/SecurityTutorial/verschluesselung.html

[Fu/Moaver, 1986]
Moaver, B., Fu, K.S.
„ A Tree System Approach for Fingerprint Recognition " 1986

[Galton, 1892]
Galton, F.
„Fingerprints"
Macmillan, London, 1892

[Hanson/Maio, 1997]
Maio, D., Hanson, A.R.
„Direct Gray-Scale Minutiae Detection in Fingerprints"
1997

[Henry, 1900]
Henry, E.R.
„Classification And Uses Of Fingerprints"
Routledge, London, 1900

[Hung, 1993]
Hung, D.C.D.
„Enhancement and Feature Purification of Fingerprint Images“
1993

[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)

[Isenor/Zaky, 1986] Isenor, D.K., Zaky, S.G.
„Fingerprint Identification Using Graph Matching“ 1986

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

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

[Matsumoto, 2002]
Homepage der Yokohama National University, Graduate School of Environment and Information Sciences
„Impact of Artificial "Gummy" Fingers on Fingerprint Systems”
Tsutomu Matsumoto, 2002
http://cryptome.org/gummy.htm

[Microsoft Developer’s Libary, 2001]
„Microsoft Developer’s Library”
http://msdn.microsoft.com

[Microsoft Platform SDK, 2001]
„Microsoft Platform Software Development Kit”
ftp://ftp.microsoft.com/developr/platformsdk

[Nickeron und O’Gorman, 1989]
Nickeron, J.V., O’Gorman, L.
„An Approach to Fingerprint Filter Design“ 1989

[Ratha/Karu/Shayon/Jain, 1996]
Ratha, N.K., Karu, K., Shayoun, C., Jain, A.K.
„A Real-Time Matching System for Large Fingerprint Databases“ 1996

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

[Schmidt, 2001]
Jeff Schmidt
„Windows 2000 Security: Kryptografie, Kerberos, Authentifizierung“
Markt+Technik Verlag, München, 2001

[Tecchannel, 2002]
„Vor – und Nachteile der Biometrie“
Verfasser: Tecchannel
http://www.tecchannel.de/software/824/0.html

[Wilson, 1993]
Wilson, G.L., Candela, G., Grother, P.J., Watson, C.I. and Wilkinson, R.A.
„Neural Network Fingerprint Classification“ 1993

B: Abbildungs-und Tabellenverzeichnis

C: Plakat „Testmodule für die Fingerabdruckerkennung”