Praktische Anwendbarkeit künstlicher neuronaler Netze für die Gesichtserkennung in der biometrischen Authentikation

Betreuer
Prof. Dr. Klaus Brunnstein

Studienarbeit vorgelegt von
Aleksander Koleski

Dezember 2002

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

Inhaltsverzeichnis

1 Einleitung

1.1 Vorwort

In dieser Arbeit behandle ich das Thema, in wie weit künstliche neuronale Netze für die Gesichtserkennung verwendet werden können. Dabei möchte ich speziell klären, ob sie sich für die praktische Anwendung in der biometrischen Authentikation eignen, und deren Vorteile und Nachteile aufzählen. Dazu beantworte ich u.a. folgende Fragen:

- Was ist biometrische Authentikation?
- Welche Anforderungen werden in der biometrischen Authentikation gestellt?
- Was muss ein System leisten, welches biometrische Authentikation durchführt?
- Was ist Gesichtserkennung?
- Wie lässt sich die Gesichtserkennung in der biometrischen Authentikation verwenden?
- Was sind künstliche neuronale Netze?
- Wie können künstliche neuronale Netze für die Gesichtserkennung verwendet werden?
- In wie weit lassen sich künstliche neuronale Netze in der biometrischen Authentikation praktisch anwenden?

Ich möchte mich auf diesem Wege bei Herrn Prof. Brunnstein für die Betreuung bedanken. Mein Dank geht auch an Arslan Brömme, der mich bis zum 30. September mitbetreut hat.

1.2 Überblick

- **Kapitel 2 - Grundlagen:** Für den Einstieg in das Thema Biometrik führe ich zunächst grundlegende Begriffe und Definitionen auf. Im Anschluss beschreibe ich wie man einen biometrischen Algorithmus bewerten kann und wie die Mustererkennung in der biometrischen Authentikation erfolgt. Dann gebe ich eine Einführung in die Gebiete Neuronale Netze und Gesichtserkennung.
- **Kapitel 3 - Untersuchung verschiedener künstlicher neuronaler Netze bezüglich Eignung für die Gesichtserkennung, insbesondere durch die Simulation von**

künstlichen neuronalen Netzen: In diesem Abschnitt sollte eigentlich eine Simulation durchgeführt werden, die dann aber aus Mangel an Zeit nicht durchführbar war.

- **Kapitel 4 - Bewertung und Integration von KNN gestützten Gesichtserkennungsverfahren:** Hier wird erläutert, wie man generell künstliche neuronale Netze in den Prozess der biometrischen Authentikation integrieren kann. Außerdem wird erläutert, wie man künstliche neuronale Netze in das Rahmenwerk von [Brömme2002] integrieren kann.
- **Kapitel 5 - Ergebnisse und Diskussion:** Hier fasse ich noch mal zusammen, welche Ergebnisse bei dieser Studienarbeit entstanden sind, und ob sich künstliche neuronale Netze für die Gesichtserkennung in der biometrischen Authentikation generell eignen.
- **Kapitel 6 - Zusammenfassung und Ausblick:** Anhand der Zusammenfassung lässt sich ein Ausblick machen, welche Themen noch bearbeitet werden könnten.

2 Grundlagen

2.1 Grundbegriffe

2.1.1 biometrische Signatur

Biometrische Signaturen werden gebraucht, um die biometrischen Merkmale von Personen in einer Datenbank vorzuhalten. Es ist per Gesetz nicht erlaubt, vollständige biometrische Merkmale, z.B. Fotos von Gesichtern, in einer Datenbank abzuspeichern. Außerdem ist es sinnvoll eine Datenreduktion der biometrischen Merkmale durchzuführen, da man sonst viel

- **Speicherplatz** benötigt für die Originalaufnahmen und viel
- **Rechenzeit** benötigt für den Vergleich der aktuellen Aufnahme, mit der, in der Datenbank.

Aus diesen Gründen führt man eine Datenreduktion mit Hilfe von Merkmalsextraktions-verfahren durch (siehe Kapitel 2.4.4). Es folgt nun eine Definition der biometrischen Signatur:

biologisches Merkmal (BioL):

- Statisch-, dynamisch-physiologisches sowie Verhaltenscharakteristikum eines Lebewesens **[Brömme2001a]**

Aus einem biologischen Merkmal wird durch Scanning und Capturing ein biometrisches Merkmal. **[Brömme2001a]**

biometrisches Merkmal (BioM):

- Erfasstes biologisches Merkmal (BioL) für die computergestützte Verarbeitung **[Brömme2001a]**

Eine Hashfunktion macht aus einem biometrischen Merkmal eine biometrische Signatur **[Brömme2001a].**

Dafür können verschiedene Merkmalsextraktionsverfahren verwendet werden. Weiter unten in Kapitel 2.4.4 erfolgt eine Beschreibung der gängigsten Verfahren.

biometrische Signatur (BioS):

- Bitfolge, die das biometrische Merkmal in Informatiksystemen repräsentiert **[Brömme2001a]**

2.1.2 Biometrik

Um den Begriff Biometrik zu definieren wird erst mal der Begriff Biometrie eingeführt. Zu unterscheiden bei der Definition der Biometrie ist einmal der populäre Ansatz und die fachliche Definition:

Populärer Ansatz:

Definition 1: Biometrie (nach [Duden1995]) :

- Wissenschaft von der Zählung und [Körper]messung an Lebewesen; biologische Statistik;
- Zählung und [Körper]messung an Lebewesen.

Fachliche Definition:

Definition 2: Biometrie (nach [Lorenz1996]) :

- 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! [Lorenz1996]

Nachfolgend wird der Begriff Biometrik definiert. Dieser Begriff setzt sich zusammen aus Biometrie und Metrik:

Definition 3: Biometrik (= Biometrie + Metrik) :

- 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 **[Brömme2001a]**:

2.1.3 biometrische Identifikation

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) **[Brömme2001a]**

In der biometrischen Identifikation wird also ermittelt, um welche Person es sich handelt. Dabei wurde **vorher** die zu identifizierende Person in das System eingelernt (Enrollment). Während des Einlernens wird eine biometrische Signatur aus einem biometrischen Merkmal (z.B. vom Gesicht) erzeugt und in eine Datenbank abgespeichert. Bei der biometrischen Identifikation wird z.B. von dem aktuellen Kamerabild ein Gesicht aufgenommen und daraus eine „aktuelle“ Signatur erzeugt. Diese „aktuelle“ Signatur wird dann mit allen Signaturen in der Datenbank verglichen und die „ähnlichste“ Signatur (wobei der Ähnlichkeitsgrad eingestellt werden kann) führt zur Identifizierung der Person. Falls keine der gespeicherten Signaturen hinreichend ähnlich ist, kann keine Identifikation erfolgen. Dann ist die Person dem System unbekannt.
Für die biometrische Identifikation muss ein Kompromiss eingegangen werden zwischen Genauigkeit und Schnelligkeit des Vergleichens bzw. Suchens.

Fallbeispiel für die biometrische Identifikation - Kaufhaus:

Es sollen registrierte Kleinkriminelle in einem Kaufhaus ausfindig gemacht und mit der Kamera verfolgt werden. Dazu überwachen mehrere Kameras das Kaufhaus. Aus den Kamerabildern werden von einem Computersystem laufend Signaturen erstellt, und mit Signaturen aus der Datenbank verglichen. Diese Datenbank wurde vorher mit biometrischen Signaturen von Gesichtern (denn Bilder von Gesichtern dürfen aus datenschutzrechtlichen Gründen nicht abgespeichert werden) von Kleinkriminellen gefüllt, die von der Polizei zur Verfügung gestellt wurden. Ist die „aktuelle“ biometrische Signatur

der gespeicherten hinreichend ähnlich, kann das Kamerasystem dazu veranlasst werden, den Kleinkriminellen weiterhin aufzunehmen bzw. zu verfolgen, um mögliche Diebstähle sofort registrieren zu können.

2.1.4 biometrische Verifikation

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) **[Brömme2001a]**

In der biometrischen Verifikation wird nun ermittelt, ob eine Person, die sich als Person X ausgibt, wirklich Person X ist. Dabei sei erwähnt, dass es sich wieder um Wahrscheinlichkeiten handelt. Es wird also betrachtet, wie ähnlich die „aktuelle“ biometrische Signatur mit der ist, die in der Datenbank abgespeichert wurde für Person X. Dabei müssen aber nicht alle Datensätze der Datenbank für den Vergleich hinzugezogen werden, sondern nur der Datensatz für Person X. Dieses erleichtert und beschleunigt das Verfahren, da nicht alle Datensätze der Datenbank mit der „aktuellen“ biometrischen Signatur verglichen werden müssen. So kann für die biometrische Verifikation eine biometrische Signatur abgespeichert werden, die mehr Informationen aus dem biologischen Merkmal enthält.
Der grundlegende Unterscheid zwischen der biometrischen Identifikation und der Verifikation ist, dass bei der ersteren die Datenbank durchsucht werden muss nach einer passenden biometrische Signatur, während man bei der biometrischen Verifikation gezielt eine biometrische Signatur aus der Datenbank abruft und diese mit der „aktuellen“ Signatur vergleicht.

Fallbeispiel für die biometrische Verifikation - der Bankautomat:

Anstatt einem Geldautomaten die eigene Identität gegenüber durch Kenntnis der PIN (persönliche Identifikationsnummer) nachzuweisen, kann sich 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 Vergleichsbasis abgelegt sein. Der Geldautomat berechnet nun aus dem eingescannten Fingerabdruck der Person eine biometrische Signatur, und vergleicht diese mit der auf der Karte gespeicherten. Wenn der Vergleich positiv verläuft, wird der Zugriff auf das Konto gestattet. **[BARG2002]**

2.1.5 biometrische Authentikation

Nach dem Fachlichen Informatikansatz:

Definition 6: biometrische Authentikation

(im weiteren Sinne): Der gesamte Vorgang (Prozess), mit dem eine Person konfrontiert wird, um Zugriff auf Systemressourcen zu erhalten. **[Brömme2001a]**

Der Vorgang bis zum Zugriff auf die Systemressourcen sieht so aus:

Triviales Phasenmodell: [Brömme2001a]

- 1. Phase: Einlernvorgang
- 2. Phase: Biometrische Authenti(fiz|s)ierung
- 3. Phase: Autorisation
- 4. Phase: Zugriff auf Systemressourcen

Daraus lässt sich die biometrische Authentikation im engeren Sinne ableiten:

Biometrische Authentikation: [Brömme2001a]

- Phase 2 im Phasenmodell:
  - Biometrische Authenti(fiz|s)ierung

Nach dem Populären Informatikansatz gilt folgendes:

Biometrische Authentikation = Biometric Authentication (also biometrische Verifikation) **[Brömme2001a]**

Bei der Authentikation geht es darum, eine vorher angegebene Identität zu **verifizieren** oder zu **falsifizieren**. Man weist anhand seiner biometrischen Signatur gegenüber einem IT-System nach, dass man tatsächlich die Person ist, die man vorgibt zu sein. **[BARG2002]**

2.1.6 Biometrischen Merkmale

Es gibt verschiedene biometrische Merkmale die benutzt werden können für die Identifizierung bzw. Verifizierung einer Person. Dabei sind einige Merkmale besser geeignet als andere, da sich einige Merkmale im Laufe der Zeit ändern können, durch:

- „Abnutzung“ (z.B. Fingerabdruck)
- Alterung (z.B. Gesicht, Handgeometrie)
- Verhaltensänderungen (z.B. Gangart, Unterschrift)

Dieses erfordert dann ein weiteres Einlernen (Enrollment) in das System.

Folgende biometrische Merkmale gibt es u.a.:

- Gesicht
- Fingerabdruck
- Handgeometrie
- Irismuster
- Gefäßstruktur der Retina
- Stimme
- Ohren
- Gangart
- Tastaturanschlagsdynamik
- Körperbewegungen
- Unterschrift
- DNA (Achtung! → dieses biometrische Merkmal kann auch missbraucht werden. s.u.)

2.1.6.1 Vorteile der Gesichtserkennung

Im Vergleich zu den anderen Techniken, hat die Gesichtserkennung den Vorteil, dass sie ohne „Störung“ und Änderung der Verhaltensweise durchführbar ist, bzw. keine bis geringe Kooperation mit der zu erkennenden Person nötig ist **[Jain 1999]**. Die betreffende Person braucht also nicht zu wissen ob sie beobachtet wird oder nicht. Dies ist vorteilhaft, wenn z.B. in einem Stadion kriminelle Personen entdeckt werden sollen.
Außerdem reichen bereits kleine Bilder aus, damit Gesichtserkennung erfolgen kann.
Die Nachteile werden weiter unten im Kapitel 2.4.1 besprochen.

2.1.6.2 Klassifizierung der biometrischen Merkmale

Bei der Klassifizierung der biometrischen Merkmale unterscheidet man folgenden Merkmalstypen:

Genotypisch: Die Erscheinung genotypischer Merkmale ist vollständig durch die Erbanlagen des Trägers festgelegt. Dieses führt dazu, dass genotypische Merkmale bei eineiigen Zwillingen die gleiche Signatur erzeugen. Ein Beispiel für ein genotypisches Merkmal ist die DNA eines Menschen. **[BARG2002]**

Phänotypisch: Die Ausprägungen phänotypischer Merkmale werden neben den Erbanlagen auch von den Umwelteinflüssen, denen der Träger zu einem frühen Zeitpunkt seiner Entwicklung ausgesetzt war, bestimmt. Dieses führt dazu, dass diese Merkmale sich auch bei Menschen mit den selben Erbanlagen unterscheiden. Ein Beispiel für phänotypische Merkmale sind die Strukturen der menschlichen Iris und der Fingerabdruck. **[BARG2002]**

Außerdem kann man noch Verfahren unterscheiden, die ohne und mit Einwilligung der zu erkennenden Person funktionieren. Die betreffende Person muss im ersteren also nicht explizit das biometrische Merkmal irgendwo präsentieren, sondern es wird einfach aufgenommen und von einem System ausgewertet. Im zweiten Fall muss die betreffende Person explizit einverstanden sein und das Merkmal zur Aufnahme dem System präsentieren.

2.1.7 Bewertung eines biometrischen Algorithmuses - FAR/FRR

Die Ergebnisse der Anwendung eines biometrischen Algorithmus auf unterschiedliche Aufnahmen des selben Merkmals (beispielsweise verschiedene Bilder der selben Iris) sind i.A. nicht 100% identisch, sondern nur nahe beieinander. Aus diesem Grund muss ein biometrischer Algorithmus innerhalb eines gewissen Toleranzrahmens Signaturen als zu dem selben Merkmal (bzw. zu dem selben Träger) gehörend erkennen. Ähnliche Signaturen werden als “gleich” und Signaturen, deren Abstand außerhalb des Toleranzrahmen liegen, als “unterschiedlich” bewertet. Die Festlegung dieses Toleranzrahmens besitzt signifikanten Einfluss auf die Güte eines biometrischen Algorithmus. Legt man den Toleranzrahmen zu großzügig fest, kann es leichter zu Fehlurteilen kommen, ist er zu eng gewählt, kann es passieren, dass auch der Träger der Signatur nicht korrekt erkannt wird (z.B. bei zu schlechter Qualität der Bilddaten).
In diesem Zusammenhang spricht man von zwei Kenngrößen: der *FAR* und der *FRR*. **[BARG2002]**

False Acception Rate (FAR): Bezeichnet die Rate der fehlerhaften Zuordnungen einer Signatur zu einen Träger. Je höher also die FAR, desto größer ist die Wahrscheinlichkeit, dass ein Betrüger erfolgreich eine falsche Identität vortäuschen kann. **[BARG2002]**

False Rejection Rate (FRR). Bezeichnet die Rate der fehlerhaft fehlgeschlagenen Zuordnungen von Signaturen, also die Wahrscheinlichkeit, mit der einem Kontobevollmächtigten der Zugriff verweigert wird. **[BARG2002]**

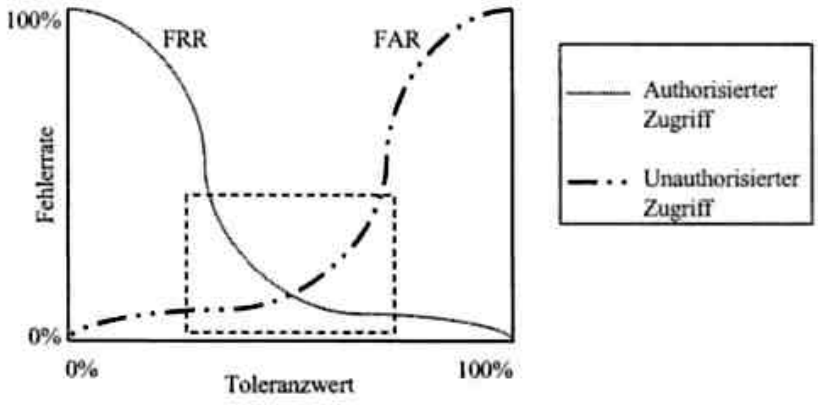

Abbildung1: Die Fehlerraten des autorisierten Zugriffs (FRR) und des unautorisierten Zugriffs (FAR) in Abhängigkeit zum Toleranzwert (aus [Henke1999])

Die Kenngrößen FRR und FAR sind i.A. von einander abhängig. Eine Verbesserung der einen Größe hat im allgemeinen eine Verschlechterung der anderen zur Folge. Wenn der Toleranzrahmen für die Signaturen eingeengt wird, führt dieses z.B. zu einer niedrigeren FAR, da das Kriterium für die Erkennung einer Signatur verschärft wurde, resultiert aber ebenso in einer Erhöhung der FRR, da nun auch die Anforderungen an die Aufnahme des Merkmals erhöht wurden. **[BARG2002]**

2.2 Mustererkennung in der biometrischen Authentikation

In der biometrischen Authentikation spielt die Mustererkennung eine entscheidende Rolle, da anhand des aktuellen Bildes (verrauschtes Muster) entschieden werden soll, ob es in eine bestimmte Klasse fällt oder nicht.
Die Anwendungsmöglichkeiten der Mustererkennung liegen also überall dort, wo einzelne Objekte anhand von Merkmalen in eine überschaubare Zahl von Klassen eingeordnet werden sollen.

Mustererkennung im engeren Sinn ist ein Formalismus zur Objekterkennung, bei dem ein Objekt mit einem Merkmalsvektor beschrieben und anhand seiner Lage im Merkmalsraum klassifiziert wird. **[Görz1995]**

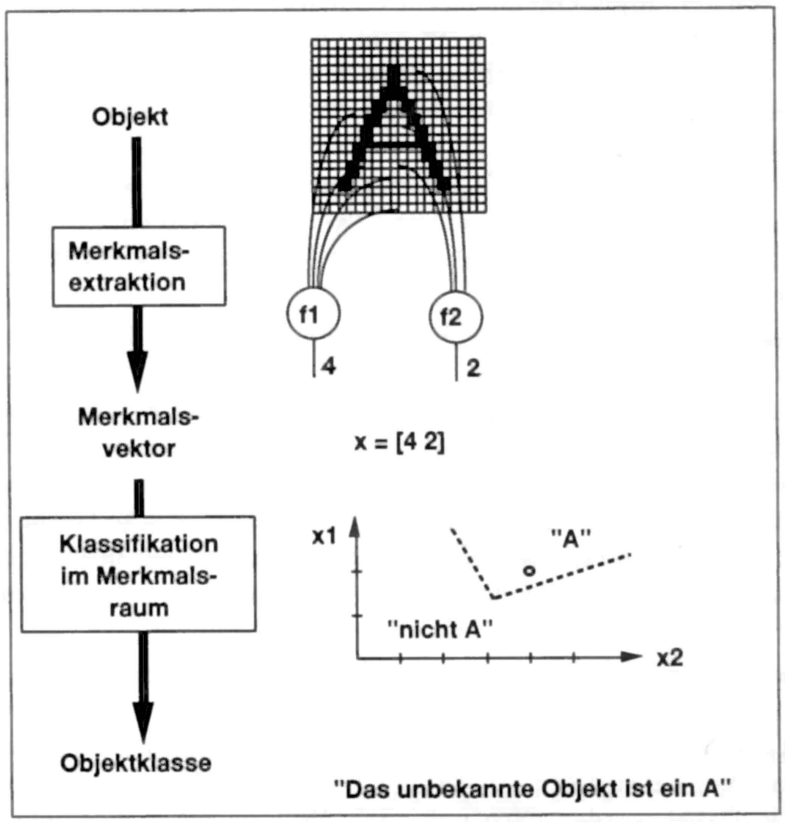

Abbildung 2: Schematische Darstellung des Mustererkennungsparadigmas (aus [Görz1995])

2.2.1 Integration der Mustererkennung in die Biometrik

Um nun die Mustererkennung in die Biometrik zu integrieren muss man den Prozess der Mustererkennung aufteilen in Merkmalsextraktion und Klassifikation.

Im ersten Schritt wird in der Merkmalsextraktion aus einem biometrischen Merkmal eine biometrische Signatur extrahiert. Im zweiten Schritt werden in der Klassifikation vorhandene Muster mit dem aktuellen Muster verglichen und es wird entschieden, in welche Klasse das aktuelle Muster gehört.

In der „biometrischen Mustererkennung“ werden also folgende Schritte durchlaufen:

- Person X gibt sich durch eine PIN oder Chipkarte als Person X aus
- biometrische Merkmale werden aufgenommen (**Merkmalsextraktion**)
- aus dem biometrischen Merkmal wird eine biometrische Signatur erstellt
- es wird die aktuelle biometrische Signatur mit der biometrischen Signatur verglichen, die in einer Datenbank für Person X abgespeichert ist (**Klassifikation**)
- Person X wird verifiziert bzw. abgelehnt

Die detaillierte Beschreibung der Integration erfolgt weiter unten im Kapitel 4.

2.2.2 Merkmalsextraktion

Für die Merkmalsextraktion bieten sich folgende Verfahren an, die weiter unten im Abschnitt 2.4.4 beschrieben werden:

- Template Matching
- Geometrische Merkmale
- Fourier-Transformation
- Gabor-Wavelets
- Elastische Graphen (elastic bunch graph)
- Eigenfaces

2.2.3 Klassifikation

Für die Klassifikation bieten sich folgende Verfahren an, die weiter unten in Abschnitt 2.4.6 beschrieben werden:

- Künstliche Neuronale Netze
- Summe der Fehlerquadrate
- euklidische Norm

- Nearest-Neighbour-Methode

Dabei spielt das Lernen eine wichtige Rolle, denn mit der Zeit verändert sich das Gesicht, so dass das System angepasst werden muss. Diese Anpassung kann entweder manuell erfolgen durch einen menschlichen Bediener, der dem System sagt, nun lerne das neue Gesicht. Oder aber, ein neuronales Netz wird verwendet, welches z.B. jedes mal, wenn eine Person erfolgreich authentisiert wurde, das aktuelle Bild dazulernt. Dadurch passt sich das Netz automatisch an die neuen Verhältnisse an.

2.3 Neuronale Netze

Wie im vorhergehenden Abschnitt beschrieben, werden die neuronalen Netze für die Klassifikation benötigt. Deshalb wird in diesem Abschnitt die Funktionsweise der neuronalen Netze beschrieben.

Als erstes folgt eine Beschreibung der biologischen Grundlagen von neuronalen Netzen. Ausgehend vom Neuron, dem grundlegenden Element der Informationsverarbeitung im Gehirn, wird die Funktionsweise des Lernens beschrieben. Grundsätzlich kann gesagt werden, je mehr Neurone vorhanden sind in einem System, desto „leistungsfähiger“ der Verbund.

2.3.1 Biologische neuronale Netze

2.3.1.1 Das Neuron

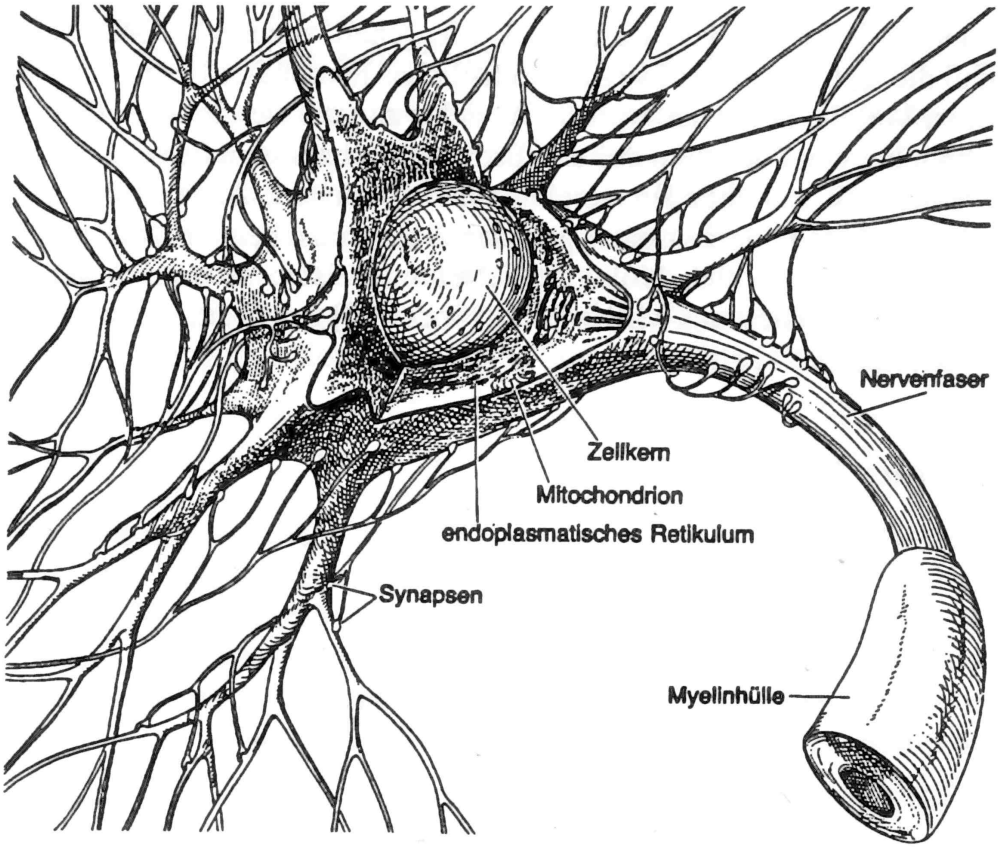

Abbildung 3: Aufbau einer Nervenzelle mit Zellkern im Innern des Zellkörpers, Nervenfaser (Axon) und Dendriten, die über Synapsen Nachrichten von Vorgängerzellen erhalten [aus [Zell1996])

Nervenzellen oder Neurone sind die Grundbausteine des Gehirns. Sie bestehen aus einem bis zu 0,25mm großen Zellkörper (Soma). Im Gegensatz zu anderen Zellen bilden Neurone Fortsätze aus. Dabei gibt es zwei Arten von Fortsätzen:

- **Dendriten:** Sie sind für die Aufnahme und Weiterleitung von Eingangssignalen zum Zellkörper zuständig.
- **Axone:** Sie sorgen für die Weiterleitung von Aktionspotentialen vom Zellkörper zu anderen Zellen oder Muskeln.

Die Fortsätze sind also für die Kommunikation zwischen Zellen und zwischen Zellen und Muskeln notwendig.

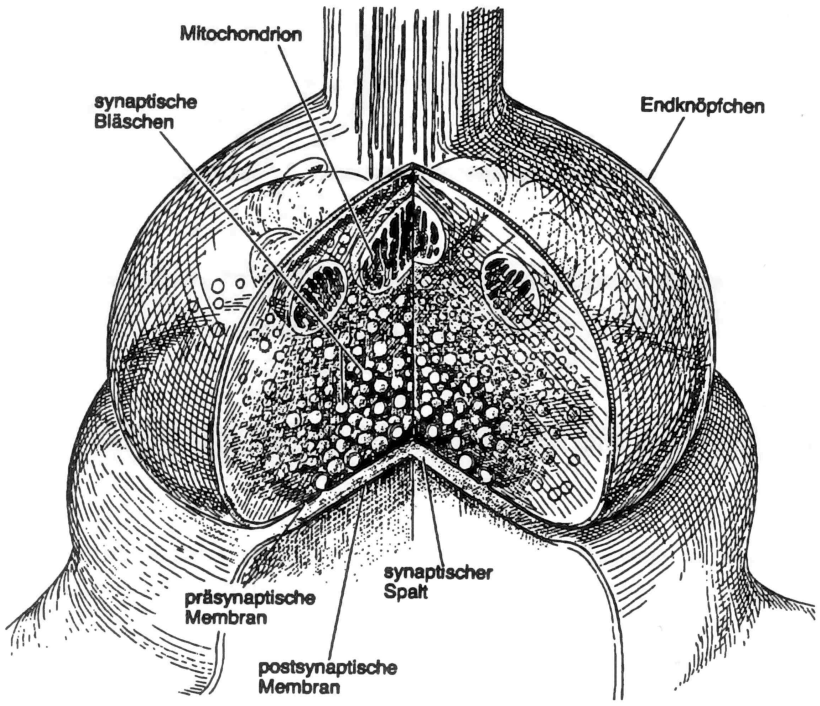

Abbildung 4: Schnitt durch eine Synapse (aus [Zell1996])

Am Ende der Fortsätze befinden sich Verdickungen, die sogenannten Synapsen. Diese bilden Kontaktstellen zwischen einzelnen Nerven- oder Muskelzellen. Außerdem sind die Synapsen Andockstellen für viele Hormone und Psychopharmaka.
Menschliche Neurone besitzen zwischen 1000 und 10.000 solcher Synapsen. Manche Zellen, wie die Purkinje-Zellen, die sich im Kleinhirn befinden, besitzen bis zu 150.000 Synapsen.
Dabei gibt es folgende Verknüpfungsarten:

- **axodendritische Synapse**: Kontaktstelle zwischen den Enden des Axons und dem Dendrit eines anderen Neurons
- **dendrodendritische Synapse** (selten): Synapse zwischen Dendriten
- **axoaxonische Synapse** (selten): Synapse zwischen zwei Axone

Synapsen spielen im Verbund von Neuronen eine Schlüsselrolle, da hier das Lernen stattfindet.

2.3.1.2 Funktionsprinzip und Ort des Lernens

Die Übertragung der Informationen geschieht, wie weiter oben erwähnt, über Axone bzw. Dendriten. Dabei erfolgt die Informationsübertragung in Form von Spikes. Ein Spike ist nichts anderes als ein Aktionspotential (AP), welches durch den Ladungsunterschied an der Zellmembran erzeugt wird. Da ein Aktionspotential entweder vorhanden ist oder nicht und das Alles-oder-Nichts-Prinzip für Aktionspotentiale gilt, werden über Axone bzw. Dendriten **binäre** Informationen übertragen (0 oder 1). Allerdings spielt, im Gegensatz zu einer herkömmlichen Metallleitung, der Ort des Aktionspotentials eine Rolle. Axone wie auch Dendriten können zum selben Zeitpunkt **mehrere** Aktionspotentiale weiterleiten. Wohingegen in einer Metallleitung prinzipiell entweder überall der gleiche Strom fließt oder nicht.
Daraus folgt, das die Leistungsfähigkeit des Gehirns nicht nur durch die hohe Verschaltung zustande kommt, sondern durch die hohe Integrität von Informationen.

Das Gehirn arbeitet nach aktuellen Kenntnissen mit folgenden Gedächtnisarten bzw. -stufen:

- **Sensorisches Gedächtnis**
- **Kurzzeitgedächtnis**
- **Langzeitgedächtnis**

Es folgt eine kurze Beschreibung der Gedächtnisstufen Kurzzeitgedächtnis und Langzeitgedächtnis.

2.3.1.2.1 Kurzzeitgedächtnis

Das Kurzzeitgedächtnis wird nach heutigem Kenntnisstand dadurch gebildet, dass an den Synapsen sich die Ausschüttung des Neurotransmitters an der präsynaptischen Membran

erhöht. Diese erhöhte Ausschüttung hält von einigen Minuten bis Stunden an. Bei darauffolgender Nichtbenutzung dieser Synapsen verringert sich wieder die Ausschüttung an Neurotransmittern und der Gedächtnisinhalt erlischt.

Bei den künstlichen neuronalen Netzen existiert so eine Art Kurzzeitgedächtnis nicht. Wenn einem künstlichen neuronalen Netz Informationen antrainiert werden, bleiben diese für immer erhalten.

2.3.1.2.2 Langzeitgedächtnis

Das Langzeitgedächtnis beruht auf der Synthese neuer Proteine und der Ausbildung neuer synaptischer Verbindungen. Gegenüber dem Kurzzeitgedächtnis werden so die Informationen längerfristig behalten, da ja eine Veränderung der Netzstruktur vonstatten geht. Da beim Langzeitgedächtnis sich nun die Struktur des Netzes ändert und dieses bei den künstlichen neuronalen Netzen in Form von Gewichtsveränderungen ebenfalls der Fall ist, lässt sich beim Vergleichen sagen, dass künstliche neuronale Netze ebenfalls Langzeitgedächtnisse sind. Denn jede Veränderung in den Gewichten bei den künstlichen neuronalen Netzen bleibt nach dem Trainingsprozess bestehen.

Nun ist es so, dass sich das Kurzzeitgedächtnis und das Langzeitgedächtnis nicht strikt trennen lassen. Es ist vielmehr ein Übergang vom Kurzzeitgedächtnis ins Langzeitgedächtnis. Je länger Informationen aufgenommen werden, desto öfter werden bestimmte Bahnen bzw. Synapsen benutzt. Dies führt dazu, dass an bestimmten Stellen mehr vom neuralen Wachstumsfaktor in den synaptischen Spalt und in die Umgebung ausgeschüttet wird. Dieses bewirkt wiederum, dass nur die Synapsen bzw. Axone neue Verbindungen aufbauen bzw. verstärken, die sehr aktiv sind. Denn der neurale Wachstumsfaktor wird nur durch die präsynaptische Endigung aufgenommen, wenn vorher Neurotransmitter ausgeschüttet wurde, und dieser wieder aufgenommen wird, zusammen mit dem neuralen Wachstumsfaktor. Das ist das grobe Funktionsprinzip des Lernprozesses für das Langzeitgedächtnis.

2.3.2 Künstliche neuronale Netze

Nun werden die grundlegenden Prinzipien beschrieben, aus denen sich die Funktionsfähigkeit eines künstlichen neuronalen Netzes ersehen lässt.

2.3.2.1 Abstraktion von den biologischen neuronalen Netzen

Die künstlichen neuronalen Netze sind gegenüber den biologischen sehr stark idealisiert. Folgende Unterschiede gibt es u.a. (aus **[Zell1994]**):

- **Viel geringere Zahl von Neuronen**: Während man das Gehirn eines Menschen auf ca. 10^{11} Neuronen schätzt, werden in den meisten Simulationen künstlicher neuronaler Netze 10^2 bis 10^4 Neuronen verwendet. Es ist sehr wahrscheinlich, dass sich viele kognitive Fähigkeiten erst mit einer deutlich größeren Zahl von Neuronen realisieren lassen.
- **Viel geringere Zahl von Verbindungen**: Während die Gehirne von Säugetieren im Durchschnitt eine Konnektivität von ca. 10^4 Synapsen pro Neuron besitzen, lassen sich derzeit technisch nur sehr kleine Netze mit hoher Konnektivität realisieren.
- **Meist nur ein Parameter für die Stärke der synaptischen Kopplung**: Die Stärke einer Synapse wird meist nur durch einen numerischen Parameter, das Gewicht, bestimmt. Zeitliche Phänomene der synaptischen Kopplung oder der Einfluss verschiedener Neurotransmitter werden in den meisten Simulationen derzeit nicht berücksichtigt.
- **Amplitudenmodulation statt Frequenzmodulation**: Simulatoren verwenden üblicherweise keine impulskodierte Informationsübertragung (Frequenzmodulation), wie sie im Axon vorkommt, sondern rechnen mit einem numerischen Aktivierungswert, der eher einer Amplitudenmodulation entspricht.
- **Lokalitätsprinzip für Synapsen ist verletzt**: Die Hebbsche Lernregel in der allgemeinen Form, auf der die meisten Lernverfahren basieren ist zwar lokal für eine Zelle, aber nicht lokal für die jeweilige Synapse. Da sich bei dieser Regel die Stärke einer Synapse ändert, wenn die Vorgängerzelle und die Nachfolgerzelle gleichzeitig erregt sind, stellt sich die Frage, wie eine Synapse die Aktivierung der Nachfolgerneurons, in welchem die Aktivierung sehr vieler Synapsen über die dendritischen Bäume aufsummiert wird, erfahren soll.

- **Keine Modellierung der synaptischen Struktur der Dendriten**: Die baumartig verästelte Struktur der Dendriten, die Signale von anderen Zellen zum eigenen Zentrum der Zelle weiterleiten, wird üblicherweise nicht modelliert. Stattdessen werden direkte Verbindungen zwischen Zellen simuliert.
- **Keine genauere Modellierung der zeitlichen Vorgänge der Nervenleitung:** Die zeitlichen Vorgänge der Nervenleitung werden ebenfalls üblicherweise vernachlässigt.
- **Keine Berücksichtigung chemischer Einwirkungen räumlich benachbarter Neuronen:** In biologischen Systemen werden räumlich benachbarte Gruppen von Neuronen neben der Nervenreizung auf elektrischer Basis auch durch chemische Modulatorsubstanzen (z.B. Hormone) beeinflusst und als Gruppe gehemmt oder erregt. Dies wird bisher in Simulationen künstlicher neuronaler Netze auch nicht berücksichtigt.
- **Biologisch unplausible Lernregeln:** Die erfolgreichsten Lernregeln für technische Anwendungen (z.B. Backpropagation, Hopfield-Netze, Boltzmann-Maschine etc.) wurden bisher zumeist aus mathematischen oder physikalischen Modellen entwickelt (Gradientenabstieg im Fehlerraum, Fehlerminimierung, Simuliertes Ausglühen etc.) und sind teilweise biologisch völlig unplausibel.

2.3.2.2 Aufbau und Bestandteile von künstlichen neuronalen Netzen

Allgemein sind künstliche wie auch biologische neuronale Netze aus Zellen aufgebaut die über Verbindungen mit anderen Zellen Signale austauschen.

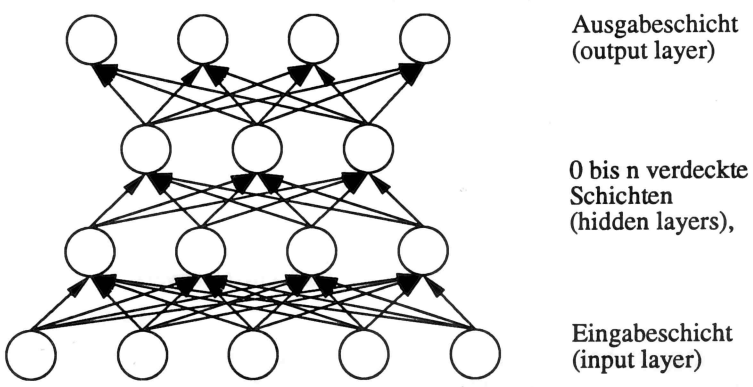

Abbildung 5: Ein feedforward-Netzwerk mit 3 Schichten von Verbindungen und 4 Zellschichten (aus [Zell1994])

In Abbildung 5 erkennt man den prinzipiellen Aufbau von künstlichen neuronalen Netzen. Die Eingabeschicht führt dem neuronalen Netz Eingabeinformationen zu und die Ausgabeschicht gibt die „berechneten“ Ausgabeinformationen aus. Es gibt nun künstliche neuronale Netze die mit verdeckten Schichten (z.B. feedforward Netze) und welche, die mit einer Eingabeschicht und einer Ausgabeschicht (z.B. Kohonen Netz) arbeiten. Dabei gibt die Eingabeschicht die anliegenden Informationen nur weiter an die darauffolgende Schicht. Während des Lernens werden nun die Gewichte der Verbindungen der darauffolgenden Schichten, inklusive der Ausgabeschicht, verändert.

Künstliche neuronale Netze sind im allgemeinen aus folgenden Komponenten aufgebaut (aus **[Zell1994]**):

- **Zellen (units)**: Zellen besitzen folgende Bestandteile:
  - Aktivierungszustand (activiation) $a_i(t)$: Er gibt den Grad der Aktivierung der Zelle an.
  - Aktivierungsfunktion f_{act}: Sie gibt an, wie sich ein neuer Aktivierungszustand $a_j(t+1)$ des Neurons j aus der alten Aktivierung $a_j(t)$ und der Netzeingabe (net input) $net_j(t)$ ergibt, meist nach der allgemeinen Formel

    $$a_j\,(t+1) = f_{act}\,(a_j\,(t), net_j\,(t), ?_j),$$

    wobei $?_j(t)$ der Schwellenwert des Neurons j ist und f_{act} die Aktivierungsfunktion, die aus den angegebenen Parameter die neue Aktivierung berechnet.
  - Ausgabefunktion f_{out}. Die Ausgabe der Zelle j wird durch eine sogenannte Ausgabefunktion aus der Aktivierung der Zelle bestimmt.

    $$o_j = f_{out}\,(a_j)$$
- **Verbindungsnetzwerk der Zellen**: Ein neuronales Netz kann als gerichteter, gewichteter Graph angesehen werden, wobei die Kanten die gewichteten Verbindungen zwischen den Neuronen darstellen. Das Gewicht (weight) der Verbindung von Zelle i nach Zelle j wird hier durch w_{ij} bezeichnet. Man beachte die Reihenfolge der Indizes, weil es zwei gegensätzliche Konventionen der Schreibweise gibt. Die Matrix der Verbindungen aller Zellen (Gewichtsmatrix) wird dann mit W bezeichnet.
- **Propagierungsfunktion**: Sie gibt an, wie sich die Netzeingabe eines Neurons aus den Ausgaben der anderen Neuronen und den Verbindungsgewichten berechnet. Die Netzeingabe $net_j(t)$ von Zelle j berechnet sich nach

  $$net_j\,(t) = ?_i\, o_i\,(t)\, w_{ij}$$

aus der Summe der Ausgaben $o_i(t)$ der Vorgängerzellen multipliziert mit dem jeweiligen Gewicht w_{ij} der Verbindung von Zelle i nach Zelle j.

- **Lernregel**: Die Lernregel ist ein Algorithmus, gemäß dem das künstliche neuronale Netz lernt, für eine vorgegebene Eingabe eine gewünschte Ausgabe zu produzieren. Lernen erfolgt in neuronalen Netzen meist durch Modifikation der Stärke der Verbindungen als Ergebnis der wiederholten Präsentation von Trainingsmustern. Oft wird dabei versucht, den Fehler zwischen erwarteter Ausgabe und tatsächlicher Ausgabe für alle Trainingsmuster zu minimieren.

2.3.2.3 Lernverfahren für künstliche neuronale Netze

Der Lernalgorithmus muss während des Lernens bestimmte Eigenschaften bzw. Parameter des Netzes ändern. Folgende Parameter lassen sich an einem künstlichen neuronalen Netz prinzipiell ändern:

- Entwicklung neuer Verbindungen
- Löschen vorhandener Verbindungen
- Modifikation der Stärke w_{ij} von Verbindungen
- Modifikation des Schwellenwertes von Neuronen
- Modifikation der Aktivierungs-, Propagierungs- oder Ausgabefunktion,
- Entwicklung neuer Zellen
- Löschen von Zellen

In gängigen Simulationen wird die Veränderung der Stärke von Verbindungen verwendet.

Allgemein gibt es folgende 3 unterschiedliche Arten wie einem Netz etwas antrainiert werden kann (aus **[Zell1994]**):

- **überwachtes Lernen**: Hier gibt ein externer „Lehrer“ zu jedem Eingabemuster der Trainingsmenge das korrekte bzw. beste Ausgabemuster dazu an. Dies bedeutet, dass dem künstlichen neuronalen Netz immer gleichzeitig ein vollständig spezifiziertes Eingabemuster und das korrekte bzw. optimale vollständig spezifizierte Ausgabemuster für diese Eingabe vorliegen muß. Aufgabe des Lernverfahrens ist es, die Gewichte des Netzes so zu ändern, dass das Netz nach wiederholter Präsentation der Paare von Eingabe- und Ausgabemustern diese Assoziation selbstständig vornehmen kann und dies auch für unbekannte, ähnliche

Eingabemuster tun kann (Generalisierung). Diese Art des Lernens ist üblicherweise die schnellste Methode, ein Netz für eine Aufgabe zu trainieren. Nachteilig bei diesem Ansatz ist, dass er biologisch nicht plausibel ist, da hier die erwünschten Aktivierungen alle Ausgabeneuronen vorgegeben werden müssen.

- **bestärkendes Lernen**: Hier gibt der Lehrer zu jedem Eingabemuster der Trainingsmenge nur an, ob es richtig oder falsch klassifiziert wurde, jedoch nicht die korrekte (beste) Ausgabe. Das Netzwerk muss die korrekte Ausgabe selbst finden. Diese Art des Lernens ist deutlich langsamer als überwachtes Lernen, dafür aber biologisch plausibler.
- **unüberwachtes Lernen**: Hier gibt es überhaupt keinen externen Lehrer. Lernen geschieht durch Selbstorganisation, dem Netz werden nur Eingabemuster präsentiert. Durch das Lernverfahren versucht das Netz ähnliche Eingabemuster in ähnliche Kategorien zu klassifizieren, bzw. sie durch die Aktivierung der gleichen oder räumlich benachbarten Neuronen als ähnlich zu identifizieren. Das bekannteste Beispiel unüberwachten Lernens sind die selbstorganisierenden Karten von Kohonen (self-organizing feature maps). Diese Art des Lernens, bei der die statistischen Eigenschaften der Eingabemustermenge extrahiert werden, ist biologisch am plausibelsten, ist aber in dieser Form nicht für alle Fragestellungen geeignet, bei denen die anderen Verfahren anwendbar sind.

2.3.3 Welche Art von künstlichen neuronalen Netzen ist für die Klassifikation von Gesichtern in der biometrischen Authentikation geeignet?

Um Entscheiden zu können, welche Art von künstlichen neuronalen Netzen für die Gesichtserkennung am besten geeignet ist, wird noch mal kurz eine Kernanforderung beschrieben:

- Verschiedene Ansichten eines bestimmten Gesichtes sollen verknüpft werden mit der Information, zu welcher Person diese Ansichten gehören. Da von dem Gesicht aus verschiedenen Blickwinkeln Aufnahmen gemacht werden, kann es sein, dass das künstliche neuronale Netz beim unüberwachten Lernen „falsch“ klassifiziert, bzw. es länger dauert, ehe es allen Blickwinkeln eine gemeinsame Klasse zuweist.

Außerdem stellt sich die Frage, wann genau man unüberwachte Lernverfahren benutzt? Generell lässt sich sagen, dass unüberwachte Lernverfahren benutzt werden, wenn man von vornherein nicht weiß, welche Informationen in einer Klasse gruppiert werden sollen.

Man möchte also von künstlichen neuronalen Netzen durch Selbstorganisation Klassen gebildet bekommen.
Da nun in der Gesichtserkennung genau bekannt ist, welche Gesichtsaufnahme welcher Person zugeordnet werden soll, lässt sich daraus schließen, dass künstliche neuronale Netze, die mit überwachtem Lernen funktionieren, besser dafür geeignet sind.
Man möchte also nicht die selbstständige Klassifizierungsfähigkeit von künstlichen neuronalen Netzen mit unüberwachtem Lernverfahren verwenden, sondern die Fehlertoleranz und die Generalisierungsfähigkeit.

In Tabelle 1 ist ein Vergleich zu sehen mit verschiedenen Arten von künstlichen neuronalen Netzen und ihren Erkennungsleistungen. Dabei wurden die Netze mit 5 Bildern pro Person trainiert. Ausgangsbasis für den Vergleich ist die Olivetti Research Laboratory (ORL) Datenbank. Sie enthält 400 Bilder von 40 Personen. Dabei sind die Bilder konstant in bezug auf Beleuchtung, Position und Ausrichtung des Gesichtes.

Technik	Erkennungsleistung in Prozent	Trainingszeit	Klassifizierungs-zeit
Hidden Markov Modell (HMM)	87	?	?
Pseudo 2-D HMM	95	?	4min
Eigenfaces	89	?	?
PCA + MLP	59	?	?
SOM + MLP	60	?	?
PCA + CN	92	?	?
SOM + CN	96	4hr	<0.5min
PDBNN	96	20 min	<0.1min
n-tuple	81	0.9s	0.025min
cont n-tuple	95	0.9s	0.33min
1-NN	97	0s	1s
RBF before discard	86	8s	0.01s
RBF after discard	95	8s	0.01s

Legende: PCA: principal components analysis, **MLP:** multi-layer perceptron, **SOM:** self-organizing map, **CN:** convolutional network, **PDBNN:** probalistic, decision-based neural network, **n-tuple:** n-tuple classifiers, **cont n-tuple:** continuous n-tuple classifiers, **1-NN:** 1-nearest-neighbor, **RBF:** Radial Basis Function, **?:** es lagen keine Daten vor

Tabelle 1: Erkennungsleistung (in Prozent der richtig erkannten Gesichter) von verschiedenen Arten von künstlichen neuronalen Netzen (aus [Jain1999])

Scheinbar wurde das beste Ergebnis mit der 1-Nearest-Neighbor Methode erzielt, wobei [Jain1999] anmerkt, das es mit der konstanten Ausrichtung und Beleuchtung der Gesichter zusammenhängt.
Die Erkennungsleistung mit der Technik „SOM + CN“ liegt bei 96%, wobei sich diese Technik weniger für den praktischen Einsatz eignet, da die Trainingszeit, bedingt durch die Selbstorganisation, bei 4 Stunden liegt!
Generell ist fraglich, in wie weit sich die Ergebnisse aus Tabelle 1 verwenden lassen für die Bestimmung, welche Art von künstlichen neuronalen Netzen sich für den praktischen Einsatz am besten eignet.
Eigentlich sollte in dieser Arbeit eine Simulation durchgeführt werden, mit verschiedenen Arten von künstlichen neuronalen Netzen. Die Ergebnisse sollten im Kapitel 3 aufgeführt werden. Leider konnte diese Simulation aus Mangel an Zeit nicht stattfinden.

2.4 Gesichtserkennung

In der Gesichtserkennung wird die Mustererkennung (wie schon im vorangehenden Kapitel erläutert) verwendet, um erstens die relevanten Informationen aus dem Gesicht zu extrahieren (**Merkmalsextraktion**), und um anschließen zu entscheiden um welches Gesicht es sich handelt (**Klassifikation**). Weiter unten werden dazu die gängigsten Verfahren zur Merkmalsextraktion und für die Klassifikation aufgeführt.

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

- merkmalsbasierte Gesichtserkennung
- holistischer Ansatz

Im ersten Fall werden einzelne markante Merkmale (features) aus dem Gesicht extrahiert und benutzt für die Erstellung der biometrischen Signatur.
Im zweiten Fall wird das komplette Bild betrachtet, welches von dem Gesicht gemacht wurde. Ein mögliches Verfahren wäre hier z.B. die Fourier-Transformation. Interessant bei der Fourier-Transformation ist, dass hier nicht alle Frequenzen für die Erstellung der Signatur benutzt werden brauchen, sondern nur die niedrigen Frequenzen, da sich hier ein Großteil der Informationen befindet. Das hat wiederum zur Folge, dass die Signatur bei der Fourier-Transformation klein gehalten werden kann.

Um überhaupt Merkmale extrahieren zu können, ist ein Gesichtserfassungsgerät (Kamera) notwendig, welches digitale Bilddaten liefert. So kann ein Computer mit einem geeigneten Verfahren die Bilddaten analysieren.

Aus datenschutzrechtlicher Perspektive ist es nicht erlaubt, ganze Bilder in einer Datenbank abzuspeichern für einen späteren Vergleich, deshalb ist es notwendig aus dem Bild eine biometrische Signatur zu erstellen. Ausserdem darf aus der Signatur nicht das Originalbild rekonstruierbar sein. Diese Signatur wird dann in eine Datenbank abgespeichert und beim Authentikationsversuch mit der „aktuellen“ Signatur verglichen.

Damit ein Gesichtserkennungssystem effektiv arbeiten kann, ist es wichtig, die markantesten Merkmale des Gesichtes zu isolieren und zu extrahieren. Somit werden nur die nötigsten Informationen aus dem Gesicht in die Signatur übernommen.

Eines der größten Probleme der Computer Vision, speziell in der Gesichtserkennung, ist die Dimensionsreduktion, um die redundanten Informationen aus den Originalbildern zu entfernen. Hierzu gibt es verschiedene Verfahren zur Merkmalsextraktion. Einige werden weiter unten im Kapitel 2.4.3 beschrieben.

2.4.1 Probleme von Gesichtserkennungssystemen in der Praxis

Folgende Probleme bereitet die Gesichtserkennung in der Praxis:

- **Lichtverhältnisse**: Schwankungen in den Lichtverhältnissen erschweren die Wiedererkennung bereits gelernter Gesichter. Es sollte aber bei der Aufnahme des Gesichtes darauf geachtet werden, dass viel Licht verwendet wird, da dadurch bessere Aufnahmen mit einer Kamera erzielt werden.
- **Schattenwurf**: Es sollte auch darauf geachtet werden, dass durch den Lichteinfall keine Schatten geworfen werden, da durch das Gesichtserkennungssystem dadurch fälschlicherweise eine Kante interpretiert werden kann, was zur Verfälschung der Signatur führt.
- **Ausrichtung des Kopfes:** Bei der Aufnahme sollte darauf geachtet werden, dass das Gesicht frontal aufgenommen wird, da sich die relevanten Wiedererkennungs-merkmale im Gesicht befinden, und durch die frontale Aufnahme gewährleistet wird, dass diese auch optimal eingefangen werden.
- **Verdeckung des Gesichtes:** Probleme bei der Erkennung können dadurch entstehen, dass das Gesicht durch Gegenstände verdeckt wird, wie z.B. (Sonnenbrille-)Brille, Schal, Hut, Mundschutz.
- **Alterung der Menschen:** Durch die Alterung der Menschen bilden sich Falten und Hautlappen die zu einer Veränderung der biometrischen Signatur führen können. Dem kann entgegengewirkt werden, durch eine automatische ständige Anpassung der Signatur bei einer erfolgreichen Authentikation durch diese Person.
- **Veränderungen des Gemütszustandes:** Das Gesicht hat ein anderes Erscheinen bei einem freudigen Gemütszustand als bei einem traurigen. Bei einem niedrigen Toleranzwert kann dies zu einem Problem führen.
- **Permanente Veränderungen des Gesichtes:** Diese können z.B. durch Gesichtsoperation und Verletzungen verursacht werden.
- **Temporäre Veränderungen des Gesichtes:** Diese Veränderungen können zeitweilig durch folgende Gegebenheiten verursacht werden:

  - Make-up
  - Schweiß auf dem Gesicht (dadurch entstehen Reflexionen)
  - Reflexionen auf den Pupillen
  - Schmutz auf dem Gesicht
- **Eineiige Zwillinge**: Dies scheint ein bisher ungelöstes Problem zu sein, da sich die eineiigen Zwillinge im Gesicht normalerweise kaum bis gar nicht unterscheiden.

Ausgehend von diesen Problemen, werden nun einige Anforderungen an das Gesichtserfassungssystem beschrieben zur Lösung bzw. Verringerung dieser Probleme.

2.4.2 Anforderungen an ein Gesichtserkennungssystem

Je nachdem, in welchem Gebiet das System angewendet werden soll, werden unterschiedliche *allgemeine* Anforderungen gestellt *(in Klammern stehen die Anforderungen)*:

- *Authentikation* für den Zugang zu bestimmten Ressourcen (Computer, gesicherte Bereiche, Kraftfahrzeuge, etc.) *(sehr genaue und sichere Erkennung)*
- *Identifikation* von Personen an bestimmten Orten (Stadien, Flughäfen, Kaufhäuser etc.) *(schnelle Erkennung, wenn es geht sicher)*
- Profilaktivierung an Fernsehgeräten, etc. *(schnelle Erkennung; braucht nicht unbedingt sicher zu sein, da es sich nicht um sicherheitsrelevante Gebiete handelt)*

Ausgehend von den Anwendungsgebieten sollte das System folgende *technische* Anforderungen erfüllen:

- Lernen von neuen Gesichtern (**enrollment**)
- „Vergessen“ von bekannten Gesichtern (**derollment**)
- Das Lernen eines neuen Erscheinungsbildes von bereits bekannten Gesichtern
- Das Lernen von Gesichtern bestimmter Personen, denen nur zeitlich begrenzt Zugang gewährt wird.
- Das Verknüpfen eines Gesichtes mit der Information, ob diese Person ggf. gefährlich ist, explizit Hausverbot bekommen hat etc.
- Genügend Licht bei der Aufnahme
- Das Vorhandensein eines Schwellwertes um sich an unterschiedliche Umgebungen und Anforderungen anpassen zu können.

2.4.3 Anforderungen an das Gesichtsaufnahmegerät

Je nach Anwendungsgebiet werden an das Gesichtsaufnahmegerät (Kamera) bestimmte Anforderungen gestellt um möglichst viele Informationen für die Erstellung der Signatur zu benutzen. Im folgenden werden die wichtigsten technischen Parameter aufgelistet:

- **Auflösung:** (Bildpunkte pro Flächeneinheit) → je mehr Bildpunkte pro Flächeneinheit vorhanden sind, desto mehr Informationen (Feinheiten) stehen zur Verfügung für die Erstellung der Signatur.
- **Bildgröße:** (Anzahl der Bildpunkte) → Die Anzahl der Bildpunkte im gesamten Bild sollte möglichst hoch sein, um für die Analyse viele Informationen zu haben. Allerdings sollten dabei nicht „unnötige“ Informationen vorhanden sein, wie z.B. der Bildhintergrund. Das Gesicht sollte möglichst viel Platz im Bild einnehmen.
- **Bilder pro Sekunde:** (Verringerung der Bewegungsunschärfe) → Um Bewegungsunschärfe zu vermeiden (was zur Verringerung der Qualität des Bildes führen könnte) sollte die Anzahl der Bilder pro Sekunde möglichst hoch sein.
- **Format:** (Ausgangssignals der Kamera (digital, analog)) → Für die Weiterverarbeitung der Bilder ist ein digitales System zu bevorzugen, da das Bild im Computer analysiert wird und außerdem die Qualitätseinbußen durch ein digitales System verringert werden.
- **Lichtstärke:** (Erhöhung des Kontrastes) Eine hohe Lichtstärke ist wünschenswert, um ein möglichst kontrastreiches Bild zu erzeugen.

2.4.4 Verfahren für die Merkmalsextraktion

Damit ein Gesichtserkennungssystem effektiv arbeiten kann ist es wichtig, dass die markantesten Merkmale in den Eingabedaten herausextrahiert werden, um das Gesicht am effizientesten zu repräsentieren. **[Jain1999]**

Das größte Problem in der Bildverarbeitung, besonders in der Gesichtserkennung, ist die Dimensionsreduktion um den größten Teil an redundanten Informationen aus den Originalbildern zu entfernen.

Die einzelnen Verfahren versuchen nun die markantesten Merkmale des Gesichtes zu extrahieren.

Die Informationen die von den einzelnen Verfahren extrahiert werden dienen der Erstellung der biometrischen Signatur.

2.4.4.1 Template Matching

Abbildung 6: Referenzbild und Template der Augenpartie (aus [Hofmann2002])

Abbildung 7: 4 Templates für Augen, Nase, Mund und das ganze Gesicht (aus [Hofmann2002])

Ein sehr häufig verwendetes Verfahren der Gesichtserkennung ist das Template Matching. Dabei wird die Ähnlichkeit zwischen einem Bild und einem Template t berechnet. Ein Template ist eine vorgegebene Maske, die einem Bild oder einem Teil eines Bilds ähnlich ist. Die einfachste Form des Template Matching für die Gesichtererkennung ist es, ein Bild mit einem Template zu vergleichen, welches das ganze Gesicht oder Teile des Gesichts repräsentiert. [..] Für die Identifikation eines unbekannten Gesichts wird ein Vergleich dieses Gesichts mit allen in der Datenbank gespeicherten Bildern durchgeführt. Als Ergebnis erhält man einen Vektor, in dem die Ähnlichkeit der jeweiligen Merkmale enthalten ist. Die unbekannte Person wird dann als die Person mit der höchsten kumulativen Ähnlichkeit aller Merkmale identifiziert. Diese kann beispielsweise über die Summe der Fehlerquadrate berechnet werden. Die Qualität der Ergebnisse beim Template Matching hängt stark von der Qualität der verwendeten Maske ab. Die Maske muß bei möglichst vielen unterschiedlichen Personen "passen" und sollte möglichst unabhängig von Helligkeits- oder Kontraständerungen sein. Das größte Problem beim Template Matching ist jedoch, daß es sehr rechenaufwendig und somit zeitaufwendig ist. [**Hofmann2002**]

Dieses Verfahren birgt in der Praxis Risiken, da es teilweise ganze Ausschnitte von Bildern in einer Datenbank abspeichern muss. Dies könnte nach datenschutzrechtlichen Gründen nicht akzeptiert werden.

2.4.4.2 Geometrische Merkmale

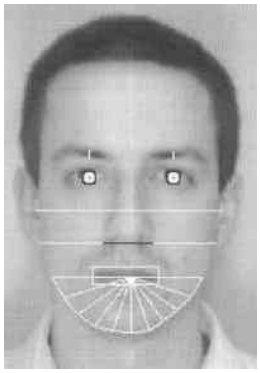

Abbildung 8: 22 Merkmale im Gesicht, die zur Identifikation einer Person verwendet werden (aus [Hofmann2002])

Bei dieser Methode werden geometrische Merkmale (features) des Gesichts, wie zum Beispiel Position der Nase, der Augen oder des Munds und ihre relative Position zueinander aus einem Bild extrahiert und als Zahlenwerte in einem Vektor gespeichert. [**Hofmann2002**]

2.4.4.3 Fourier-Transformation

Abbildung 9

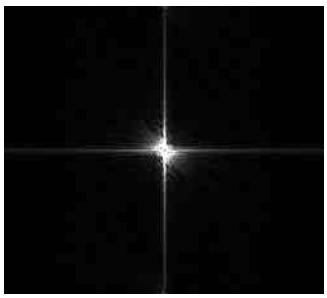

Abbildung 10

Gesicht und seine Transformation in den Frequenzbereich:
Abbildung 9: Originalbild, Abbildung 10: Spektrum des Bilds (Amplitudenspektrum) (aus [Hofmann2002])

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

Ortsbereich in den Frequenzbereich, der häufig auch als Ortsfrequenzbereich bezeichnet wird. [**Hofmann2002**]

2.4.4.4 Elastische Graphen (elastic bunch graph)

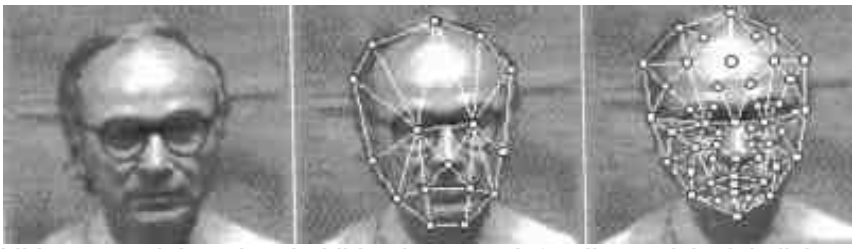

Abbildung 11: Links: Eingabebild; Mitte: Graph für die Gesichtslokalisierung; Rechts: Graph zum Auffinden der Landmarks (aus [Hofmann2002])

Bei dieser Methode wird dem Gesicht ein Gitternetz zugeordnet, das als "Labeled Graph" bezeichnet wird. An den Knoten dieses Graphen berechnet ein Algorithmus bestimmte Merkmale des Gesichts. Soll nun ein gespeicherter Graph mit einem neuen Gesicht verglichen werden, dann versucht der Algorithmus auf dem aktuellen Bild ein Gitter zu erzeugen, das dem bereits vorhandenen Gitter stark ähnelt.
Die Extraktion der Merkmale erfolgt mit Hilfe von Jets, die an *signifikanten Punkten* des Gesichts platziert werden. Diese Jets bestehen aus mehreren Gabor Wavelets. [**Hofmann2002**]

2.4.4.5 Gabor Wavelets

Die Gabor Wavelets werden oft in Kombination mit dem Elastic Bunch Graph Verfahren benutzt. Sie sind biologisch motivierte Faltungskernel. Sie sollen ähnliche Antworten liefern wie die retinale Ganglionschicht im Auge.

2.4.4.6 Eigenfaces

Abbildung 12: Von links nach rechts: durchschnittliches Gesicht und die ersten vier Eigengesichter (aus [Hofmann2002])

Die Methode der Eigenfaces basiert auf dem Verfahren der Karhunen-Loeve-Transformation (KLT), auch Principal Component Analysis (PCA) genannt. Sie wird zur

Dimensionsreduzierung bei Vektoren eingesetzt. Eine Dimensionsreduzierung ist beim diesem Verfahren auch nötig, da hier jedes Bild als ein Vektor der Dimension Breite x Höhe angesehen wird. Bei einem Bild von der Größe 1024 x 786 Pixel resultiert daraus ein Vektor mit 804864 Dimensionen. Jedoch lassen sich Gesichter durch eine allgemeine Klassifikation in einen kleinen Bereich des Vektorraums aller Bilder anordnen. Ziel ist es nun einen geeigneten Untervektorraum für Gesichtsbilder zu suchen. Die Basisvektoren dieses Untervektorraumes sind die sogenannten principal components. Originalgesichter können durch Linearkombination dieser Basisvektoren (Eigenvektoren) wieder angenähert werden.

2.4.5 Welche Verfahren gibt es für die Klassifikation?

Als Verfahren für die Klassifikation benutzt man die folgenden Verfahren:

- künstliche neuronale Netze
- Summe der Fehlerquadrate
- Euklidische Norm
- Nearest-Neighbour-Methode

Im folgenden wird nur die Klassifikation durch künstliche neuronale Netze besprochen, da diese Thema der Studienarbeit sind.

2.4.5.1 Neuronale Netze

Der Vorteil der künstlichen neuronalen Netze im Vergleich zu den anderen Verfahren liegt darin, dass bei verrauschten und unvollständigen Gesichtern, z.B. durch eine Überdeckung eines Schales, das künstliche neuronale Netz bis zu einem gewissen Grad dennoch das Gesicht erkennen kann. Es arbeitet also höchst tolerant gegenüber fehlenden Daten. Außerdem kann ein künstliches neuronales Netz von, aus verschiedenen Winkeln aufgenommenen, einzelnen Gesichtern dahingehend abstrahieren, dass es auch Gesichter interpolieren kann, die während der Trainingsphase nicht antrainiert wurden. Es kann aber keine Gesichter erkennen aus Winkeln, die sich außerhalb des gelernten Bereiches befinden. Es kann also nicht extrapolieren.

3 Untersuchung verschiedener künstlicher neuronaler Netze bezüglich Eignung für die Gesichtserkennung, insbesondere durch die Simulation von künstlichen neuronalen Netzen

An dieser Stelle sollten eigentlich die Ergebnisse einer Simulation präsentiert werden, die mit dem Programmpaket SNNS bzw. JNNS gemacht werden sollten. Diese Simulation sollte zeigen (und extrapolieren) wie schnell ein künstliches neuronales Netz in der Praxis konvergieren kann bei einem Bild eines Gesichtes einer bestimmten Größe. Außerdem sollte die Erkennungsleistung von verschiedenen Arten von neuronalen Netzen getestet werden.

Da einige Schwierigkeiten auftraten bei der Benutzung und Einbindung von SNNS in eigene Programme und die Zeit langsam zu Ende ging, habe ich mich entschieden in dieser Studienarbeit nur eine theoretische Analyse zu machen.

Um ein künstliches neuronales Netz mit Bildinformationen zu trainieren, müssen vorher per Merkmalsextraktion bestimmte Merkmale der Gesichter extrahiert werden. Dazu entschied ich mich für einfache rezeptive Felder.

Das Programm sollte in der Programmiersprache C geschrieben werden. Dadurch hätte ich die Möglichkeit gehabt den Kernel von SNNS direkt über Funktionen anzusprechen. Im C Programm hätte ich also selbst Funktionen schreiben müssen die Bilder einlesen, daraus die Merkmale extrahieren und dann dem Kernel in einem bestimmten Format übergeben. Da ich in C nur über grundlegende Kenntnisse verfüge hätte es den zeitlichen Rahmen für eine Studienarbeit gesprengt, mich nun tiefer mit C und den Kernelfunktionen zu beschäftigen. Außerdem hätte ich, um brauchbare Ergebnisse zu erzielen, einige Gesichter gebraucht zum testen. Ich habe zwar eine Gesichtsdatenbank im Internet gefunden, aber um die Daten zu benutzen, die in einem Rohformat abgespeichert sind, hätte ich wieder einigen zeitlichen Aufwand benötigt, was mindestens im Rahmen einer Diplomarbeit machbar wäre.

4 Bewertung und Integration von KNN gestützten Gesichtserkennungsverfahren

Biometrische Systeme werden im Labor entwickelt und außerhalb des Labors in anderen Umgebungen unter den verschiedensten Verhältnissen eingesetzt. Daher sollte es auch ein Verfahren geben, mit dem man einen biometrischen Algorithmus unter Realbedingungen testen und bewerten kann.

4.1 Rahmenwerk zur Bewertung und Integration biometrischer Algorithmen

Für das Testen von biometrischen Algorithmen kann das Rahmenwerk, welches in **[Brömme2002]** beschrieben wird, verwendet werden. Hier ist jeder einzelne Schritt, in dem Daten verändert bzw. analysiert werden, getrennt und die jeweiligen Ergebnisse der Module mit den Teilergebnissen werden in einer Datenbank aufgezeichnet für spätere Fehler- bzw. Leistungsanalysen. Durch die Hinzunahme einer biometrischen Datenbank in das Testrahmenwerk, lassen sich kontrolliert verschiedene Verfahren in verschiedenen Umgebungen automatisiert testen. In das Rahmenwerk lassen sich durch die Modularisierung nun auch KNN einfach integrieren.

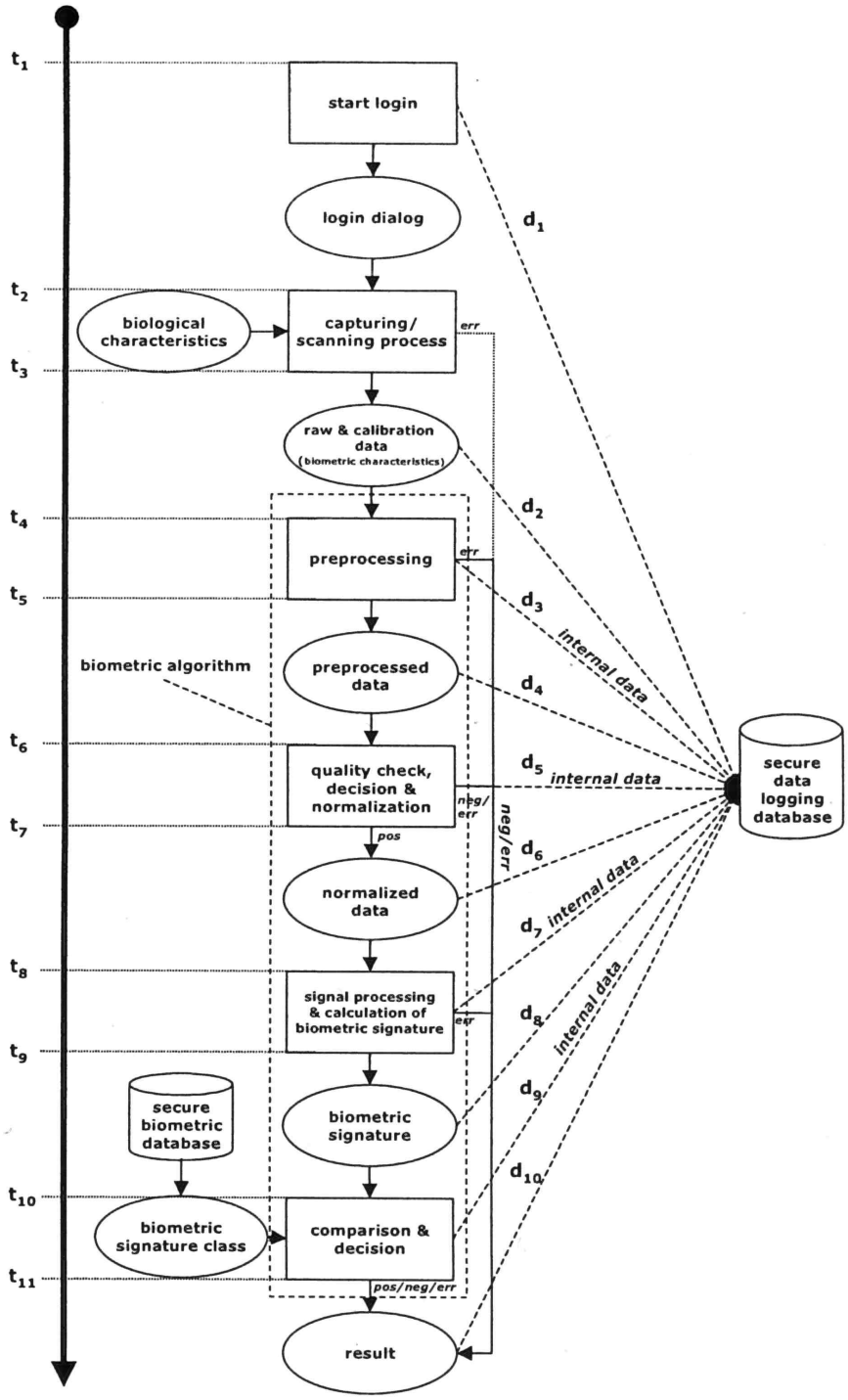

Abbildung 13: Prozess der biometrischen Authentikation mit Prozessdatenaufzeichnung (aus [Brömme2002])
(Mit freundlicher Genehmigung von Arslan Brömme)

Das Rahmenwerk besteht aus folgenden vier Modulen:

- **P-Modul**: Vorverarbeitung (preprocessing)
- **Q-Modul**: Qualitätsüberprüfung (quality check, decision & normalization)
- **S-Modul**: Berechnung der biometrischen Signatur mit Hilfe eines **Merkmalextraktionsverfahren** (signal processing & calculation of biometric signature)

- **D-Modul**: Vergleich und Entscheidung mit Hilfe eines Klassifikationsverfahrens (comparison & decision)

Im P-Modul werden die biometrischen Informationen vorverarbeitet (z.B. Kontrastverstärkung). Danach werden die vorverarbeiteten Informationen weitergereicht zum Q-Modul. Dieses Modul ist für die Qualitätsüberprüfung zuständig und führt eine Normalisierung durch, so dass nahezu alle erfassten biometrischen Informationen ein ähnliches Format besitzen.
Falls die Qualitätsüberprüfung positiv verläuft, wird z.B. das normalisierte Bild zum S-Modul weitergereicht, wo aus den biometrischen Merkmalen mit Hilfe von **Merkmalsextraktionsverfahren** eine Signatur erzeugt wird. Wichtig ist zu erwähnen, dass aus der Signatur aus datenschutzrechtlichen Gründen nicht wieder die biometrischen Merkmale, wie z.B. das Gesicht, rekonstruiert werden können sollten!

Um nun eine Auswertung der Authentikationsversuche zu ermöglichen, werden in den einzelnen Modulen quantitative Daten in eine sichere Datenaufzeichnungs-Datenbank aufgenommen. Folgende Informationen werden aufgenommen:

- Start- und Endzeit der Verifikation, sowie Eintrittszeit und Austrittszeit in bzw. aus den einzelnen Modulen
- Interne Zustandsdaten der einzelnen Module, sowie
- Ausgabedaten der einzelnen Module wie z.B.: normalisiertes Bild (Q-Modul) oder biometrische Signatur (S-Modul)

Durch diese Informationen wird gewährleistet, dass man genau zurückverfolgen kann, wo evtl. Fehler auftreten, bzw. Probleme und man kann die Leistungsfähigkeit der einzelnen Verfahren analysieren. Durch die Benutzung des Rahmenwerkes lässt sich auch die Leistungsfähigkeit der einzelnen Verfahren testen, sei es für die Merkmalsextraktion, wie auch für die Klassifikation.

4.2 Integration von künstlichen neuronalen Netzen in das Rahmenwerk für die biometrischen Authentikation

Ein künstliches neuronales Netz (KNN) ist generell für die Klassifikation zu verwenden, wie das weiter oben beschrieben wurde. Da nun im Rahmenwerk das D-Modul für die

Entscheidung zuständig ist, ob die aktuelle Signatur der gespeicherten ähnlich ist, können also künstliche neuronale Netze an dieser Stelle verwendet werden.

Das KNN muss bei der Verwendung im D-Modul folgende **Anforderungen** erfüllen (Punkte wurden aus Kapitel 2.4.2 übernommen):

- **Anforderung 1**: Hinzufügen einer neuen Person in das System(**enrollment**)
- **Anforderung 2**: Löschen einer Person aus dem System (**derollment**)
- **Anforderung 3**: Anpassung an ein neues Aussehen der authentizierten Person
- **Anforderung 4**: Vorhandensein eines Schwellenwertes um sich an unterschiedliche Umgebungen und Anforderungen anpassen zu können.
- **Anforderung 5**: Das Verknüpfen eines Gesichtes mit der Information, ob diese Person ggf. gefährlich ist, bzw. wie verfahren werden soll, z.B. soll Alarm geschlagen werden oder soll der Person nur temporär Eintritt gewährt werden (von 9 Uhr bis 20 Uhr)

Wie könnte nun die genaue Integration in das Modul aussehen?
Da die Realisierung des D-Moduls durch eine herkömmliche Datenbank erfolgen kann, muss für jede Person ein Datensatz vorhanden sein, welcher z.B. per PIN oder Name angesprochen wird. In diesem Datensatz ist nun ebenfalls ein KNN abgespeichert, welches mit den Merkmalen (aus der Merkmalsextraktion) der betreffenden Person trainiert wurde. Die aktuellen Merkmalsdaten werden nun dem KNN präsentiert, und das KNN entscheidet, ob die aktuellen Merkmalsdaten den abgespeicherten hinreichend ähnlich sind. Dabei kommen nun auch die Vorteile der KNN zum Zuge.

Um den Anforderungen gerecht zu werden, lassen sich folgende Lösungen verwenden:

- **Zu Anforderung 1:** Für jede neu anzulernende Person wird ein bereits „präpariertes“ KNN genommen und mit den aktuellen Merkmalsdaten der Person trainiert. Dieses kann automatisch erfolgen im Hintergrund oder/und auf einem anderen Rechner, wenn das Training des KNN etwas länger dauert.
- **Zu Anforderung 2:** Es wird lediglich der Datensatz aus der Datenbank gelöscht, so dass die Person sich nicht mehr in der Datenbank befindet. Es kann aber auch eine Markierung erfolgen, das diese Person keine Berechtigung mehr hat einzutreten. Dadurch kann bei fehlgeschlagenen Authentikationsversuchen genau zurückverfolgt werden, ob es sich bei der Person um eine bereits aus der Datenbank logisch gelöschten handelt.

- **Zu Anforderung 3:** Da einem künstlichen neuronalen Netz immer wieder neue Dinge antrainiert werden können, kann man auch, unter der Voraussetzung einer erfolgreichen Authentikation, dem künstlichen neuronalen Netz das veränderte Gesicht antrainieren. Da aus datenschutzrechtlichen Gründen keine Bilder abgespeichert werden dürfen von vorherigen Authentikationsversuchen, kann mit künstlichen neuronalen Netzen hier einfach und sicher eine automatische Anpassung an ein neues Aussehen erfolgen.
- **Zu Anforderung 4:** Da Ausgaben eines künstlichen neuronalen Netzes generell nicht mit ja oder nein erfolgen, sondern meistens eine reelle Zahl zwischen 0 und 1 ausgegeben wird, kann hier eine Schwelle definiert werden und die Ausgabe so durch einen einfachen Vergleich abgeprüft werden.
- **Zu Anforderung 5:** Da hier eine herkömmliche Datenbank verwendet wird, können in einem Datensatz beliebig viele (nur begrenzt durch das RDBMS-System) Informationen abgespeichert werden.

Bei der Inbetriebnahme eines Gesichtserkennungssystems, das die Klassifikation mit künstlichen neuronalen Netzen vornimmt, ist auf folgendes zu achten:

- Ein KNN muss vorher mit Gesichtern trainiert worden sein, um bereits verschiedene Klassen gebildet zu haben. Denn in der Klassifikation geht es ja darum, zu überprüfen, ob zu den aktuellen Merkmalsdaten, das KNN die „richtige“ Klasse ausgibt. Deshalb müssen vorher dem KNN bereist verschiedene Klassen antrainiert worden sein, damit es auch eine Unterscheidung geben kann.
- Es muss zu Anfang ein bestimmtes Merkmalsextraktionsverfahren ausgewählt worden sein, und während der gesamten Betriebszeit beibehalten werden. Denn mit dem ausgewählten Merkmalsextraktionsverfahren wird eine biometrische Signatur erzeugt, die dem künstlichen neuronalen Netz antrainiert wird. Wird nun während des Betriebes das Merkmalsextraktionsverfahren gewechselt, werden entsprechend andere Signaturen erzeugt als vorher, so dass das trainierte künstliche neuronale Netz normalerweise keine erfolgreiche Klassifikation mehr vornehmen kann.

Beim Aufnehmen einer neuen Person in das Gesichtserkennungssystem muss auf folgendes geachtet werden:

- Für das Training des künstlichen neuronalen Netzes sollten möglichst viele Gesichter aus verschiedenen Winkeln aufgenommen werden. Da ein künstliches

neuronales Netz zwischen verschiedenen Blickwinkeln interpolieren kann, ist es sinnvoll, einen großen Winkelbereich abzudecken.

Ziel bei der Benutzung eines Rahmenwerkes ist es, quantitative Aussagen treffen zu können, welches Verfahren für die Merkmalsextraktion und die Klassifikation in der Praxis in der Gesichtserkennung am besten geeignet ist. Durch die Aufzeichnung sämtlicher Daten die beim Prozess der Gesichtserkennung entstehen, können genaue Aussagen getroffen werden, welches Verfahren

- in kürzester Zeit, und
- mit dem besten Erkennungsergebnis

die Aufgabe erfüllt. Damit können bei Realtests Aussagen getroffen werden, ob das gewählte Verfahren gut genug ist.

5 Ergebnisse und Diskussion

Grundsätzlich ist hierbei herausgekommen, dass künstliche neuronale Netze durchaus eingesetzt werden können für die Gesichtserkennung in der biometrischen Authentikation.

Die Anforderungen die an ein Gesichtserkennungssystem gestellt werden, können durch das Benutzen von künstlichen neuronalen Netzen erfüllt werden. Dabei sind gewisse Probleme, die bei einem Gesichtserkennungssystem auftreten, weder ein Problem der Merkmalsextraktion noch der Klassifikation. Denn Zwillinge wird man in absehbarer Zukunft selbst mit den besten Gesichtserkennungssystemen nicht auseinanderhalten können.
Deshalb wird die Gesichtserkennung nur in begrenztem Maße eingesetzt werden können, wie z.B. für die Profilaktivierung an technischen Geräten oder zur Identifizierung von Kriminellen in einem Stadion, was durchaus schon praktiziert wird. Die Benutzung in sicherheitsrelevanten Bereichen wie z.B. in Hochsicherheitstrakten ist jedoch nicht zu empfehlen, da die Wahrscheinlichkeit hoch ist, dass das System einer nicht berechtigten Person Zutritt gewährt. Eine Kombination von Gesichtserkennung und Stimmenerkennung ist in solchen Bereichen ebenfalls fragwürdig, da man die Stimme mit einem Stimmenrekorder aufnehmen kann.

Das sicherste biometrische Merkmal ist im Moment die DNA. Die DNA kann allerdings missbraucht werden, da die DNA nicht nur einmalig ist für jede Person die es gibt, sondern auch Informationen enthält über mögliche genetisch veranlagte Krankheiten. Das nächstsicherste biometrische Merkmal ist die Iriserkennung. Allerdings kann die Iriserkennung im Moment nur in bestimmten Bereichen eingesetzt werden, denn für das Einscannen der Iris muss die betreffende Person die Iris noch einem Apparat präsentieren, also explizit wollen, dass sie erkannt wird. Für die Erkennung von Kriminellen in einem Stadion oder die Erkennung „auf der Straße“, lässt sich die Iriserkennung noch nicht verwenden.

6 Zusammenfassung und Ausblick

Gesichtserkennungssysteme lassen sich nur in bestimmten Bereichen zufriedenstellend einsetzen. Dabei spielen nicht so sehr die Verfahren eine Rolle, sondern die Tatsache, dass das biometrische Merkmal Gesicht nicht geeignet ist in sicherheitsrelevanten Bereichen eingesetzt zu werden, da die Wahrscheinlichkeit, dass zwei Personen ähnliche Gesichter haben, nicht so gering ist als eigentlich erwünscht.
Künstliche neuronale Netze lassen sich aus den genannten Vorteilen in der Gesichterkennung verwenden. Allgemein können künstliche neuronale Netze auch mit anderen biometrischen Merkmalen verwendet werden. Dabei hilft die Integration in das beschriebene Rahmenwerk, da sich dort modular verschiedene Merkmale, die dazugehörigen Merkmalsextraktionsverfahren und Klassifikationsverfahren einsetzen lassen.

Da eine Simulation von verschiedenen Arten von künstlichen neuronalen Netzen in dieser Arbeit nicht stattfinden konnte, überlasse ich es einem Nachfolger dieses zu versuchen. Dabei kann und sollte das beschriebene Rahmenwerk verwendet werden, da es sich meiner Meinung nach am besten für den Vergleich und für den praktischen Einsatz eignet. Erst dadurch lässt sich genau bestimmen, welche Art von künstlichen neuronalen Netzen sich am besten eignet für die Gesichtserkennung im praktischen Einsatz.

Interessant wäre eine Untersuchung, ob und wie sich künstliche neuronale Netze für die biometrische *Identifikation* benutzen lassen können. Dabei käme ein weiterer Vorteil von künstlichen neuronalen Netzen zum Zuge. Denn bei der Identifikation geht es ja darum, zu einem Gesicht die dazugehörige Person zu ermitteln. Mit Verfahren, die keine künstlichen neuronalen Netze benutzen, muss man dabei eine ganze Datenbank durchsuchen. Dabei braucht man, je nachdem welches System verwendet wird, viel Zeit und viel Speicherplatz. Es muss also ein Kompromiss eingegangen werden zwischen

- Geschwindigkeit der Erkennung
- Speicherplatz für die Signaturen
- Genauigkeit bzw. Sicherheit der Erkennung (davon hängen Schnelligkeit und Speicherplatz ab).

Bei einem Einsatz von künstlichen neuronalen Netzen erfolgt die Erkennung ohne eine langwierige Suche und braucht nur den Platz des neuronalen Netzes. Denn neuronale Netze geben sofort die dazugehörige Klasse aus zu einem Eingabemuster. Problem dabei wäre u.a. das Verlernen bzw. derollment.

Ich werde mich in meiner Diplomarbeit nicht mehr mit dem Thema Biometrik beschäftigen, sondern werde übergehen zur Simulation von biologischen neuronalen Netzen. Hier haben Arbeiten von **[Maass2000]** ,**[Maass2001]** und **[Maass2002]** gezeigt, das pulsierende neuronale Netze, die ähnlich dem biologischen Prinzip funktionieren, berechnungsstärker sind als herkömmliche künstliche neuronale Netze.

Es wird momentan versucht, mit mathematisch-logischen Verfahren Maschinen Intelligenz, Lernfähigkeit, Anpassungsfähigkeit und Abstraktionsfähigkeit „beizubringen“. Aber meiner Meinung nach sind gerade diese Dinge die Domäne von neuronalen Netzen. Deshalb werde ich mich in meiner Diplomarbeit damit beschäftigen.

7 Literaturliste

[Arbib1998] Arbib, Michael A. ed.: The Handbook of Brain Theory and Neural Networks. MIT-Press (Cambridge, MA), 1998.

[BARG2002] Broschüre *„Biometrik in der Gesellschaft“ ,* Biometric Authentication Research Group, University of Hamburg Januar 2002, http://agn-www.informatik.uni-hamburg.de/hct/biomtrie.pdf

[Bartlett2001] Bartlett, Marian Stewart: Face Image Analysis by Unsupervised Learning, Kluwer Academic Publishers, 2001

[Brömme2001a] 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

[Brömme2002] Brömme, A., Kronberg, M., Ellenbeck, O., Kasch, O.: A Conceptual Framework for Testing Biometric Algorithms within Operating Systems’ Authentication, SAC 2002, Madrid

[Duden1995] DUDEN - Das Fremdwörterbuch © Bibliographisches Institut & F.A. Brockhaus AG, Mannheim 1995

[Görz1995] Görz, Günther (Hrsg.): Einführung in die Künstliche Intelligenz, Addison-Wesley, 1995

[Hofmann2002] http://www.markus-hofman.de

[Henke1999] Henke, Stefan: Verfahren der biometrischen Authentisierung und deren Unterstützung durch Chipkarten, 1999

[Jain1999] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.:Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.

[Kandel1991] Kandel, E., Schwartz, J.H., Jessel, T.M.: Principles of Neural Science, 3rd Edition, Appleton & Lange, 1991.

[Lorenz1996] Lorenz, Rolf J., *„Grundbegriffe der Biometrie“* Gustav Fischer Verlag, Stuttgart/Jena/Lübeck/Ulm, 1996

[Maass2000] Maass, W. Computing with Spikes, 2000

[Maass2001] Maass, W., Bishop, C. M.: Pulsed Neural Networks. MIT-Press (Cambridge, MA), 2001

[Maass2002] Maass, W., Markram, H.(2002): On the Computational Power of Recurrent Circuits of Spiking Neurons, 2002

[Rojas1996] Rojas, Raúl:Theorie der neuronalen Netze - Eine systematische Einführung. 4. korrigierter Nachdruck. Springer, 1996.

[Zell1994] Zell, Andreas: Simulation Neuronaler Netze. 1. edition. Addison-Wesley, 1994.