

Universität Regensburg
Wirtschaftswissenschaftliche Fakultät
Institut für Wirtschaftsinformatik

Diplomarbeit

Biometrische Zugangskontrolle durch Gesichtserkennung

vorgelegt von

Christian Maier

Online-Version: www.chmai.de

Eingereicht am 01. September 2005

Betreuer:

Prof. Dr.-Ing. Hannes Federrath,
Dipl.-Wirtsch-Inf. Klaus Plöbl

Aufgabenstellung

Thema: Biometrische Zugangskontrolle durch Gesichtserkennung

Bereits seit Jahren wird im Bereich der Biometrie intensiv an Verfahren gearbeitet, die zum Zweck der merkmalsbasierten Authentifizierung eingesetzt werden. Ein Anwendungsbeispiel dafür ist ein Zugangskontrollsystem, das berechnete Personen anhand biometrischer Eigenschaften erkennt und nur diesen Zugang gewährt.

Diese Arbeit soll untersuchen, welche Anforderungen an Authentifizierungsverfahren abhängig von deren Einsatzzweck gestellt werden. Es soll auf die Unterschiede zwischen merkmalsbasierten und besitz- bzw. wissensbasierten Authentifizierungsverfahren eingegangen werden.

Es ist zu untersuchen, ob die bekannten Verfahren der Gesichtserkennung die erarbeiteten Anforderungen erfüllen und wo die Schwächen dieser Verfahren liegen. Zu Demonstrationszwecken ist ein Prototyp eines Gesichtserkennungssystems zu entwickeln und gegebenenfalls in ein vorhandenes chipkartenbasiertes Zugangskontrollsystem zu integrieren.

Abstract

Diese Diplomarbeit vergleicht Authentifizierungsverfahren, die auf Wissen, Besitz und biometrischen Merkmalen basieren. Es wird zuerst ein Überblick gegeben, in dem die verschiedenen Methoden vorgestellt werden. Dabei werden die Grundlagen der Biometrie näher erläutert.

Der Vergleich der wissens-, besitz- und merkmalsbasierten Ansätze erfolgt anhand von Anforderungen, die an Authentifizierungsverfahren gestellt werden. In drei Anwendungsszenarien wird zudem gezeigt, welche Fragestellungen sich beim Einsatz biometrischer Authentifizierung in der Praxis ergeben können.

Das biometrische Verfahren der Gesichtserkennung wird im Anschluss daran detaillierter betrachtet. Zur Veranschaulichung der Erkennungsleistung dieser Authentifizierungstechnik werden die Ergebnisse einiger Evaluationen beschrieben. Außerdem wird der Prototyp eines Gesichtserkennungssystems vorgestellt, der im Rahmen dieser Diplomarbeit entwickelt wurde.

Inhaltsverzeichnis

Inhaltsverzeichnis	iv
1 Einleitung	1
2 Grundlagen der Authentifizierung	3
2.1 Begriffe	3
2.2 Authentifizierung im Kontext der IT-Sicherheit	4
3 Gruppierung der Authentifizierungsverfahren	6
3.1 Wissensbasierte Verfahren	6
3.2 Besitzbasierte Verfahren	6
3.2.1 Magnetstreifenkarten	7
3.2.2 Chipkarten	7
3.2.3 RFID-Systeme	8
3.2.4 Eindeutige Erkennung eines Gegenstandes	8
3.3 Biometrische Verfahren	9
3.3.1 Ablauf der Authentifizierung	10
3.3.2 Anforderungen an biometrische Merkmale	12
3.3.3 Klassifizierung der untersuchten Merkmale	13
3.3.4 Beispiele biometrischer Merkmale	14
3.3.5 Messgrößen der Leistungsfähigkeit biometrischer Systeme	18
3.3.6 Zusammenfassung	24
4 Anforderungen an die Authentifizierung: Ein Vergleich der Verfahren	26
4.1 Authentifizierung einer Person	26
4.2 Sicherheit und Robustheit gegen Überwindungsversuche	27
4.2.1 Angreifer beherrscht das Authentifizierungssystem	27
4.2.2 Angriff ohne bewusste Unterstützung durch berechtigte Benutzer	28
4.2.3 Angriff mit bewusster Beteiligung berechtigter Benutzer	30
4.2.4 Zusammenfassung	31
4.3 Reaktionsmöglichkeiten bei Kompromittierung der Authentifizierungsdaten	31
4.4 Datenschutz und Verbraucherschutz	33
4.5 Benutzerfreundlichkeit und Benutzerakzeptanz	35
4.6 Niedrige Kosten und hohe Geschwindigkeit	37
4.7 Übersicht und Vergleich der Verfahren	39
4.8 Anforderungen in unterschiedlichen Szenarien	39
4.8.1 Zutrittskontrolle im Zoo von Hannover	40
4.8.2 Zutrittskontrolle zu Lehrstuhlräumen an der Universität Regensburg	41
4.8.3 Kritische Betrachtung der Speicherung biometrischer Daten in Reisepässen	42

5	Gesichtserkennung	45
5.1	Grundlagen der Gesichtserkennung	46
5.1.1	Spezifische Problemstellung der Gesichtserkennung	46
5.1.2	Erfassung des Merkmals	48
5.1.3	Ablauf der Gesichtserkennung: Vom Bild zum Template	49
5.1.4	Matching	52
5.2	Ergebnisse bedeutender Evaluationen von Gesichtserkennungssystemen .	53
5.2.1	Face Recognition Vendor Test 2002	54
5.2.2	BioFace	57
5.2.3	BioP I und II	59
5.2.4	Zusammenfassung	60
6	Prototypische Implementierung einer Gesichtserkennung	61
6.1	Das Verfahren der Eigenfaces	61
6.2	Entwicklung des Prototyps	63
6.2.1	Einsatzszenario	63
6.2.2	Anforderungen an den Prototyp	63
6.2.3	Implementierung	64
6.3	Übersicht der Funktionen	65
6.3.1	Initialisierung des Gesichtsraumes	65
6.3.2	Erzeugen der Referenztemplates bekannter Benutzer	65
6.3.3	Die Ausführungsmodi der Gesichtserkennung	66
6.3.4	Konfiguration des Prototyps zur Nutzung von Webcam-Bildern .	67
6.4	Test des Prototyps	68
6.4.1	Vorbereitung des Bildmaterials	68
6.4.2	Ablauf des Tests	70
6.4.3	Auswertung der Testergebnisse	71
6.4.4	Beurteilung der Testergebnisse	71
6.4.5	Kritische Beurteilung des Tests	73
6.5	Möglichkeiten für die weitere Entwicklung des Prototyps	73
7	Zusammenfassung und Ausblick	75
7.1	Ziele	75
7.2	Vorgehensweise zur Erreichung der Ziele	75
7.3	Ergebnisse	75
7.4	Ausblick	76
	Anhang	77
	Literaturverzeichnis	I
	Datenträgerverzeichnis	VIII

1 Einleitung

Die weite Verbreitung und Verwendung von Informations- und Kommunikationstechnologie führt immer mehr zu einer Abhängigkeit von IT-Systemen. Sowohl Industriebetriebe als auch weite Teile der Dienstleistungsbranche sind ohne die Unterstützung durch Computer und moderne Kommunikationsnetze nicht mehr vorstellbar. Dies betrifft auch öffentliche Behörden und Einrichtungen vieler Staaten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht in [Bun04a] von einer weiter zunehmenden Abhängigkeit aus und begründet dies mit folgenden Entwicklungen: Der *steigende Vernetzungsgrad* erhöht die Bedeutung von robusten Datennetz-Infrastrukturen. Damit ist auch eine „Öffnung der IT-Systeme nach außen“ verbunden, was Angriffe über Netzwerkverbindungen erst ermöglicht. Die *IT-Verbreitung* nimmt zu und erstreckt sich auf neue Bereiche, die bisher noch ohne IT-Unterstützung ausgekommen sind. Dies lässt sich auch durch die *steigende Leistungsfähigkeit* der Hard- und Software begründen. Durch die zunehmende Abhängigkeit steigt das Gefährdungspotential überproportional, was unter anderem durch mangelhaftes Wissen und eine immer größere Angriffsfläche begründet wird.

Die zunehmende Abhängigkeit ist ein Grund für das wachsende Bedürfnis nach IT-Sicherheit, also dem weitestgehenden Ausschluss von Risiken und Gefahren in Bezug auf IT-Systeme. Von hoher Bedeutung ist in diesem Zusammenhang die Feststellung und Überprüfung der Identität einer Person. Viele Verfahren und Maßnahmen zur Erreichung einer höheren Sicherheit setzen voraus, dass zwischen berechtigten und unberechtigten Benutzern unterschieden werden kann.

Auch außerhalb des Kontextes der IT-Sicherheit nimmt die Bedeutung der Identitätskontrolle zu. Seitdem die Bekämpfung des internationalen Terrorismus zum Ziel vieler Regierungen erklärt wurde, fordern verschiedene Stellen die Einführung von sicheren Ausweisdokumenten. Zusätzlich zu dem bereits vorhandenen Passbild sollen biometrische Daten, wie zum Beispiel der Fingerabdruck, maschinenlesbar gespeichert werden. Insbesondere beim grenzüberschreitenden Reiseverkehr soll dadurch das Vortäuschen einer falschen Identität verhindert werden.

Die Identitätskontrolle ist also ein aktuelles Thema, das nicht nur im Bereich der IT-Sicherheit von großer Bedeutung ist. Auch die Diskussion um die Einführung von biometrischen Merkmalen in Ausweisen trägt zur Motivation dieser Arbeit bei. Ein Verfahren, das sowohl im Kontext der IT-Sicherheit, als auch im Zusammenhang mit Biometrie-Reisepässen oft genannt wird, ist die Gesichtserkennung.

Es soll in Abschnitt 2 zunächst auf die Grundlagen und Begriffe der Identitätsfeststellung eingegangen werden. Abschnitt 3 stellt die Gruppierung in wissens-, besitz- und merkmalsbasierte Authentifizierungsverfahren vor und dient als Einführung in das Thema Biometrie. Danach werden in Abschnitt 4 die Anforderungen an Authentifizierungsmethoden erläutert. Wissens-, besitz- und merkmalsbasierte Ansätze werden auf die Erfüllung dieser Anforderungen hin untersucht und dabei miteinander verglichen. Um die Leistungsfähigkeit von Gesichtserkennungssystemen besser einschätzen zu können,

werden in Abschnitt 5 die Grundlagen dieser Authentifizierungstechnik erläutert und im Anschluss daran die Ergebnisse einiger Evaluationen beschrieben. In Abschnitt 6 wird schließlich der Prototyp vorgestellt, der im Rahmen dieser Diplomarbeit entwickelt wurde. Abschnitt 7 fasst die Ergebnisse dieser Arbeit zusammen.

2 Grundlagen der Authentifizierung

2.1 Begriffe

Der Begriff **Authentifizierung** bezeichnet nach Abts und Mülder „den Nachweis der Identität eines Benutzers“ [AM04, S. 138]. Dies entspricht der Definition des englischen Wortes *authentication* von Peltier et al. in [PPB05, S. 236]: „The act of verifying the identity of a system entity [...] and the entity’s eligibility to access computerized information.“ In der deutschsprachigen Literatur werden die Begriffe *Authentifikation*, *Authentikation* und *Authentisierung* häufig gleichbedeutend mit Authentifizierung verwendet. So schreibt Aebi in [Aeb04, S. 13]: „Unter Authentifikation (oder auch Authentisierung) versteht man die Identifizierung und Sicherstellung, dass man auch diejenige Person (Organisation, Programm, ...) ist, die man vorgibt zu sein.“ Eine einheitliche Übersetzung des englischen „Authentication“ konnte sich bisher nicht durchsetzen. In dieser Arbeit wird durchgängig Authentifizierung verwendet und als die Überprüfung und Feststellung der Identität einer Person verstanden. Auch die Identität von Komponenten eines IT-Systems, zum Beispiel eines Rechners im Netzwerk, muss in vielen Fällen geprüft werden. Man spricht auch hier von Authentifizierung. Da biometrische Verfahren bei technischen Geräten nicht anwendbar sind, beschränkt sich diese Arbeit auf die Authentifizierung von Personen.

Nach dem „Abgleichsverfahren“ [Nol02, S. 22] werden die Authentifizierungsarten **Verifikation** und **Identifikation** unterschieden. Bei der Verifikation wird geprüft, ob eine Person auch diejenige ist, die sie vorgibt zu sein. Es erfolgt also ein 1:1-Vergleich. Im Gegensatz dazu ist die Identifikation ein 1:n-Vergleich: Es wird kontrolliert, ob eine Person eine aus vielen bekannten Personen ist und um welche der bekannten Personen es sich handelt. Die Identifikation soll eine „zunächst unbekannte Person [...] identifizieren“ [Nol02, S. 22].

Die Authentifizierung dient in vielen Fällen dazu, zwischen berechtigten und unberechtigten Personen zu unterscheiden. Ein IT-System soll nach [FP02, S. 10] die Identität seiner Kommunikationspartner prüfen und nur mit berechtigten Partnern weiter kommunizieren. Dieser Vorgang wird als **Zugangskontrolle** bezeichnet, wobei Zugang hier die Nutzung von Informations- und Kommunikationstechnologie bedeutet. Um Verwechslungen zu vermeiden, wird das Betreten eines Geländes oder einer Raumzone (Gebäude, Raum...) als Zutritt definiert [MS02, S. 386], die zugehörige Berechtigungsprüfung als **Zutrittskontrolle**.

Die bisher genannten Kontrollen unterscheiden nur berechtigte und unberechtigte Personen. Dies ist in vielen Bereichen der Informationstechnologie nicht ausreichend und wird deshalb um die **Zugriffskontrolle** ergänzt. Einer Person werden bestimmte Rechte eingeräumt, der Vorgang der Rechtevergabe wird als **Autorisation** bezeichnet [FP02, S. 11]. Ein gewährtes Recht kann bei einem IT-System zum Beispiel darin bestehen, dass ein Subjekt (Benutzer) eine bestimmte Operation (Lesen, Schreiben, Löschen...) an einem bestimmten Objekt (Datei) ausführen darf. Diese Rechte können mittels einer Zugriffskontrollmatrix, über definierte Rollen oder in anderer Form verwaltet werden. Die

Autorisation ist erst nach einer Authentifizierung sinnvoll, da die Identität der Person bekannt und geprüft sein muss.

2.2 Authentifizierung im Kontext der IT-Sicherheit

In der Einleitung wurde bereits erwähnt, dass die Feststellung und Überprüfung der Identität einer Person im Zusammenhang mit IT-Sicherheit von hoher Bedeutung ist. Dies soll, gegliedert nach den drei Schutzziele der IT-Sicherheit, näher erläutert werden. Die Schutzziele werden mit den Begriffen *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* zusammengefasst. In Anlehnung an [Fed02] werden diese im Folgenden genauer beschrieben. Durch Beispiele soll zudem die Bedeutung einer korrekten Authentifizierung und damit deren Relevanz im Kontext der IT-Sicherheit dargestellt werden.

Vertraulichkeit

Vertraulichkeit ist gegeben, wenn Informationen nur berechtigten Personen zugänglich sind; Daten müssen also vor unberechtigter Kenntnisnahme geschützt sein. Bei der Übertragung von Daten über Netzwerke wird durch Verschlüsselungsverfahren oder Steganographie¹ ein Verlust der Vertraulichkeit verhindert. Ein ungewollter Informationsgewinn kann auch schon dadurch entstehen, dass Unberechtigte die Verbindung zweier Kommunikationspartner entdecken können, um so eine Informationsflussanalyse zu erstellen. Deshalb zählen auch die Verfahren der Anonymität und Unbeobachtbarkeit zum Gebiet der Vertraulichkeit.

Da innerhalb eines nicht-öffentlichen IT-Systems, zum Beispiel in einem Unternehmen, Daten oft unverschlüsselt gespeichert und übertragen werden, ist es wichtig, dass nur berechtigte Personen Zugang haben. Dies wird dadurch realisiert, dass sich Personen zur Nutzung eines Rechners anmelden müssen und nur so auf vertrauliche Daten zugreifen können. Die Authentifizierung erfolgt in der Regel mit Benutzername und Passwort.

Integrität

Integrität bezeichnet den Schutz der Daten vor unberechtigter Manipulation und die Zurechenbarkeit zu einer verantwortlichen Person. Es muss möglich sein, eine Veränderung von Daten zu erkennen, insbesondere wenn diese über öffentliche Kommunikationsnetze transportiert werden. Mit kryptographischen Verfahren können Prüfsummen, sogenannte *Message Authentication Codes*, erstellt werden, die eine Verfälschung des Inhalts einer Nachricht erkennbar machen. *Qualifizierte elektronische Signaturen* ermöglichen sogar die Zurechenbarkeit: Eine vertrauenswürdige Stelle bestätigt mit einem Zertifikat, dass ein bestimmter Signaturschlüssel einer bestimmten Person gehört. Der private Signaturschlüssel dient zum Signieren von Nachrichten oder Dateien, die Überprüfung der

¹Einbettung der vertraulichen Informationen in unverdächtige Hülldaten, wodurch die Existenz einer geheimen Nachricht verborgen werden kann.

Signatur erfolgt mit dem öffentlichen Schlüssel. Somit ist die Integrität einer signierten Nachricht² gewährleistet und außerdem die Nachricht dem Inhaber des Zertifikats zurechenbar [SL02].

Der private Signaturschlüssel darf nur dem Inhaber zugänglich sein, da ansonsten jeder andere in seinem Namen Nachrichten oder Dateien signieren könnte. Deshalb schreibt die Signaturverordnung [Bun01] in §15 Absatz 1 vor, dass der Signaturschlüssel nicht preisgegeben werden darf. Danach müssen sichere Signaturerstellungseinheiten gewährleisten, dass eine „Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale“ [Bun01, §15, Abs. 1, Satz 1] stattgefunden hat, bevor der Signaturschlüssel angewandt wird. In der Praxis bedeutet dies, dass der private Schlüssel auf einer Chipkarte gespeichert ist und erst nach Eingabe einer PIN³ ein Signaturvorgang durchgeführt werden kann.

Verfügbarkeit

Sind Daten oder andere Ressourcen zu einem vorgegebenen Zeitpunkt für berechtigte Personen nutzbar, ist die Verfügbarkeit gegeben. Die Erreichbarkeit, das heißt die Möglichkeit der Kontaktierung einer Person oder einer Maschine, ist ein ähnliches Schutzziel. Nach [Fed02] gibt es bisher „keine ausgereiften Verfahren“ zum Schutz vor dem Verlust von Verfügbarkeit. Zumindest vor Angriffen, die einen physischen Zugang zum IT-System bedingen, kann eine sichere Authentifizierung bei der Zutrittskontrolle schützen. Sabotage oder Diebstahl durch nicht zutrittsberechtigte Personen wird verhindert, wenn diese nicht zu den schützenswerten IT-Systemen gelangen können.

Zusammenfassung

Die Authentifizierung kann also durchaus als eine Voraussetzung für weitergehende Maßnahmen der IT-Sicherheit angesehen werden. Denn nur wenn IT-Systeme zwischen berechtigten und unberechtigten Personen unterscheiden können, sind viele Maßnahmen zur Erhöhung der IT-Sicherheit erst möglich. Damit ist die Authentifizierung auch ein Ansatzpunkt für mögliche Angriffe: Gelingt es einem Angreifer, die Identität eines berechtigten Benutzers vorzutäuschen, so kann er mit dessen Rechten im IT-System agieren und möglicherweise großen Schaden anrichten.

Das Vorgehen zum Erreichen eines Grundschutzes für IT-Systeme und verschiedene Maßnahmen sind in [Bun04a] ausführlich beschrieben. Es ist aber wichtig zu beachten, dass allein mit einer verlässlichen Authentifizierung kein sicherer IT-Betrieb gewährleistet ist. Denn auch berechtigte Benutzer können Angreifer auf ein IT-System sein. Dies sollte in einem Sicherheitskonzept natürlich berücksichtigt werden.

²Nachricht steht in diesem Zusammenhang für die signierten Daten, zum Beispiel Nachrichtentexte oder Dateien.

³Persönliche Identifikationsnummer

3 Gruppierung der Authentifizierungsverfahren

Um ein dem Schutzbedarf angemessenes Sicherheitsniveau zu erreichen, muss ein geeignetes Authentifizierungsverfahren eingesetzt werden. Man unterscheidet die folgenden drei Gruppen von Methoden:

- Authentifizierung durch **Wissen**
- Authentifizierung durch **Besitz**
- Authentifizierung durch **personenspezifische Merkmale (Biometrie)**

Werden Techniken aus verschiedenen Gruppen kombiniert, so spricht man von einer Multifaktor-Authentifizierung [LP04, S. 13]. Die einzelnen Verfahren werden nun vorgestellt. Anschließend werden in Abschnitt 4 die Anforderungen an Authentifizierungsverfahren dargestellt und die verschiedenen Techniken miteinander verglichen.

3.1 Wissensbasierte Verfahren

Die Authentifizierung erfolgt durch die Prüfung von Wissen. Nur wer ein Passwort, eine persönliche Identifikationsnummer (PIN) oder Transaktionsnummer (TAN) kennt, wird als berechtigte Person identifiziert. Die Eingabe des geforderten Wissens erfolgt über eine Tastatur oder eine andere, einfach zu bedienende Benutzerschnittstelle. Ein Passwort kann zeitlich beschränkt oder nur für eine bestimmte Anzahl an Authentifizierungsvorgängen gültig sein. Ein Beispiel dafür sind die im Online-Banking eingesetzten Transaktionsnummern, die nur ein einziges Mal verwendet werden können.

3.2 Besitzbasierte Verfahren

Der Besitz eines Gegenstandes wird geprüft und so der Besitzer authentifiziert. Das einfachste Beispiel für einen solchen Gegenstand ist ein Schlüssel, der den Besitzer dazu berechtigt, ein bestimmtes Schloss zu öffnen [MS02, S. 126f]. Auch Ausweise und andere von Behörden ausgestellte Dokumente, wie zum Beispiel der Führerschein, können zur Authentifizierung verwendet werden.

Für den Einsatz besitzbasierter Verfahren in Informations- und Kommunikationssystemen ist es wichtig, dass die Prüfung maschinell durchgeführt werden kann. Weit verbreitet sind deshalb Kunststoffkarten, auf denen die für die Authentifizierung verwendete Information gespeichert ist. Die wichtigsten Kartentypen werden nun vorgestellt. Anschließend werden zwei Verfahren gezeigt, mittels derer die Zuordnung von Authentifizierungsgegenständen zu einer bestimmten Person erfolgen kann.

3.2.1 Magnetstreifenkarten

Die Daten werden auf einem Magnetstreifen gespeichert, der auf der Oberfläche einer Kunststoffkarte angebracht ist. Zum Datenaustausch ist, wie bei allen Kartentypen, ein Kartenleser erforderlich, wobei diese Bezeichnung nach [RE02, Glossar] auch für solche Geräte gilt, die einen schreibenden Zugriff ermöglichen. Magnetstreifenkarten müssen zur Datenübertragung immer in einen Kartenleser eingeführt werden, eine kontaktlose Übertragung ist nicht möglich. Auf die Daten des Magnetstreifens kann sowohl schreibend als auch lesend zugegriffen werden. Wie dies geschieht ist abhängig von der verwendeten Technologie: Nach [MS02, S. 130] gibt es unterschiedliche Eigenschaften des Magnetstreifens, Codiertechniken und Spurlagen, die durch die ISO-Norm 7811 spezifiziert sind. Weitere Spezifikationen, unter anderem zum magnetischen Material und den Schreib- und Leseverfahren, werden nach [MS02, S. 130 und S. 137] durch die Normen DIN 9785, DIN 66010, ISO 2894 und ISO 3554 definiert.

3.2.2 Chipkarten

Chipkarte ist nach [RE02, Glossar, S. 8] der „allgemeine Begriff für eine Karte, meist aus Kunststoff, die ein oder mehrere Halbleiterchips enthält.“ Man unterscheidet Speicherkarten und Mikroprozessorkarten. Erstere verfügen über „eine einfache Logikschaltung mit zusätzlichem schreib- und lesbaren Speicher“ [RE02, Glossar, S. 35]. Letztere sind mit einem Mikroprozessor, Arbeitsspeicher und dauerhaftem Speicher ausgestattet und haben ein eigenes Betriebssystem, um Anwendungen auf der Karte auszuführen. Da Mikroprozessorkarten selbst Berechnungen durchführen können, werden sie auch als Smart Cards bezeichnet, um ihren Vorteil gegenüber Speicherkarten hervorzuheben.

Die Datenübertragung zwischen Chipkarte und Kartenleser kann sowohl kontaktbehaftet als auch kontaktlos erfolgen. Chipkarten, die beide Übertragungswege ermöglichen, werden nach [RE02, Glossar, S. 12] Dual-Interface-Karten genannt. Die Schnittstelle bei der kontaktbehafteten Übertragung besteht aus sechs bis acht Kontaktflächen, über die die Daten mit elektrischen Signalen übertragen werden [RE02, Glossar, S. 21]. Bei der kontaktlosen Datenübertragung muss die Chipkarte die Daten senden, wofür Energie notwendig ist. Chipkarten verfügen aber in der Regel nicht über eine eigene Energiequelle, wie zum Beispiel eine Batterie. Deshalb erfolgt die Energieübertragung durch induktive Kopplung, so wie es auch in Transformatoren der Fall ist [MS02, S. 157]: Das Lesegerät erzeugt ständig ein elektromagnetisches Feld. Befindet sich eine Chipkarte im Bereich des Magnetfeldes, so nutzt eine Spule in der Chipkarte dieses Feld zur Energieaufnahme. Die normgerechte Bezeichnung nach ISO für diese Karten ist CICC (contactless integrated chip card). Diese Übertragungstechnik kann sowohl bei Speicherkarten als auch Mikroprozessorkarten Anwendung finden.

Gegenüber Magnetstreifenkarten haben Chipkarten einige Vorteile: Die Speicherkapazität ist deutlich höher, Smart Cards können frei programmiert werden und die Möglichkeit der kontaktlosen Datenübertragung erhöht den Komfort für den Benutzer und eröffnet neue Einsatzmöglichkeiten.

3.2.3 RFID-Systeme

Radio-Frequency-Identification ist nicht wie Magnetstreifenkarten oder Chipkarten ein bestimmter Kartentyp, sondern vielmehr eine Bezeichnung für alle „Verfahren zur automatischen Identifizierung von Objekten über Funk“ [IEB04, S. 15]. Die zu identifizierenden Gegenstände, bei RFID Transponder oder Tags genannt, können Personen zugeordnet und so zur Authentifizierung eingesetzt werden. Passive Transponder nutzen zur Energie- und Datenübertragung induktive Kopplung, kapazitive Kopplung oder das Backscatter-Verfahren, das auf dem Radarprinzip beruht. Eine Beschreibung der technischen Einzelheiten dieser Systeme würde in dieser Arbeit zu weit führen und ist für das Verständnis nicht erforderlich. Der interessierte Leser sei auf [Fin02] verwiesen.

RFID-Systeme können aber auch aktive Transponder verwenden, die über eine eigene Energiequelle verfügen oder an eine externe Energieversorgung angeschlossen werden. Für die Authentifizierung von Personen sind aktive Transponder aufgrund der Größe und des höheren Gewichts weniger geeignet.

RFID-Transponder gibt es in den unterschiedlichsten Bauformen, je nach verwendeter Frequenz und entweder aktiver oder passiver Ausführung. Kleinste passive Transponder könnten in Banknoten integriert werden, um die Fälschungssicherheit zu erhöhen. Hitachi hat solche Transponder bereits entwickelt [Hit03], die Medienberichten zufolge ab 2005 in die Banknoten der Europäischen Zentralbank integriert werden sollen [Sti03].

Die maximal mögliche Entfernung, bei der ein Datenaustausch zwischen Lesegerät und Transponder stattfinden kann, variiert je nach verwendeter Frequenz, Bauform und Energieversorgung des Transponders. Sie reicht von einigen Zentimetern bis zu über zehn Metern. Systeme mit Reichweiten von über 100 Metern befinden sich noch im Entwicklungsstadium [IEB04, S. 40].

Dank der Flexibilität und Anpassbarkeit an verschiedenste Anforderungen kann die RFID-Technologie in vielen Bereichen eingesetzt werden: Klebeetiketten bei der Warenkennzeichnung, Ohrmarken zur Identifikation von Zuchtvieh und aktive Transponder, die zum Zweck der Mautgebührenerfassung in Fahrzeuge eingebaut sind. Für die Authentifizierung von Personen wird RFID bereits eingesetzt, zum Beispiel in Form von Mitarbeiterausweisen zur Zutrittskontrolle [IEB04, S. 11]. Die kontaktlose Datenübertragung birgt jedoch auch Risiken: Daten könnten von unberechtigten Personen gelesen werden oder Angreifer das System mit gefälschten Daten täuschen. Die Probleme, die sich dadurch im Bereich der Authentifizierung von Personen ergeben, werden in Abschnitt 4.2 dargestellt. Für weitere Informationen zu den Chancen und Risiken des Einsatzes von RFID-Systemen sei auf [IEB04] verwiesen.

3.2.4 Eindeutige Erkennung eines Gegenstandes

Ein Authentifizierungssystem wird in den meisten Fällen nicht nur eine einzige Person erkennen müssen. Es gibt demzufolge für jeden Benutzer des Systems einen Gegenstand, zum Beispiel eine Chipkarte, der dem Benutzer zugeordnet ist. Damit sich die Chipkarte

eines Benutzers von den Chipkarten anderer Benutzer unterscheidet, muss sie eindeutig erkennbar sein. Zwei verbreitete Erkennungsmethoden werden hier vorgestellt.

Die erste Methode ist recht einfach und kann mit den verschiedensten Magnetkarten, Chipkarten und RFID-Transpondern sowie mit von Menschen lesbaren Ausweisen umgesetzt werden: Jeder Gegenstand erhält eine eindeutige Bezeichnung, die ihn von allen anderen Gegenständen unterscheidet. Dies kann zum Beispiel eine einfache Seriennummer bei Mitarbeiterausweisen oder die Kartenummer bei Kreditkarten sein. Diese Bezeichnung kann von einem Lesegerät erfasst werden und das Authentifizierungssystem kann eindeutig die zugeordnete Person feststellen. Man spricht daher von einer Identifikationsnummer.

Eine andere Möglichkeit sind sogenannte Challenge-Response-Verfahren, die meist auf symmetrischer Kryptographie basieren. Dazu muss die Karte in der Lage sein, Berechnungen durchzuführen. Magnetstreifenkarten oder einfache Speicherchipkarten können hier aufgrund fehlender Rechenleistung nicht zum Einsatz kommen. Für dieses Verfahren ist in jeder Karte ein individueller Schlüssel gespeichert, der nicht mit einem Kartenleser erfasst werden kann. Nur das Authentifizierungssystem darf diesen Kartenschlüssel kennen. Zur Authentifizierung wird eine zufällige Nachricht, zum Beispiel eine sehr große Zufallszahl, an die Karte geschickt. Die Karte berechnet aus dieser „Challenge“ und dem Schlüssel mittels eines kryptographischen Verfahrens eine Antwort („Response“). Die Antwort wird zusammen mit einer Identifikationsnummer an das Authentifizierungssystem zurück geschickt. Dieses kann anhand der Identifikationsnummer bestimmen, welchen Schlüssel die Karte verwendet und berechnet die zu erwartende Antwort. Nur wenn die empfangene mit der erwarteten Antwort übereinstimmt, gilt die Person als authentifiziert. Da es sich normalerweise um relativ große Zahlen handelt, ist ein zufälliges Erraten der richtigen Response nahezu ausgeschlossen.

3.3 Biometrische Verfahren

Authentifizierungsverfahren, die auf der Überprüfung von individuellen körperlichen Merkmalen von Personen basieren, werden biometrische Verfahren genannt. Der Begriff *Biometrie* setzt sich aus den griechischen Worten *bios* (Leben) und *metron* (Maß) zusammen und bezeichnet demnach die „Wissenschaft von der Körpermessung an Lebewesen“ [No102, S. 20].

Die ursprüngliche Bedeutung des Begriffs Biometrie beschränkt sich nicht auf die Personenerkennung, sondern umfasst „alle Bereiche der Lebenswissenschaften, in denen mit Hilfe von empirischen Untersuchungen, also anhand von Zahlen, Erkenntnisse über medizinische, biologische, psychologische oder ökologische Zusammenhänge gewonnen werden“ [Deu03, S. 2]. Um eine klare begriffliche Trennung zu erreichen, bezeichnet *biometrische Authentifizierung* die automatische Identifikation oder Verifikation der Identität einer Person, basierend auf deren physiologischen und verhaltenstypischen Merkmalen („the automatic identification or identity verification of an individual based on physiological and behavioral characteristics“ [Way00, S. 21]). Sowohl in der wissenschaftlichen

Literatur als auch im allgemeinen Sprachgebrauch wird Biometrie als Kurzform des Begriffs „biometrische Authentifizierung“ verwendet, so auch in dieser Arbeit.

Es wird nun zuerst der Ablauf biometrischer Authentifizierungsverfahren geschildert und in einer Grafik dargestellt. Danach soll die Frage beantwortet werden, welche individuellen, körperlichen Merkmale zur Authentifizierung überprüft werden können. Dazu werden zuerst die Anforderungen an die Merkmale aus [Mun02, S. 148] und [Bro05] zusammengefasst und beschrieben. Es wird eine Möglichkeit der Klassifizierung biometrischer Merkmale vorgestellt und auf die Varianten der Entstehungsursachen personenspezifischer Merkmale eingegangen. Die bedeutendsten biometrischen Merkmale werden erläutert. Nach einer Einführung in die Kennzahlen der Leistungsfähigkeit biometrischer Systeme werden die Ergebnisse dieses Abschnitts zusammengefasst.

3.3.1 Ablauf der Authentifizierung

Unabhängig vom untersuchten Merkmal läuft die biometrische Authentifizierung, wie bei [Bun05c, S. 1–2] beschrieben, immer nach dem gleichen Schema ab: Das Merkmal einer zu authentifizierenden Person wird von einem geeigneten Sensor erfasst. Aus den Rohdaten werden bestimmte Ausprägungen extrahiert und zu einem *Template* zusammengefasst. Das Template, das aus den aktuellen Rohdaten extrahiert wurde, ist das Anfragetemplate. Dieses wird beim *Matching* mit einem vorher gespeicherten Referenztemplate verglichen und als Ergebnis des Vergleichs ein bestimmter Ähnlichkeitswert (Score) errechnet. Eine *Akzeptanzschwelle* definiert das Maß an Ähnlichkeit, das mindestens erreicht werden muss, damit die Person als authentifiziert gilt. Wird die Person erkannt und damit authentifiziert, ist das Ergebnis *Match*. Ist die Ähnlichkeit nicht ausreichend, lautet die Entscheidung *Non-Match*. Zur Veranschaulichung ist der Ablauf der Authentifizierung in Abbildung 1 dargestellt.

Die Referenztemplates müssen natürlich vor der Authentifizierung erzeugt und gespeichert werden. Dies geschieht im sogenannten *Enrollment*. Das Merkmal wird auch hier mit einem geeigneten Sensor erfasst, die relevanten Informationen werden extrahiert und als Template zusammengefasst. Zu einer Person können bei Bedarf auch mehrere Templates gespeichert werden. Dies ist abhängig vom verwendeten System und vom untersuchten Merkmal.

Das Matching, der Vergleich von Anfrage- und Referenztemplates, wird in der Praxis nie zu einer absoluten Übereinstimmung führen. Zwei affine Aufnahmen, das heißt die Rohdaten desselben biometrischen Merkmals derselben Person, werden immer Unterschiede aufweisen. Diese können auf Veränderungen der Ausprägung des Merkmals, zum Beispiel durch Alterung, Krankheit oder Verletzung, zurückgeführt werden. Auch beabsichtigte Änderungen am äußeren Erscheinungsbild einer Person, zum Beispiel eine geänderte Frisur, Kosmetik oder Sehhilfen, können bei manchen Merkmalen einen Einfluss haben. Zuletzt spielt auch die Variation der Aufnahmebedingungen eine Rolle, zum Beispiel unterschiedliche Lichtverhältnisse, die Positionierung des Merkmals am Sensor und andere Faktoren.

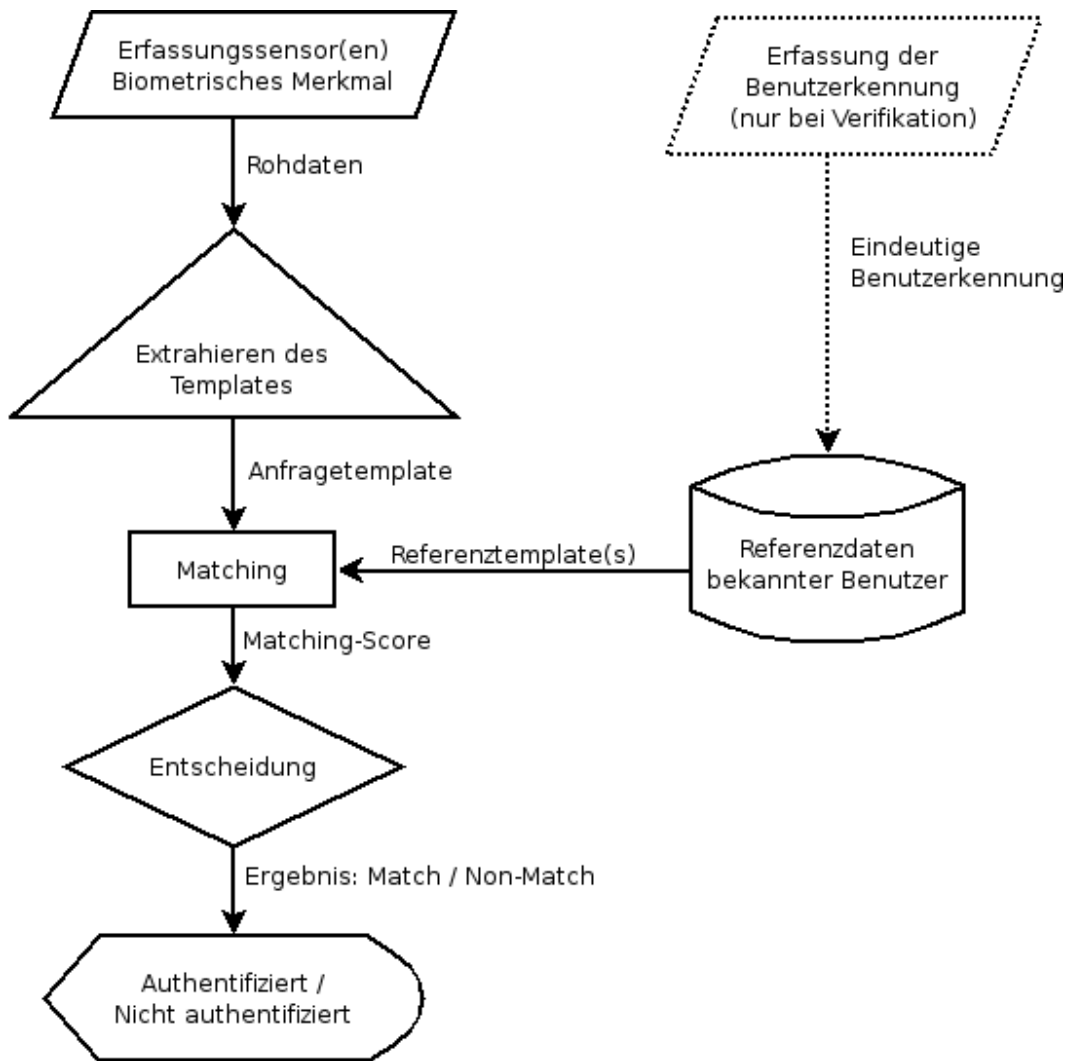


Abbildung 1: Ablauf einer biometrischen Authentifizierung

Bei Identifikation und Verifikation (siehe Abschnitt 2.1) unterscheidet sich der Ablauf geringfügig. Zur Identifikation der Person wird das Anfragetemplate mit allen gespeicherten Referenztemplates verglichen. Dagegen soll bei der Verifikation nur geprüft werden, ob das Anfragetemplate ausreichende Ähnlichkeit zu den Templates⁴ genau einer Person hat. Dazu muss bekannt sein, welche Person zu authentifizieren ist, denn nur dann können die passenden Referenztemplates gefunden werden. Zu diesem Zweck wird eine eindeutige Benutzerkennung an einem zusätzlichen Eingabegerät erfasst. Kommt dabei zum Beispiel eine Chipkarte zum Einsatz, handelt es sich um eine Multifaktor-Authentifizierung.

Die Form der Speicherung der Referenztemplates kann sich bei den beiden Verfahren unterscheiden. Zur Identifikation muss ein Vergleich mit allen Referenztemplates erfolgen, es liegt also nahe, die Daten zentral an einer Stelle zu speichern. Bei der Verifikation hat man die Wahl zwischen zentraler und dezentraler Datenhaltung. Es ist also auch möglich, das Referenztemplate zum Beispiel auf einer Chipkarte zu speichern, die dem Benutzer ausgehändigt wird. Bei der Authentifizierung wird dann verglichen ob der, der die Chipkarte benutzt, auch derjenige ist, dessen Referenztemplate auf der Karte gespeichert ist. Da nur der Benutzer über die Daten verfügt, gilt diese Speicherungsform als datenschutzfreundlicher als die zentrale Speicherung [Pro02, S. 123].

Welcher Sensortyp zum Einsatz kommt, hängt vom erfassten Merkmal ab. Bei sogenannten *multimodalen Verfahren* werden mehrere biometrische Merkmale erfasst und ausgewertet. Dazu sind unter Umständen unterschiedliche Typen von Sensoren nötig. Bei multimodalen Verfahren ist es abhängig von der Implementierung, wie die Daten der unterschiedlichen Sensoren zusammengefasst werden: Es ist denkbar, aus den Rohdaten nur ein Template zu erstellen und damit den Vergleich durchzuführen. Die andere Variante ist, für jeden Sensortyp einzelne Templates zu speichern, jedes Template mit den entsprechenden Referenztemplates zu vergleichen und dann die Ergebnisse der einzelnen Vergleiche zu einem Gesamtergebnis zusammenzufassen.

3.3.2 Anforderungen an biometrische Merkmale

Folgende Anforderungen werden an Merkmale gestellt, die in biometrischen Authentifizierungsverfahren untersucht werden. Die Anforderungen an die Verfahren selbst werden in Abschnitt 4 behandelt.

- **Einzigartigkeit:** Zwei verschiedene Personen dürfen nicht dieselbe Ausprägung des Merkmals aufweisen. Nur so ist die eindeutige Authentifizierung einer Person möglich.
- **Verbreitung:** Möglichst viele Personen müssen dieses Merkmal in auswertbarer Form aufweisen.

⁴Gilt auch für den Fall, dass nur ein Template zur Person gespeichert ist.

- **Zeitliche Dauerhaftigkeit:** Die Ausprägung des Merkmals soll sich im Laufe der Zeit nicht oder nur sehr wenig verändern. Insbesondere darf sich das Merkmal nicht in kurzen Zeitabständen ändern.
- **Messbarkeit:** Das Merkmal muss mit technischen Instrumenten messbar sein. Die Dauer der Erfassung sollte im Bereich von wenigen Sekunden liegen.
- **Benutzerfreundlichkeit:** Die Messung der Merkmalsausprägung muss für den Benutzer möglichst einfach und komfortabel sein.
- **Lebenderkennung:** Es muss überprüfbar sein, ob ein untersuchtes Merkmal von einer lebenden Person stammt oder ob es sich um einen Täuschungsversuch handelt.

In [Mun02, S. 148] werden nur die ersten drei Anforderungen genannt, da diese die Grundvoraussetzung bilden, um ein Merkmal zu Authentifizierungszwecken heranzuziehen. Bromba [Bro05] ergänzt diese um die beiden Bedingungen Messbarkeit und Benutzerfreundlichkeit, wodurch die Anwendbarkeit in der Praxis besser berücksichtigt wird. Nach Meinung des Autors dieser Arbeit, hat die Durchführbarkeit einer Lebenderkennung einen entscheidenden Einfluss auf die Sicherheit eines Authentifizierungssystems.

3.3.3 Klassifizierung der untersuchten Merkmale

Die Merkmale werden üblicherweise in *aktive* und *passive Merkmale* unterteilt [Nol02, S. 21]. Erstere sind verhaltenstypische Merkmale, für deren Erfassung die zu authentifizierende Person ein bestimmtes Verhalten aktiv ausführen muss. In [Thi02, S. 315] werden Verfahren, die auf aktiven Merkmalen beruhen, *dynamische Verfahren* genannt. Sie haben die Eigenschaft, dass diese nicht ohne die Interaktion einer Person erfasst werden können. Passive Merkmale sind physiologische Eigenschaften, ihre Ausprägung beschreibt also eine Beschaffenheit des Körpers. Die darauf beruhenden Verfahren werden als *statische Verfahren* bezeichnet.

Die Einzigartigkeit der einmaligen, unverwechselbaren Ausprägung eines Merkmals kann verschiedene Ursachen haben. Bromba nennt drei Ursachen [Bro05]: Die Ausprägung kann *genotypisch*, das heißt durch Vererbung, bestimmt sein. Andere Eigenschaften werden zufällig ausgebildet, oft bereits in einer frühen Phase der embryonalen Entwicklung. Diese Entstehungsform nennt man *randotypisch*. Eine weitere Ursache für verschiedene Ausprägungen sind *konditionierte*, das heißt erlernte Eigenschaften. Nicht alle Merkmale lassen sich ausschließlich einer Entstehungsursache zuordnen.

Will man die Merkmale nach ihrer Brauchbarkeit zur Authentifizierung bewerten, muss die Entstehungsform berücksichtigt werden [Bro05]: Durch rein genotypische Merkmale lassen sich eineiige Zwillinge nicht unterscheiden. Äußere Einflüsse und Stimmungen wirken auf stark konditionierte Merkmale. Da es sich bei diesen um erlernte Eigenschaften handelt, können rein konditionierte Merkmale nachgeahmt werden. Um wirkliche Eindeutigkeit zu erreichen, sollte die Entstehungsursache randotypische Anteile enthalten. Nur dann können auch eineiige Zwillinge unterschieden werden.

3.3.4 Beispiele biometrischer Merkmale

Es werden nun einige bedeutende biometrische Merkmale vorgestellt. Hier kann jedoch nur ein Überblick gegeben werden, in dem nicht alle Aspekte der einzelnen Merkmale und deren Erfassungsverfahren genannt werden. Es wird das Ziel verfolgt, dem Leser einen Einblick in die Fähigkeiten, aber auch Grenzen biometrischer Systeme zu geben. Dies ist erforderlich, um die Authentifizierung auf Basis von Wissen, Besitz und Biometrie miteinander vergleichen zu können. Das Gesicht als Merkmal und das Verfahren der Gesichtserkennung wird in Abschnitt 5 selbstverständlich noch detaillierter behandelt. In [Bre02, S. 35–82] findet sich eine ausführliche Übersicht zahlreicher biometrischer Merkmale, die deren Erfassung über verschiedene Sensoren, Verfahren zur Extraktion relevanter Eigenschaften und die jeweiligen Vor- und Nachteile der Verfahren beinhaltet. Auf Grundlage dieser Quelle wurde auch die folgende Übersicht erstellt.

Fingerabdruck

Der Fingerabdruck, auch Daktylogramm genannt, ist der Abdruck der Fingerbeere⁵ auf Gegenständen. Papillarlinien, das sind schleifen-, wirbel- und bogenförmig angeordnete Hautleisten, ergeben ein Muster, das sich bereits im Embryonalstadium randotypisch ausbildet. Es gilt als absolut einzigartig und bleibt ein Leben lang konstant. Abnutzung durch manuelle Tätigkeiten, Krankheiten und Verletzungen können allerdings bewirken, dass der Fingerabdruck nicht mehr ausreichend ausgeprägt ist, um damit eine Authentifizierung durchzuführen. So wird in [Uni02, S. 148] davon ausgegangen, dass bei zwei bis fünf Prozent der Bevölkerung der Fingerabdruck nicht erfasst werden kann.

Mittlerweile gibt es zahlreiche Technologien zur Erfassung des Fingerabdrucks. Am verbreitetsten sind die optischen und die kapazitiven Sensoren. Zur Lebenderkennung können die Temperatur und Leitfähigkeit der Haut sowie der Puls gemessen werden. Allerdings wurde in den letzten Jahren mehrfach festgestellt, dass sich nahezu alle verfügbaren Sensoren mit einfachen Mitteln täuschen lassen. Ein sehr bekanntes Paper stammt vom japanischen Kryptographen Tsutomu Matsumoto [MMYH02], der elf Sensoren mit Attrappen aus Gelatine täuschen konnte. Ähnliche Untersuchungen wurden auch vom Chaos Computer Club [Sta04b] und der Zeitschrift c't [TKZ02] erfolgreich durchgeführt. Trotzdem ist die Authentifizierung durch Fingerabdruck die Technologie mit dem höchsten Marktanteil⁶ und umfasst mit 48% knapp die Hälfte des Umsatzes der biometrischen Industrie im Jahr 2004 [Unb05, S. 9].

Gesicht

Der Mensch erkennt ihm bekannte Personen in erster Linie an deren Gesicht. Es liegt deshalb nahe, auch dieses Merkmal zur Authentifizierung zu verwenden. Das Gesicht ist definiert als der vordere Teil des Kopfes, der die Bereiche Stirn, Augen und Mund umfasst. Knochenbau, Gesichtsmuskulatur und Haarwuchs beeinflussen maßgeblich die

⁵Tastballen am Ende der Innenseite eines jeden Fingers [Wik05a].

⁶Marktanteile der anderen Technologien werden in Tabelle 2 auf Seite 25 angegeben.

Ausprägung des Merkmals Gesicht. Da es sich um ein genotypisches Merkmal handelt, unterscheiden sich eineiige Zwillinge kaum. Die Frage nach der Eindeutigkeit eines Gesichtes kann nur schwer beantwortet werden. Man müsste voraussetzen, dass objektiv festgestellt werden kann, ob ein Gesicht gleich einem anderen ist: Obwohl die Gesichter eineiiger Zwillinge auf den ersten Blick identisch aussehen, lassen sich selbst bei diesen Unterschiede feststellen. Die Einzigartigkeit hängt also letztendlich davon ab, wie gut ein System Gesichter unterscheiden kann.

Die Erfassung des Gesichtes erfolgt mit einer Kamera, die einzelne Bilder oder Videos aufzeichnet. Stehen mehrere Kameras zur Verfügung, so ist es möglich eine dreidimensionale Darstellung des Gesichtes zu berechnen. Die berührungslose Erfassung gilt als besonders benutzerfreundlich. Zweidimensionale Gesichtserkennung erfordert auf jeden Fall eine Lebenderkennung, da sonst bereits mit einem einfachen Foto eine Täuschung des Systems möglich ist. Die Registrierung des Augenzwinkerns oder der Reflexionseigenschaften menschlicher Haut können zumindest diesen einfachen Angriff abwehren.

Iris

Das menschliche Auge kann ebenfalls zur Authentifizierung genutzt werden. Ein auswertbares Merkmal ist die Iris, der farbige Ring um die Pupille. Das komplexe, mehrschichtige Gewebegeflecht entsteht im dritten bis achten Schwangerschaftsmonat und bleibt ein Leben lang stabil. Lediglich die Farbe der Iris kann sich ändern. Die Farbinformation wird bei der Iriserkennung allerdings nicht ausgewertet und hat somit keinen Einfluss auf das Ergebnis. Das Merkmal entsteht zufällig und sogar die Iris im linken und rechten Auge derselben Person unterscheiden sich signifikant. Die Wahrscheinlichkeit, dass zwei Iris identisch sind, wird mit $1 : 10^{32}$ angegeben.

Die Erfassung erfolgt mit einer Videokamera und nicht, wie oft fälschlicherweise angenommen wird, durch Laserabtastung. Es gibt mehrere Techniken, die eine Lebenderkennung ermöglichen: Die Pupille verengt und erweitert sich kontinuierlich und bewirkt eine stetige, elastische Verformung des Irismusters. Attrappen wie bedruckte Kontaktlinsen, Glasaugen oder Fotos sind statisch und können so als Fälschung erkannt werden. Zusätzlich können natürlich auftretende Reflexionen des Auges mit Infrarotlicht getestet werden. Aufgrund der hohen Einzigartigkeit des Merkmals und einer verlässlichen Lebenderkennung eignet sich die Iriserkennung zur Authentifizierung bei sehr hohem Schutzbedarf.

Retina

Die Retina, auch Netzhaut genannt, liegt im Inneren des Augapfels und dient zur Aufnahme von Lichtreizen, die dann an das Gehirn weitergeleitet werden. Direkt hinter der Retina liegt eine Aderhaut, die Chorioidea, die aus Bindegewebsfasern und zahlreichen Blutgefäßen besteht. Sie ist das eigentlich untersuchte Merkmal, der Begriff Retinaerkennung ist daher nicht korrekt. Das Merkmal gilt als einzigartig, auch eineiige Zwillinge können dadurch unterschieden werden. Es gilt als das konstanteste physiologische Merkmal des Menschen.

Die Aufnahme des Musters der Adern erfolgt optisch mit Infrarotlicht. Eine genaue Positionierung des Auges vor der Kameraöffnung ist erforderlich. Zur Lebenderkennung können dieselben Techniken verwendet werden, wie sie beim Merkmal Iris beschrieben wurden. Wie die Iriserkennung wird auch die Retinaerkennung zum Einsatz bei hohem Schutzbedarf empfohlen.

Handgeometrie

Bei der Vermessung der Hand können verschiedene Eigenschaften erfasst werden, zum Beispiel Länge, Breite und Krümmung der Finger oder Stärke und Position von Gelenken. Die meisten Systeme erfassen nur den Umriss der Hand mit einer Kamera. Details wie Linien, Farben oder Narben werden bei den meisten Systemen nicht ausgewertet. Problematisch ist bei diesem Merkmal, dass es erst nach Abschluss des Wachstums einigermaßen stabil bleibt und selbst dann Alterungsprozesse und Umgebungseinwirkungen auftreten. Wie beim Gesicht ist es auch hier schwierig, eine Aussage über die Einzigartigkeit zu treffen.

Es wurde bereits erwähnt, dass die Erfassung mit einer Kamera erfolgt. Die Hand muss dazu in einer bestimmten Position auf eine Auflagefläche gelegt werden. Zur Lebenderkennung können dieselben Techniken wie bei der Fingerabdruckerkennung zum Einsatz kommen.

Dynamik der Unterschrift

Beim Unterschreiben eines Dokuments erzeugt eine Person einen Schriftzug des eigenen Namens. Diese Unterschrift gilt in Gesetz und Handel als Willenserklärung und kann deshalb als einzigartig angenommen werden. Dabei ist jedoch nicht nur der Schriftzug einzigartig, sondern auch die Dynamik der Erstellung. Variieren können zum Beispiel Schreibgeschwindigkeit, Beschleunigung, Anpressdruck und Neigungswinkel des Stiftes. Die Dynamik der Unterschrift ist hauptsächlich konditioniert, wird aber auch durch vererbte Eigenschaften beeinflusst (z. B. die Ausbildung der Muskulatur in Hand und Arm). Wie einzigartig das Merkmal ist, hängt sehr davon ab, welche Ausprägungen erfasst werden.

Für die Erfassung der einzelnen Kenngrößen der Dynamik existieren entsprechende Sensoren, die zum Beispiel den Schreibdruck oder den Neigungswinkel des Stiftes messen. Es existieren drei Varianten, wie diese Sensoren zu einer „Erfassungseinheit“ kombiniert werden: Bei der ersten Variante kommen spezielle sensitive Tablett zum Einsatz, auf denen mit einem herkömmlichen Stift oder einem Spezialstift (ohne Sensorik) geschrieben wird. Die zweite Variante integriert alle Sensoren in einen Spezialstift, der auch über eine gewöhnliche Schreibeinheit verfügt. So kann auf normalem Papier unterschrieben werden. Schließlich gibt es noch Systeme, die die Sensoren auf Tablett und Spezialstift aufteilen und beides in Kombination einsetzen. Die Dynamik der Unterschrift ist ein aktives Merkmal, eine Lebenderkennung ist daher überflüssig.

Stimme

Die Stimme des Menschen wird sowohl durch angeborene anatomische Unterschiede als auch durch konditionierte Sprachgewohnheiten geprägt. Es kann keine allgemein gültige Aussage über die Einzigartigkeit getroffen werden. Man nimmt an, dass diese weit unter der Eindeutigkeit eines Fingerabdrucks liegt. Die Stimme ändert sich besonders in der Wachstumsphase während der Pubertät und bleibt danach relativ konstant. Durch relativ häufig auftretende Erkrankungen, wie Erkältungen oder Heiserkeit, kann das Merkmal bei einzelnen Personen über einen längeren Zeitraum nicht verfügbar sein. Die Erfassung der Stimme erfolgt mit einem Mikrofon. Bei der Auswertung wird in textabhängige und textunabhängige Verfahren unterschieden, je nachdem ob das Erkennungssystem vom Benutzer einen bestimmten Text erwartet oder nicht. Die Lebenderkennung zu realisieren gestaltet sich schwierig. Mit hochwertigen Geräten können Aufnahmen erzeugt werden, deren Qualität für eine erfolgreiche Täuschung ausreichend ist. Abhilfe sollen textabhängige Systeme schaffen, die bei jedem Authentifizierungsvorgang einen von mehreren, vorher festgelegten Texten prüfen. Wenn die Texte nicht ständig geändert werden und mehrfache Abfragen desselben Textes zulässig sind, erhöht das jedoch nur den zeitlichen Aufwand des Angreifers.

Dynamik des Tastaturanschlages

Die Dynamik des Tastaturanschlages, auch als Tipprrhythmus oder Tippverhalten bezeichnet, wird durch Kenngrößen wie Geschwindigkeit, Korrektur- und Pausenverhalten sowie die Fehlerhäufigkeit bestimmt. Auch der Gebrauch der Shifttaste und Buchstabendreher können als Kenngröße verwendet werden. Je nach Anzahl der erfassten Merkmale und der Länge des geprüften Textes variiert die Einzigartigkeit des Merkmals. Das Tippverhalten ist konditioniert und bei geübten Schreibern relativ stabil. Personen, die nur wenig bis gar nicht mit einem Computer arbeiten, dürften dieses Merkmal nicht in auswertbarer Form aufweisen.

Die Verwendung einer herkömmlichen Tastatur zur Erfassung des Tippverhaltens hat den Vorteil, dass keine zusätzliche Hardware gebraucht wird. Eine Lebenderkennung ist überflüssig, da die Details der Tippdynamik in der erforderlichen Genauigkeit nur schwer erfasst und noch schwerer nachgeahmt werden können.

Andere Merkmale

Es sind auch noch andere Merkmale zur Authentifizierung von Personen geeignet, die hier jedoch nicht alle genannt werden können. Einige interessante Ansätze sollen dennoch erwähnt werden. Die Ohrmustererkennung befindet sich, ebenso wie die Erfassung der Gangart, noch in der Entwicklung. Die Bewegung der Lippen wird in Kombination mit Gesichts- und Stimmerkennung bereits in einem biometrischen Erkennungssystem verwendet. Auch der Träger der menschlichen Erbinformation, die DNS⁷, kann zur eindeutigen Erkennung dienen. Die Analyse ist jedoch sehr zeitaufwändig. Zudem kann aus der Erbinformation auf eventuell bestehende Erbkrankheiten geschlossen werden,

⁷Desoxyribonukleinsäure

was verständlicherweise zu Bedenken bezüglich des Datenschutzes führt. Ein Einsatz in automatischen Authentifizierungssystemen ist auf absehbare Zeit nicht vorstellbar.

3.3.5 Messgrößen der Leistungsfähigkeit biometrischer Systeme

Um die Leistungsfähigkeit eines biometrischen Systems zu beurteilen, werden verschiedene Kennzahlen ermittelt. Diese werden jeweils für verschiedene Arten von Fehlern berechnet, die in diesem Abschnitt vorgestellt werden.

Fehler bei der Entscheidung Match oder Non-Match

Beim Vergleich von Anfrage- und Referenztempleate können verschiedene Fälle auftreten, wie sie in [Bun05a, S. 3] beschrieben sind: Werden Aufnahmen desselben Merkmals derselben Person verglichen (affine Merkmale), so nennt man diese Fälle *Genuines*. Dagegen sind *Impostors* diejenigen Fälle, bei denen nicht affine Merkmale verglichen werden, zum Beispiel der Fingerabdruck des rechten Daumens von einer Person mit dem Fingerabdruck des rechten Daumens einer anderen Person. Auch wenn der Fingerabdruck des Daumens einer Person mit dem Fingerabdruck des Zeigefingers derselben Person verglichen wird, spricht man von nicht affinen Merkmalen.

Ein Fehler tritt dann auf, wenn ein Authentifizierungssystem bei nicht affinen Merkmalen die Entscheidung Match ermittelt. Es handelt sich demnach um eine falsche Akzeptanz. Hierfür wird auch in der deutschen Fachliteratur meist der englische Begriff **False Acceptance** verwendet. Am Beispiel eines Zutrittskontrollsystems bedeutet das, dass einer Person der Zutritt gewährt wird, die eigentlich nicht dazu berechtigt ist.

Ein weiterer möglicher Fehler ist die falsche Rückweisung, also die Entscheidung Non-Match bei affinen Merkmalen. In der Fachliteratur wird dies als **False Rejection** bezeichnet. Bei der Zutrittskontrolle würde in diesem Fall eine eigentlich zutrittsberechtigte Person zurückgewiesen. Der Authentifizierungsvorgang muss wiederholt werden.

Alle Fälle, die auftreten können, werden in Tabelle 1 dargestellt.

Ermitteltes Ergebnis	Tatsächlich sind die Merkmale	
	affin (Genuines)	nicht affin (Imposters)
Match	True Acceptance	False Acceptance
Non-Match	False Rejection	True Rejection

Tabelle 1: Mögliche Fehler bei der Entscheidung Match oder Non-Match (Tabelle erstellt nach [Bun05a, S. 4])

Die Anzahl der auftretenden Fehler ist für eine Bewertung der Leistungsfähigkeit eines Verfahrens nicht ausreichend. Um eine aussagekräftige Kenngröße zu erhalten, muss die Anzahl der Fehler in Relation zur Gesamtzahl der Vergleiche betrachtet werden. Man

unterscheidet, analog zu den zwei Fehlertypen, zwei Fehlerraten, die in [Bun05a, ab S. 5] beschrieben werden.

Die **False Acceptance Rate (FAR)** ist die Wahrscheinlichkeit, dass ein nicht affines Merkmal akzeptiert wird. Die FAR wird berechnet als das Verhältnis der Anzahl der False Acceptances zu der Gesamtzahl der Vergleiche nicht affiner Merkmale.

$$FAR = \frac{\text{Anzahl der False Acceptances}}{\text{Gesamtzahl der Vergleiche nicht affiner Merkmale}}$$

Die **False Rejection Rate (FRR)** ist die Wahrscheinlichkeit, dass ein affines Merkmal zurückgewiesen wird. Man berechnet die FRR als das Verhältnis der Anzahl der False Rejections zu der Gesamtzahl der Vergleiche affiner Merkmale.

$$FRR = \frac{\text{Anzahl der False Rejections}}{\text{Gesamtzahl der Vergleiche affiner Merkmale}}$$

Welche Faktoren beeinflussen nun die Fehlerraten? Die Anzahl der Fehler entspricht falschen Entscheidungen für Match oder Non-Match und diese Entscheidung hängt letztlich nur von der gewählten Akzeptanzschwelle ab. Unter der Annahme, dass alle Rahmenbedingungen unverändert bleiben, wird eine Veränderung des Schwellenwertes eine Auswirkung auf beide Fehlerraten haben.

Wird die Akzeptanzschwelle erhöht, so bedarf es eines höheren Matching-Scores um akzeptiert zu werden. Demzufolge wird die Gesamtzahl der Matches sinken. Dies führt einerseits zu einer geringeren FAR, da nun weniger nicht affine Vergleiche zu der Entscheidung Match führen. Andererseits steigt die Zahl der False Rejections, da auch bei den affinen Vergleichen weniger Matches erreicht werden. Die FRR steigt also an.

Das Senken der Akzeptanzschwelle wirkt in umgekehrter Richtung: Die Gesamtzahl der Matches steigt. Damit steigt die FAR, die FRR sinkt.

Wie sind diese Fehlerraten nun in der Praxis zu interpretieren? Die falsche Zurückweisung einer eigentlich berechtigten Person mag für die betroffene Person lästig sein. Es ist ein erneuter Versuch notwendig, der Zeit und, je nach untersuchtem Merkmal, ein gewisses Maß an Benutzerinteraktion erfordert. Die FRR ist also eine Kennzahl des Komforts: Nur Verfahren mit einer relativ geringen FRR werden auf Dauer von den Benutzern akzeptiert.

Die FAR ist dagegen eine sicherheitsrelevante Kennzahl, denn jede fälschlicherweise akzeptierte Person könnte einen Schaden verursachen. Vor allem beim Einsatz in Bereichen mit sehr hohem Schutzbedarf muss die FAR so gering wie möglich sein.

Fehler bei der Identifikation

Ein Fehler, der nur bei der Identifikation und nicht bei der Verifikation auftreten kann, ist die Falschzuordnung. Eine Person wird identifiziert, allerdings stimmt die vom Authentifizierungssystem zugewiesene Identität nicht mit der wahren Identität der Person

überein. Die Häufigkeit, mit der dieser Fehler auftritt, wird als **False Identification Rate (FIR)** bezeichnet [Bro05].

Bei Merkmalen mit einer relativ geringen Einzigartigkeit wird die FIR besonders hoch ausfallen. Da bei diesen Merkmalen auch die FAR höher ist als bei Merkmalen mit hoher Einzigartigkeit, wird empfohlen, sie nur zur Verifikation einzusetzen. Welche Verfahren für die Identifikation geeignet sind zeigt Tabelle 2 in Abschnitt 3.3.6.

Fehler bei der Merkmalerfassung

Bei manchen biometrischen Verfahren müssen die Rohdaten für die Extraktion des Templates in sehr hoher Qualität vorliegen. Das bedeutet, dass relevante Eigenschaften und Details in ausreichender Genauigkeit erkennbar sein müssen. Sind zum Beispiel die Fingerkuppen aufgrund manueller Tätigkeiten verschmutzt oder abgerieben, so können beim Extrahieren des Templates die charakteristischen Eigenschaften des Fingerabdrucks einer Person nicht erkannt werden. Die Ausprägung eines Merkmals variiert zudem bei Personen unterschiedlicher demographischer oder ethnischer Gruppen. So gelten die Fingerabdrücke einiger asiatischer Bevölkerungsgruppen als schwer vergleichbar [Uni02, S. 148]. Aus diesem Grund ist bei Systemen, die eine hohe Qualität der Rohdaten und eine klar erkennbare Ausprägung des Merkmals voraussetzen, in der Regel eine Qualitätskontrolle implementiert. Nur wenn die Aufnahme des Merkmals qualitativ hochwertig genug ist, wird die Aufnahme akzeptiert und weiter verarbeitet. Wie diese Qualität bestimmt wird, hängt in erster Linie vom Merkmal ab. Bei einem Fingerabdruck-Scan könnte die Erkennbarkeit von Papillarlinien ein Kriterium sein. Bei der Dynamik des Tastaturanschlags ist die Länge des eingegebenen Textes entscheidend.

Die Anzahl der Zurückweisungen von Aufnahmen ist für den Vergleich von Authentifizierungssystemen sicherlich interessant. Je nachdem in welcher Situation eine Aufnahme zurückgewiesen wird, werden zwei Kennzahlen unterschieden, die im Folgenden vorgestellt werden.

Personen, deren Merkmale bereits beim Enrollment nicht akzeptiert werden, können ein Authentifizierungssystem nicht nutzen. Man spricht daher von *Nutzerausfall* oder **Failure To Enroll**. Das Fehlschlagen des Enrollments kann durch zeitlich begrenzte oder dauerhafte Beeinträchtigungen hervorgerufen werden. Verschmutzungen oder Verletzungen sind temporär auftretende Ursachen und somit nur für eine bestimmte Zeitspanne ein Hindernis. Dagegen können eine körperliche Behinderung oder nicht heilbare Folgen einer Krankheit oder eines Unfalls dazu führen, dass eine Person ein bestimmtes biometrisches Merkmal überhaupt nicht oder nicht in auswertbarer Form aufweist. Eine betroffene Person ist auf Dauer vom Benutzerkreis ausgeschlossen.

Setzt man die Zahl der nicht „enrollbaren“ Personen ins Verhältnis zu der Gesamtzahl an Benutzern, erhält man die **Failure To Enroll Rate (FTE)** [Bun05a, S. 5].

Die zweite mögliche Situation ist, dass bei einem Authentifizierungsvorgang die Rohdaten als nicht auswertbar zurückgewiesen werden. Fehler dieser Art werden als **Failure To Acquire** bezeichnet. Es wird nur der „Normalbetrieb“ betrachtet, in dem Personen Authentifizierungsvorgänge durchführen. Die **Failure To Acquire Rate (FTA)** ergibt

sich aus dem Verhältnis der Anzahl der zurückgewiesenen Aufnahmen zur Gesamtzahl der Aufnahmen.

Ein Failure To Acquire hat natürlich zur Folge, dass der Authentifizierungsvorgang mit einem Non-Match abgeschlossen wird. Für die Berechnung der FAR und FRR ist die Ursache eines Non-Match allerdings unerheblich, es wird nicht zwischen Erfassungsfehlern und Unterschreiten der Akzeptanzschwelle unterschieden. Sollen diejenigen Non-Matches unberücksichtigt bleiben, die durch einen Failure To Acquire verursacht wurden, werden zwei weitere Kennzahlen herangezogen. Es werden nur die Authentifizierungsvorgänge betrachtet, bei denen das Merkmal in auswertbarer Form erfasst werden konnte. Analog zu den bekannten Fehlerarten unterscheidet man die **False Match Rate (FMR)** ($\hat{=}$ FAR) und **False Non-Match Rate (FNMR)** ($\hat{=}$ FRR).

Vergleichbarkeit von Systemen anhand der Kennzahlen

Ein Vergleich der Kennzahlen verschiedener Verfahren und Implementierungen kann nur unter bestimmten Voraussetzungen zu aussagekräftigen Ergebnissen führen. Die wichtigsten Bedingungen, die es zu beachten gilt, werden hier kurz vorgestellt. Eine ausführlichere Betrachtung der Kennzahlen und ihrer wechselseitigen Zusammenhänge findet der interessierte Leser in [Bro05].

Zunächst sei erwähnt, dass die Nennung einer False Acceptance Rate ohne die Nennung der False Rejection Rate keine verwertbare Information darstellt. Gleiches gilt natürlich umgekehrt. Durch Verschieben der Akzeptanzschwelle lassen sich beliebig hohe oder niedrige Werte erreichen. Ein Hersteller eines Authentifizierungssystems könnte zum Beispiel für sein Produkt eine FAR von 0,0001% angeben, es aber unerwähnt lassen, dass damit eine FRR von 75% oder mehr verbunden ist. Es wäre zwar ein relativ sicheres, aber auch ein in der Praxis unbrauchbares System.

Selbst wenn beide Kennzahlen angegeben werden, ist die Vergleichbarkeit zweier Systeme nur dann gegeben, wenn eine der Kennzahlen bei beiden Systemen den gleichen Wert hat. Beispielsweise sind zwei gegebene False Acceptance Rates verschiedener Verfahren nur dann vergleichbar, wenn sie zur selben False Rejection Rate berechnet wurden. Um dieses Problem zu umgehen, wird oft die **Equal Error Rate (EER)** angegeben: Die Wahrscheinlichkeit für einen Fehler, wobei gilt $FAR = FRR$. Abbildung 2 veranschaulicht den Zusammenhang von FAR, FRR und EER.

Ein weiteres Problem besteht darin, dass die Akzeptanzschwellen verschiedener Verfahren meist nicht vergleichbar sind. Der Score, das Maß für die Ähnlichkeit von Anfrage- und Referenztemplate, kann in unterschiedlichen Wertebereichen definiert sein und auf zwei Arten interpretiert werden: Soll der Score die Ähnlichkeit darstellen, so wird eine größere Ähnlichkeit durch einen höheren Score ausgedrückt. Umgekehrt könnte der Score aber auch als Abstand zwischen Anfrage- und Referenztemplate interpretiert werden. In diesem Fall gilt: Je kleiner der Score (und damit der Abstand), desto größer ist die Ähnlichkeit. Die Darstellung der FAR und FRR in Abhängigkeit vom Schwellenwert (wie in Abbildung 2) kann also nur dann zum Vergleich von Authentifizierungsverfahren

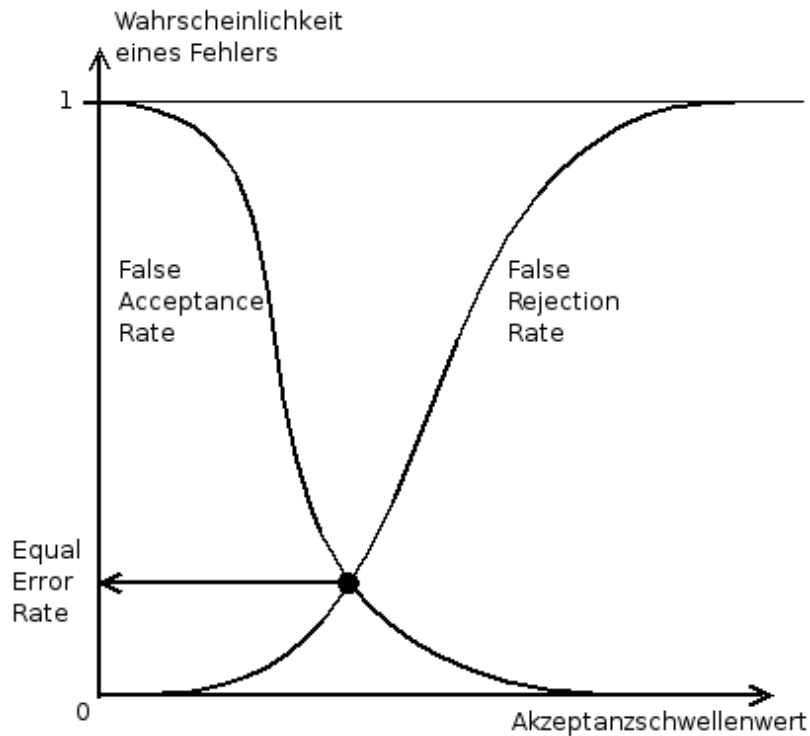


Abbildung 2: FAR, FRR und ERR (Erstellt nach [Bro05] und [Bun05a, S. 7].)

dienen, wenn dieselbe Interpretation, Dimension und Skalierung des Scores zugrunde gelegt wird. Diese Voraussetzung ist in der Regel nicht erfüllt.

Abhilfe schafft die Darstellung der *Receiver Operating Characteristic (ROC)* [Bun03, S. 26]. Hierzu wird die FAR als Funktion der FRR abgebildet. Die Definition der Akzeptanzschwelle bzw. des Scores hat somit keine Auswirkung auf den Verlauf der Kurve. Die ROC-Kurven verschiedener Verfahren sind direkt vergleichbar: Je näher die Kurve an den Achsen verläuft, desto weniger Fehler treten bei einem System auf. Abbildung 3 zeigt ein typisches ROC-Diagramm, ähnlich der Abbildung in [Bun03, S. 59].

Auf den ersten Blick mag die Failure To Enroll Rate als eine von den anderen Fehlerraten unabhängige Kennzahl erscheinen. Doch auch sie beeinflusst die FAR und FRR und muss deshalb beim Vergleich verschiedener Systeme beachtet werden. Die beim Enrollment erfassten Rohdaten oder das erzeugte Referenztemplate werden mit einer Qualitätsmaßzahl bewertet und je nach Erreichen einer bestimmten Mindestqualität entweder akzeptiert oder zurückgewiesen. Die FTE kann daher auch als eine Kennzahl für die Qualität der erfassten Referenztemplates interpretiert werden. Qualitativ hochwertigere Referenztemplates führen in der Regel zu niedrigeren Fehlerraten FAR und FRR, erhöhen aber die FTE. Umgekehrt werden bei einer niedrigeren FTE auch Referenztemplates geringerer Qualität akzeptiert, was in höheren False Acceptance und False Rejection Rates resultiert.

Als letzter wichtiger Punkt beim Vergleich verschiedener Systeme sei der Stichprobenum-

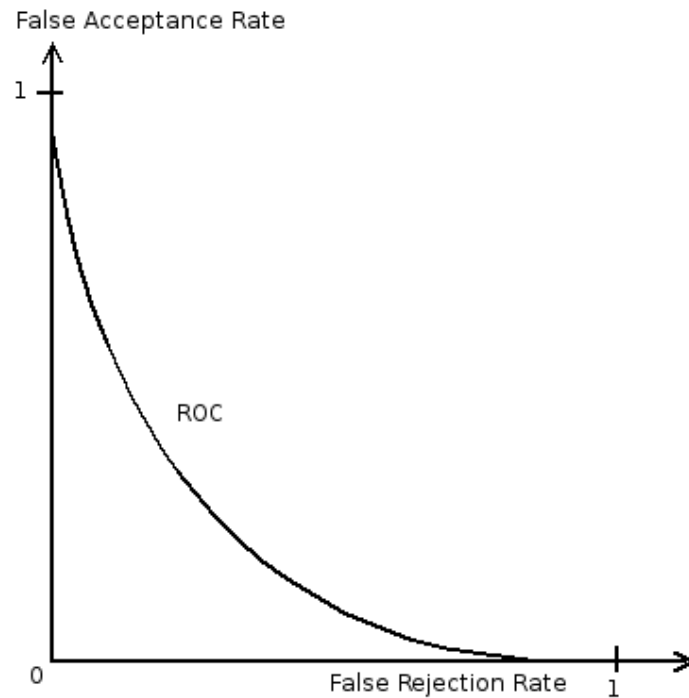


Abbildung 3: Typischer Verlauf einer ROC-Kurve (Erstellt nach [Bun03, S. 59].)

fang genannt, der zur Ermittlung der Kennzahlen verwendet wurde. Je mehr Enrollment- und Authentifizierungsvorgänge durchgeführt werden, desto verlässlicher sind die errechneten Fehlerraten. Ab welchem Stichprobenumfang ein Ergebnis als statistisch signifikant bezeichnet werden kann, lässt sich bei biometrischen Systemen nur schwer feststellen [Bro05]. Porter empfiehlt in [Por00] die Anwendung der Faustregel, die George Doddington 1985 vorstellte: Ein biometrisches System sollte demnach mindestens so lange getestet werden, bis 30 Fehler aufgezeichnet wurden. Nimmt man also zum Beispiel an, dass bei einem Authentifizierungsverfahren eine FAR von 0,001 erreicht wird, so treten die geforderten 30 Fehler voraussichtlich erst nach 30000 Versuchen auf. Die angegebene FAR gilt also nur als vertrauenswürdig, wenn 30000 Versuche durchgeführt wurden und die Anzahl der erwarteten Fehler mit der Anzahl der tatsächlich auftretenden Fehler übereinstimmt.

Zusammenfassend kann festgestellt werden, dass die Ergebnisse verschiedener Studien nur bedingt miteinander vergleichbar sind. Gleiches gilt für die Kennzahlen, die die Hersteller von Authentifizierungssystemen für ihre Produkte angeben. Nur wenn die Rahmenbedingungen und Parameter verschiedener Tests und Untersuchungen bekannt sind, lässt sich feststellen, ob deren Ergebnisse überhaupt vergleichbar sind. Auch die Hersteller sollten detailliert offen legen, wie die berechneten Kennzahlen für ein Produkt zustande gekommen sind.

3.3.6 Zusammenfassung

Um biometrische Authentifizierung mit wissens- und besitzbasierten Verfahren vergleichen zu können, wurden in diesem Abschnitt die wichtigsten Grundlagen der Biometrie vermittelt. Es konnte gezeigt werden, dass es eine Vielzahl unterschiedlicher Merkmale und Methoden gibt, die jeweils für verschiedene Einsatzgebiete geeignet sind.

Als kompakte Übersicht werden die Eigenschaften der in Abschnitt 3.3.4 vorgestellten biometrischen Merkmale in Tabelle 2 zusammengefasst. Die Symbole + und – kennzeichnen Eigenschaften eines Merkmals, die sich gegenüber den Eigenschaften anderer Merkmale positiv bzw. negativ hervorheben. Eigenschaften, die nicht eindeutig positiv oder negativ bewertet werden können, werden mit ○ gekennzeichnet.

Es soll außerdem ein Anhaltspunkt gegeben werden, welcher finanzielle Aufwand bei den Verfahren zu erwarten ist. Die Gesamtkosten und die Kosten pro Benutzer werden durch viele Faktoren beeinflusst, so dass eine Kostenschätzung nur schwer möglich ist. Die Angabe in der Tabelle bezieht sich deshalb nur auf die Kosten der Erfassungssensoren. Merkmale, die durch besonders kostengünstige Sensoren zu erfassen sind, werden mit + gekennzeichnet, bei besonders teuren Sensoren mit –. Oft ist keine pauschale Aussage möglich, da die Erfassung in sehr unterschiedlichen Ausführungen realisierbar ist und davon abhängig die Kosten stark variieren können. Diese Fälle sind mit ○ gekennzeichnet.

Bei einigen Merkmalen mit durchschnittlicher oder geringer Einzigartigkeit wird dazu geraten, diese nur zur Verifikation einzusetzen [Bre02, S. 35 - 82]. Bei der Identifikation sind mit diesen Verfahren hohe Fehlerraten, insbesondere FAR und FIR, zu erwarten. Es sei betont, dass es sich um eine Empfehlung handelt: Es ist durchaus möglich, anhand dieser Merkmale eine Identifikation durchzuführen. Man muss dann aber mit höheren Fehlerraten rechnen, als das mit geeigneteren Merkmalen der Fall wäre.

Die angegebenen Marktanteile beziehen sich auf den Gesamtumsatz der biometrischen Industrie im Jahr 2004 und stammen aus dem Biometric Industry Report, nachzulesen in [Unb05, S. 9]. Für 2004 wird der Gesamtumsatz mit 707 Millionen US-\$ angegeben, 2006 sollen 1,86 Milliarden US-\$ erreicht werden. Mit 815 Millionen US-\$ (2004) und 2,08 Milliarden US-\$ (2006) geht die International Biometric Group sogar von noch höheren Umsätzen aus [Unb05, S. 9].

Im Rahmen dieser Arbeit konnte nur kurzer Einblick in das Thema Biometrie gegeben werden. Es gibt auf diesem Gebiet sicherlich eine Vielzahl interessanter Fragestellungen, die in weiteren Diplomarbeiten ausführlicher behandelt werden sollten. Als Beispiel seien die Stichworte Datenschutz und Überwindungssicherheit genannt. Interessierten wird als Einführung das Buch „Biometrische Verfahren“ [BIO02] empfohlen.

Biometrisches Merkmal	Typ	Einzigartigkeit	Verbreitung	Dauerhaftigkeit	Messbarkeit	Benutzerfreundlichkeit	Lebenderkennung	Kosten	Eignung für Identifikation	Marktanteil
Fingerabdruck	Passiv	+	-	+	+	○	-	○	Ja	48%
Gesicht	Passiv	○	○	○	+	+	○	○	Nein	14%
Iris	Passiv	+	○	+	+	+	+	-	Ja	10%
Retina	Passiv	+	○	+	+	○	+	-	Ja	k.A.
Handgeometrie	Passiv	○	○	○	+	○	○	○	Nein	6%
Dynamik der Unterschrift	Aktiv	○	○	○	+	○	+	○	Ja	5%
Stimme	Aktiv	-	-	○	+	○	-	○	Nein	7%
Tippdynamik	Aktiv	○	-	○	+	○	+	+	Ja	k.A.

Tabelle 2: Vergleich biometrischer Merkmale

4 Anforderungen an die Authentifizierung: Ein Vergleich der Verfahren

In diesem Abschnitt werden Anforderungen an Authentifizierungsverfahren erläutert und jeweils dargestellt, inwieweit wissens-, besitz- und merkmalsbasierte Methoden diese Anforderungen erfüllen. Dabei wird im Besonderen auf die Vor- und Nachteile der biometrischen Verfahren eingegangen. Die Ergebnisse werden in einer Tabelle zusammengefasst, um einen übersichtlichen Vergleich der Verfahren zu erhalten. Im Anschluss werden einige Szenarien, in denen eine Authentifizierung erforderlich ist, konstruiert und mögliche Lösungswege erarbeitet.

Nach Meinung des Autors dieser Arbeit stellen die hier aufgeführten Anforderungen die bedeutendsten Beurteilungskriterien für Authentifizierungssysteme dar. Die einzelnen Punkte wurden aus verschiedenen Quellen, die zum Entstehen dieser Arbeit beigetragen haben, erarbeitet. Die Zusammenstellung wurde in dieser Form nach Wissen des Autors bisher nicht veröffentlicht.

4.1 Authentifizierung einer Person

Das Ziel einer Authentifizierung ist, wie bereits in Abschnitt 2.1 beschrieben, die Überprüfung und Feststellung der Identität einer Person. Die Bezeichnung Authentifizierungsverfahren lässt zunächst einmal vermuten, dass alle Methoden diese Anforderung erfüllen. Doch das ist so nicht richtig: Wissensbasierte Verfahren prüfen lediglich, ob das Wissen korrekt reproduziert wurde; besitzbasierte Verfahren kontrollieren nur, ob ein bestimmter Gegenstand verfügbar ist. Wissen und Besitz dienen als Hilfsmittel, die mit der Identität einer zu authentifizierenden Person verknüpft werden. Es ist jedoch in keinster Weise sichergestellt, dass beim Vorgang der Authentifizierung auch genau diese Person die Hilfsmittel vorweist [Nol02, S. 28]. Wissens- und besitzbasierte Verfahren haben also den Nachteil, dass es sich nur um eine indirekte Authentifizierung handelt: Nicht die Identität der Person selbst, sondern nur das Wissen bzw. der Besitz werden geprüft.

Biometrische Verfahren dagegen untersuchen die charakteristischen Eigenschaften einer Person und vergleichen diese mit vorher erfassten Referenzdaten. Es wird direkt eine Person authentifiziert, unabhängig davon, ob es sich um Identifikation oder Verifikation handelt. Die zu prüfenden Merkmale werden von einem Sensor erfasst, demzufolge kann die Authentifizierung nur durchgeführt werden, wenn die Person physisch anwesend ist. Täuschungsversuche mit Attrappen sollen an dieser Stelle unberücksichtigt bleiben, sie werden im nächsten Abschnitt behandelt.

Im Gegensatz zur Prüfung von Wissen und Besitz ist das Ergebnis einer biometrischen Authentifizierung immer mit einer gewissen Unsicherheit verbunden. Ein Passwort kann richtig oder falsch eingegeben werden, ein Gegenstand kann verfügbar sein oder nicht. Es gibt hier also immer eine eindeutige Antwort. Nicht so bei biometrischen Verfahren, denn

hier ist die Merkmalerfassung immer mit Variationen des Merkmals (z. B. Kosmetik bei Gesichtserkennung) oder der Aufnahmebedingungen (z. B. Position vor dem Sensor) verbunden. Folglich muss die Entscheidung des Authentifizierungssystems anhand eines berechneten Ähnlichkeitswertes getroffen werden, was zu verschiedenen Fehlern führen kann (wie in Abschnitt 3.3.5 beschrieben).

Das „Dilemma“ der Biometrie ist demnach, dass zwar direkt eine Person authentifiziert wird, es aber nicht mit absoluter Sicherheit feststellbar ist, ob das Ergebnis der Erkennung korrekt ist. Ist das Ziel eine direkte Authentifizierung der Person mit sehr geringen Fehlerraten, dann empfiehlt sich die Kombination biometrischer Verifikation mit wissens- oder besitzbasierten Verfahren. Bei dieser Multifaktor-Authentifizierung muss die zu authentifizierende Person anwesend sein und Wissen oder Besitz nachweisen können.

4.2 Sicherheit und Robustheit gegen Überwindungsversuche

Ein Authentifizierungssystem ist in der Regel nur ein Baustein im Sicherheitskonzept eines größeren, komplexen Systems. Es kann zum Beispiel zur Absicherung eines Firmengeländes beitragen oder den Zugang zu einem Computersystem kontrollieren. Die Sicherheitsanforderungen an das Authentifizierungssystem sind demnach vom Schutzbedarf des Gesamtsystems abhängig und können von diesem abgeleitet werden. An die Zutrittskontrolle bei einem Atomkraftwerk oder einer Waffenkammer werden sicherlich andere Ansprüche gestellt als an ein Bezahlssystem in der Kantine einer Firma. Es wird hier davon ausgegangen, dass der Schutzbedarf des Gesamtsystems und die daraus abgeleiteten Sicherheitsansprüche an das Authentifizierungssystem schon bekannt sind. Die Schutzbedarfsermittlung wird in diesem Kontext nicht näher erläutert.

Im Folgenden sollen drei verschiedene Angreifermodelle berücksichtigt werden, die sich in der Verbreitung des Angreifers und im Mitwirken eines berechtigten Benutzers unterscheiden. Natürlich könnte man weitere Angreifermodelle konstruieren oder die hier genannten Varianten noch detaillierter festlegen, doch ist das für den Vergleich der Authentifizierungsverfahren nicht zielführend.

4.2.1 Angreifer beherrscht das Authentifizierungssystem

Im ersten Fall wird davon ausgegangen, dass ein Angreifer das Authentifizierungssystem selbst manipulieren kann. Es wird also angenommen, dass die Kommunikation innerhalb des Systems „abgehört“ werden kann und der Angreifer Anwendungen und Daten verändern kann. Somit könnten eingegebene Passwörter erfasst oder die Akzeptanzschwelle bei biometrischen Verfahren modifiziert werden. Kontrolliert ein Angreifer das gesamte Authentifizierungssystem oder zumindest wesentliche Teile davon, so spielt das verwendete Verfahren für die Sicherheit keine Rolle mehr. Lediglich bei den Folgen und Auswirkungen eines solchen Angriffs unterscheiden sich die Verfahren (siehe dazu Unterabschnitte 4.3 und 4.4).

4.2.2 Angriff ohne bewusste Unterstützung durch berechtigte Benutzer

Das zweite Modell beschreibt einen Angreifer, der das Authentifizierungssystem nicht manipulieren kann und der keine bewusste Unterstützung durch einen berechtigten Benutzer erhält. Je nach eingesetztem Verfahren unterscheiden sich die Angriffsmöglichkeiten und der Aufwand, der dafür nötig ist.

Relativ einfach ist das Ausspionieren eines Passwortes oder einer PIN. Das kann durch direkten Sichtkontakt oder unter Verwendung kleiner Videokameras erfolgen. Bei IT-Systemen könnten auch Keylogger zum Einsatz kommen, die zum Beispiel mit einem trojanischen Pferd auf den Rechner gelangen und alle Tastatureingaben des Benutzers an den Angreifer übermitteln. Relativ nutzlos ist für den Angreifer ein ausgespähtes Einmalpasswort, wie zum Beispiel eine Transaktionsnummer beim Online-Banking, da es unmittelbar nach dem Ausspionieren schon nicht mehr gültig ist. Nur wenn der Nutzer darin gehindert wird, seine Transaktion abzuschließen, kann der Angreifer die TAN selbst einsetzen.

Eine andere Option ist ein Brute-Force Angriff, bei dem versucht wird, das geforderte Wissen zu erraten. Da viele Benutzer dazu neigen, recht einfache Passwörter zu verwenden, kann der Versuch unter Umständen sehr schnell erfolgreich sein. Bei einigen Anwendungsfällen gibt es jedoch effiziente Schutzmechanismen gegen solche Angriffe. Zum Beispiel kann ein Benutzeraccount für ein Computersystem temporär gesperrt werden, wenn das Passwort mehrmals falsch eingegeben wurde.

Will ein Angreifer in den Besitz eines zur Authentifizierung eingesetzten Gegenstandes kommen, so ist Diebstahl eine Möglichkeit. Nach einiger Zeit, spätestens beim nächsten Authentifizierungsvorgang, wird der Verlust jedoch vom Benutzer bemerkt. Daraufhin kann eine Sperrung veranlasst werden, womit der entwendete Gegenstand für weitere Authentifizierungsvorgänge nutzlos ist. Reicht dem Angreifer die Zeitspanne vom Diebstahl bis zur Sperrung für seine Ziele aus, dann ist Diebstahl eine durchaus geeignete Methode.

Wenn der Angreifer über die technischen Möglichkeiten verfügt, kann auch ein Duplikat des Authentifizierungsgegenstandes erzeugt werden. Der Gegenstand des Benutzers verbleibt in dessen Besitz und der Angreifer kann das Duplikat über längere Zeit unbemerkt einsetzen. Eine Sperrung erfolgt erst, wenn dem Benutzer oder Dritten der entstandene Schaden auffällt. Wie die Kopie erstellt wird, hängt vom eingesetzten Gegenstand ab. Relativ einfach dürfte es sein, die Identifikationsnummern von drahtlosen Chipkarten und RFID-Transpondern auszuspionieren. Dazu muss der Angreifer ein möglichst unauffälliges Lesegerät so positionieren, dass innerhalb dessen Reichweite eine Übertragung stattfinden kann. Auch die bei Geldautomaten verwendeten Magnetstreifenkarten können problemlos auf Blankokarten kopiert werden. Um an die zu kopierenden Daten zu kommen, könnte ein Angreifer an der Eingangstür zu einer Bank ein eigenes Lesegerät installieren. Außerhalb der Schalteröffnungszeiten dienen solche Geräte normalerweise als Zutrittskontrolle, um nur Bankkunden den Zugang zum Geldautomaten zu gewähren. Der Kartenleser des Angreifers kann so über dem Kartenleser der Bank

positioniert werden, dass die Daten der Karte vollständig ausgelesen werden und der Türöffner der Bank weiterhin problemlos funktioniert. Kombiniert der Angreifer das Kopieren der Bankkarte noch mit dem Ausspionieren der PIN per Videokamera, dann ist diese Multifaktor-Authentifizierung überwunden.

Erfolgt die Ermittlung der Karten-Identität mit einem Challenge-Response-Verfahren, so ist ein einfaches Kopieren der Karte nicht möglich, da der kryptographische Schlüssel der Karte nicht mit einem normalen Lesegerät erfasst werden kann. Es bieten sich dann zwei Angriffswege: Wenn man ein Paar aus Challenge und Response kennt, zum Beispiel durch Abhören drahtloser Kommunikation zwischen Karte und Lesegerät, dann kann ein Brute-Force-Angriff mit dem Durchprobieren aller möglichen Schlüssel zum Erfolg führen. Um zu wissen, wie aus Challenge und Schlüssel die Antwort zu berechnen ist, muss der Angreifer auch das eingesetzte kryptographische Verfahren kennen. Wenn man den richtigen Schlüssel hat, dann kennt man auf alle weiteren Challenges die richtige Antwort. Eine andere Möglichkeit an den Schlüssel zu kommen ist das direkte Auslesen aus dem Speicher der Karte. Dafür ist ein hohes Maß an technischer Fachkenntnis und die entsprechende Ausstattung mit Geräten und Werkzeugen erforderlich. Da mechanische Veränderungen, zum Beispiel ein Abschleifen der Kunststoffhülle, notwendig sind, wird dieses Vorgehen zu Schäden an der Karte, meistens wohl auch zu deren Zerstörung führen. Bemerkt der Benutzer das Fehlen seiner Chipkarte und lässt diese frühzeitig sperren, dann war der ganze Aufwand des Angreifers umsonst.

Ein relativ einfacher Angriff auf ein Challenge-Response-Verfahren mit drahtloser Kommunikation wäre, sehr viele Challenge-Response-Paare abzuhören. Der Angreifer könnte dann möglichst viele Authentifizierungsversuche durchführen und hoffen, dass er für eine Challenge die Antwort bereits kennt. Genauso einfach wie dieser Reply-Angriff ist aber auch die Gegenmaßnahme: Jede Challenge sollte nur genau ein einziges Mal verwendet werden. Abgehörte Challenge-Response-Paare sind somit für einen Angriff nutzlos.

Biometrische Merkmale sollten niemals als geheime Daten betrachtet werden, wie es beispielsweise bei einem Passwort der Fall ist. Einige Merkmale sind problemlos von Angreifern zu erfassen: Das Gesicht und die Hände können auch in größerer Entfernung mit einer entsprechenden Kamera aufgenommen werden. Jeder Mensch hinterlässt in vielen Situationen seine Fingerabdrücke, z. B. auf Gläsern oder der Autotür. Andere Merkmale wiederum sind schwieriger zu erfassen und ein Angreifer benötigt dazu eventuell spezielle technische Geräte. Dazu zählen die Iris und Retina sowie alle aktiven Merkmale. Trotzdem sollte auch hier nicht davon ausgegangen werden, dass ein Angreifer nicht zur Merkmalerfassung in der Lage ist. Welche Attrappen ein Angreifer herstellen und einsetzen kann, hängt von der Zeit und den finanziellen Mitteln ab, die ihm zur Verfügung stehen. Einfache Nachbildungen eines Fingerabdrucks sind sehr günstig und ohne besonderes Equipment anzufertigen. Als Ausgangsmaterial eignet sich zum Beispiel Gelatine [MMYH02] oder Holzleim [Sta04b]. Bei Gesichtserkennungssystemen reicht die Palette der Attrappen von ausgedruckten Fotos bis hin zu professionell angefertigten Masken.

Geht man davon aus, dass ein Angreifer jedes passive Merkmal mit Attrappen nachbilden kann, dann wird klar, dass eine zuverlässige Lebenderkennung immanent wichtig für die

Sicherheit eines biometrischen Systems ist. Die meisten aktiven Merkmale sind für einen Angreifer schwieriger zu erfassen und noch schwieriger nachzuahmen. Es wird momentan davon ausgegangen, dass nur ein Mensch diese aktiven Merkmale aufweist und somit auch nur ein Mensch die zu erfassende Aktion (z. B. eine Unterschrift) leisten kann.

4.2.3 Angriff mit bewusster Beteiligung berechtigter Benutzer

Die Voraussetzungen sind denen im letzten Abschnitt ähnlich, nur dass in diesem Fall der Angreifer die bewusste Unterstützung eines berechtigten Benutzers erhält. Das Ausspähen von Passwörtern, das Anfertigen von Duplikaten oder die Erfassung biometrischer Merkmale durch einen Angreifer geschehen in der Regel derart, dass der Benutzer es nicht bemerkt. Einfacher hat der Angreifer es dann, wenn der Benutzer ihn bei seinem Überwindungsversuch unterstützt. Ob dem berechtigten Benutzer bewusst ist, dass durch sein Handeln die Sicherheit des Gesamtsystems gefährdet wird, ist für die Beurteilung des Authentifizierungsverfahrens unerheblich. Was letztlich zählt ist, ob es einem Angreifer gelingt, eine falsche Identität vorzutäuschen.

Der einfachste Fall ist wohl der, dass ein berechtigter Benutzer sein Passwort an einen Kollegen oder Bekannten weitergibt, weil er sich dadurch Vorteile verspricht (z. B. Hilfe bei Problemen mit einer Software). Auch wenn hier kein wirklicher Angriff vorliegt, zeigt es dennoch, wie einfach sich eine wissensbasierte Authentifizierung umgehen lässt.

Eine andere Methode ist das Social Engineering: Der Angreifer fordert einen berechtigten Benutzer unter einem Vorwand dazu auf, ein bestimmtes Passwort oder eine PIN preiszugeben. Dazu könnte der Angreifer zum Beispiel beim Mitarbeiter einer Firma anrufen und sich als Systemadministrator ausgeben. Aus Hilfsbereitschaft oder auch aus Angst vor Beschwerden beim eigenen Vorgesetzten werden viele Personen die erfragte Information herausgeben.

Das mittlerweile häufig vorkommende Phishing ist ebenfalls ein Versuch, der die bewusste Interaktion des Benutzers erfordert. Ziel des Angreifers ist es, Kontonummern, Benutzernamen, Passwörter, PINs oder TANs auszuspähen. Dazu werden E-Mails verschickt, die den Empfänger dazu auffordern, auf einer bestimmten Webseite seine Authentifizierungsdaten (z. B. zum Online-Banking) einzugeben. Als Begründung werden oft Sicherheitsprüfungen oder drohende Sperrung des Zugangs genannt. Die vom Angreifer kontrollierte Webseite sieht meist den Seiten des angeblichen E-Mail-Absenders (z. B. der Bank) recht ähnlich. Die eingegebenen Zugangsdaten werden an den Angreifer übermittelt, der diese später zu seinen Zwecken missbrauchen kann.

Bei besitz- und merkmalsbasierten Verfahren erleichtert eine Mitwirkung des berechtigten Benutzers das Erfassen der Identifikationsnummer einer Chipkarte oder der biometrischen Charakteristika. Ist der Benutzer eines Authentifizierungsgegenstandes bereit, diesen einer nicht berechtigten Person zu leihen, dann entfällt auch der Aufwand für die Anfertigung eines Duplikats. Dies ist bei biometrischen Systemen selbstverständlich nicht möglich, denn ein persönliches Merkmal kann man nicht einfach an eine beliebige andere Person weitergeben.

4.2.4 Zusammenfassung

Zusammenfassend sei Folgendes festgestellt: Gegen einen Angreifer, der das Authentifizierungssystem oder wesentliche Teile davon beherrscht, kann keines der Verfahren schützen. Für eine sicherheitskritische Betrachtung muss man sich deshalb auf Angriffe beschränken, bei denen ein Angreifer versucht, eine falsche Identität vorzutäuschen, ohne dass dieser das Authentifizierungssystem manipulieren kann. Erhält der Angreifer Unterstützung durch einen berechtigten Benutzer, so kann der Aufwand für den Angriff teilweise drastisch gesenkt werden. Am einfachsten zu überwinden scheinen wissensbasierte Verfahren, da sich Wissen sehr einfach „kopieren“ lässt. Bei Mitwirkung des berechtigten Benutzers sind auch besitzbasierte Verfahren leicht zu umgehen. Ohne bewusste Beteiligung des Benutzers heben sich nur diejenigen besitzbasierten Systeme als relativ sicher hervor, die auf ein Challenge-Response-Verfahren setzen. Alle anderen gelten als leicht abzuhören oder zu kopieren.

Bei den biometrischen Verfahren liegt der größte Aufwand im Beschaffen der biometrischen Daten und dem Erstellen geeigneter Attrappen. Dem kann durch Lebenderkennung oder der Verwendung aktiver Merkmale entgegen gewirkt werden. Die bisher implementierten Verfahren der Lebenderkennung lassen sich aber immer noch täuschen und erhöhen bisher nur den Aufwand für einen Angreifer. Absolute Sicherheit kann es bei der Authentifizierung, wie auch in vielen anderen Bereichen der IT-Sicherheit, auf absehbare Zeit nicht geben.

Aufgrund der vorhandenen Schwächen einzelner Verfahren sollte bei hohen Sicherheitsanforderungen immer eine Multifaktor-Authentifizierung gewählt werden. Diese könnte zur erfolgreichen Identifikation zum Beispiel eine biometrische Erkennung mehrerer passiver Merkmale und den kontaktbehafteten Nachweis einer Challenge-Response-Chipkarte erfordern. Es sind viele Kombinationen vorstellbar, was eine Anpassung an das geforderte Sicherheitsniveau möglich macht.

4.3 Reaktionsmöglichkeiten bei Kompromittierung der Authentifizierungsdaten

Das Problem der Kompromittierung tritt auf, wenn es einem Angreifer gelungen ist, auf die Authentifizierungsdaten eines Benutzers zuzugreifen. Der Angreifer könnte dafür ein Passwort oder die Identifikationsnummer einer Chipkarte ausspioniert oder biometrische Daten eines Benutzers erfasst haben. Es soll hier die Frage geklärt werden, welche Auswirkungen eine Kompromittierung bei den einzelnen Verfahren hat und wie darauf reagiert werden muss.

Hatte ein Angreifer Zugriff auf ein Passwort einer Person, so kann das Passwort geändert werden. Dies ist bei den meisten Authentifizierungssystemen ein häufiger Vorgang, der problemlos durchführbar ist. Schwieriger wird die Situation, wenn der Benutzer das gleiche Passwort bei mehreren Systemen verwendete, um sich nur ein Passwort merken zu müssen. In diesem Fall sollte das Passwort bei allen Systemen ausgetauscht werden.

Sonst wäre womöglich einem Angreifer, der die Logindaten für das E-Mail-Postfach kennt, auch der Zugang zum Online-Banking offen.

Bei besitzbasierten Systemen ist die Situation ähnlich. Eine gestohlene oder möglicherweise kopierte Karte kann einfach gesperrt werden, wodurch sie für den Dieb oder Angreifer nutzlos wird.

Wie bereits in Abschnitt 4.2 erwähnt, darf man bei biometrischen Daten nie davon ausgehen, dass es sich um geheime Daten handelt. Ein Erfassen der persönlichen Merkmale durch einen Angreifer und die Berechnung eines Templates aus diesen Rohdaten ist aber einer Kompromittierung gleichzusetzen. Eine simple Reaktion wie das Austauschen von Passwörtern und Sperren von Chipkarten ist hier unmöglich. Das Verwenden unterschiedlicher Fingerabdrücke funktioniert nur zehn Mal und bei anderen Merkmalen, wie zum Beispiel dem Gesicht, hat man gar keine Wahlmöglichkeit. Eine „Änderung“ der biometrischen Daten, beispielsweise durch einen medizinischen Eingriff, ist selbstverständlich keine akzeptable Lösung.

Man nimmt also an, dass ein Angreifer über die biometrischen Rohdaten oder die daraus berechneten Templates verfügt. Dies hat weit reichende Auswirkungen auf die Anforderungen an die Implementierung biometrischer Verfahren. Es muss verhindert werden, dass der Angreifer die verfügbaren Daten zum Überwinden des Authentifizierungssystems einsetzen kann. Einerseits müssen die bereits genannten Mechanismen der Lebenserkennung die Verwendung von Nachbildungen erschweren. Andererseits darf es dem Angreifer nicht gelingen, die erfassten Daten direkt zu verwenden. Über nicht vertrauenswürdige Geräte, die mit dem System kommunizieren, könnte der Angreifer die Erfassung der biometrischer Daten vortäuschen. Die Lösung liegt in einer Abschirmung des gesamten Authentifizierungssystems. Die Vertraulichkeit und Integrität aller Kommunikationswege und sämtlicher Komponenten des Systems muss gewährleistet sein. Befindet sich das gesamte Authentifizierungssystem im Einflussbereich des Betreibers, zum Beispiel die Zutrittskontrolle in einem Unternehmen, reicht unter Umständen eine bauliche Abschirmung aus. Bei einer räumlichen Verteilung der Komponenten an verschiedenen Orten kann dies nicht durchgeführt werden. Die Hard- und Software befinden sich dann möglicherweise nicht mehr im Einflussbereich des Betreibers und zudem wird die Kommunikation über unsichere Leitungen notwendig sein. Zur Absicherung kann in diesem Fall auf kryptographische Methoden zurückgegriffen werden: Challenge-Response-Verfahren gewährleisten, dass nur berechtigte Hardware-Module miteinander kommunizieren. Zudem sichern Verschlüsselung und digitale Signatur die Vertraulichkeit und Integrität der übertragenen Daten.

Zusammenfassend muss man feststellen, dass die Auswirkungen einer Kompromittierung bei wissens- und besitzbasierten Verfahren mit einfachen Mitteln begrenzt werden können. Wichtig ist in diesem Zusammenhang, dass die Reaktion möglichst zeitnah erfolgt. Zwischen Kompromittierung und Reaktion kann ein Angreifer bei diesen Verfahren problemlos die Authentifizierung umgehen. Biometrische Merkmale können auf Dauer nicht geheim gehalten werden. Dies muss bei der Implementierung eines biometrischen Authentifizierungssystems unbedingt berücksichtigt werden.

4.4 Datenschutz und Verbraucherschutz

Die Forschung im Bereich der Technikfolgen-Abschätzung versucht, frühzeitig die Chancen und Risiken neuer Technologien zu ermitteln. Dabei wird häufig auf zwei wichtige „Nebenbedingungen“ beim Einsatz biometrischer Verfahren hingewiesen: Den Schutz personenbezogener Daten sowie den Verbraucherschutz. Der Sachstandsbericht des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag [PS02] kann hier als Einstieg in das Thema dienen.

Zunächst werden Gefahren beschrieben, die im Zusammenhang mit biometrischen Authentifizierungssystemen genannt werden. Danach wird darauf eingegangen, wie im Gegensatz dazu wissens- und besitzbasierte Verfahren eingeschätzt werden.

Biometrische Merkmale sind inhärent personenbezogen. Alle gespeicherten biometrischen Daten, sowohl die Rohdaten als auch Referenztemplates, sind daher vor unbefugtem Zugriff zu schützen. Dabei spielt es keine Rolle, dass es sich bei biometrischen Merkmalen nicht um geheime Informationen handelt. Allein die Tatsache, dass personenbezogene Daten gespeichert vorliegen, erfordert ein höchstes Maß an Vertraulichkeit. Als besonders datenschutzfreundlich gilt die dezentrale Speicherung der Daten, zum Beispiel auf einer Chipkarte. Auf diese Weise hat nur der Besitzer der Chipkarte Zugriff auf die biometrischen Informationen. Gelingt es einem Angreifer in das Authentifizierungssystem einzudringen, so wird zwar die Sicherheit des Systems nicht mehr gewährleistet sein, doch auf personenbezogene Authentifizierungsdaten hat der Angreifer keinen Zugriff.

Damit ein Angreifer keine eigenen, gefälschten Chipkarten verwenden kann, muss die Authentizität der Chipkarten bei der dezentralen Speicherung mittels kryptographischer Verfahren geprüft werden. Beispielsweise könnten die Daten auf der Karte mit dem privaten Schlüssel des Ausstellers signiert werden. Bei jedem Authentifizierungsvorgang erfolgt eine Verifikation der Signatur mit dem öffentlichen Schlüssel.

Der Verbraucher wird bei dezentraler Datenhaltung vor einer weiteren Gefahr geschützt: Möglicherweise lassen sich aus den biometrischen Rohdaten oder unter Umständen auch aus den Templates Rückschlüsse auf Krankheiten oder Lebensgewohnheiten einer Person ziehen. Schon jetzt ist bekannt, dass man über die Retina Alkoholismus, Bluthochdruck und andere Krankheiten erkennen kann [Fey02, unter Berufung auf Prof. Klaus Brunnstein von der Universität Hamburg]. Probst erwähnt in [Pro02, S. 119, unter Berufung auf [Woo99]], dass möglicherweise auch Fingerabdruckmuster auf Krankheiten wie Brustkrebs oder Leukämie hinweisen. Weitere, bislang unbekannt Zusammenhänge könnten erst in der Zukunft entdeckt werden. Bei der dezentralen Speicherung auf Chipkarten kann der Benutzer auch auf neue Erkenntnisse der Biostatistik reagieren: Wird festgestellt, dass eine ansonsten nicht sichtbare Krankheit zu einer bestimmten Merkmalsausprägung führt, dann kann der Benutzer selbst entscheiden, ob er das Authentifizierungssystem weiter verwenden möchte. Bei zentraler Datenhaltung könnte der Betreiber des Systems den Datenbestand systematisch nach solchen Zusammenhängen untersuchen und daraus eventuell Informationen ableiten, auf die bei dezentraler Datenhaltung kein Zugriff bestehen würde.

Die Rohdaten haben in der Regel einen höheren Informationsgehalt als ein daraus extrahiertes Template und sind daher tendenziell besser für Rückschlüsse auf Krankheiten und Lebensgewohnheiten geeignet. Demzufolge sollten datenschutzfreundliche Systeme auf die Speicherung der Rohdaten verzichten.

Ein weiterer Kritikpunkt an biometrischen Verfahren ist, dass eine Überwachung von Personen und das Erstellen von Bewegungs- und Tätigkeitsprofilen realisierbar wird. Ein flächendeckendes Netz von Videokameras auf Straßen und öffentlichen Plätzen könnte mit einem Gesichtserkennungssystem kombiniert werden, um Personen automatisch verfolgen und Bewegungsprofile erstellen zu können. Je weiter die Verbreitung biometrischer Systeme zunimmt, desto dichter wird das Netz an Überwachungspunkten und desto detaillierter lassen sich die Profile zu einzelnen Personen erstellen. Die persönlichen, körperlichen Merkmale können, wie bereits erwähnt, nicht einfach geändert werden. Demnach ist eine Person über einen sehr langen Zeitraum, womöglich ein Leben lang, eindeutig zu identifizieren. Geht man davon aus, dass Betreiber verschiedener Authentifizierungssysteme zusammenarbeiten und sich die Verbreitung biometrischer Verfahren weiter erhöht, so wird eine lückenlose, dauerhafte Überwachung denkbar.

Aus Sicht des Verbraucherschutzes werden sich biometrische Verfahren nur durchsetzen, wenn ein diskriminierungsfreier Einsatz erreichbar ist [Alb02]. Personen dürfen nicht deshalb von der Nutzung eines Authentifizierungssystems ausgeschlossen werden, weil sie entweder ein Merkmal nicht aufweisen oder mit dem Erfassungssensor nicht umgehen können. Ein Ausschluss von Authentifizierungsverfahren käme in einer modernen Gesellschaft einer sozialen Ausgrenzung gleich. Für die betroffenen Personen muss daher immer eine weitere Möglichkeit der Authentifizierung angeboten werden.

Bei wissens- und besitzbasierten Authentifizierungssystemen sind die Bedenken von Seiten des Daten- und Verbraucherschutzes vergleichsweise gering. Auch die hier verwendeten Identifikationsnummern oder eindeutigen Benutzernamen könnten als personenbezogene Daten deklariert werden. Es gibt jedoch bedeutende Unterschiede zum Personenbezug der biometrischen Daten: Da es sich um zugeordnete Informationen handelt, kann diese Zuordnung einfach aufgehoben werden. Im Extremfall, zum Beispiel im Rahmen eines Zeugenschutzprogramms, könnte eine betroffene Person sogar Namen und Adresse ändern und ein falsches Geburtsdatum im Ausweis eintragen lassen. Bei weit verbreitetem Einsatz von biometrischer Authentifizierung wäre diese neue, vorgetäuschte Identität jedoch leicht als solche zu erkennen.

Auch die potentielle ubiquitäre Überwachung von Personen wird bei wissens- und besitzbasierten Systemen schwieriger umzusetzen sein. Denn bei den unterschiedlichen Betreibern von Authentifizierungssystemen wird eine Person in der Regel unterschiedliche Benutzernamen und Identifikationsnummern haben. Eine eindeutige, systemübergreifende Zuordnung ist nur bei biometrischen Merkmalen möglich, denn diese sind untrennbar mit einer Person verbunden.

Als weiterer Unterschied sei genannt, dass Passwörter oder Chipkarten keine Rückschlüsse auf den Gesundheitszustand oder die Lebensgewohnheiten des Benutzers zulassen. Die

bisher erreichte Verbreitung der wissens- und besitzbasierten Verfahren lässt auch nicht die Gefahr einer Diskriminierung einzelner Bevölkerungsgruppen erkennen.

Die wissens-, besitz- und merkmalsbasierten Verfahren unterscheiden sich also auch bezüglich den Aspekten Datenschutz und Verbraucherschutz. Der Vorteil biometrischer Verfahren, eindeutig eine Person zu identifizieren (siehe Abschnitt 4.1), wird aus Sicht des Datenschutzes zum Nachteil. Mit technischen und organisatorischen Maßnahmen lassen sich die meisten Probleme vermeiden, doch bleibt die berechtigte Befürchtung, dass diese nicht in ausreichendem Maße umgesetzt werden. Vor allem die zentrale Datenspeicherung könnte sich als gefährlich herausstellen, insbesondere dann, wenn eine Verknüpfung mit medizinischen Daten erfolgt [Pfi05]. Verfahren auf Basis von Wissen oder Besitz sind als relativ unproblematisch zu bewerten, da nur eine indirekte Beziehung zwischen Person und Wissen bzw. Besitz besteht.

4.5 Benutzerfreundlichkeit und Benutzerakzeptanz

Ein Authentifizierungssystem, das schwierig zu bedienen ist oder von den Benutzern nicht angenommen wird, kann sich auf Dauer nicht am Markt durchsetzen. Deshalb sind Benutzerfreundlichkeit und Benutzerakzeptanz zwei entscheidende Eigenschaften eines Systems, die nicht außer Acht gelassen werden dürfen. Da die Ansprüche von Benutzern sehr unterschiedlich sein können, wird die Bewertung eines Authentifizierungssystems nie wirklich objektiv erfolgen. Es soll daher ein möglichst allgemeiner Überblick gegeben werden, welche Faktoren die Benutzerfreundlichkeit und Akzeptanz der verschiedenen Verfahren beeinflussen.

Bei wissensbasierten Verfahren besteht ein Zielkonflikt zwischen Sicherheit und Benutzerfreundlichkeit: Kurze, einfache Passwörter sind von einem Angreifer leicht zu erraten, vor allem wenn ein Bezug zum Benutzer herstellbar ist (zum Beispiel Geburtsdatum, Telefonnummer oder Vorname des Ehepartners als Passwort). Um auch vor automatisierten Angriffen über einen längeren Zeitraum geschützt zu sein, sollte ein Passwort aus Zahlen und Buchstaben bestehen, wenn möglich auch Sonderzeichen enthalten und es sollte nicht in einem Wörterbuch zu finden sein. Außerdem ist die Länge des Passwortes entscheidend, da der Aufwand eines Angriffs exponentiell mit der Länge des Passwortes zunimmt. Für jede Anwendung, die eine Authentifizierung durch Wissen erfordert, sollte zudem ein anderes Passwort verwendet werden. Dadurch wird verhindert, dass ein Angreifer, der ein Passwort eines Benutzers kennt, damit gleich mehrere Authentifizierungssysteme umgehen kann.

Komplizierte, lange Passwörter kann sich der Benutzer jedoch nur in begrenztem Umfang merken. Um dem Vergessen des Passwortes vorzubeugen, schreiben manche Benutzer das Passwort auch auf, was im Allgemeinen nicht empfohlen wird. Im schlechtesten Fall befindet sich dann das Passwort für den Arbeitsplatzrechner auf einem Zettel, der am Monitor klebt, oder die PIN direkt auf der EC-Karte. Mittlerweile wird auch diskutiert, ob es nicht doch besser ist, wenn Benutzer ihre Passwörter aufschreiben und

dieses Schriftstück sicher verwahren [Bac05]. Auf diese Weise könnten sich Benutzer viele verschiedene, komplexe Passwörter merken. Eine sicherere Alternative zum Notieren auf Papier stellen Passwort-Manager dar, die dafür sorgen, dass Passwörter verschlüsselt gespeichert werden. Der Benutzer braucht sich dann im Idealfall nur noch das Passwort für den Passwort-Manager merken.

Eine andere Alternative ist die Verwendung einfacher, kurzer Passwörter in Verbindung mit organisatorischen Maßnahmen. Ein Beispiel ist die PIN bei Kreditkarten, die nur aus vier Zahlen besteht und somit einfach zu merken ist. Zur Vermeidung von Angriffen durch zufälliges Ausprobieren, wird die Karte nach mehrmals falsch eingegebener PIN gesperrt.

Die Benutzerfreundlichkeit der besitzbasierten Verfahren zeichnet sich dadurch aus, dass der Benutzer einfach nur einen Gegenstand mit sich führen muss. Zur Authentifizierung muss dieser entweder in ein Lesegerät eingeführt werden oder sich in der Reichweite einer kontaktlosen Übertragungseinheit befinden. Die Bedienung der Geräte ist recht einfach und kann meist mit einer einfachen Darstellung verständlich erklärt werden. Allein die Tatsache, dass ein bestimmter Gegenstand mitzuführen ist, könnte aber zu Problemen bei Benutzern führen. Zum einen kann der Gegenstand einfach vergessen werden. Zum anderen beanspruchen auch Plastikkarten oder Chips in anderen Bauformen einen gewissen Platz, der beim Menschen, abhängig von der jeweiligen Situation, begrenzt ist. Die Geldbörse ist sicherlich der häufigste Aufbewahrungsort für Kunststoffkarten, Chips anderer Bauart kann man zum Beispiel am Schlüsselbund befestigen. Welche maximale Zahl an Authentifizierungsgegenständen eine Person bereit ist mitzuführen, hängt dabei sowohl von den verwendeten Gegenständen als auch der persönlichen Meinung des Einzelnen ab. Tendenziell wird mit einer höheren Anzahl an Gegenständen die Akzeptanz der Benutzer abnehmen.

Biometrische Verfahren gelten im Allgemeinen als sehr benutzerfreundlich: Man muss sich keine Passwörter oder Wissen in anderer Form merken und benötigt auch keine Gegenstände zur Authentifizierung. Man kann weder Besitz verlieren noch Wissen vergessen, denn die persönlichen Merkmale reichen zur Authentifizierung aus. Höchster Komfort für den Benutzer ist bei einigen passiven Merkmalen, wie zum Beispiel dem Gesicht, realisierbar, denn diese Merkmale lassen sich vollkommen berührungslos und ohne Interaktion mit dem Benutzer erfassen. Es wäre also eigentlich zu erwarten, dass die Akzeptanz unter den Anwendern groß ist. Doch das trifft nicht zu und viele Personen stehen der Biometrie skeptisch gegenüber. Dieser Widerspruch soll hier näher erläutert werden.

Zunächst sei erwähnt, dass die Akzeptanz sehr vom untersuchten biometrischen Merkmal abhängt. Es kann also keine Bewertung abgegeben werden, die für alle Merkmale gleichermaßen gilt. Außerdem sei darauf hingewiesen, dass zur Verifikation die zu prüfende Identität dem System übermittelt werden muss. Dies erfordert oft zusätzliches Wissen oder Besitz, was einige der hier genannten Vorteile zunichte macht und gleichzeitig die oben genannten Probleme wissens- oder besitzbasierter Verfahren mit sich bringt.

Die Akzeptanz durch die Benutzer hängt auch von der Wahl eines geeigneten Schwel-

lenwertes beim Matching ab: Eine sehr niedrige False Acceptance Rate ist nur dann in der Praxis umsetzbar, wenn damit nicht eine sehr hohe False Rejection Rate verbunden ist. Auf Dauer wird es sehr frustrierend für einen berechtigten Benutzer sein, wenn er häufig zurückgewiesen wird. Es muss deshalb ein Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit gefunden werden.

Die einzelnen Verfahren unterscheiden sich sehr nach ihrer Bedienbarkeit, was in hohem Maße mit dem eingesetzten Erfassungssensor zusammenhängt. Systeme, die eine genaue Positionierung oder Ausrichtung des Merkmals erfordern, sind besonders anfällig für Bedienungsfehler, die dann zu einer False Rejection führen. Dazu gehören die Merkmale des Auges, also Iris und Retina. Andere Verfahren sind für Bedienungsfehler weniger anfällig, wie zum Beispiel die Gesichtserkennung. Manche Systeme lokalisieren ein Gesicht im aufgenommenen Foto oder Video automatisch und erlauben sogar eine Authentifizierung „im Vorbeigehen“.

Bei Fingerabdruck- und Handgeometriescannern haben manche Menschen hygienische Bedenken, da diese eine Berührung des Sensors erfordern. Das Problem scheint vor allem im asiatischen Kulturraum aufzutreten [Bre02, S. 40]. Für die Erfassung von Fingerabdrücken wird deshalb bereits an einem berührungslosen Sensor geforscht [Kui02, S. 375].

Als weiterer Vorbehalt sei die Sorge um gesundheitliche Schäden genannt. Viele Benutzer gehen fälschlicherweise davon aus, dass die Merkmale Iris und Retina durch „Laserabtastung“ erfasst werden [Bre02, S. 51 und S. 54]. Tatsächlich werden nur Bilder im Wellenbereich des sichtbaren und infraroten Lichtes von einer Kamera aufgenommen, eine Gefährdung für die Gesundheit besteht nicht.

Bereits in Abschnitt 4.4 wurde auf die Probleme und noch offenen Fragen des Datenschutzes bei biometrischen Verfahren genauer eingegangen. Auch diese Bedenken tragen zu der Skepsis gegenüber biometrischen Systemen bei.

Bei Benutzerfreundlichkeit und Akzeptanz lässt sich in der Zusammenfassung kein eindeutig vorteilhaftes Verfahren feststellen. Die schon weit verbreiteten Authentifizierungsmethoden durch Wissen und Besitz sind bezüglich der Benutzerfreundlichkeit den meisten biometrischen Systemen unterlegen. Momentan leiden viele biometrische Verfahren dagegen noch unter Akzeptanzproblemen, die bei wissens- und besitzbasierten Verfahren nicht in diesem Maße auftreten. Durch eine konsequente Berücksichtigung des Datenschutzes, Transparenz durch Aufklärung der Bevölkerung und weitestgehende Benutzerfreundlichkeit kann es gelingen, die bestehenden Bedenken auszuräumen. Wenn dies bei der weiteren Entwicklung beachtet wird, werden sich biometrische Verfahren in Zukunft durch eine höhere Benutzerakzeptanz positiv hervorheben.

4.6 Niedrige Kosten und hohe Geschwindigkeit

Die Auswahl eines geeigneten Authentifizierungsverfahrens hängt nicht zuletzt auch von den zu erwartenden Kosten des Systems und der Dauer eines Authentifizierungsvorganges ab. Dabei werden sich die Ziele und Anforderungen an Kosten und Geschwindigkeit

in Abhängigkeit vom Einsatzzweck stark unterscheiden. Wichtige Einflussfaktoren sind die zu erwartende Zahl unterschiedlicher Benutzer, die Anzahl der Benutzer, die in einem bestimmten Zeitraum authentifiziert werden müssen, und die benötigte Anzahl an Authentifizierungsstationen. Da sehr viele Einflussfaktoren eine Rolle spielen, kann ein konkreter Betrag der Kosten nicht genannt werden. Es soll dennoch ein Überblick gegeben werden, wie sich die Kostenfaktoren bei den wissens-, besitz- und merkmalsbasierten Verfahren unterscheiden.

Zunächst soll, unabhängig vom eingesetzten Verfahren, geklärt werden, welche Kosten auftreten und wie diese interpretiert werden können. In [Tel02, S. 48] werden für biometrische Verfahren einmalige Kosten und laufende Kosten unterschieden. Diese Unterscheidung erscheint auch bei wissens- und besitzbasierten Verfahren sinnvoll. Die einmaligen Kosten enthalten zum Beispiel die Kosten für Hard- und Software, Installation und Schulungsmaßnahmen, während die laufenden Kosten sich aus dem Aufwand für Updates, Wartung sowie der Registrierung neuer Benutzer zusammensetzen. Zum Vergleich von Verfahren, die in unterschiedlichen Situationen eingesetzt werden, könnte man daraus verschiedene Kennzahlen berechnen, zum Beispiel die Kosten pro Benutzer oder die Kosten pro Authentifizierungsvorgang.

Wissensbasierte Verfahren sind bei deren Einsatz im IT-Umfeld meist eine sehr günstige Lösung. Die Eingabe erfolgt über die bereits vorhandene Tastatur und die benötigte Anwendungslogik ist relativ einfach zu implementieren. Selbst wenn kein Computer als Plattform dienen kann, sind Terminals zur Erfassung des geforderten Wissens aufgrund der Massenproduktion solcher Geräte günstig zu realisieren.

Besitzbasierte Verfahren erfordern einerseits ein Gerät zur Erfassung des zu besitzenden Gegenstandes, andererseits muss für jeden Benutzer ein solcher Gegenstand vorhanden sein. Je nach eingesetzter Technologie unterscheiden sich die Preise für Lesegeräte und Authentifizierungsgegenstände.

Die unterschiedlichen Kosten der Erfassungssensoren bei biometrischen Systemen wurden schon in Abschnitt 3.3.6 aufgezeigt. Hinzu kommen noch Kosten für weitere Hard- und Software, deren Höhe wiederum in Abhängigkeit vom eingesetzten Merkmal unterschiedlich ausfällt. Da die Verbreitung biometrischer Verfahren noch nicht sehr hoch ist, müssen Betreiber und Benutzer solcher Systeme geschult werden. Hinzu kommt, dass das Enrollment Zeit in Anspruch nimmt und die zu erfassende Person dafür anwesend sein muss. Bei einer längerfristigen Betrachtung muss man auch berücksichtigen, dass von einigen Personen aufgrund geänderter Merkmalsausprägung (z. B. durch Alterung oder Narbenbildung nach einer Verletzung) eventuell mehrmals Referenztemplates erfasst werden müssen.

Alle Verfahren ermöglichen im Normalfall eine Authentifizierung in wenigen Sekunden. Somit ist auch in zeitkritischen Anwendungsfällen ein Einsatz dieser Verfahren denkbar. Ein solcher Fall könnte zum Beispiel in einem Unternehmen auftreten, bei dem jeweils zum Schichtwechsel mehrere hundert Personen die Zutrittskontrolle passieren müssen. Dafür steht in der Regel nur ein begrenzter Zeitraum und eine begrenzte Anzahl an Zutrittskontrollstationen zur Verfügung. Eine Verzögerung beim Authentifizierungsvorgang

könnte dazu führen, dass nicht alle Arbeiter zum Schichtbeginn an ihrem Arbeitsplatz sind und dadurch die Produktion erheblich gestört wird. Die Gefahr solcher Verzögerungen besteht vor allem bei biometrischen Systemen mit hoher False Rejection Rate. Bei zeitkritischen Systemen ist die False Rejection Rate demnach nicht nur eine Maßzahl für den Komfort sondern auch ein wichtiges Kriterium für die Praxistauglichkeit. Kann aufgrund hoher Sicherheitsansprüche keine Anpassung des Schwellenwertes zur Reduzierung der False Rejection Rate vorgenommen werden, so ist das gewählte biometrische Verfahren womöglich nicht für den Anwendungszweck geeignet.

Die zu den Gesamtkosten beitragenden Faktoren konnten hier näher vorgestellt werden. Als sehr günstig kann man die Authentifizierung durch Wissen einstufen. Bei besitz- und merkmalsbasierten Systemen sind die Kosten davon abhängig, welche Technologie bzw. welches Merkmal verwendet wird. Bei zeitkritischen Anwendungen muss zudem auf die False Rejection Rate biometrischer Systeme geachtet werden.

4.7 Übersicht und Vergleich der Verfahren

In den letzten Abschnitten wurden unterschiedliche Anforderungen an Authentifizierungsverfahren vorgestellt und die verschiedenen Verfahren bezüglich der Erfüllung dieser Anforderungen miteinander verglichen. Es wurde klar, dass einige dieser Anforderungen in Konflikt mit anderen Anforderungen stehen, so zum Beispiel Sicherheit und Benutzerfreundlichkeit. Welcher dieser Anforderungen in der Praxis eine höhere Priorität beigemessen wird, hängt hauptsächlich von den Rahmenbedingungen im einzelnen Anwendungsfall ab.

Ein „optimales Authentifizierungsverfahren“ wurde, wie zu erwarten war, nicht gefunden. Die verschiedenen Verfahren haben jeweils spezifische Vor- und Nachteile und erfüllen die an sie gestellten Anforderungen in unterschiedlichem Maße. Tabelle 3 soll die Ergebnisse dieses Abschnittes übersichtlich zusammenfassen. Hierbei kennzeichnen die Symbole + und – Anforderungen, die ein Verfahren besonders gut erfüllt bzw. nicht erfüllt. Anforderungen, die nur teilweise erfüllt werden oder bei denen keine eindeutig Bewertung abgegeben werden kann, werden mit ○ gekennzeichnet.

Es sei an dieser Stelle nochmals auf die Multifaktor-Authentifizierung hingewiesen. Dabei werden unterschiedliche Verfahren kombiniert, um auf diese Art möglichst viele Anforderungen zu erfüllen. In einigen Anwendungsfällen, vor allem bei hohen Sicherheitsansprüchen, lassen sich dadurch bessere Ergebnisse erzielen als mit einem Verfahren, das entweder auf Wissen, Besitz *oder* Biometrie beruht.

4.8 Anforderungen in unterschiedlichen Szenarien

Anhand von drei Szenarien soll gezeigt werden, welche Fragestellungen und Probleme bei der Einführung von biometrischen Authentifizierungsverfahren in der Praxis auftreten

Anforderungen	Authentifizierung durch		
	Wissen	Besitz	Biometrie
Identifikation einer Person	–	–	+
Sicherheit, Robustheit	–	○	○
Reaktionsmöglichkeiten bei Kompromittierung	+	+	○
Datenschutz, Verbraucherschutz	+	+	○
Benutzerfreundlichkeit	–	○	+
Benutzerakzeptanz	○	+	–
Niedrige Kosten	+	○	○
Hohe Geschwindigkeit	+	+	○

Tabelle 3: Vergleich der Authentifizierungsverfahren bezüglich der Erfüllung gestellter Anforderungen

können. Der erste Fall beschreibt ein schon länger im Betrieb befindliches Gesichtserkennungssystem und nennt die Gründe, die zur Entscheidung für die Gesichtserkennung geführt haben. Im zweiten Fall wird eine Lösung für eine aktuelle Fragestellung an der Universität Regensburg gesucht. Als letztes wird kurz die von der Bundesregierung geplante Speicherung biometrischer Daten in Reisepässen vorgestellt und dazu die bedeutendsten Kritikpunkte und Forderungen genannt. Diese drei Szenarien wurden gewählt um zu zeigen, dass biometrische Verfahren sinnvoll eingesetzt werden können, es aber auch Fälle gibt, in denen sie die gestellten Anforderungen nicht erfüllen.

4.8.1 Zutrittskontrolle im Zoo von Hannover

Der Zoo in Hannover bietet seinen Besuchern neben den normalen Tageskarten auch Jahreskarten, sogenannte ZooCards, an. Der Preis der ZooCards beträgt in etwa das Dreifache⁸ des Preises der Einzelkarte, so dass vor allem Familien, die den Tierpark regelmäßig besuchen, sich für die Jahreskarte entscheiden. Die ZooCards sind nicht übertragbar, das heißt die Karten dürfen nur von der Person genutzt werden, die dafür bezahlt hat. Bis Ende der 90er Jahre ließ sich dies jedoch nur mit sehr hohem Personalaufwand kontrollieren und eine Lösung mit auf Magnetstreifenkarten gedruckten Fotos erwies sich als nicht ausreichend [Zie03].

Die Anforderungen in diesem Szenario waren die Erhöhung der Sicherheit eines bestehenden Authentifizierungssystems, bei gleichzeitig hoher Benutzerfreundlichkeit und hoher Zuverlässigkeit. Der Inhaber einer ZooCard muss verifiziert werden, damit nur derjenige den Tierpark mit einer ZooCard betreten kann, für den diese ausgestellt wurde. Der Zoo will sich also vor Angriffen schützen, bei denen der Inhaber einer ZooCard mit dem „Angreifer“ kooperiert, indem er diesem seine Karte aushändigt. Eine Authentifizierung durch Wissen würde die Sicherheit auch nicht erhöhen, da auch dieses Wissen einfach weitergegeben werden kann. Man entschied sich deshalb für ein biometrisches Verfahren.

⁸Stand Sommer 2005

Wie in [Zie03] beschrieben, wurden zunächst ab Mai 2001 Fingerabdruck-Scanner installiert. Es zeigten sich dabei jedoch deutliche Schwächen des eingesetzten Systems: Fingerabdrücke von Kindern - immerhin mehr als die Hälfte der Besucher - konnten oft bereits beim Enrollment nicht erfasst werden. Zudem bereiteten kalte Außentemperaturen den freistehenden Scannern Probleme, so dass vor allem im Winter vermehrt Ausfälle des Systems auftraten. 2003 entschied man sich deshalb, statt des Fingerabdrucks in Zukunft das Gesicht als Merkmal zur Verifikation zu verwenden. Seit April 2003 ist das Gesichtserkennungssystem ZN-Face des Herstellers ZN Vision Technologies in Betrieb.

Die Sicherheitsanforderungen an das biometrische System kann man als relativ niedrig bezeichnen. Eine False Acceptance Rate im einstelligen Prozentbereich kann nach Ansicht des Autors dieser Arbeit beim vorliegenden Szenario toleriert werden. Auf diese Weise sind False Rejection Rates möglich, die für die Besucher des Zoos akzeptabel sind. Genaue Angaben, wie hoch die Fehlerraten in Zoo von Hannover sind, liegen nicht vor.

Auf der Veranstaltung „Biometrische Verfahren im praktischen Einsatz“ im Februar 2004 bezeichnete der Leiter des Projekts, Herr Klaus-Michael Machens, den bisherigen Verlauf als erfolgreich [Ver04]. 72900 Inhaber von Jahreskarten haben demnach das System benutzt, die Akzeptanz sei „erfreulich hoch“. Kritisch betrachtet werden sollte die Speicherung der Rohdaten des Gesichtsbildes. Zwar sind keine detaillierten Informationen zur Implementierung bekannt, doch lässt eine Anmerkung im Artikel [Kur04a] darauf schließen. Darin heißt es, die Besucher könnten auf einem Bildschirm ihr aktuelles Bild mit dem des letzten Besuches vergleichen. Aus Rücksichtnahme auf den Datenschutz sollte allerdings auf die Speicherung der Rohdaten verzichtet werden, denn für die Authentifizierung ist das erzeugte Template alleine ausreichend.

4.8.2 Zutrittskontrolle zu Lehrstuhlräumen an der Universität Regensburg

In diesem Szenario soll die Frage beantwortet werden, ob sich durch den Einsatz biometrischer Verfahren der Komfort eines vorhandenen Zutrittskontrollsystems erhöhen lässt. Bisher ist im vorliegenden Fall ein besitzbasiertes Verfahren implementiert: Mitarbeiter des Lehrstuhls können sowohl mit einem mechanischen Schlüssel als auch mit Chipkarten die Eingangstür öffnen. Die Übertragung der Identifikationsnummer der Chipkarte erfolgt drahtlos, ein entsprechendes Lesegerät befindet sich direkt neben der Tür.

Zur Erhöhung des Komforts sollte den Mitarbeitern des Lehrstuhls künftig auch nach einer berührungslosen Identifikation durch Gesichtserkennung der Zutritt gestattet werden. Dabei ist als „Nebenbedingung“ unbedingt darauf zu achten, dass der Sicherheitslevel der bestehenden Authentifizierung auf keinen Fall gesenkt werden darf. False Acceptances dürfen unter keinen Umständen auftreten. Wie im Rahmen der bisherigen Arbeit schon gezeigt werden konnte, steht dieser hohe Sicherheitsanspruch aber im Konflikt mit dem Ziel der Benutzerfreundlichkeit. Die Gesichtserkennung im Modus der Identifikation wird bei einer sehr niedrigen False Acceptance Rate eine inakzeptabel hohe False Rejection Rate aufweisen. Soll der Sicherheitslevel beibehalten werden, muss daher auf einen Einsatz der Gesichtserkennung zur Erhöhung des Komforts verzichtet werden.

4.8.3 Kritische Betrachtung der Speicherung biometrischer Daten in Reisepässen

Die Reisepässe von EU-Bürgern sollen in Zukunft um elektronisch gespeicherte biometrische Daten erweitert werden, um die Richtlinien der International Civil Aviation Organisation (ICAO) zu erfüllen. Der Bundesinnenminister Otto Schily sieht dies als „wichtigsten Baustein im Gesamtkonzept der Terrorismusbekämpfung“ [Kur04b]. Die biometrischen Daten sollen eine automatische Verifikation des Ausweisinhabers erlauben und auf diese Weise verhindern, dass Personen mit einem fremden Ausweis Grenzkontrollen passieren können [Una04]. Zudem soll das Fälschen von Ausweisen verhindert werden [Una04]. In diesem Szenario wird dargestellt, wie das Vorhaben umgesetzt werden soll, und welche Kritikpunkte von zahlreichen Seiten, insbesondere von Datenschützern, immer wieder genannt werden.

In einem ersten Schritt sollen Reisepässe ab 1. November 2005 [BK05] ein Bild des Gesichtes des Ausweisinhabers in elektronisch auslesbarer Form enthalten. Zur Speicherung und Datenübertragung entschied man sich für die RFID-Technologie. Um unabhängig von bestimmten Extraktions-Algorithmen zu sein, werden nicht Templates gespeichert, sondern die Rohdaten in Form eines etwa 20 Kilobyte großen Passbildes [BK05]. Voraussichtlich ab März 2007 sollen dann zusätzlich auch die Fingerabdrücke des Passinhabers aufgenommen werden.

Bei Grenzkontrollen sollen die „biometrischen Reisepässe“ die automatische Verifikation möglich machen. Ein Gesichtserkennungssystem vergleicht dazu das im Pass gespeicherte Bild mit dem aktuellen Bild der Person, das direkt bei der Grenzkontrolle aufgenommen wird. Die biometrischen Daten wurden bei der Herstellung des Ausweises von der ausstellenden Behörde, der Bundesdruckerei, mit deren privaten Schlüssel signiert. Über den öffentlichen Schlüssel der Behörde kann die Signatur bei der Grenzkontrolle geprüft werden, wodurch gefälschte Ausweise problemlos erkannt werden können.

Da die Datenübertragung kontaktlos erfolgt, müssen die biometrischen Daten vor unberechtigtem Auslesen geschützt werden. Das im Auftrag des BSI⁹ entwickelte Golden Reader Tool implementiert dafür die sogenannte Basic Access Control [Bun05b]. Dabei ist eine Datenübertragung nur über einen sicheren Kanal möglich, für den ein bestimmter Schlüssel benötigt wird. Dieser kann nur berechnet werden, wenn der Ausweis vorgelegt und darin enthaltene, maschinenlesbare Daten optisch erfasst werden. Ab 2007 soll über kryptographische Verfahren zudem gewährleistet werden, dass nur autorisierte Lesegeräte Zugriff auf die Daten erhalten (Extended Access Control).

Von Seiten der Kritiker gibt es Bedenken, dass die technische Machbarkeit des Projektes noch nicht geklärt ist. Feldversuche mit einer ausreichend großen Zahl an Testpersonen wurden bisher nicht durchgeführt [Sta04a]. Untersuchungen des BSI und des Büros für Technikfolgen-Abschätzung des Bundestages zeigten, „dass die Anzahl von fehlerhaft erkannten und fehlerhaft zurückgewiesenen Personen erheblich sein dürfte“ [KK05]. Dadurch würden eine große Anzahl an Personen in den Verdacht geraten, einen fremden Ausweis zur Einreise zu benutzen. Speziell das Merkmal Fingerabdruck könnte zu

⁹Bundesamt für Sicherheit in der Informationstechnik

einer Diskriminierung derjenigen Personen führen, die das Merkmal nicht in auswertbarer Form aufweisen. Gesichts- und Fingerabdruckerkennung gilt momentan als nicht überwindungssicher, so dass ein Einsatz nur in einer überwachten Umgebung stattfinden sollte [SHZ05]. Eine vollautomatische Grenzkontrolle wird es also auch mit den neuen Ausweisen nicht geben. Es ist außerdem ungeklärt, ob die Haltbarkeit der Transponder ausreicht [SHZ05]. Immerhin beträgt die Gültigkeitsdauer eines Reisepasses 10 Jahre (bei Antragstellern ab 26 Jahren).

Berechtigte Kritik üben zahlreiche Datenschutzexperten, wie der Bundesbeauftragte für den Datenschutz, Peter Schaar, der ein Moratorium für die Einführung der neuen Pässe fordert [Sch05]. Vertreter des Chaos Computer Club kritisieren, dass sich mit dem Merkmal Gesicht „die Möglichkeit der großflächigen automatischen Überwachung“ bietet, da dieses auch auf große Entfernung zur Personenerkennung genutzt werden kann [Sta04a]. Die ausgelesenen biometrischen Daten könnten zu diesem Zweck bei der Einreise in ein Land zentral gespeichert werden. Zwar ist in Deutschland die zentrale Auswertung und Speicherung biometrischer Daten verboten [Una04], doch ob auch andere Länder, insbesondere die USA, ein solches Verbot umsetzen, ist fraglich [BK05]. Die Speicherung von Templates statt der Rohdaten wäre aus Sicht des Datenschutzes zwar zu begrüßen, würde jedoch eine Festlegung auf ein bestimmtes Erkennungsverfahren und damit die „Gefahr der Monopolisierung“ bedeuten [Sta04a].

Ungeklärt sind zudem die Kosten der Einführung der neuen Pässe. Geplant sind bisher eine Gebühr von 59 Euro für den 10 Jahre gültigen Pass [SW05]. Mit der Gebühr sollen die Kosten für die Ausstellung des Passes in vollem Umfang gedeckt werden [KK05]. Es ist jedoch zu erwarten, dass die Kosten deutlich darüber liegen werden und so ab der Einführung der Fingerabdrücke 2007 die Gebühren deutlich angehoben werden müssen [SW05].

Trotz vieler Kritikpunkte und ungeklärter Fragen wird an der Einführung der biometrischen Daten in Reisepässen unbeirrt festgehalten. Als Ziel wird dabei immer wieder auf die Bekämpfung des internationalen Terrorismus verwiesen, wobei nicht ersichtlich ist, wie die neuen Reisepässe das ermöglichen sollen. Einzig die Fälschung von Pässen und das Verwenden eines fremden Passes wird erschwert. Terroristen können gefälschte Ausweise aus Ländern einsetzen, die keine biometrischen Daten im Reisepass speichern. Ein Schutz vor Terroristen mit gültigem, nicht gefälschtem Ausweis wird in keiner Weise erreicht. Die Anschläge vom 7. Juli 2005 in London haben gezeigt, dass es sich bei Terroristen nicht zwangsläufig um Ausländer handeln muss: Drei der vier mutmaßlichen Täter waren Briten [Wik05b].

Der erzielbare Sicherheitsgewinn steht also in keinem Verhältnis zu dem hohen finanziellen Aufwand und den Risiken der Einführung dieser neuen Pässe. Auch wenn internationale Verbände wie die ICAO oder einzelne Staaten vorschreiben, dass biometrische Daten in Reisepässen zu speichern sind, so rechtfertigt dies in keiner Weise die Missachtung der Interessen der deutschen Bürger. Die Kritik der Datenschützer sollte deshalb ernst genommen werden, zumal die Einführung der neuen Pässe auch einen Eingriff in das Recht des Einzelnen auf informationelle Selbstbestimmung bedeutet. „Es nützt der Frei-

heit nichts, dass wir sie abschaffen, um sie zu schützen.“ (Wolfgang Thierse, Präsident des Deutschen Bundestages [Wik05c])

5 Gesichtserkennung

Im letzten Abschnitt wurden bewusst Szenarien ausgewählt, die sich mit den Einsatzmöglichkeiten der Gesichtserkennung befassen. Die computergestützte Erkennung von Gesichtern ist bereits seit mehr als 30 Jahren Gegenstand intensiver Forschung. Während dieser Zeit wurde eine Vielzahl von Algorithmen und Vorgehensweisen entwickelt, die jeweils unterschiedliche Teilprobleme der Gesichtserkennung zu lösen versuchen. Die enorme Steigerung der Rechenleistung von Computersystemen erlaubt es heute, die oft rechenintensiven Ansätze auf Standard-PCs in Bruchteilen einer Sekunde auszuführen. Damit ist eine Merkmalsextraktion aus einem Bild in so kurzer Zeit realisierbar, dass sich die Gesichtserkennung zur Authentifizierung von Personen einsetzen lässt. [Pam02]

Gegenüber anderen biometrischen Authentifizierungsverfahren hat die Gesichtserkennung den Vorteil, dass die Erfassung des Merkmals Gesicht völlig berührungslos erfolgt und somit äußerst benutzerfreundlich ist. Kameras zur digitalen Erfassung des Gesichts sind mittlerweile Massenware und kostengünstig zu beschaffen. In einigen Anwendungsfällen, zum Beispiel bei der Zutrittskontrolle, kann es außerdem von Vorteil sein, dass Bilder der erfassten Gesichter archiviert werden können. Die gespeicherten Bilder erlauben die „manuelle“ Überprüfung der vom Gesichtserkennungssystem getroffenen Entscheidung, da auch der Mensch andere Personen an deren Gesicht erkennen kann. Ob die Protokollierung der Bilder mit dem Datenschutz vereinbar ist, muss im jeweiligen Anwendungsfall entschieden werden.

Interessant ist die Gesichtserkennung auch für Überwachungsaufgaben. Hierfür kann nur ein biometrisches Merkmal dienen, das aus unterschiedlichen Entfernungen und ohne aktive Beteiligung der überwachten Person erfasst werden kann. Diese beiden Eigenschaften erfüllt die Gesichtserkennung. Ein verbreiteter oder gar flächendeckender Einsatz dieses Verfahrens birgt natürlich die Gefahr der ubiquitären Überwachung und sollte daher sehr kritisch betrachtet werden.

Die Szenarien im letzten Abschnitt haben gezeigt, dass bereits jetzt die Gesichtserkennung eingesetzt wird. Zudem gibt es eine Vielzahl von Anwendungsfällen, in denen wegen der vielseitigen Verwendbarkeit und der hohen Benutzerfreundlichkeit über die Einführung dieses biometrischen Authentifizierungsverfahrens nachgedacht wird. Im Folgenden werden die nötigen Grundlagen der Gesichtserkennung vermittelt und die spezifischen Schwierigkeiten und Problemstellungen bei der Erfassung und Auswertung des Merkmals Gesicht erörtert. Da es eine große Menge verschiedener Verfahren gibt, kann hier nur ein Überblick geboten werden. Um die Leistungsfähigkeit moderner Gesichtserkennungssysteme einschätzen zu können, wird auf die Ergebnisse verschiedener Studien zu diesem Thema eingegangen.

5.1 Grundlagen der Gesichtserkennung

5.1.1 Spezifische Problemstellung der Gesichtserkennung

Die meisten Gesichtserkennungssysteme verarbeiten zweidimensionale Bilddaten, die von einer Kamera aufgenommen werden. Wie bei allen biometrischen Merkmalen ist auch das Erfassen des Gesichtes mit verschiedenen Variationen verbunden, so dass zwei Aufnahmen zu unterschiedlichen Zeitpunkten nie exakt das gleiche Bild ergeben werden [Bre02, S. 44]. Im Vergleich zu anderen biometrischen Merkmalen wird die Erfassung durch besonders viele Faktoren beeinflusst und dadurch die Erzeugung des Templates erschwert. Für die Qualität eines Gesichtserkennungssystems ist daher entscheidend, ob trotz zahlreicher Herausforderungen eine hohe Erkennungsleistung und niedrige Fehleraten erreicht werden können. Es folgt eine Auflistung und Erläuterung dieser spezifischen Problemstellungen bei der Gesichtserkennung, zusammengestellt nach den Angaben in [Pam02, S. 302–305], [GSC01, S. 2–3] und [Lu03, S. 4–5]. Dabei ist zu beachten, dass in praktischen Anwendungsfällen die Variationen und Probleme nicht einzeln auftreten und daher immer in Kombination betrachtet werden sollten [GSC01].

- **Position:** Das Gesicht kann innerhalb des erfassten Bildes an verschiedenen Positionen zu finden sein. Abhängig vom Anwendungsfall können die möglichen Positionen mehr oder weniger variieren: Bei einer Zutrittskontrolle wird die zu authentifizierende Person in der Regel vor einer Kamera stehen, eventuell hilft ein Spiegel bei der Positionierung des Kopfes. Das Gesicht wird sich in der Mitte des Bildes befinden. Dagegen kann bei der Überwachung öffentlicher Plätze nicht von einer zu erwartenden Position ausgegangen werden. Ein Teilproblem der Gesichtserkennung ist daher die Gesichtsentdeckung (Face Detection). Dabei werden Bilder untersucht, um festzustellen, ob überhaupt ein Gesicht enthalten ist und, wenn ja, wo sich das Gesicht befindet. Je nach Implementierung des Verfahrens können auch die Positionen mehrerer Gesichter in einem Bild festgestellt werden.
- **Hintergrund:** Die Beschaffenheit des Hintergrundes, vor dem sich das zu lokalisierende Gesicht befindet, kann auf unterschiedliche Arten variieren, zum Beispiel in Farbe oder Struktur. Der Hintergrund kann zudem statisch sein oder sich dynamisch verändern. Dies wird besonders bei schwenkbaren Kameras ersichtlich, bei denen in unterschiedlichen Positionen der Kamera völlig andere Hintergründe erfasst werden. Die Beschaffenheit und Variation des Hintergrundes ist vor allem für die Gesichtsentdeckung von Bedeutung.
- **Größe des Gesichtes:** Je nach Entfernung der erfassten Person von der Kamera schwankt auch die Größe des erfassten Gesichtes im Bild. Je weiter die Person entfernt ist, desto kleiner wird der Ausschnitt im Bild, der das Gesicht enthält. Je kleiner dieser Ausschnitt ist, desto weniger Informationen können daraus extrahiert werden und desto schlechter wird die Erkennungsleistung ausfallen. Bis zu welcher Entfernung eine Erkennung möglich ist, hängt von den verwendeten Verfahren und von der Auflösung des erfassten Bildes ab.

- **Kopfhaltung:** Die Haltung des Kopfes kann stark variieren, so dass unter Umständen nur Teile des Gesichtes zu erkennen und andere verdeckt sind. Die Profilansicht von der Seite enthält zum Beispiel nur eine Hälfte des Gesichtes. Außerdem bewirken unterschiedliche Betrachtungswinkel des dreidimensionalen Objektes Gesicht Variationen bei der Abbildung auf ein zweidimensionales Bild. Die optimale Position ist in der Regel die frontale Ansicht, bei der die zu authentifizierende Person geradeaus in Richtung der Kamera blickt. Je größer der Winkel der Abweichung von der Frontal-Ansicht ist, desto schlechter werden die Erkennungsraten ausfallen [GSC01, S. 16]. Diese Aussage ist jedoch nicht allgemein gültig, da dies abhängig vom eingesetzten Verfahren und den verwendeten Referenztemplates ist.
- **Helligkeit:** Unterschiede in der Helligkeit stellen eine besondere Herausforderung dar. Licht kann bestimmte Eigenschaften eines Gesichtes besonders betonen oder deren Erkennbarkeit abschwächen. Schatten oder zu geringe Beleuchtung können dazu führen, dass Teile des Gesichtes nicht oder nur schwach zu erkennen sind [GSC01, S. 2]. Ein Änderung der Helligkeit ist in den meisten Anwendungsfällen unvermeidbar, da allein die Sonneneinstrahlung im Laufe eines Tages zu unterschiedlichen Lichtverhältnissen führt.
- **Gesichtsausdruck:** Der Mensch ist in der Lage über Veränderungen seiner Gesichtszüge Emotionen oder Stimmungen auszudrücken. Ein lachender, trauriger oder erstaunter Gesichtsausdruck unterscheidet sich deutlich von einem neutralen. Die Artikulation von Sprache, sei es normales Sprechen oder lautes Schreien, hat ebenso Auswirkungen auf die Geometrie des Gesichtes. Die Vielzahl möglicher Variationen des Gesichtsausdrucks, deren Anzahl nach [GSC01, S. 2] in die Tausende geht, ist also eine weitere Herausforderung für die Gesichtserkennung.
- **Bedeckung von Teilen des Gesichts:** Selbst für den Menschen wird die Erkennung von Gesichtern schwierig, wenn diese teilweise verdeckt sind. Im Bereich der Augen kann das durch Sehhilfen, insbesondere Sonnenbrillen, erfolgen. Der untere Teil des Gesichtes kann durch einen Schal oder ein anderes Kleidungsstück verborgen sein. Hüte und andere Kopfbedeckungen können, abhängig von der Kameraposition, möglicherweise das gesamte Gesicht überdecken. Neben diesen vom Menschen getragenen Utensilien verursachen natürlich auch andere Objekte, die sich zwischen Kamera und Gesicht befinden, eine Bedeckung [GSC01, S. 3].
- **Veränderung des Merkmals:** Wie jedes biometrische Merkmal, ändert sich auch das Gesicht durch den kontinuierlichen Prozess des Alterns. Bedeutend schnellere Variationen werden durch die Person selbst herbeigeführt oder beeinflusst, zum Beispiel durch eine neue Frisur oder die Anwendung von Make-up. Das Gesicht eines bärtigen Mannes unterscheidet sich, je nach vorhandenem Bart mehr oder weniger deutlich, von dessen Gesicht nach einer Rasur.
- **Individuelle Eigenschaften:** Die Gesichter von Männern und Frauen sowie von Personen unterschiedlicher ethnischer Herkunft weisen jeweils individuelle Eigenschaften auf [GSC01, S. 3]. Für den Menschen ist es in der Regel einfach, am Gesicht

einer Person deren Geschlecht zu erkennen oder die Zugehörigkeit zu einer ethnischen Gruppe abzuleiten. Die Erkennungsraten von Gesichtserkennungssystemen sollten durch diese spezifischen Eigenschaften nicht negativ beeinflusst werden.

Wie sehr die oben genannten Variationen tatsächlich schwanken, hängt mit dem jeweiligen Anwendungsfall und den zu authentifizierenden Personen zusammen. Dabei ist es ganz entscheidend, wie kooperativ sich eine Person verhält. In [Tel02, S. 49–50] werden die Benutzer hierfür in verschiedene Gruppen unterteilt. Die kooperativen Nutzer sind darum bemüht, die Authentifizierung positiv abzuschließen, weil sie sich dadurch Vorteile erhoffen. Diese Personen werden sich bemühen, möglichst optimale Aufnahmen zu erzielen, und sind bereit, dafür zum Beispiel eine Brille abzunehmen oder einen neutralen Gesichtsausdruck zu zeigen. Die nicht-kooperativen Benutzer sind der biometrischen Authentifizierung gegenüber negativ eingestellt und sehen keine Vorteile in der Nutzung des Systems. Möglicherweise wollen sie eine Erkennung durch das Authentifizierungssystem sogar vermeiden. Ein Straftäter, der nicht vom Gesichtserkennungssystem der Strafverfolgungsbehörden erkannt werden will, könnte zum Beispiel sein Gesicht so weit wie möglich verdecken und auf diese Weise die Erfassung und Identifikation verhindern.

5.1.2 Erfassung des Merkmals

Zur Erfassung des Merkmals Gesicht werden Kameras verwendet, die entweder Bilder oder Bildsequenzen (Videos) aufzeichnen [Bre02, S. 41–42]. In welcher Form die Rohdaten vorliegen müssen, ist abhängig von den Verfahren, die zur Erzeugung des Templates eingesetzt werden. Einige Systeme erfordern Farbinformationen, anderen wiederum reicht ein Graustufenbild aus. Wieder andere erfassen zusätzlich Informationen aus dem Bereich des infraroten Lichtes [Bre02, S. 41].

Digitalisierte Fotos und einzelne Frames eines Videos sind zweidimensionale Objekte, bei denen zu jedem Bildpunkt ein Farb- oder Graustufenwert gespeichert ist. Es existieren jedoch mittlerweile einige Ansätze, die auch die dreidimensionale Form des Gesichtes auswerten, um bessere Erkennungsraten bei unterschiedlichen Kopfhaltungen zu erreichen. In [CH04] wird ein solches Verfahren vorgestellt: Aus zwei Bildern, die aus zueinander rechtwinkligen Kameraperspektiven aufgenommen wurden, wird ein dreidimensionales Modell des Gesichtes berechnet. Es sind demnach zwei Aufnahmen aus unterschiedlichen Blickwinkeln nötig. Die Bilder können, wie in [CH04] vorgeschlagen, von einer Kamera erfasst werden, wenn die zu erkennende Person den Kopf vor der Kamera dreht. Eine andere Möglichkeit, die deutlich benutzerfreundlicher sein dürfte, ist die Aufnahme von Bildern mit zwei Kameras, die aufeinander abgestimmt positioniert werden.

Eine andere Technologie zur Erfassung von dreidimensionalen Objekten ist die optische Entfernungsmessung. Mit sogenannten 3D-Scannern werden 3D-Bilder erzeugt, die zusätzlich zu den Farbinformationen auch den gemessenen Abstand zu jedem Pixel speichern. Für eine hochwertige Aufnahme müssen die Scanner die Entfernung möglichst präzise und schnell messen. Schnell deshalb, da sich während des Erfassungsvorgangs

das Gesicht bewegen kann und diese Bewegung das Ergebnis verfälscht [BCF04, S. 10]. Moderne Scanner¹⁰ erfassen Objekte typischerweise in einer Entfernung von bis zu 2,5 Metern. Ein Scanning-Vorgang dauert 2,5 Sekunden und erlaubt bei einer optimalen Entfernung des Objektes von 1,2 Metern eine sehr hohe Genauigkeit (Abweichung von wenigen Zehntel Millimetern in allen drei Dimensionen) [Kon05]. Schnellere Scanning-Vorgänge sind durchführbar, allerdings fehlt eine Angabe zu deren Genauigkeit.

5.1.3 Ablauf der Gesichtserkennung: Vom Bild zum Template

Wie bei anderen biometrischen Verfahren muss auch bei der Gesichtserkennung aus dem erfassten Merkmal ein Template errechnet werden. Der Ablauf bei einem „typischen“ Gesichtserkennungssystem wird in drei Teile gegliedert, wie in [Bre02, S. 43] und [Pam02, S. 303] beschrieben. Diese werde nun vorgestellt. Abbildung 4 stellt im Anschluss den Ablauf schematisch dar.

Gesichtsentdeckung

Nach der Definition in [YKA02, S. 34] ist das Ziel der *Gesichtsentdeckung* (*Face Detection*), für ein beliebiges Bild festzustellen, ob keines, eines oder mehrere Gesichter im Bild vorhanden sind. Falls eines oder mehrere Gesichter gefunden werden, soll deren Position und Ausmaß bestimmt werden. Dies ist bedeutend für den späteren Prozess der Erzeugung des Templates, da sich dieser auf den Bereich des Gesichtes beschränken soll.

Mit der Gesichtsentdeckung begegnet man demnach den ersten drei der Herausforderungen, die in Abschnitt 5.1.1 genannt wurden: Der Variabilität von Position, Hintergrund und Größe. Die Herausforderung, alle im Bild vorhandenen Gesichter zu finden, wird durch die ebenfalls schon genannten Faktoren (Kopfhaltung, Helligkeit, Gesichtsausdruck usw.) erschwert.

Neben der Face Detection werden in [YKA02, S. 34–35] noch weitere Begriffe genannt und voneinander abgegrenzt. Danach stellt die *Gesichtslokalisierung* (*Face Localization*) eine Vereinfachung der Gesichtsentdeckung dar, da dabei angenommen wird, dass sich nur ein einzelnes Gesicht im Bild befindet. Die *Entdeckung von Gesichtsmarkmalen* (*Facial Feature Detection*) sucht nach Vorkommen und Position einzelner „Bestandteile“ eines Gesichtes, zum Beispiel von Augen, Mund und Nase. Bei Bildsequenzen und Videos bestimmt die *Gesichtsverfolgung* (*Face Tracking*) in Echtzeit die Veränderung der Position eines Gesichtes.

Bereits 2002 gab es über 150 verschiedene Ansätze und Methoden zur Gesichtsentdeckung, die an dieser Stelle nicht näher betrachtet werden sollen. Eine umfangreiche Bestandsaufnahme der Verfahren und Algorithmen findet sich in [YKA02]. Hierin werden unterschiedliche Herangehensweisen kategorisiert und bewertet. Das sehr ausführliche Literaturverzeichnis kann bei der Suche nach weiterführenden Informationen sicherlich hilfreich sein.

¹⁰Als Referenz dient der Scanner „Vivid 910“ von Konica Minolta.

Normalisierung

Für die weitere Auswertung müssen die Bilder der Gesichter in einer bestimmten Größe und Ausrichtung vorliegen. Dazu werden im Vorgang der *Normalisierung* die relevanten Bildregionen ausgeschnitten, eventuell rotiert und auf eine vorgegebene Größe skaliert [Pam02, S. 303]. An welchen Positionen Gesichter zu finden sind und welche Ausmaße diese haben, wurde, wie oben beschrieben, bereits im Schritt der Gesichtsentdeckung bestimmt.

Merkmalsextraktion und Erzeugung des Templates

Zur Gesichtserkennung soll das Gesicht einer erfassten Person mit einem oder mehreren bekannten Gesichtern verglichen werden. Damit dieser Vergleich effizient und mit hohen Erkennungsraten abläuft, wird aus dem Bild eines Gesichtes ein Template erzeugt [Pam02, S. 305–306]. Das gleiche Verfahren wurde beim Enrollment der bekannten Gesichter angewandt, so dass auch für diese ein Template vorliegt. Es werden demnach bei der Gesichtserkennung nicht die Bilder von Gesichtern direkt verglichen, sondern die daraus erzeugten Templates.

Ein Template ist das Ergebnis einer Reduktion der Informationen, die im Bild des Gesichtes enthalten sind. Dabei werden all diejenigen Informationen verworfen, die nicht zu einer Unterscheidung von verschiedenen Gesichtern beitragen [Pam02, S. 306]. Gleichzeitig wird die Komplexität derart reduziert, dass ein Vergleich verschiedener Templates effizient abläuft. Bei der Identifikation ist Effizienz von besonderer Bedeutung, da hier das Anfragetemplate mit allen Referenztemplates verglichen werden muss und jeder Vergleichsvorgang Rechenzeit und Speicherplatz benötigt. Je größer die Anzahl der in der Referenzdatenbank gespeicherten Templates ist, desto bedeutender wird die effiziente Vergleichbarkeit.

Das Erzeugen von Templates und der Vergleich von Anfrage- und Referenztemplate ist der Teil eines Gesichtserkennungssystems, der die eigentliche Erkennung leistet. Über die letzten 30 Jahre haben Erkenntnisse aus verschiedenen Forschungsrichtungen zur Entwicklung von zahlreichen Verfahren und Algorithmen beigetragen, die diese Aufgaben auf unterschiedliche Art zu lösen versuchen. Die Lösungsansätze sind jeweils von unterschiedlichen Fachrichtungen beeinflusst und weiterentwickelt worden, so zum Beispiel die Forschung in den Bereichen Psychologie, Mustererkennung und neuronale Netze. Im Folgenden wird eine kurze Übersicht der verschiedenen Herangehensweisen gegeben. Als tiefer gehende Einführung in dieses Thema seien dem interessierten Leser die Studien [ZCPR03] und [BCF04] empfohlen. Zhao et al. geben einen detaillierten Einblick in verschiedene Verfahren und Ansätze, die zweidimensionale Bilder oder Videos verarbeiten. Bowyer et al. decken in ihrer Arbeit die Algorithmen ab, die zum Vergleich bzw. zur Erzeugung von Templates die dreidimensionale Form des Gesichtes nutzen und ergänzen dadurch die Arbeit von Zhao et al.

Zunächst werden in [ZCPR03, S. 3] Verfahren unterschieden, die auf unbewegten Bildern oder Videos aufbauen. Die Video-Gesichtserkennung war bis vor kurzem nur eine Abwandlung der auf Bildern basierenden Verfahren [ZCPR03, S. 33–34]: Einzelne Bilder aus

dem Video wurden wie unbewegte Bilder verarbeitet. Lediglich zur einfacheren Gesichtserkennung wurde die zusätzliche Information „Bewegung“ verwendet. Zur Verbesserung der Erkennungsleistung konnten die Ergebnisse mehrerer hintereinander folgender Erkennungsvorgänge kombiniert werden.

In der nächsten Entwicklungsstufe der videobasierten Systeme wurde das Merkmal Gesicht mit anderen Merkmalen kombiniert [ZCPR03, S. 33]. Ein Beispiel ist die Kombination von Gesicht, Lippenbewegung und Stimme [Die98].

Erst neuere Entwicklungen verdienen nach [ZCPR03, S. 30] die Bezeichnung „true video-based face recognition“. Dabei werden die zeitlichen und räumlichen Informationen des Videos direkt zur Gesichtserkennung bzw. Template-Erzeugung genutzt, beispielsweise um aus dem zweidimensionalen Bildmaterial ein dreidimensionales Modell des Gesichtes zu berechnen.

Algorithmen zur Erzeugung von Templates lassen sich zudem danach unterscheiden, ob zwei- oder dreidimensionale Daten verarbeitet werden. Die zweidimensionalen Daten sind einfache Farb- oder Graustufenbilder, wie sie von einer normalen Kamera aufgenommen werden können. Eine dreidimensionale Darstellung des Gesichtes kann direkt von einem 3D-Scanner erfasst werden. Eine andere Möglichkeit ist die Berechnung der dreidimensionalen Form aus mehreren zweidimensionalen Bildern, die aus verschiedenen Perspektiven aufgenommen wurden [CH04]. Die Motivation zur Nutzung von dreidimensionalen Informationen liegt vor allem darin begründet, dass dabei von einer höheren Genauigkeit, verglichen mit 2D-Systemen, ausgegangen wird. Als weiterer Vorteil wird in [BCF04, S. 3–4] genannt, dass Variationen von Aufnahmewinkel und Helligkeit bei Betrachtung der dreidimensionalen Daten kein Problem darstellen.

Die beiden genannten Unterscheidungen beziehen sich auf die Eigenschaften der zu verarbeitenden Daten. Unabhängig davon lassen sich auch die Verfahren, die aus den Daten des Gesichtes Templates errechnen, in Gruppen aufteilen. In den meisten Studien wird von drei Gruppen ausgegangen, so auch in [ZCPR03, S. 13]. Diese werden im Anschluss kurz vorgestellt. Interessanterweise geht man in der Psychologie, bei der Erforschung der Wahrnehmung und Erkennung von Gesichtern durch Menschen, ebenfalls von diesen drei Erklärungsmodellen menschlicher Wahrnehmung aus. Dies ist ein Beispiel dafür, dass die Gesichtserkennung nicht nur ein Forschungsgebiet der Mathematik oder Informatik ist, sondern die Entwicklung in diesem Bereich durch Erkenntnisse aus vielen anderen Fachrichtungen beeinflusst wird. Ein Überblick der für die Gesichtserkennung relevanten Sachfragen der Psychologie und Neurologie findet sich in [ZCPR03, S. 7–10].

Holistische Methoden analysieren das Gesicht als einheitliches Ganzes ¹¹. Viele der holistischen Methoden basieren auf einem multivariaten Verfahren aus der Statistik, der Hauptkomponentenanalyse. Dafür wird auch in der deutschen Literatur meist der englische Ausdruck „Principal Component Analysis“ verwendet, abgekürzt mit PCA. Wie die Bezeichnung vermuten lässt, wird dabei versucht, die Hauptkomponenten, also die wichtigen Bestandteile eines Gesichtes, zu finden. Bezogen auf die Gesichtserkennung

¹¹Holistisch $\hat{=}$ Ganzheitlich

wären das diejenigen Merkmale und Eigenschaften eines Gesichtes, die am meisten zur Unterscheidbarkeit und Einzigartigkeit eines Gesichtes beitragen. Dabei werden nicht etwa Merkmale wie Augen, Nase oder Mund herangezogen, denn das Gesicht wird hierbei als Einheit betrachtet. Die Hauptkomponenten werden vielmehr mit mathematischen und statistischen Methoden anhand der Betrachtung des ganzen Gesichtes berechnet. Mit den Hauptkomponenten lassen sich dann alle Gesichter beschreiben und kompakt, beispielsweise als Vektor, darstellen.

Die **merkmalsbasierten, strukturellen Methoden** analysieren verschiedene lokale Merkmale („local features“, [ZCPR03, S. 13]), zum Beispiel Augen, Nase und Mund. Dabei können sowohl die geometrische Lage dieser Features zueinander, als auch bestimmte Eigenschaften der Features zur Erzeugung des Templates genutzt werden. Eine sehr bekannte und erfolgreiche Methode ist das Elastic Bunch Graph Matching [ZCPR03, S. 23]. Dabei wird, vereinfacht dargestellt, ein Gitternetz über das Gesicht gelegt und jeweils an den Knotenpunkten des Netzes die Merkmalsausprägung mit Gabor-Wavelet-Transformationen, einem Verfahren aus der Bildbearbeitung, analysiert. Das Netz ist elastisch, das heißt die Knotenpunkte können in einem begrenzten Umfang verschoben werden. Elastic Bunch Graph Matching gilt als robust gegenüber Verzerrung, Drehung, Skalierung und Helligkeitsveränderungen des erfassten Gesichtes [ZCPR03, S. 23].

Hybride Methoden stellen die dritte Gruppe dar. Gemeint sind damit alle Verfahren, die holistische *und* merkmalsbasierte, strukturelle Methoden einsetzen. Nach [ZCPR03, S. 13] könnten solche Systeme die Vorteile beider Methoden bieten und so bessere Ergebnisse erzielen als rein holistische bzw. rein merkmalsbasierte, strukturelle Methoden.

Überblick

Abbildung 4 fasst die einzelnen Schritte der Template-Erzeugung noch einmal zusammen. Es sei an dieser Stelle angemerkt, dass der Ablauf nicht bei allen Systemen so implementiert sein muss. Gesichtserkennungssysteme könnten zum Beispiel auf die Gesichtsentdeckung verzichten, wenn die Position des Gesichtes nur in fest definierten, engen Grenzen variiert.

5.1.4 Matching

Wie bereits erwähnt, müssen die Templates so vorliegen, dass sie möglichst effizient miteinander verglichen werden können. Dabei kann in der Regel ein Template, das mit einem bestimmten Verfahren erzeugt wurde, nur mit einem Template verglichen werden, das ebenfalls mit diesem Verfahren generiert wurde. Einige Algorithmen lassen bestimmte Anpassungen über Parameter zu, um zum Beispiel die Genauigkeit des Templates einzustellen (vgl. Abschnitt 6.1). Da auch diese Einstellungen Auswirkungen auf das entstehende Template haben können, kann bei geänderten Parameterwerten die Vergleichbarkeit nicht mehr gewährleistet sein.

Wie ein Vergleich technisch umgesetzt wird, hängt in erster Linie von den zu vergleichenden Templates ab. Es kommen häufig Methoden der Mathematik und Statistik,

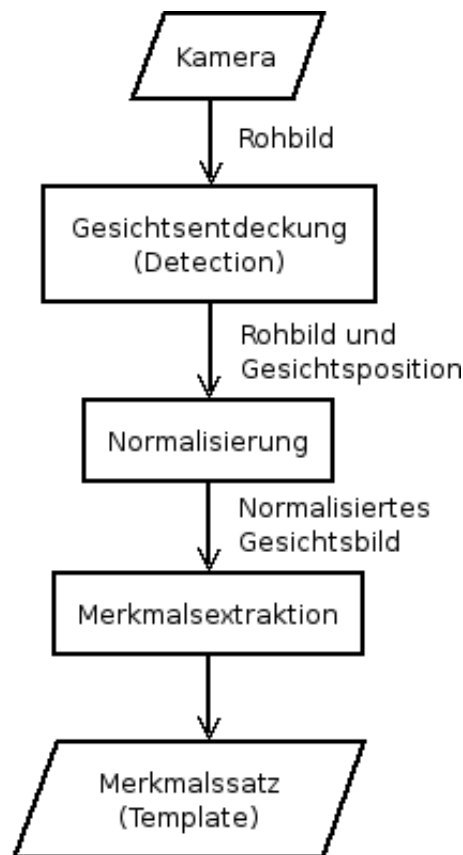


Abbildung 4: Ablauf der Template-Erzeugung bei der Gesichtserkennung (Erstellt nach [Pam02, S. 303].)

insbesondere auch der Wahrscheinlichkeitsrechnung, zur Anwendung. Meist wird bei der Vorstellung eines Algorithmus zur Template-Erzeugung auch gleich ein passender Algorithmus für den Vergleichsvorgang in der Fachliteratur vorgestellt. Denn bereits bei der Entwicklung oder Verbesserung von Verfahren muss eine Prüfung stattfinden, in welchem Maß sich die Templates zur Erkennung von Gesichtern eignen. Damit die Ergebnisse später nachvollziehbar sind, wird der zur Evaluation eingesetzte Vergleichsalgorithmus meist mit veröffentlicht.

5.2 Ergebnisse bedeutender Evaluationen von Gesichtserkennungssystemen

Ein Ziel dieser Arbeit ist die Untersuchung, inwieweit Verfahren der Gesichtserkennung die Anforderungen an Authentifizierungsverfahren erfüllen. Für biometrische Systeme im Allgemeinen wurde diese Frage bereits in Abschnitt 4 beantwortet. Hier soll nun im Speziellen auf die Gesichtserkennung, insbesondere auf die zu erwartende Erkennungsleistung, eingegangen werden. Auch die Schwächen der Systeme sollen aufgezeigt werden.

Die Algorithmen werden bereits von Ihren Entwicklern, in der Regel Universitäten und

ähnlichen Forschungseinrichtungen, genau analysiert, um deren Fähigkeit zur Unterscheidung von Gesichtern einschätzen zu können. Dabei werden die Verfahren der einzelnen Abschnitte der Template-Erzeugung jeweils getrennt voneinander betrachtet, um einer gegenseitigen Beeinflussung vorzubeugen. Anhand der Ergebnisse können bestimmte Verfahren optimiert oder verbessert werden. Auch ein Vergleich von neu entwickelten Verfahren mit bereits existierenden Verfahren ist möglich.

Damit diese „Labortests“ auch untereinander vergleichbar sind, muss von möglichst gleichen Bedingungen bei verschiedenen Tests ausgegangen werden. Eine Grundvoraussetzung für die Durchführung von Evaluationen und das Erstellen von Benchmarks war daher die Schaffung von Datenbanken mit Bildern von Gesichtern. Auf diese Art konnten weltweit Untersuchungen auf Basis desselben Rohmaterials durchgeführt werden. Für aussagekräftige Ergebnisse mussten die „Face Databases“ möglichst umfangreich sein und solche Daten enthalten, die beim Einsatz in der Praxis auftreten [ZCPR03, S. 40]. Dies sind zum Beispiel Bilder mit unterschiedlicher Kopfhaltung, verschiedenen Gesichtsausdrücken, geänderter Helligkeit und anderen Variationen, so wie in Abschnitt 5.1.1 beschrieben.

Die größte frei verfügbare Datenbank ist die FERET Database¹², die seit 1995 in zahlreichen Testserien verwendet und immer wieder erweitert wurde. In [ZCPR03, S. 64] findet sich eine Übersicht mit zahlreichen weiteren Datenbanken. [Lu03, S. 27] enthält zu einigen Datenbanken die Angabe, welche Variationen bei den Bildern vorliegen.

Neben den Algorithmestests gibt es auch noch vergleichende Untersuchungen von Gesichtserkennungssystemen, bei denen ein Praxiseinsatz simuliert oder tatsächlich durchgeführt wurde. Auf diese Art wird deutlich, wie das Zusammenspiel von verschiedenen Algorithmen funktioniert und ob ein System in der Praxis überhaupt einsetzbar ist. Untersuchungsgegenstand sind in der Regel kommerzielle Systeme verschiedener Hersteller. Nach Meinung des Autors dieser Arbeit sind die Ergebnisse solcher Studien am bedeutendsten für die Beurteilung der Erfüllung von Anforderungen an Authentifizierungssysteme. In diesem Abschnitt werden deshalb zwei vergleichende Untersuchungen der Erkennungsleistung von Gesichtserkennungssystemen vorgestellt und deren Ergebnisse zusammengefasst. Die Evaluationen wurden ausgewählt, da dazu umfangreiche Informationen frei verfügbar sind. Außerdem wird auf eine vor kurzem veröffentlichte Studie eingegangen, die eine Verwendung biometrischer Verifikationssysteme im Zusammenhang mit Personaldokumenten untersuchte. Hieraus werden die Erkenntnisse zur Gesichtserkennung vorgestellt.

5.2.1 Face Recognition Vendor Test 2002

Der Face Recognition Vendor Test (FRVT) 2002 ist Teil einer Reihe von Untersuchungen, die seit 1994 von verschiedenen Institutionen der Vereinigten Staaten durchgeführt werden. 1994, 1995 und 1996 wurden die FERET-Evaluationen¹³ durchgeführt, deren

¹²Face Recognition Technology, <http://www.itl.nist.gov/iad/humanid/feret/> [Inf04]

¹³Face Recognition Technology

Ergebnisse einen Beitrag zur Entwicklung erster Prototypen von Gesichtserkennungssystemen leisteten. Im Jahre 2000 waren zum ersten Mal kommerzielle Systeme Gegenstand der Evaluation, um den Fortschritt bei der Entwicklung der Gesichtserkennung zu beurteilen. FERET wurde deshalb in Face Recognition Vendor Test¹⁴ umbenannt. [DAR]

Erklärtes Ziel des FRVT 2002 war die Bereitstellung von Kennzahlen, die eine Aussage über die Praxistauglichkeit verschiedener automatischer Gesichtserkennungssysteme zulassen [PGM⁺03, S. 2]. Diese Kennzahlen beziehen sich auf die Erkennungsleistung, das heißt die Fähigkeit eines Systems, Gesichter korrekt zu erkennen. Dabei wurden verschiedene Faktoren betrachtet, die einen Einfluss auf die Erkennungsleistung haben. Es wurde versucht, diesen Einfluss zu quantifizieren. Der FRVT stellt eine eher technische Evaluation dar, mit deren Hilfe die zu erwartenden Fehlerraten eingeschätzt werden können. Eine Beurteilung der Benutzerfreundlichkeit oder anderer Eigenschaften erfolgte nicht. [PGM⁺03, S. 13]

FRVT war eine Offline-Untersuchung, das heißt es wurden keine lebenden Personen von einer Kamera erfasst (das entspräche einer Online-Untersuchung) [GMP03, S. 1]. Die Datenbasis bildeten insgesamt 121589 Bilder und Videos von 37437 unterschiedlichen Personen. Gegenstand der Untersuchung waren zehn Gesichtserkennungssysteme verschiedener Hersteller. Die Teilnehmer können einer Tabelle in [PGM⁺03, S. 4]¹⁵ entnommen werden.

Drei Aufgaben eines Gesichtserkennungssystems wurden von den Systemen bearbeitet und die Ergebnisse analysiert. Die erste Aufgabe war die bereits bekannte **Verifikation**. Hier wurden die Kennzahlen False Acceptance Rate und Recognition Rate berechnet [PGM⁺03, S. 6–8]. Dabei ist die Recognition Rate nur eine andere Darstellung der False Rejection Rate:

$$\text{Recognition Rate} = 1 - \text{False Rejection Rate}$$

Die Aufgabe der **Identifikation** ist beim FRVT folgendermaßen definiert: Das Gesichtserkennungssystem hat für jede der 37437 Personen ein Bild gespeichert. Es soll nun für ein beliebiges Bild festgestellt werden, welche der 37437 Personen der Person auf dem Bild am ähnlichsten sind. Der Fall, dass die Person nicht in der Datenbank vorkommt, ist per Definition ausgeschlossen. Die gefundenen Personen werden der Ähnlichkeit nach geordnet, so dass die am ähnlichsten aussehende Person an erster Stelle steht. Eine Person gilt als richtig identifiziert, wenn die wahre Identität mindestens einen bestimmten Rang erreicht. Als „Schwellenwerte“ wurden beispielsweise die Ränge 1, 10 und 50 gewählt. Rang 1 beschreibt den Fall, dass die wahre Identität auch die absolut höchste Ähnlichkeit aufweist. Rang 10 bedeutet, dass sich die wahre Identität noch unter den ersten zehn befindet (analog für Rang 50). [PGM⁺03, S. 8–9]. Als Kennzahl wurde die Identifikationsrate für verschiedene Ränge berechnet.

¹⁴Vendor $\hat{=}$ Anbieter, Lieferant

¹⁵Alternativ auch <http://www.frvt.org/FRVT2002/Participants.asp>

Die dritte Aufgabe wird als **Watch List** bezeichnet und stellt eine Verallgemeinerung von Verifikation und Identifikation dar [GMP03, S. 3]. Eine bestimmte Anzahl an Personen steht unter Beobachtung, das heißt ein Bild dieser Person befindet sich auf der Watch List. Für ein beliebiges Bild muss das Gesichtserkennungssystem feststellen, ob es sich um eine Person auf der Watch List handelt. Falls dies zutrifft, muss die Identität der Person bestimmt werden. Nur wenn eine auf der Watch List vorkommende Person richtig erkannt wird, gilt die Aufgabe als korrekt gelöst. Es werden auch hier zwei Kennzahlen berechnet: Die *Detection and Identification Rate* gibt den Anteil korrekt erkannter, auf der Watch List befindlicher Personen an. Ein falscher Alarm liegt vor, wenn eine Person identifiziert wird, die gar nicht auf der Watch List vorkommt. Die entsprechende Kennzahl ist die False Alarm Rate. [PGM⁺03, S. 9]

Im Folgenden werden die wichtigsten Ergebnisse des FRVT 2002 zusammengefasst. Für weitere Ergebnisse und detaillierte Informationen zu den Analysen sei der Leser auf [PGM⁺03], [GMP03] und [DAR] verwiesen. Die in dieser Zusammenfassung gemachten Angaben beziehen sich jeweils auf die besten Gesichtserkennungssysteme im Test (vgl. [ZCPR03, S. 44–45]).

- Die Erkennungsleistung war bei normal schwankender Helligkeit innerhalb eines Gebäudes annähernd konstant. Bei einer False Acceptance Rate von 1% lag die Erkennungsrate bei 90%.
- Aufnahmen außerhalb von Gebäuden bereiteten schwerwiegende Probleme. Die Erkennungsrate brach deutlich ein auf 50% bei einer False Acceptance Rate von 1%.
- Interessant ist auch der Verlauf der Erkennungsleistung in Abhängigkeit von der Zeit, die zwischen zwei Aufnahmen vergangen ist. Je mehr Zeit zwischen den Aufnahmen vergangen war, desto schlechter war die Erkennungsleistung. Bei den besten Systemen ging die Erkennungsrate um ungefähr 5% pro Jahr zurück.
- Auch der Einfluss verschiedener Datenbankgrößen bei den Aufgaben Identifikation und Watch List wurde untersucht. Dabei konnte festgestellt werden, dass eine höhere Anzahl an Personen und Bildern die Erkennungsleistung negativ beeinflusst.
- Die Erkennungsleistung wurde auch in Abhängigkeit von demographischen Faktoren betrachtet. Dabei stellte sich heraus, dass die Erkennungsrate bei Männern höher lag als bei Frauen. Außerdem waren ältere Menschen einfacher zu erkennen als junge.
- Eine im FRVT 2000 noch nicht untersuchte Technologie war die Berechnung eines dreidimensionalen Modells des Gesichtes aus „normalen“ zweidimensionalen Bildern. Es wurden deutliche Verbesserungen der Erkennungsleistung bei Anwendung dieser Technologie erkannt.

- Ein weitere „neue“ Technologie war die Analyse von Video-Daten. Hierbei konnte keine Verbesserung gegenüber der Erkennungsleistung bei unbewegten Bildern ermittelt werden.

Derzeit wird der FRVT 2005 vorbereitet. Diese Evaluation soll die Entwicklung und den Fortschritt auf dem Gebiet der Gesichtserkennung seit dem FRVT 2002 quantifizieren. Es werden dabei zum ersten Mal auch Systeme getestet, die dreidimensionale Daten verarbeiten, wie sie ein 3D-Scanner erzeugt. Die Durchführung der Evaluation ist für den Zeitraum von September bis Oktober 2005 geplant.

5.2.2 BioFace

BioFace ist ein gemeinschaftliches Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BIS) und des Bundeskriminalamtes (BKA). Die Durchführung erfolgte mit Unterstützung des Fraunhofer Instituts für Graphische Datenverarbeitung. [Bun03, S. 5]

Das Projekt ist aufgeteilt in die Abschnitte BioFace I und BioFace II. Das erste Teilprojekt befasste sich mit der Sammlung von Bildern aus verschiedenen Quellen. Die Bilder wurden auf ihre Nutzbarkeit hin kontrolliert und nach bestimmten Störungen klassifiziert. Zugelassen wurden dabei nur Aufnahmen, die bildfüllend eine Frontalaufnahme des Gesichtes zeigten. Profilaufnahmen und Bilder, die andere Körperteile als den Kopf enthielten, wurden aussortiert. Die Klassifikation erfolgte nach Störungen, die entweder durch die Person selbst (z. B. Mimik, Verdeckung des Gesichtes) oder die Aufnahmebedingungen (z. B. unzureichende Helligkeit, abweichende Aufnahmeperspektive, Unschärfe) begründet waren. [Bun03, S. 12–14]

Die im Rahmen von BioFace I gesammelten Daten dienten bei BioFace II zur Durchführung von zwei vergleichenden Untersuchungen der Erkennungsleistung von Gesichtserkennungssystemen. Dabei sollte der Einfluss von Störfaktoren sowie die Leistungsfähigkeit in Abhängigkeit von der Größe des Datenbestandes evaluiert werden [Bun03, S. 5]. Die erste Untersuchung war ein Algorithmentest, bei dem drei Algorithmen in den Modi Verifikation und Identifikation geprüft wurden. Der zweite Teil von BioFace II war ein Systemtest, bei dem vier unterschiedliche Gesichtserkennungssysteme im Eingangsbereich des Gebäudes des Bundeskriminalamtes in Wiesbaden installiert wurden. In einer ersten Testphase (Phase I) wurden die Referenzbilder direkt von den Kameras im Eingangsbereich erfasst. In Phase II wurden die Referenzbilder aus Phase I ersetzt durch Bilder, die mittels einer Digitalkamera aufgenommen wurden.

Im Folgenden werden die Ergebnisse von BioFace II vorgestellt, wie sie in [Bun03, S. 7–9] zusammengefasst sind.

Wie zu erwarten war, zeigte sich beim Algorithmentest im Modus der Verifikation kein nennenswerter Einfluss der Datenbankgröße auf die Erkennungsleistung. Außerdem wurden keine schwerwiegenden Probleme in den Fällen festgestellt, bei denen zwischen Aufnahmezeitpunkt des Referenzbildes und Aufnahmezeitpunkt des Vergleichsbildes mehrere Jahre Unterschied bestanden. Die von den Algorithmen berechneten Ähnlichkeitswerte

zeigten jedoch eine starke Überlagerung von Matches und Non-Matches. Dies bedeutet, dass ein Vergleich von zwei Bildern unterschiedlicher Gesichter in vielen Fällen so hohe Ähnlichkeitswerte erreichte, wie der Vergleich von zwei Bildern desselben Gesichtes. Die Algorithmen sind demnach nicht in der Lage, ein zuverlässiges Ergebnis eines Vergleiches zu liefern. Es wird in diesem Zusammenhang jedoch darauf verwiesen, dass Qualität der Referenzbilder einen sehr großen Einfluss auf die Erkennungsleistung hat. Daraus lässt sich ableiten, dass die Erfassung der Referenzbilder mit möglichst hoher Sorgfalt erfolgen sollte, da nur so geringe Fehlerraten zu erreichen sind.

Im Modus der Identifikation zeigte sich eine deutliche Abhängigkeit der Erkennungsleistung von der Datenbankgröße. Mit wachsender Größe der Referenzdatenbank erreichten die Non-Matches immer bessere Ähnlichkeitswerte, wodurch eine korrekte Identifikation immer schwieriger wurde. Wie bereits bei der Verifikation, war auch bei der Identifikation eine Überlagerung von Matches und Non-Matches feststellbar. Für einen praktischen Einsatz zur Identifikation scheinen die Algorithmen ungeeignet.

Am Systemtest nahmen 20 Personen teil. Insgesamt enthielt die Referenzdatenbank je ein Bild der 20 Personen und zusätzlich 500 Bilder anderer Personen. Jedes der vier teilnehmenden Systeme erfasste die Bilder über eine eigene Kamera, in die die Personen direkt schauen sollten. Da alle Personen sich beim Zutritt an einem Zeiterfassungssystem anmeldeten, konnte festgestellt werden, wie oft die 20 Testpersonen tatsächlich die Zutrittskontrolle passiert hatten. Für jeden Zutritt einer Testperson wurde festgestellt, ob das Gesichtserkennungssystem die Identifikation korrekt durchgeführt hatte. Dabei erkannte selbst das beste System im Test nicht einmal die Hälfte der Testpersonen richtig. Das schlechteste System kam auf eine False Rejection Rate von 99,7% und erkannte damit fast keine der Testpersonen.

Die Angaben der False Rejection Rate sind jedoch wenig aussagekräftig. In der Dokumentation zum Systemtest wird an keiner Stelle erwähnt, wie der Schwellenwert ermittelt wurde oder welche False Acceptance Rate zu erwarten ist. Ob der Systemtest als Grundlage wissenschaftlicher Arbeit dienen kann, darf bezweifelt werden. Ein Vergleich und eine Bewertung der vier Systeme, wie in [Bun03, S. 127], ist ohne Angaben zur False Acceptance Rate nicht zu gebrauchen. Außerdem sind 20 Testpersonen nicht ausreichend, um statistisch belastbare Ergebnisse zu liefern. Darauf wird in [Bun03, S. 9] jedoch hingewiesen.

Einige Erkenntnisse kann der Systemtest trotzdem bieten: Die Erkennungsleistung war bei allen Systemen besser, wenn die Referenzbilder mit der Kamera aufgenommen wurden, die auch die Bilder beim Zutritt erfasste. Die Veränderung der Umgebung und die unterschiedlichen optischen Eigenschaften der Kamera werden als Ursachen dafür genannt, dass in Phase II (Referenzbilder mit Digitalkamera erfasst) die Erkennungsleistung abnahm [Bun03, S. 8]. Die teilweise sehr schlechte Verfügbarkeit der Systeme und der unzureichende Support durch einige Hersteller werden in der Studie ebenfalls bemängelt [Bun03, S. 9], genauere Angaben fehlen.

BioFace II lässt erkennen, dass die getesteten Algorithmen und Systeme vor dem Einsatz in der Praxis noch umfangreicher Verbesserungen bedürfen. Es konnten nicht alle

gesetzten Ziele des Projektes erreicht werden: Die Messung des Einflusses einiger Störfaktoren (z. B. Mimik, Helligkeit, Kopfdotation) wurde nicht durchgeführt, da geeignetes Bildmaterial fehlte. Diese Untersuchung war Inhalt des Projektes BioFace III, dessen Ergebnisse bisher nicht veröffentlicht sind.

5.2.3 BioP I und II

Die Studie BioP I untersuchte die Leistungsfähigkeit kommerzieller Gesichtserkennungssysteme in Bezug auf deren Einsatz bei biometrischen Ausweisdokumenten [Bun04c, S. 5]. Der „Testsieger“, ein Komplettsystem des Unternehmens Cognitec Systems GmbH, wurde in der Studie BioP II weitergehend analysiert und mit anderen biometrischen Authentifizierungssystemen verglichen. Dabei nutzten drei der Systeme die Fingerabdruckerkennung und eines die Iriserkennung. Bei biometrischen Ausweisdokumenten ist nur die Leistung bei der Verifikation relevant, weshalb die Leistung bei der Identifikation nicht geprüft wurde. Die Abschlussberichte von BioP I [Bun04c] und BioP II [Bun04b] sind sehr ausführlich und die Ergebnisse der Untersuchungen gut nachvollziehbar. Im Folgenden werden kurz die Testbedingungen des Projekt BioP II erläutert und die Erkenntnisse zum Gesichtserkennungssystem zusammengefasst.

Eingesetzt wurde das Gesichtserkennungssystem am Flughafen Frankfurt am Main. Insgesamt nahmen 2000 freiwillige Testpersonen an der zweimonatigen Untersuchung teil. Die Testteilnehmer waren Mitarbeiter der Fraport AG, der Lufthansa AG und des Bundesgrenzschutzes [Bun04b, S. 10]. Sie wurden aufgefordert, täglich mindestens zweimal einen der Teststandorte aufzusuchen und Authentifizierungsvorgänge an verschiedenen Systemen durchzuführen. Der Ausgang des Authentifizierungsvorganges wurde den Testpersonen mitgeteilt, hatte aber sonst keine Auswirkungen (also keine Kopplung an eine Zutrittskontrolle oder ähnliches) [Bun04b, S. 11].

Die Erfassung des Referenzbildes erfolgte mit einer Digital-Spiegelreflexkamera nach den Richtlinien der ICAO (International Civil Aviation Organisation) [Bun04b, S. 26–30]. Zudem wurde ein Template direkt durch das Gesichtserkennungssystem erzeugt (herstellerspezifisches Enrollment) [Bun04b, S. 73–75].

Neben der Ermittlung der Fehlerraten zur Beurteilung der Erkennungsleistung wurden noch weitergehende Untersuchungen durchgeführt, zum Beispiel Befragungen zu Benutzbarkeit und Akzeptanz. Auch die Überwindungssicherheit wurde getestet, jedoch sind im Abschlussbericht zu BioP II keine detaillierten Informationen dazu enthalten. Bei der nun folgenden Zusammenfassung der Ergebnisse gilt es zu beachten, dass nur ein bestimmtes System getestet wurde. Diese Aussagen treffen daher nicht zwingend auch für alle anderen Gesichtserkennungssysteme zu.

- Es besteht ein eindeutiger Zusammenhang zwischen False Rejection Rate und Nutzungshäufigkeit. So genannte „Vielnutzer“ wurden deutlich weniger häufig zurückgewiesen als Personen, die das System weniger nutzten. [Bun04b, S. 162–163]

- Ein Training der Testpersonen war kaum erforderlich [Bun04b, S. 168]. Trotzdem ist beim Gesichtserkennungssystem eine Verbesserung der Benutzerführung und des Feedbacks empfehlenswert, da viele Benutzer damit unzufrieden waren [Bun04b, S. 140].
- Die Lichtverhältnisse der Umgebung haben einen großen Einfluss auf die Erkennungsraten. Eine homogene Ausleuchtung des Gesichtes muss gewährleistet sein. [Bun04b, S. 167]
- Bei hohen Sicherheitsanforderungen ist das Gesichtserkennungssystem nicht geeignet [Bun04b, S. 168]. Bei einer False Acceptance Rate von 0,001% lag die False Rejection Rate zwischen 15% und 50%. Eine FAR von 1% erlaubte eine FRR zwischen 1% und 7%. [Bun04b, S. 164]
- Mit den herstellereigenen Templates wurden bessere Ergebnisse erzielt, als mit den nach ICAO-Richtlinien erstellten Fotos. [Bun04b, S. 165]
- Alle Personen konnten das Gesichtserkennungssystem nutzen. Die Failure to Enroll Rate betrug 0%. [Bun04b, S. 94]
- Zur Überwindungssicherheit liegt nur eine Bewertung auf einer Notenskala von 1 bis 6 vor, Details dazu fehlen. Das Gesichtserkennungssystem erreichte die Note 4. Dies bedeutet, dass eine Überwindung mit mittlerem Aufwand erfolgreich war. [Bun04b, S. 158–161]

5.2.4 Zusammenfassung

Die vorgestellten Studien hatten jeweils eigene Zielsetzungen. Sie unterschieden sich deutlich in der Art der Durchführung der Untersuchungen, vom reinen Labortest bis hin zum praxisnahen Anwendungsszenario. Eine Zusammenfassung der verschiedenen Studien zu einem „Gesamtergebnis“ ist daher schwierig. Die Berechnung von „globalen Kennzahlen“ aus den einzelnen Kennzahlen der Studien würde keine wissenschaftlich belastbaren Ergebnisse liefern. Lediglich einige allgemeine Aussagen sollen an dieser Stelle genannt werden.

Die Authentifizierung durch Gesichtserkennung eignet sich für Anwendungen, die nur geringe Ansprüche an die Sicherheit stellen. Sind die Sicherheitsansprüche höher, so wäre der Einsatz eines Gesichtserkennungssystems mit einer hohen False Rejection Rate verbunden.

Bei der Verwendung von Gesichtserkennung zur Verifikation ist eine geringere Fehlerrate zu erwarten als bei der Nutzung zur Identifikation. Mit steigender Anzahl an Nutzern nimmt die Fehlerrate bei der Identifikation zu.

Die Untersuchungen in praxisnahen Anwendungsszenarien haben gezeigt, dass die Bedienbarkeit kein großes Problem darstellt.

6 Prototypische Implementierung einer Gesichtserkennung

Zu Demonstrationszwecken wurde im Rahmen dieser Arbeit der Prototyp eines Gesichtserkennungssystems implementiert. In diesem Abschnitt soll gezeigt werden, welches Verfahren verwendet wurde und warum sich der Autor dieser Arbeit für dieses Verfahren entschieden hat. Es wird kurz auf die Entwicklung des Programmes eingegangen, eine Dokumentation des Quelltextes erfolgt hier nicht. Details sind den Kommentaren im Quelltext zu entnehmen. Die beim Prototyp verfügbaren Funktionen und Konfigurationsmöglichkeiten werden vorgestellt. Für ein Szenario, das in der Testphase des Programms zu Versuchszwecken aufgebaut wurde, werden die einzelnen Arbeitsschritte dokumentiert. Nach dieser Anleitung kann das Gesichtserkennungssystem auch zu Demonstrationszwecken eingesetzt werden. Zum Abschluss werden noch mögliche Erweiterungen des Funktionsumfangs des Prototyps genannt, die eventuell in einer weiteren Diplomarbeit umgesetzt werden könnten.

6.1 Das Verfahren der Eigenfaces

Das Verfahren der Eigenfaces ist ein holistischer Ansatz, basierend auf der Hauptkomponentenanalyse (Principal Component Analysis, PCA). Die informationstheoretischen Grundlagen des Algorithmus und die Möglichkeit, das Verfahren zur Gesichtserkennung einzusetzen, wurden von Turk und Pentland bereits 1991 im Artikel „Eigenfaces for Recognition“ [TP91] vorgestellt. Darin wird auch erläutert, welche mathematischen Methoden bei den einzelnen Schritten des Algorithmus angewandt werden. Im Rahmen dieser Arbeit wird nicht näher auf diese Details eingegangen. Es folgt ein Überblick, der in kompakter Form zeigen soll, wie die Gesichtserkennung beim Verfahren Eigenfaces abläuft und welche Konsequenzen sich daraus für die Implementierung des Prototyps ergaben.

1. Training: Erzeugen der Eigenfaces

Aus einer Menge an Bildern, dem sogenannten „training set“, werden Komponenten berechnet, die zur Beschreibung dieser Bilder dienen können. Da die Trainingsdaten nur Bilder von Gesichtern enthalten, kann mit Hilfe der Komponenten jedes beliebige Gesicht beschrieben werden. Da es sich aus mathematischer Sicht um Eigenvektoren einer Matrix handelt und die Darstellung eines solchen Vektors als Bild einem Gesicht ähnlich sieht, wird die Bezeichnung Eigenfaces für die Vektoren verwendet.

Mit mathematischen Verfahren lassen sich die Hauptkomponenten bestimmen, die Gesichter am besten beschreiben. Dazu werden die Eigenwerte der Komponenten berechnet und diejenigen Komponenten mit den höchsten Eigenwerten ausgewählt. Je mehr Hauptkomponenten gewählt werden, desto genauer kann ein Gesicht beschrieben werden. Allerdings steigt dadurch auch der Rechenaufwand bei jeder

einzelnen Template-Erzeugung. Turk und Pentland geben an, dass etwa 40 Hauptkomponenten für die genaue Beschreibung eines Gesichtes ausreichen. Bei der Verwendung des Eigenface-Verfahrens zur Gesichtserkennung kann auch eine geringere Zahl gewählt werden [TP91, S. 75].

2. Templates der bekannten Benutzer berechnen

Die Eigenfaces sind linear unabhängige Vektoren, die einen Gesichtsraum, den sogenannten „face space“, bilden. Wurden die M Hauptkomponenten mit den höchsten Eigenwerten gewählt, so hat der Gesichtsraum M Dimensionen. Bilder lassen sich in diesen Gesichtsraum projizieren. Das Ergebnis der Projektion ist ein Vektor der Länge M , der das Bild als Gewichte der Eigenvektoren beschreibt.

Das Gesicht eines jeden bekannten Benutzers wird in den Gesichtsraum abgebildet. Die berechneten Vektoren werden als Template gespeichert.

3. Gesichter erkennen

Zur Gesichtserkennung wird das Bild eines unbekanntes Gesichtes in den Gesichtsraum projiziert. Man erhält auf diese Weise das Anfragetemplate. Ähnliche Gesichter werden durch ähnliche Vektoren beschrieben. Den Unterschied zwischen Vektoren kann man sehr einfach berechnen, zum Beispiel mittels der Euklidischen Distanz. Dieses Verfahren wird auch von Turk und Pentland vorgeschlagen [TP91, S. 76]. Für alle Referenztemplates wird die Distanz zum Anfragetemplate berechnet. Je niedriger diese Distanz ausfällt, desto ähnlicher sind die Gesichter. Es kann ein Schwellenwert definiert werden, bei dessen Unterschreitung ein Gesicht als erkannt gilt.

Aus informationstheoretischer Sicht kann man das Verfahren in einem Satz zusammenfassen: „[...] extract the relevant information in a face image, encode it as efficiently as possible, and compare one face encoding with a database of models encoded similarly.“ [TP91, S. 73]

Bei der Implementierung des Prototyps galt es, diese dreistufige Gliederung des Algorithmus so umzusetzen, dass der Benutzer des Prototyps zur Einhaltung der korrekten Reihenfolge gezwungen wird. Nach dem Start des Programms ist zuerst der Gesichtsraum aus einer Menge an Trainingsbildern zu bestimmen. Erst wenn dieser Vorgang abgeschlossen ist, können die Templates der bekannten Benutzer berechnet werden. Bei einer Änderung des Gesichtsraumes zu einem späteren Zeitpunkt (z. B. geänderte Anzahl an Eigenvektoren) müssen die Referenztemplates neu berechnet werden. Nachdem der Gesichtsraum berechnet ist und mindestens ein Referenztemplate erfasst wurde, kann die eigentliche Gesichtserkennung beginnen.

Die Bilder werden als Vektoren dargestellt, wobei die Auflösung des Bildes die Länge des Vektors bestimmt. Eine Änderung der Auflösung führt zu anderen Eigenvektoren und beeinflusst damit den gesamten Prozess der Gesichtserkennung. Daher muss die Auflösung bereits vor der Berechnung des Gesichtsraumes festgelegt werden. Wird sie später geändert, müssen Gesichtsraum und Referenztemplates neu berechnet werden.

Das Verfahren der Eigenfaces wurde gewählt, weil die einzelnen Schritte des Algorithmus gut dokumentiert sind und sich einfach nachvollziehen lassen. Der Quellcode einiger Eigenface-Gesichtserkennungssysteme ist frei verfügbar, so dass sich die Implementierung des Prototyps daran orientieren konnte. Das Verfahren der Eigenfaces eignet sich außerdem, um eine Gesichtsentdeckung durchzuführen [TP91, S. 76–79].

6.2 Entwicklung des Prototyps

Bevor mit der Entwicklung des Prototyps begonnen wurde, erfolgte eine Erhebung von Anforderungen und Zielen, die der Prototyp erfüllen sollte. Dafür wurde zunächst ein Einsatzszenario entwickelt, aus dem die Anforderungen an den Prototyp und damit an die Entwicklungsumgebung abgeleitet wurden.

6.2.1 Einsatzszenario

Der Prototyp kommt bei Präsentationen zum Einsatz, um die grundlegenden Funktionen eines Gesichtserkennungssystems zu demonstrieren. Dies umfasst die Speicherung von Referenztemplates bekannter Personen sowie den Vergleich beliebiger anderer Bilder mit diesen Referenztemplates. Außerdem soll es möglich sein, einfache Labortests durchzuführen.

Der Prototyp soll Bilder verarbeiten können, die von einer Webcam aufgenommen werden. Das erfasste Bild und die Ergebnisse des Template-Vergleichs sind übersichtlich darzustellen. Die Konfiguration und Initialisierung des Systems soll möglichst intuitiv durchzuführen sein.

Neben den Bildern einer Webcam sollen auch andere Bilder ausgewertet werden können, die der Benutzer auf lokalen Laufwerken gespeichert hat. Dies ist besonders dann von Bedeutung, wenn die Bedingungen der Präsentation die Nutzung einer Webcam nicht zulassen.

Die verwendeten Bilder können unter kontrollierten Aufnahmebedingungen erfasst und bei Bedarf nach Qualität sortiert werden. Es wird davon ausgegangen, dass ein Bild größtenteils vom Gesicht ausgefüllt wird. Die Implementierung einer Gesichtsentdeckung scheint daher nicht erforderlich.

Zur Beurteilung der Erkennungsleistung muss eine große Anzahl an Vergleichen durchgeführt werden. Für die Auswertung werden die Ergebnisse der Vergleiche in eine Anwendung zur Tabellenkalkulation importiert.

6.2.2 Anforderungen an den Prototyp

Aus dem Einsatzszenario lassen sich einige Anforderungen an den Prototyp ableiten. Zunächst ist festzustellen, dass es sich um eine Anwendung mit graphischer Benutzeroberfläche handelt. Diese Benutzeroberfläche muss übersichtlich und ansprechend gestaltet

werden, so dass bei einer Präsentation des Prototyps die dargestellten Informationen leicht verständlich sind. Das aktuell geprüfte Bild soll angezeigt werden. Zur Verarbeitung von Bildern müssen passende Schnittstellen vorhanden sein. Die Bilder der zur Verfügung stehenden Webcam können in den Grafikformaten JPEG und BMP abgespeichert werden. Der Prototyp sollte mindestens diese beiden Grafikformate verstehen. Außerdem müssen verschiedene Berechnungen mit Matrizen durchgeführt werden. Die Implementierung der Rechenoperationen an Matrizen sollte möglichst wenig Rechenleistung in Anspruch nehmen, da mit relativ großen Matrizen (> 100000 Zeilen) gerechnet werden muss.

6.2.3 Implementierung

Der Prototyp wurde in der Programmiersprache C++ mit der Klassenbibliothek Qt (Version 3.3.4) implementiert. Qt ist für Linux, Mac OS, Windows und andere Betriebssysteme verfügbar. Es enthält eine Vielzahl von Klassen, die zur Erstellung von Anwendungen mit graphischer Benutzeroberfläche nützlich sind. Beispielsweise existieren Qt-Klassen, mit denen Grafiken geöffnet und in der Anwendung dargestellt werden können. Für mehr Informationen über Qt sei auf die Homepage des Herstellers Trolltech verwiesen (<http://www.trolltech.com/products/qt/>).

Für die Entwicklung von Software, die gemäß der GNU General Public License¹⁶ als freie Software veröffentlicht wird, kann Qt im Rahmen der sogenannten „Open Source Edition“ kostenlos verwendet werden. Bei Qt 3 beschränkte sich dies jedoch auf die Linux-Version, weshalb die Entwicklung auf Basis dieses Betriebssystems erfolgte. Auf dem Entwicklungsrechner wurde dazu Suse Linux in der Version 9.3 installiert. Seit der Veröffentlichung der Qt-Version 4 gibt es die Bibliothek auch für Windows und Mac OS in der Open Source Edition. Version 4 war jedoch erst nach Abschluss der Implementierung des Prototyps verfügbar.

Zur Berechnung der Eigenvektoren war eine zusätzliche Bibliothek notwendig. Es wurden hier Teile des frei verfügbaren „CSU Face Identification Evaluation System“¹⁷ der Colorado State University genutzt.

Die eingesetzte Webcam, das Modell TerraCAM USB (Version 2) des Herstellers Teratec, ist unter Linux leider nicht verwendbar, da dafür keine Treiber existieren. Das Problem kann jedoch umgangen werden, indem die Kamera an einen Rechner mit dem Betriebssystem Windows angeschlossen wird. Über eine Netzwerkverbindung können die von der Kamera erfassten Bilder dann auf den Linux-Rechner übertragen werden. In Abschnitt 6.3.4 wird diese Konfiguration detailliert dargestellt.

¹⁶Online unter <http://www.gnu.org/copyleft/gpl.html>, letzter Zugriff am 31.08.2005

¹⁷Online unter <http://www.cs.colostate.edu/evalfacerec/>, letzter Zugriff am 31.08.2005

6.3 Übersicht der Funktionen

Analog zu der dreiteiligen Gliederung des Eigenface-Verfahrens, die in Abschnitt 6.1 beschrieben wurde, ist auch der Prototyp in drei Funktionsbereiche gegliedert. Die Funktionen werden in diesem Abschnitt vorgestellt. Für jeden der Funktionsbereiche ist ein Screenshot im Anhang dieser Arbeit abgebildet.

6.3.1 Initialisierung des Gesichtsraumes

Zur Berechnung der Eigenvektoren sind Trainingsbilder erforderlich. Diese können sich in einem beliebigen Verzeichnis befinden. Das Verzeichnis wird mittels eines Dialogfensters ausgewählt oder kann direkt eingegeben werden. Als Vorgabewert ist das Home-Verzeichnis des aktuellen Benutzers eingestellt. Es werden alle Dateien als Trainingsbilder verwendet, die sich im Trainingsverzeichnis befinden und die das Programm als Grafikdateien erkennt (u. a. JPEG, BMP, PNG). Dateien in Unterverzeichnissen bleiben unberücksichtigt.

Sämtliche Bilddateien werden auf eine einheitliche Größe skaliert. Diese muss vor der Initialisierung des Gesichtsraumes festgelegt werden. Der Benutzer kann die gewünschte Auflösung frei wählen, indem er die Höhe und die Breite des Bildes in Pixel angibt. Dabei sollte darauf geachtet werden, dass das Verhältnis von Höhe und Breite auch dem der verwendeten Bilder entspricht, da es ansonsten zu Verzerrungen kommt.

Vor der Initialisierung kann auch noch eine maximale Zahl an Eigenvektoren vorgegeben werden. Sind mehr Bilder im Verzeichnis der Trainingsdaten enthalten, so wird die Zahl der Eigenvektoren durch diese maximale Anzahl begrenzt. Sind weniger Bilder im Verzeichnis vorhanden, so wird die Zahl der Eigenvektoren, durch die Zahl der Bilder beschränkt.

Die Initialisierung des Gesichtsraumes ist sehr rechenintensiv. Die Dauer der Initialisierung ist abhängig von der Anzahl der Bilder im Verzeichnis, der gewählten Auflösung und der verfügbaren Rechenleistung. Nähere Angaben folgen in Abschnitt 6.4.

Die graphische Benutzeroberfläche für die Initialisierung des Gesichtsraumes ist in Abbildung 5 auf Seite 77 dargestellt.

6.3.2 Erzeugen der Referenztemplates bekannter Benutzer

Wenn die Initialisierung des Gesichtsraumes abgeschlossen ist, kann mit dem Aufbau einer Liste bekannter Personen begonnen werden. Das Anlegen und Löschen von Personen sowie das Hinzufügen und Löschen von Bildern gestaltet sich sehr einfach (Abbildung 6 auf Seite 78). Das Löschen von Bildern entfernt diese nur aus der Liste, die Bilddateien bleiben dabei erhalten.

Zu einer Person können auch mehrere Bilder gespeichert werden. Die Berechnung des Referenztemplates erfolgt dann unter Verwendung eines „mittleren Bildes“.

Die Liste der Personen und der zugeordneten Bilder kann in einer XML-Datei abgespeichert werden. Dies ist insbesondere dann hilfreich, wenn umfangreiche Listen angelegt werden. Werden die Listen nicht gespeichert, so gehen sie bei der Beendigung des Programms verloren. Die Bilddateien werden nicht direkt in die XML-Datei kopiert, sondern lediglich die Adresse (Pfad und Dateiname) dazu gespeichert. Beim Laden der XML-Datei wird geprüft, ob auch alle Bilder geöffnet werden können. Falls eines oder mehrere Bilder nicht an den angegebenen Stellen zu finden sind, wird eine entsprechende Warnmeldung ausgegeben.

Die Referenztemplates werden erst berechnet, wenn der Button „Initialize“ gedrückt wird. Danach ist das System bereit für die Durchführung der Gesichtserkennung. Werden neue Personen oder Bilder hinzugefügt oder vorhandene aus der Liste entfernt, so müssen die Referenztemplates neu berechnet werden.

6.3.3 Die Ausführungsmodi der Gesichtserkennung

Die Gesichtserkennung kann auf drei verschiedene Arten durchgeführt werden. Dabei wird bei allen Modi die Euklidische Distanz des Anfragetemplates zu allen Referenztemplates berechnet. Je niedriger der Wert ist, desto größer ist die Ähnlichkeit. Wie hoch die absoluten Werte ausfallen, ist abhängig von mehreren Faktoren, die in Abschnitt 6.4 ermittelt werden. Abbildung 7 auf Seite 79 zeigt, wie die Benutzeroberfläche zur Konfigurationen der drei Verfahren gestaltet wurde. Die optionale Auswahl einer Rotation des untersuchten Bildes ist vor allem beim Einsatz von Webcams hilfreich (siehe dazu Abschnitt 6.3.4).

Im Modus der „Einfachen Erkennung“ wird der Vergleich mit einer Bilddatei durchgeführt, die über einen Auswahldialog bestimmt wird („File to use for face recognition“). Die Erkennung lässt sich nur starten, wenn die gewählte Datei existiert und auch ein Bild enthält. Andernfalls ist der Button „Check File Once“ deaktiviert. Auf der linken Seite der Benutzeroberfläche wird oben das untersuchte Bild angezeigt. Darunter stehen in einer Tabelle die Namen aller bekannten Personen und zu jeder Person der berechnete Distanzwert. Abbildung 8 auf Seite 80 zeigt die gesamte Benutzeroberfläche des Prototyps; links unten ist die Tabelle mit den Distanzwerten zu erkennen.

Der zweite Modus ist die Gesichtserkennung in bestimmten Zeitintervallen. Auf diese Weise lassen sich Bilder, die von einer Webcam als Dateien abgespeichert werden, in regelmäßigen Abständen überprüfen. Dazu wird die Datei verwendet, die über den Auswahldialog der „einfachen Erkennung“ bestimmt wurde. Sobald eine gültige Bilddatei ausgewählt ist, kann der Timer gestartet werden. Als Zeitintervall lässt sich ein Wert von 200 Millisekunden bis 5 Sekunden einstellen. Änderungen des Intervalls bei laufendem Timer wirken sich sofort aus; der Timer braucht nicht neu gestartet werden. Die Gesichtserkennung wird einmal pro Zeitintervall durchgeführt, unter der Voraussetzung, dass die Bilddatei in der Zwischenzeit geändert wurde. Dies wird über den Zeitstempel der Datei geprüft. Wurde die Datei vor dem Start des Prototyps zum letzten Mal geändert, so erfolgt keine Gesichtserkennung. Das aktuell geprüfte Bild und die berechneten

Distanzen werden, wie auch im ersten Modus, in einer Tabelle auf der linken Seite der Benutzeroberfläche angezeigt.

Der dritte Modus wurde implementiert, um den Prototyp ausgiebig testen zu können. Dazu kann ein Verzeichnis angegeben werden, das Bilder für den Testdurchlauf enthält. Mit dem Button „**Start directory recognition**“ wird der Erkennungsvorgang gestartet. Es werden alle Bilder im angegebenen Verzeichnis zur Erkennung herangezogen und, wie auch in den anderen Modi, die Distanzen zu allen Referenztemplates berechnet. Allerdings erfolgt die Ausgabe der Distanzen nicht über die Benutzeroberfläche. Stattdessen wird die Datei `result.html` im gewählten Verzeichnis erzeugt und darin eine Tabelle mit den Distanzen gespeichert. Zusätzlich sind das Verzeichnis, Datum und Uhrzeit des Testdurchlaufes und die Anzahl gefundener Bilder angegeben. Unter der Tabelle ist angegeben, wie lange das Erkennen und Vergleichen aller Bilder gedauert hat. Die Tabelle lässt sich mit einem beliebigen Webbrowser betrachten und kann zur weiteren Analyse in Anwendungen zur Tabellenkalkulation importiert werden¹⁸.

6.3.4 Konfiguration des Prototyps zur Nutzung von Webcam-Bildern

Wie bereits erwähnt, lässt sich die verwendete Webcam nicht unter Linux nutzen. Der Prototyp wurde jedoch nur für dieses Betriebssystem kompiliert, da zum Zeitpunkt der Programmentwicklung nur die Linux-Variante von Qt 3 in der Open Source Edition verfügbar war. Es soll im Folgenden eine Möglichkeit zur Umgehung des Problems vorgestellt werden, die auch bei der Programmierung und den anschließenden Tests des Prototyps genutzt wurde.

Zunächst wird für die Installation und den Anschluss der Kamera ein Rechner mit Microsoft Windows Betriebssystem benötigt. Darauf wird der Windows-Treiber installiert. Ein Treiber für Mac OS ist nach Angaben des Herstellers¹⁹ für die verwendete Kamera-version („mit Snap-Shot Button“) leider nicht verfügbar.

Für die Erfassung der Bilder wird das Freeware-Programm Pryme²⁰ eingesetzt. Dieses Tool bietet eine Vielzahl von Konfigurationsmöglichkeiten und Betriebsmodi. Die erfassten Bilder können in den Formaten JPEG und BMP gespeichert werden, wobei die Kompression bei JPEG einstellbar ist. Für die Dateinamen der gespeicherten Bilder kann ein beliebiger, konstanter Name gewählt werden, ein beliebiger Name mit laufender Nummer oder ein Dateiname bestehend aus Datum und Uhrzeit der Aufnahme. Die Dateien können auf einem lokalen Laufwerk, einem Netzwerklaufwerk oder, über das File Transfer Protocol (FTP), auf einem entfernten Rechner gespeichert werden. Eine Aufnahme kann manuell getätigt werden oder automatisch im Modus „Auto Capturing“. Dafür wird entweder ein bestimmtes Zeitintervall (mindestens eine Sekunde) angegeben oder die „Motion Detection“, eine detailliert konfigurierbare Bewegungserkennung, genutzt.

¹⁸Getestet wurde der Import in Microsoft Excel, OpenOffice.org und KSpread.

¹⁹Online unter <http://supportde.terratec.net/>, letzter Zugriff am 31.08.2005

²⁰Online unter <http://www.hilo.dk/pryme.php>, letzter Zugriff am 31.08.2005

Das Zusammenspiel von Pryme zum Erfassen der Bilder auf dem Windows-Rechner und dem Prototyp zur Gesichtserkennung auf dem Linux-Rechner verlief ohne Probleme. Die im Intervall von einer Sekunde erfassten Bilder wurden im Format JPEG mit konstantem Dateinamen per FTP auf den Linux-Rechner kopiert. Der Prototyp war so konfiguriert, dass einmal pro Sekunde diese Datei überprüft und zur Gesichtserkennung verwendet wurde (zweiter Modus).

Beim Einsatz in einem IT-System mit erhöhtem Schutzbedarf sollte beachtet werden, dass beim File Transfer Protocol alle Daten, also auch Benutzername und Passwort, unverschlüsselt übertragen werden. Deshalb wurde auch eine Übertragung mit dem SMB-Protokoll (Samba) getestet, bei dem immerhin das Passwort verschlüsselt übertragen wird. Auch auf diese Art funktionierte die Kombination von Pryme und Prototyp problemlos.

Sicherlich gibt es noch weitere Möglichkeiten, wie die Daten von der Webcam auf den Linux-Rechner übertragen werden können. Die bequemste Alternative wäre die Verwendung einer anderen Kamera, die auch unter Linux genutzt werden kann. Dadurch wäre zudem *ein* Rechner ausreichend, was bei Präsentationen durchaus von Vorteil sein wird.

6.4 Test des Prototyps

Nach dem Abschluss der Programmierung wurde der Prototyp einem Test unterzogen, bei dem mit verschiedenen Konfigurationen immer dieselben Gesichter untersucht wurden. Dies sollte zeigen, welchen Einfluss die Bildgröße und die Anzahl verwendeter Eigenvektoren auf die Erkennungsleistung haben. Zudem sollte geklärt werden, wie sich die absolute Höhe der Distanzwerte in Abhängigkeit von diesen Einstellungen verändert.

6.4.1 Vorbereitung des Bildmaterials

Für den Einsatz des Prototyps bei einer Präsentation muss dieser Bilder verarbeiten, die von einer Webcam aufgezeichnet werden. Der Test des Prototyps wurde auf dieses Szenario ausgelegt. Es wurden daher keine Bilder aus einer Gesichts-Datenbank genutzt, sondern selbst angefertigte Fotos. Diese wurden mit der zur Verfügung stehenden Webcam (TerraCAM USB) im Labor des Lehrstuhls für IT-Sicherheit aufgenommen. Die Helligkeit in diesem Raum war gut kontrollierbar. Außerdem konnten die Bilder dort vor einem gleichmäßigen, weißen Hintergrund erfasst werden. Es waren Rechner mit den Betriebssystemen Windows und Linux verfügbar, so dass sowohl der Prototyp als auch die Webcam genutzt werden konnten.

Insgesamt wurden Bilder von 20 Personen gemacht, wobei jede Person mindestens sieben Mal fotografiert wurde. Die Personen wurden aufgefordert, in die Kamera zu blicken und dabei den Kopf nach links und rechts zu bewegen. Brillenträger wurden mit und ohne Brille erfasst. Von drei Personen gibt es Fotos, die an verschiedenen Tagen aufgenommen wurden. Bei diesen Fotos sind teilweise deutliche Helligkeitsunterschiede feststellbar, weil die Beleuchtung am zweiten Aufnahmetag etwas heller eingestellt wurde.

Die Aufnahme erfolgt im Hochformat, da auf diese Art das Gesicht das Bild besser ausfüllen kann. Die Bilder wurden zunächst in einer Auflösung²¹ von 640×480 (Breite \times Höhe, also Querformat) im Format BMP abgespeichert. Als Dateiname wurde die genaue Aufnahmezeit (Datum und Uhrzeit) gewählt. Die Bilder wurden dann nach Personen sortiert in Verzeichnisse abgelegt. Die Verzeichnisse wurden mit einem Buchstaben benannt, der fortan als „Benutzername“ verwendet wurde.

Die Webcam war zur Aufnahme der Hochformat-Bilder um 90° gedreht an einer Stange befestigt worden. Die Bilder wurden von der Webcam trotzdem im Querformat gespeichert, so dass die Gesichter um 90° gegen den Uhrzeigersinn „gekippt“ auf den Fotos zu sehen waren. Es gab leider keine Möglichkeit, diese Rotation bereits bei der Aufnahme zu korrigieren.

Die Rotation der Fotos und weitere Schritte der Bildaufbereitung sollten möglichst automatisiert ablaufen, da eine manuelle Nachbearbeitung jedes einzelnen Fotos zu aufwändig erschien. Es wurde daher ein Perl-Skript²² geschrieben, welches das Tool Convert nutzt. Convert erlaubt umfangreiche Manipulationen an Bildern über die Kommandozeile. Es ist Bestandteil des Paketes ImageMagick²³ und für Linux, Mac OS, Unix, FreeBSD und Cygwin verfügbar. Das Perl-Skript nutzt Convert, um das Bild zu drehen und es im Format PNG wieder abzuspeichern. PNG wurde gewählt, weil die Bilder damit verlustfrei komprimiert werden konnten. Die geringere Dateigröße war vor allem für ein Backup der Bilder von Vorteil, das jeden Abend vom Labor-Rechner über eine verschlüsselte Verbindung auf den Rechner des Autors übertragen wurde. Damit konnte Bandbreite eingespart werden.

Die Aufnahmezeit als Dateiname erwies sich im weiteren Verlauf des Test als nicht ideal. Mit Dateinamen, die eine Identifikation der abgebildeten Person zuließen, war es deutlich übersichtlicher. Das Perl-Skript wurde entsprechend erweitert. Die Bilder wurden nun nach dem Verzeichnis benannt, in dem sie sich befanden. Zusätzlich wurde eine laufende dreistellige Nummer angehängt, beginnend mit 001. Bilder im Verzeichnis „A“ wurden zum Beispiel in `A_001.png`, `A_002.png` usw. umbenannt.

Bilder, die sehr kurz hintereinander aufgenommen wurden, ließen in einigen Fällen keinen oder nur einen sehr geringen Unterschied erkennen. Solche Bilder wurden gelöscht. Ebenso wurden unscharfe Bilder aussortiert, die entstanden, wenn sich die Testperson zu schnell bewegt hatte. Insgesamt waren zum Schluss der Vorbereitungsphase 5 Bilder pro Person verfügbar, die meist geringe Variationen in Kopfdrotation, Kopfposition und Mimik aufwiesen.

Für den Test wurde von jeder Person ein Bild in das Verzeichnis `Training` abgelegt. Dafür wurden die Bilder mit der Nummer 001 verwendet. Die Liste mit den 20 Personen wurde angelegt und für jede Person das Bild mit der Nummer 001 als Referenztemplate gewählt. Die Bilder der Referenztemplates wurden in das Verzeichnis `Personen` verschoben.

²¹Auflösung wird hier im Sinne von Bildgröße verwendet. Alle Angaben in Pixel.

²²Dateiname `input_person.pl`; Skript ist auf dem beiliegenden Datenträger enthalten.

²³Online unter <http://www.imagemagick.org>, letzter Zugriff am 31.08.2005

ben. Die Liste wurde als XML-Datei gespeichert. Die restlichen drei Bilder pro Person (insgesamt 60 Stück) wurden im Verzeichnis `Vergleich` abgelegt.

6.4.2 Ablauf des Tests

Der Test sollte den Einfluss der Bildgröße und der Anzahl an Eigenvektoren bestimmen. Daher wurden zunächst drei Stufen für die Auflösung gewählt. Ausgehend von einer Auflösung von 120×160 sollten die Auswirkungen einer Verdopplung (240×320) und einer Halbierung (60×80) von Breite und Höhe getestet werden. Später wurden noch Tests für die zwei zusätzlichen Auflösungsstufen 30×40 und 15×20 durchgeführt. Die Kennzeichnung der Tests erfolgte mit den arabischen Ziffern 1 bis 5:

- Test 1: 120×160
- Test 2: 240×320
- Test 3: 60×80
- Test 4: 30×40
- Test 5: 15×20

Die Verwendung von gleich großen Bildern für alle Tests hätte eine Skalierung bei den Test mit kleinerer Auflösung erforderlich gemacht. Dies hätte jedoch die Zeiten verfälscht, die bei der Erstellung der Ergebnis-Tabelle mitprotokolliert wurden. Daher wurden für die Tests 1 bis 5 jeweils separate, vorher auf die richtige Größe skalierte Bilder zur Verfügung gestellt.

Die Anzahl der Eigenvektoren wurde für diese Versuche auf 10 eingestellt. Die Tests 1, 3 und 5 wurden auch mit 5 und 15 Eigenvektoren durchgeführt. Sie werden mit den Kleinbuchstaben a (5 Eigenvektoren) und b (15 Eigenvektoren) gekennzeichnet.

Für die Durchführung der Tests wurde der Prototyp jeweils mit dem passenden Set an Trainingsdaten initialisiert. Diese Initialisierung des Gesichtsraumes dauerte bei Test 2 wegen der hohen Auflösung und dem damit verbundenen Rechenaufwand mit 9 Sekunden am längsten. Gemessen wurde diese Zeit mit Hilfe einer Stoppuhr. Bei den Tests 4 und 5 dauerte der Vorgang weniger als eine Sekunde. Die Anzahl der Eigenvektoren beeinflusst die Dauer der Initialisierung nicht, da immer alle Eigenvektoren berechnet werden und dann nur die benötigten Vektoren weiter verwendet werden.

Die passenden XML-Dateien wurden geladen und die Referenztemplates aus den einzelnen Bildern berechnet. Dies dauerte in allen Fällen nur etwa eine Sekunde.

Der Vergleich von Anfrage- und Referenztemplates erfolgte im dritten Erkennungsmodus des Prototyps. Insgesamt wurden pro Durchlauf $60 \times 20 = 1200$ Vergleiche durchgeführt. Die Dauer der Durchführung, die den Ergebnis-Tabellen (`result.html` im Verzeichnis `Vergleich`) zu entnehmen ist, schwankte von einer halben Sekunde bis zu 13 Sekunden. Die Ergebnis-Tabellen befinden sich auf dem Datenträger, der der Diplomarbeit beiliegt.

6.4.3 Auswertung der Testergebnisse

Die Ergebnisse wurden in ein OpenOffice.org-Tabellendokument übernommen und dort analysiert. Die Tabellendokumente befinden sich ebenfalls auf dem, der Arbeit beiliegenden, Datenträger. Eine Zusammenfassung der Ergebnisse zeigt Tabelle 4.

Es wurde zunächst für alle Genuines (Vergleiche von Anfrage- und Referenztemple der selben Person) der Mittelwert der Distanzen berechnet. So konnte die Entwicklung in Abhängigkeit von Auflösung und Anzahl an Eigenvektoren ermittelt werden.

Der Mittelwert der Genuines-Distanzen wurde genutzt um insgesamt drei Schwellenwerte zu bestimmen. Als erster Schwellenwert wird der Mittelwert selbst verwendet. Für die beiden anderen Schwellenwerte wurde das 1,5-fache und das doppelte des Mittelwertes gewählt. Diese Werte wurden vom Autor dieser Arbeit bestimmt, um die Auswirkung auf die Fehlerraten zu veranschaulichen. Es sei hier darauf hingewiesen, dass bei einem Distanzmaß eine höhere Ähnlichkeit zu einem niedrigeren Wert führt. Somit entspricht eine Erhöhung des Schwellenwertes einer „Aufweichung“ der Akzeptanzschwelle. Am Beispiel von Test 1 sind die Schwellenwerte demnach:

$$\theta_I = 2294$$

$$\theta_{II} = 1,5 \times 2294 = 3441$$

$$\theta_{III} = 2 \times 2294 = 4588$$

Zur Ermittlung der Fehlerraten wurden für alle Schwellenwerte jeweils die Anzahl der False Rejections und die Anzahl der False Acceptances ermittelt. Um daraus die FRR und FAR zu berechnen, war nur noch die Gesamtanzahl der Vergleiche affiner Merkmale bzw. die Gesamtanzahl der Vergleiche nicht affiner Merkmale notwendig. Diese sind bekannt, denn die insgesamt 1200 Vergleiche teilen sich auf in 60 Genuines-Vergleiche und 1140 Impostors-Vergleiche. Folgendes Beispiel zeigt die Berechnung von FRR_I und FAR_I für den Schwellenwert θ_I im Test 1.

$$FRR_I = \frac{\text{Anzahl der False Rejections}}{\text{Gesamtzahl der Vergleiche affiner Merkmale}} = \frac{20}{60} = 0,333$$

$$FAR_I = \frac{\text{Anzahl der False Acceptances}}{\text{Gesamtzahl der Vergleiche nicht affiner Merkmale}} = \frac{7}{1140} = 0,006$$

6.4.4 Beurteilung der Testergebnisse

Ziel des Tests war es, den Einfluss der Bildgröße und der Anzahl der Eigenvektoren zu untersuchen. Die Ergebnisse werden im Folgenden zusammengefasst.

Test	Größe des Bildes (Breite × Höhe)	Anzahl Eigenvektoren	Mittlere Distanz der Genuines	FRR I	FAR I	FRR II	FAR II	FRR III	FAR III	Dauer (ms)
1	120 × 160	10	2294	0,333	0,006	0,217	0,028	0,183	0,074	4248
1a	120 × 160	5	1889	0,250	0,013	0,217	0,040	0,200	0,099	3007
1b	120 × 160	15	2519	0,350	0,005	0,217	0,022	0,167	0,061	4006
2	240 × 320	10	4591	0,333	0,006	0,217	0,028	0,183	0,074	13413
3	60 × 80	10	1147	0,333	0,006	0,217	0,027	0,183	0,075	1041
3a	60 × 80	5	945	0,267	0,013	0,217	0,040	0,200	0,101	1092
3b	60 × 80	15	1259	0,350	0,004	0,217	0,022	0,167	0,062	1778
4	30 × 40	10	581	0,367	0,007	0,217	0,030	0,167	0,081	754
5	15 × 20	10	302	0,283	0,005	0,217	0,034	0,167	0,093	508
5a	15 × 20	5	247	0,267	0,015	0,217	0,058	0,167	0,118	547
5b	15 × 20	15	336	0,300	0,003	0,217	0,029	0,150	0,095	523

Tabelle 4: Ergebnisse des Tests

Absoluter Wert der berechneten Distanzen

Der absolute Wert der Distanzen korreliert stark mit der Größe des Bildes. Eine Verdopplung von Breite und Höhe des Bildes führt, ceteris paribus, zu einer Verdopplung der Distanzwerte. Dies lässt sich am Mittelwert der Genuines-Distanzen ablesen, aber auch an jedem einzelnen Distanzwert. Details sind den Tabellen auf dem beigefügten Datenträger zu entnehmen.

Die Anzahl an Eigenvektoren hat ebenfalls einen Einfluss auf die Höhe der Distanzen. Dieser ist jedoch deutlich geringer als der Einfluss der Bildgröße.

Dauer des Vergleichs

Eine Verdopplung von Höhe und Breite eines Bildes bedeutet einen exponentiellen Anstieg der Anzahl an Bildpunkten. Zum Beispiel hat ein Bild der Größe 120 × 160 19200 Pixel. Eine Verdopplung der Größe auf 240 × 320 erhöht die Zahl der Pixel auf 76800. Damit steigt auch der Rechenaufwand deutlich an, so dass bei höherer Auflösung mit einer exponentiellen Steigerung der Ausführungsdauer zu rechnen ist.

Bei den Tests mit geringen Auflösungen (Test 3, 4 und 5) wird die Ausführungsdauer noch deutlich von Aufgaben beeinflusst, deren Ansprüche an die Rechenkapazität unabhängig von der Bildgröße sind. Deshalb bewirkt eine Verdopplung von Höhe und Breite des Bildes hier keinen so deutlichen Anstieg.

Erkennungsleistung

Auf den ersten Blick mag es den Leser verwundern, dass die Fehlerraten relativ konstant sind. Selbst im Test 5, bei einer Auslösung von nur 15×20 , ändern sich die Fehlerraten kaum. Auch die Variation der Anzahl der Eigenvektoren lässt keine einheitliche Tendenz erkennen.

Um die Ursachen des Problems zu ergründen, wurden diejenigen Personen und Bilder gesucht, die die meisten Fehler verursachten. Zu den False Acceptances ließ sich dabei kein Zusammenhang mit besonderen Eigenschaften des Fotos oder der Personen feststellen. Anders bei den False Rejections: Es wurden mehrere Bilder im Vergleichsset identifiziert, bei denen die Position des Kopfes im Bild, die Drehung des Kopfes und die Bildhelligkeit stark vom Referenzbild abwichen. Diese Variationen scheinen für den Prototyp ein Problem darzustellen, das nicht durch eine höhere Auflösung oder mehr Eigenvektoren behoben werden kann. Möglicherweise ließe sich bei einem höheren Stichprobenumfang (mehr Personen, mehr Vergleichsbilder) doch eine Veränderung der Erkennungsleistung und Fehlerraten feststellen, weil dabei einzelne ungünstige Anfrage- und Referenztemplates keinen so großen Einfluss auf das Gesamtergebnis haben.

Bei der Untersuchung der Bilder zeigte sich, dass der Prototyp bei einer Variation der Mimik und einer leichten Rotation des Kopfes durchaus eine hohe Erkennungsleistung aufweist. Auch der Vergleich eines Gesichtes einmal mit und einmal ohne Brille bereitete in den meisten Fällen keine Schwierigkeiten. Treten jedoch mehrere dieser Variationen gemeinsam auf, nimmt die berechnete Distanz deutlich zu und die Wahrscheinlichkeit einer False Rejection steigt.

6.4.5 Kritische Beurteilung des Tests

Der Stichprobenumfang des durchgeführten Tests ist relativ niedrig, so dass die berechneten Fehlerraten mit Vorsicht betrachtet werden sollten. Statistische Signifikanz wird bei diesem Test nicht gewährleistet sein. Zudem werden die verwendeten Testdaten, die „unter Laborbedingungen“ erfasst wurden, in der Praxis nicht in dieser Qualität anzutreffen sein.

Nichtsdestotrotz konnte der Test einige interessante Aspekte aufzeigen, die zu weiteren Untersuchungen und Analysen anregen. Der Test ließ in dieser Form keinen Einfluss von Bildgröße und Anzahl an Eigenvektoren auf die Erkennungsleistung erkennen. Dies sollte daher mit einer größeren Menge an Testdaten evaluiert werden. Eine andere Fragestellung ist, wie sich die Speicherung von mehreren Referenzbildern pro Person auf die Fehlerraten auswirkt und ob es eine optimale Zahl an Referenzbildern gibt. Auch dies konnte mangels umfangreicher Testdaten nicht beantwortet werden.

6.5 Möglichkeiten für die weitere Entwicklung des Prototyps

Die Testergebnisse, die im letzten Abschnitt vorgestellt wurden, haben gezeigt, dass die Erkennungsleistung relativ hoch ist, wenn sich Anfrage- und Referenztemplate nur durch

eine geringe Veränderung der Kopfposition unterscheiden. Die Fehlerraten steigen jedoch deutlich an, wenn die Position des Gesichtes im Bild stark variiert. Zur Beseitigung dieses Problems könnte eine Gesichtsentdeckung implementiert werden. Der bei der Gesichtserkennung untersuchte Bereich beschränkt sich dann auf die Fläche des abgebildeten Gesichtes. Die Position des Gesichtes im Bild hat dadurch keinen Einfluss mehr auf die Erkennungsleistung, so dass ein Rückgang der False Rejections zu erwarten ist.

Des Weiteren könnten neben der Euklidischen Distanz auch andere Distanzmetriken implementiert werden. Eine Übersicht interessanter Ansätze zur Bestimmung der Distanz findet sich in [YDB02]. Bereits bei der Programmierung des Prototyps wurde diese Erweiterungsmöglichkeit vorgesehen. Eine Implementierung ist daher mit relativ geringem Aufwand umsetzbar.

Bisher ist im Prototyp die Entscheidung auf Match oder Non-Match anhand eines Schwellenwertes nicht implementiert. Für den Einsatz bei Präsentationen ist nach Meinung des Autors die Ausgabe der berechneten Distanzen besser geeignet, als die Angabe einer Entscheidung auf Match oder Non-Match. Die Distanzwerte haben einen höheren Informationsgehalt und erlauben einen quantitativen Vergleich. Für eine Analyse von Testergebnissen kann, wie bereits gezeigt, auch eine Tabellenkalkulation genutzt werden. Dennoch ist es möglich, auch die Entscheidung, den letzten Schritt der Gesichtserkennung, in den Prototyp zu integrieren.

Der Prototyp wurde zu Demonstrationszwecken entwickelt. Für einen produktiven Einsatz, zum Beispiel für die Zutrittskontrolle, wären selbstverständlich noch einige Modifikationen und Erweiterungen notwendig. Wegen der zu erwartenden, relativ hohen Fehlerrate sollte ein Verifikationsmodus implementiert werden. Falls die Fehlerraten auf ein akzeptables Maß gesenkt werden können, sollte zudem untersucht werden, welche Verfahren der Lebenderkennung einen zuverlässigen Schutz vor Angriffen mit Attrappen bieten.

7 Zusammenfassung und Ausblick

7.1 Ziele

Das Ziel dieser Arbeit war, die Anforderungen an Authentifizierungsverfahren darzustellen und auf die Unterschiede zwischen wissens-, besitz- und merkmalsbasierten Ansätzen einzugehen. Das biometrische Verfahren der Gesichtserkennung sollte detailliert betrachtet werden. Es war zu untersuchen, ob diese Methode die gestellten Anforderungen erfüllen kann und wo ihre Schwächen liegen. Zu Demonstrationszwecken war der Prototyp eines Gesichtserkennungssystems zu entwickeln.

7.2 Vorgehensweise zur Erreichung der Ziele

Zur Erreichung der Ziele dieser Arbeit wurden zunächst die Grundlagen der Authentifizierung und der wissens-, besitz- und merkmalsbasierten Verfahren vorgestellt. Biometrische Methoden wurden dabei besonders ausführlich behandelt. Die Anforderungen an Authentifizierungsverfahren wurden erläutert und jeweils betrachtet, inwieweit die einzelnen Gruppen diese erfüllen und wo jeweils die Vor- und Nachteile der wissens-, besitz- und merkmalsbasierten Ansätze liegen. Nach einer Zusammenfassung wurden drei Anwendungsszenarien betrachtet, um zu zeigen, dass die Eignung der biometrischen Authentifizierung vom Anwendungsfall abhängt.

Die Frage nach der Erfüllung der erarbeiteten Anforderungen wurde allgemein für die biometrischen Verfahren beantwortet, ohne sich dabei auf die Gesichtserkennung zu beschränken. Die Fähigkeit, Personen korrekt zu erkennen, ist wahrscheinlich die wichtigste Eigenschaft eines biometrischen Verfahrens. Es sollte daher vermittelt werden, welche Leistung diesbezüglich von der Gesichtserkennung zu erwarten ist. Dazu wurden zuerst die Grundlagen der Gesichtserkennung erläutert und die speziellen Problemstellungen bei diesem Ansatz veranschaulicht. Danach wurden die Ergebnisse einiger bedeutender Evaluationen zusammengefasst, die auch die Schwächen von Gesichtserkennungssystemen zeigten.

Im Anschluss wurde der Prototyp vorgestellt, der im Rahmen dieser Arbeit entwickelt wurde. Die verfügbaren Funktionen wurden beschrieben und die Ergebnisse eines umfangreichen Tests vorgestellt.

7.3 Ergebnisse

Bei der Betrachtung der Anforderungen an Authentifizierungsverfahren stellte sich heraus, dass sich die biometrischen Verfahren in einem wichtigen Punkt von den wissens- und besitzbasierten Ansätzen unterscheiden: Es wird tatsächlich eine Person authentifiziert, und nicht nur ein Hilfsmittel, das einer Person zugeordnet ist.

Für einige andere Anforderungen ließ sich keine pauschale Bewertung für alle biometrischen Verfahren abgeben. Es wurde deutlich, dass diese differenziert betrachtet werden müssen, da sich zum Beispiel statische und dynamische Methoden bezüglich der Erfüllung einiger Anforderungen deutlich unterscheiden. Bei einigen Anforderungen muss auch die Speicherungsform der biometrischen Daten (zentral oder dezentral) und der Abgleichsmodus (Identifikation oder Verifikation) beachtet werden, um eine Bewertung des eingesetzten biometrischen Verfahrens zu ermöglichen.

Bezüglich der Benutzerfreundlichkeit ließ sich feststellen, dass vor allem mit passiven Merkmalen, insbesondere dem Gesicht, Authentifizierungsverfahren mit einem Höchstmaß an Benutzerfreundlichkeit realisierbar sind. Trotzdem scheinen viele Menschen diesen Verfahren skeptisch gegenüberzustehen.

Die Erkenntnisse zur Leistungsfähigkeit von Gesichtserkennungssystemen haben verdeutlicht, dass ein Einsatz auf absehbare Zeit auf die Verifikation beschränkt ist. Für die Identifikation weisen die Verfahren momentan noch zu hohe Fehlerraten auf. Selbst zur Verifikation sollte ein Einsatz nur bei moderatem Schutzbedarf erwogen werden. Bei geringeren Anforderungen an die Sicherheit kann die Gesichtserkennung auch jetzt schon sinnvoll eingesetzt werden, zum Beispiel zur Erhöhung der Sicherheit eines vorhandenen Authentifizierungssystems.

Der Test des Prototyps zeigte die Schwächen des Programms, da Variationen der Position des Gesichts im Bild zu hohen Fehlerraten führen. Zur Verbesserung des Prototyps sollte, zum Beispiel im Rahmen einer weiteren Diplomarbeit, eine Gesichtsentdeckung implementiert werden. Zur Demonstration der Funktionsweise eines Gesichtserkennungssystems scheint das Programm wegen der übersichtlichen Benutzeroberfläche und der einfachen Bedienbarkeit gut geeignet.

7.4 Ausblick

Mit der wachsenden Verbreitung von Informations- und Kommunikationssystemen steigt auch die Zahl an Einsatzmöglichkeiten moderner Authentifizierungsverfahren. Der Markt für „Biometrie“ kann seit einigen Jahren enorme Zuwachsraten verzeichnen. Dabei scheint sich das Gesicht als eines der wichtigsten biometrischen Merkmale zu etablieren, wohl auch wegen der Möglichkeit der berührungslosen Erfassung und der dadurch erreichbaren hohen Benutzerfreundlichkeit.

Allerdings sollte beachtet werden, dass viele Probleme der Gesichtserkennung noch nicht gelöst sind. Das Verfahren ist momentan völlig ungeeignet für eine Verwendung bei hohen Anforderungen an die Sicherheit. Weltweit sind jedoch eine Vielzahl von Forschern damit beschäftigt, die vorhandenen Methoden zu verbessern oder neue, sicherere Verfahren zu entwickeln. Das zeigt sich an der hohen Zahl der verfügbaren Veröffentlichungen zu diesem Thema. Eine Aussage, bis zu welchem Zeitpunkt eine „sichere Gesichtserkennung“ verfügbar sein wird, kann derzeit nicht getroffen werden.

Anhang

Screenshots des Prototyps

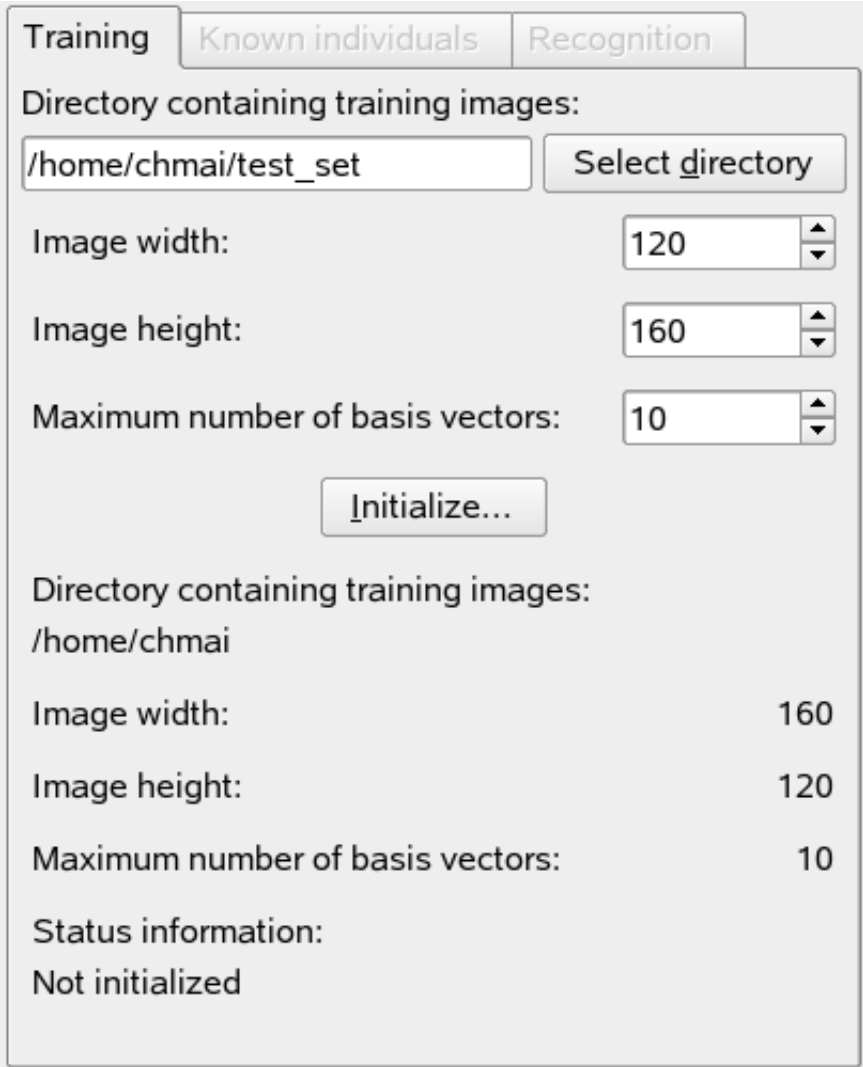


Abbildung 5: Initialisierung des Gesichtsraumes

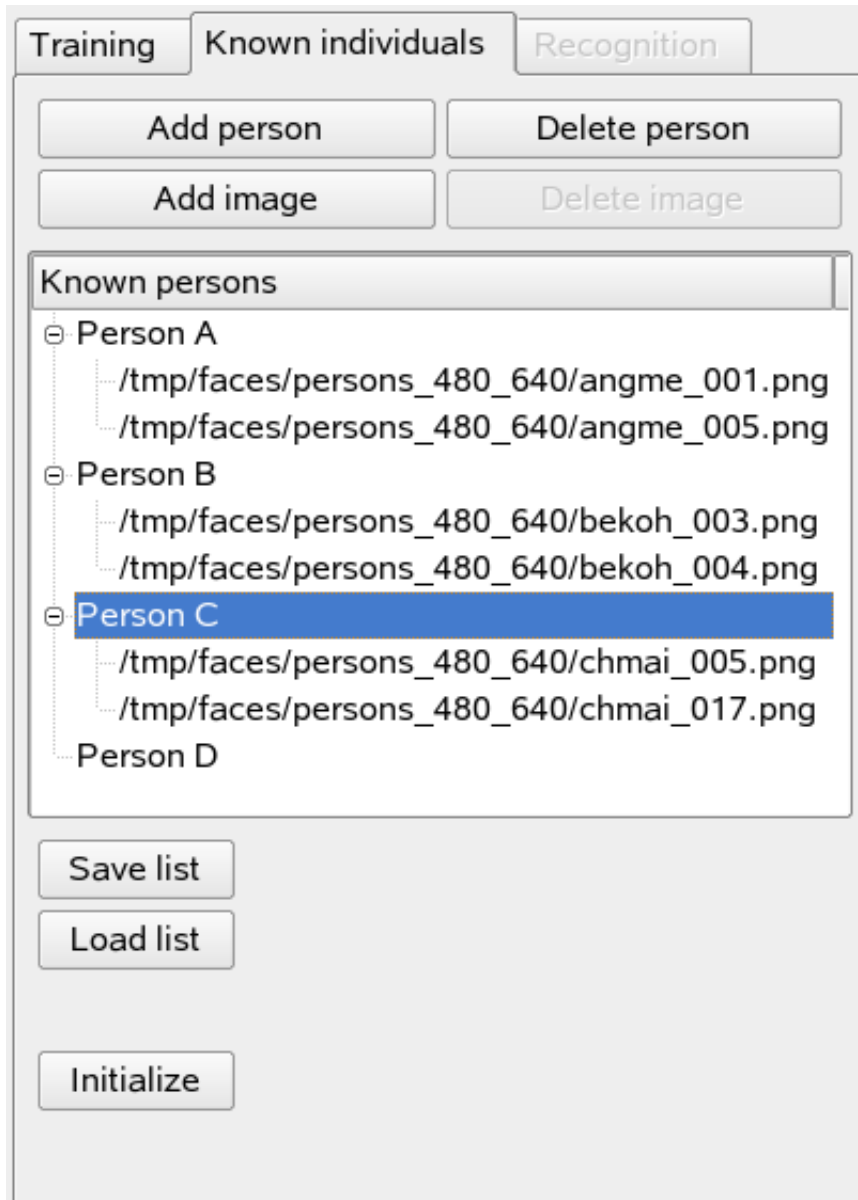


Abbildung 6: Liste bekannter Personen



Abbildung 7: Verschiedene Modi der Gesichtserkennung



Abbildung 8: Gesamtansicht des Prototyps

Literaturverzeichnis

- [Aeb04] AEBI, Daniel: *Praxishandbuch sicherer IT-Betrieb*. Gabler Verlag, 2004
- [Alb02] ALBRECHT, Astrid: Verbraucherpolitische Bedeutung der Biometrie. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 129–144
- [AM04] ABTS, Dietmar ; MÜLDER, Wilhelm: *Grundkurs Wirtschaftsinformatik*. Vieweg Verlag, 2004
- [Bac05] BACHFELD, Daniel: Microsoft: Schreibt eure Passwörter auf. In: *Heise Online* (2005), Mai. – Online unter <http://www.heise.de/security/news/meldung/59929>, letzter Zugriff am 31.08.2005
- [BCF04] BOWYER, Kevin W. ; CHANG, Kyong ; FLYNN, Patrick: A Survey Of 3D and Multi-Modal 3D+2D Face Recognition / Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, Indiana, USA. 2004. – Forschungsbericht. Online unter <http://www.cse.nd.edu/~kwb/Survey3D.pdf>, letzter Zugriff am 31.08.2005
- [BIO02] *Biometrische Verfahren*. Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002
- [BK05] BORCHERS, Detlef ; KURI, Jürgen: Biosig 2005: Ein Pass, der passt. In: *Heise Online* (2005), Juli. – Online unter <http://www.heise.de/newsticker/meldung/61964>, letzter Zugriff am 31.08.2005
- [Bre02] BREITENSTEIN, Marco: Überblick über biometrische Verfahren. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 35–82
- [Bro05] BROMBA, Manfred: *Bioidentifikation*. Juli 2005. – Online unter <http://www.bromba.com/faq/biofaqd.htm>, letzter Zugriff am 31.08.2005
- [Bun01] BUNDESREGIERUNG: *Verordnung zur elektronischen Signatur*. 2001. – Online unter <http://www.bsi.bund.de/esig/basics/legalbas/sigv2001.pdf>, letzter Zugriff am 31.08.2005
- [Bun03] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI: *BioFace – Vergleichende Untersuchung von Gesichtserkennungssystemen – Öffentlicher Abschlussbericht BioFace I & II*. 2003. – Online unter <http://www.bsi.de/literat/studien/BioFace/BioFaceIIBericht.pdf>, letzter Zugriff am 31.08.2005
- [Bun04a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI: *IT Grundschutzhandbuch*. 2004. – Online unter <http://www.bsi.bund.de/gshb/deutsch/index.htm>, letzter Zugriff am 31.08.2005

- [Bun04b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI: *Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II – Öffentlicher Abschlussbericht, Version 2.0*. August 2004. – Online unter <http://www.bsi.bund.de/literat/studien/biop/biopabschluss2.pdf>, letzter Zugriff am 31.08.2005
- [Bun04c] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI: *Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddokumenten – BioP I – Öffentlicher Abschlussbericht, Version 1.1*. April 2004. – Online unter <http://www.bsi.bund.de/literat/studien/biop/biopabschluss.pdf>, letzter Zugriff am 31.08.2005
- [Bun05a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI: *Einführung in die technischen Grundlagen der biometrischen Authentisierung*. Januar 2005. – Online unter http://www.bsi.de/fachthem/biometrie/dokumente/Technische_Grundlagen.pdf, letzter Zugriff am 31.08.2005
- [Bun05b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI: *Das Golden Reader Tool– Die Basis für interoperable elektronische Reisepässe*. August 2005. – Online unter <http://www.bsi.de/literat/faltbl/F25GRT.htm>, letzter Zugriff am 31.08.2005
- [Bun05c] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI: *Grundsätzliche Funktionsweise biometrischer Verfahren*. Januar 2005. – Online unter <http://www.bsi.de/fachthem/biometrie/einfuehrung.htm>, letzter Zugriff am 31.08.2005
- [CH04] CHEN, Ming-yu ; HAUPTMANN, Alexander G.: Towards robust face recognition from multiple views. In: *Proceedings of the 2004 IEEE International Conference on Multimedia and Expo, Taipei, Taiwan*, IEEE, Juni 2004. – Online unter <http://www.informedia.cs.cmu.edu/documents/ChenICME04Face.pdf>, letzter Zugriff am 31.08.2005, S. 1191–1194
- [DAR] DARPA, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DoD COUNTERDRUG TECHNOLOGY DEVELOPMENT PROGRAM OFFICE, NAVSEA CRANE DIVISION: *Face Recognition Vendor Test 2002*. – Online unter <http://www.frvt.org/FRVT2002/default.htm>, letzter Zugriff am 31.08.2005
- [Deu03] DEUTSCHE REGION DER INTERNATIONALEN BIOMETRISCHEN GESELLSCHAFT: *Biometrie - lebendige Zahlen*. März 2003. – Online unter http://www.dkfz.de/biostatistics/IBS/Biometriefolder_Internet.pdf, letzter Zugriff am 31.08.2005
- [Die98] DIECKMANN, Ulrich: *Kombination verschiedener Merkmale zur biometrischen Personenerkennung*, Technische Fakultät, Universität Erlangen-Nürnberg, Diss., 1998

- [Fed02] FEDERRATH, Hannes: *Die bedrohte Sicherheit von Informationsnetzen*. von Aretin, Felicitas ; Wannemacher, Bernd (Hrsg.), 2002. – Online unter <http://www-sec.uni-regensburg.de/publ/2002/informationsnetze.pdf>, letzter Zugriff am 31.08.2005
- [Fey02] FEYERABEND, Erika: Biometrische Totalerfassung. In: *Analyse & Kritik* Nr. 459 (2002). – Online unter http://www.bioskop-forum.de/themen/kriminalpolitik/biometrische_totalerfassung.htm, letzter Zugriff am 31.08.2005
- [Fin02] FINKENZELLER, Klaus: *RFID-Handbuch*. 3. aktualisierte und erweiterte Auflage. Hanser Fachbuchverlag, Wien, 2002
- [FP02] Kap. Technische Grundlagen In: FEDERRATH, Hannes ; PFITZMANN, Andreas: *Handbuch des Datenschutzrechts*. Rossnagel, Alexander (Hrsg.), 2002
- [GMP03] GROTH, Patrick ; MICHEALS, Ross ; PHILLIPS, P. J.: Face Recognition Vendor Test 2002 Performance Metrics. In: *Audio- and Video-Based Person Authentication*, 2003. – Online unter http://www.frvt.org/DLs/Avbpa_2003_evaluation_metrics.pdf, letzter Zugriff am 31.08.2005
- [GSC01] GROSS, Ralph ; SHI, Jianbo ; COHN, Jeff: Quo vadis Face Recognition? / Robotics Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA. 2001. – Forschungsbericht. Online unter http://www.face-rec.org/interesting-papers/General/gross_ralph_2001_4.pdf, letzter Zugriff am 31.08.2005
- [Hit03] HITACHI LTD.: *Hitachi Develops a New RFID with Embedded Antenna μ -Chip*. September 2003. – Online unter <http://www.hitachi.com/New/cnews/030902.html>, letzter Zugriff am 31.08.2005
- [IEB04] IZT – INSTITUT FÜR ZUKUNFTSSTUDIEN UND TECHNOLOGIEBEWERTUNG GMBH ; EMPA – Eidgenössische Materialprüfungs und Forschungsanstalt ; Bundesamt für Sicherheit in der Informationstechnik – BSI: *Risiken und Chancen des Einsatzes von RFID-Systemen*. Bundesamt für Sicherheit in der Informationstechnik – BSI, 2004. – Online unter <http://www.bsi.de/fachthem/rfid/studie.htm>, letzter Zugriff am 31.08.2005
- [Inf04] INFORMATION ACCESS DIVISION, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: *The FERET Database*. Juni 2004. – Online unter <http://www.itl.nist.gov/iad/humanid/feret/>, letzter Zugriff am 31.08.2005
- [KK05] KREMPL, Stefan ; KURI, Jürgen: Biometriepass mit verschärfter Zugangskontrolle und E-Signatur ab 2007. In: *Heise Online* (2005), Januar. – Online unter <http://www.heise.de/newsticker/meldung/54988>, letzter Zugriff am 31.08.2005

- [Kon05] KONICA MINOLTA. *VIVID 910 Product Page*. Online unter http://kmpi.konicaminolta.us/eprise/main/kmpi/content/ISD/ISD_product_pages/Vivid_910?mDetail=Specifications, letzter Zugriff am 31.08.2005. 2005
- [Kui02] KUIP, Anton: Vergleich biometrischer Erkennungssysteme sowie deren Weiterentwicklung in der Praxis. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 367–377
- [Kur04a] KURI, Jürgen: Biometrie: die Praxis ruft [Update]. In: *Heise Online* (2004), Februar. – Online unter <http://www.heise.de/newsticker/meldung/44593>, letzter Zugriff am 31.08.2005
- [Kur04b] KURI, Jürgen: Biometrie, Terrorbekämpfung und die Bundesdruckerei. In: *Heise Online* (2004), September. – Online unter <http://www.heise.de/newsticker/meldung/51402>, letzter Zugriff am 31.08.2005
- [LP04] LEITOLD, Herbert ; POSCH, Reinhard: Leitfaden Biometrie - Überblick und Stand der Technik / Zentrum für sichere Informationstechnologie - Austria. 2004. – Forschungsbericht. Online unter http://www.a-sit.at/technologie/biometrie/Leitfaden_Biometrie.pdf, letzter Zugriff am 31.08.2005
- [Lu03] LU, Xiaoguang: Image Analysis for Face Recognition - A brief survey / Department of Computer Science and Engineering, Michigan State University, East Lansing, Michigan, USA. 2003. – Forschungsbericht. Online unter http://www.cse.msu.edu/%7Elvxiaogu/publications/ImAna4FacRcg_Lu.pdf, letzter Zugriff am 31.08.2005
- [MMYH02] MATSUMOTO, Tsutomu ; MATSUMOTO, Hiroyuki ; YAMADA, Koji ; HOSHINO, Satoshi: Impact of Artificial „Gummy“ Fingers on Fingerprint Systems. In: *Optical Security and Counterfeit Deterrence Techniques IV* The International Society for Optical Engineering, 2002. – Online unter <http://cryptome.org/gummy.htm>, letzter Zugriff am 31.08.2005
- [MS02] MÜLDER, Wilhelm ; STRÖMER, Werner: *Arbeitszeitmanagement und Zutrittskontrolle mit System*. 3. Auflage. Luchterhand Verlag, 2002
- [Mun02] MUNDE, Axel: Die Evaluation biometrischer Systeme - Im internationalen Kontext. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 145–158
- [Nol02] NOLDE, Veronika: Grundlegende Aspekte biometrischer Verfahren. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 20–34
- [Pam02] PAMPUS, Jürgen: Berührungslose Biometrie: Die Mensch-Maschine-Schnittstelle der Zukunft. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 299–312

- [Pfi05] PFITZMANN, Andreas. *Werden biometrische Sicherheitstechnologien die heutige IT-Sicherheitsdebatte vor neue Herausforderungen stellen?* 2005
- [PGM⁺03] PHILLIPS, P. J. ; GROTHOR, Patrick ; MICHEALS, Ross ; BLACKBURN, Duane M. ; TABASSI, Elham ; BONE, Mike: Face Recognition Vendor Test 2002: Overview and Summary / DARPA, National Institute of Standards and Technology, DoD Counterdrug Technology Development Program Office, NAVSEA Crane Division. 2003. – Forschungsbericht. Online unter http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf, letzter Zugriff am 31.08.2005
- [Por00] PORTER, Jack E.: On the „30 error“ criterion. In: WAYMAN, James L. (Hrsg.): *National Biometric Test Center – Collected Works 1997 - 2000* San José State University, 2000. – Online unter <http://www.engr.sjsu.edu/biometrics/nbtccw.pdf>, letzter Zugriff am 31.08.2005, S. 51–56
- [PPB05] PELTIER, Thomas R. ; PELTIER, Justin ; BLACKLEY, John A.: *Information security fundamentals*. Auerbach Publications, 2005
- [Pro02] PROBST, Thomas: Biometrie aus datenschutzrechtlicher Sicht. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 115–128
- [PS02] PETERMANN, Thomas ; SAUTER, Arnold: Biometrische Identifikationssysteme – Sachstandsbericht / Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. 2002. – Forschungsbericht. Online unter <http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf>, letzter Zugriff am 31.08.2005
- [RE02] RANKL, Wolfgang ; EFFING, Wolfgang: *Handbuch der Chipkarten*. 4. Auflage. Carl Hanser Verlag, München, Wien, 2002. – Online unter <http://www.wrinkl.de/HdC/Glossar.pdf>, letzter Zugriff am 31.08.2005
- [Sch05] SCHAAR, Peter: *Übergabe des 20. Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz (2003/2004) an den Präsidenten des Deutschen Bundestages*. April 2005. – Online unter <http://www.bfd.bund.de/Presse/pm20050419.pdf>, letzter Zugriff am 31.08.2005
- [SHZ05] SCHULZKI-HADDOUTI, Christiane ; ZIEGLER, Peter-Michael: Deutschland setzt internationale Standards bei Biometrie-Reisepässen. In: *Heise Online* (2005), Mai. – Online unter <http://www.heise.de/newsticker/meldung/59512>, letzter Zugriff am 31.08.2005
- [SL02] SCHMIDT, Christiane ; LENZ, Jörg-Matthias: Authentifizierung der Nutzer elektronischer Signaturen durch Biometrie. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 263–280

- [Sta04a] STARBUG: *Forderungskatalog zum Einsatz zusätzlicher biometrischer Merkmale in Ausweisdokumenten*. Oktober 2004. – Online unter <https://www.ccc.de/biometrie/forderungen.xml>, letzter Zugriff am 31.08.2005
- [Sta04b] STARBUG: *Wie können Fingerabdrücke nachgebildet werden?* Oktober 2004. – Online unter http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=de, letzter Zugriff am 31.08.2005
- [Sti03] STIELER, Wolfgang: Euro-Banknoten mit Identifikationschips. In: *Heise Online* (2003), Mai. – Online unter <http://www.heise.de/newsticker/meldung/37063>, letzter Zugriff am 31.08.2005
- [SW05] SIETMANN, Richard ; WILKENS, Andreas: Bundesrat billigt Biometriepass-Verordnung. In: *Heise Online* (2005), Juli. – Online unter <http://www.heise.de/newsticker/meldung/61516>, letzter Zugriff am 31.08.2005
- [Tel02] TELETRUST DEUTSCHLAND E.V.: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren – Version 2.0 / TeleTrust Deutschland e.V. 2002. – Forschungsbericht
- [Thi02] THIEL, Christoph: Anforderungen an biometrische Systeme aus bankenfachlicher Sicht. In: *Biometrische Verfahren*, Nolde, Veronika ; Leger, Lothar (Hrsg.). Deutscher Wirtschaftsdienst, Köln, 2002, S. 313–321
- [TKZ02] THALHEIM, Lisa ; KRISLER, Jan ; ZIEGLER, Peter-Michael: Körperkontrolle. In: *c't* (2002), Nr. 11, S. 114
- [TP91] TURK, Matthew ; PENTLAND, Alex: Eigenfaces for Recognition. In: *Journal of Cognitive Neuroscience* (1991), S. 71–86
- [Una04] UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN: *Biometrie in offiziellen Ausweisen: Rechtliche Rahmenbedingungen*. Juni 2004. – Online unter http://www.datenschutzzentrum.de/material/themen/divers/biometrie_ausweis.htm, letzter Zugriff am 31.08.2005
- [Unb05] UNBEKANNT: 2004 Market Review. In: *Biometric Technology Today* (2005), Januar
- [Uni02] UNITED STATES GENERAL ACCOUNTING OFFICE – GAO: Technology Assessment - Using Biometrics for Border Security / United States General Accounting Office. 2002. – Forschungsbericht
- [Ver04] VERBAND FÜR SICHERHEITSTECHNIK E.V.: *Biometrie: Vfs-Veranstaltung bot umfangreiche Informationen*. Februar 2004. – Online unter <http://www.vfs-hh.de/presseBiometrie.html>, letzter Zugriff am 31.08.2005

- [Way00] WAYMAN, James L.: A Definition of „Biometrics“. In: WAYMAN, James L. (Hrsg.): *National Biometric Test Center – Collected Works 1997 - 2000* San José State University, 2000. – Online unter <http://www.engr.sjsu.edu/biometrics/nbtccw.pdf>, letzter Zugriff am 31.08.2005, S. 21–23
- [Wik05a] WIKIPEDIA: *Fingerbeere*. 2005. – Online unter <http://de.wikipedia.org/wiki/Fingerbeere>, letzter Zugriff am 31.08.2005
- [Wik05b] WIKIPEDIA: *Terroranschläge am 7. Juli 2005 in London*. 2005. – Online unter http://de.wikipedia.org/wiki/Terroranschlag_am_7._Juli_2005_in_London, letzter Zugriff am 31.08.2005
- [Wik05c] WIKIQUOTE: *Wolfgang Thierse*. 2005. – Online unter http://de.wikiquote.org/wiki/Wolfgang_Thierse, letzter Zugriff am 31.08.2005
- [Woo99] WOODWARD, John D.: Identifying Law & Policy Concerns. In: *Biometrics: Personal Identification in Networked Society*, Jain, A. ; Bolle, R. ; Pankati, S. (Hrsg.), 1999, S. 385–405
- [YDB02] YAMBOR, Wendy S. ; DRAPER, Bruce A. ; BEVERIDGE, J. R.: *Analyzing PCA-based Face Recognition Algorithms: Eigenvector Selection and Distance Measures*. Christensen, H. ; Phillips, J. (Hrsg.), 2002. – Online unter <http://www.cs.colostate.edu/evalfacerec/papers/eemcvcsu.pdf>, letzter Zugriff am 31.08.2005
- [YKA02] YANG, Ming-Hsuan ; KRIEGMAN, David J. ; AHUJA, Narendra: Detecting Faces in Images: A Survey. In: *Transactions on pattern analysis and machine intelligence*. IEEE, Januar 2002. – Online unter <http://vision.ai.uiuc.edu/mhyang/papers/pami02a.pdf>, letzter Zugriff am 31.08.2005
- [ZCPR03] ZHAO, Wen-Yi ; CHELLAPPA, Rama ; PHILIPPS, P. J. ; ROSENFELD, Azriel: Face Recognition: A Literature Survey. 2003. – Forschungsbericht. Online unter <http://www.cfar.umd.edu/~wyzhao/FaceSurvey.pdf>, letzter Zugriff am 31.08.2005
- [Zie03] ZIEGLER, Peter-Michael: Adlerauge – Europas größte Gesichtserkennungsanlage im Zoo Hannover. In: *c't* (2003), Nr. 9, S. 26–27

Datenträgerverzeichnis

Auf dem beiliegenden Datenträger ist Folgendes enthalten:

Ordner Dokumente

Die Diplomarbeit als PDF-Datei.

Die L^AT_EX-Quelldateien.

Ordner Literatur

Die als Dateien verfügbaren Quellen der Arbeit.

Ordner Prototyp

Die Quellcodes des implementierten Prototyps.

Eine ausführbare Datei des Prototyps, kompiliert für Linux.

Eine kurze Anleitung zum Kompilieren des Prototyps.

Ordner Testergebnisse

Die Ergebnisse der mit dem Prototyp durchgeführten Test.

Ordner Tools

Hilfsprogramme, die bei den Tests des Prototyps zum Einsatz kamen.

Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig angefertigt sowie keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Diese Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt.

Regensburg, den 1. September 2005

Christian Maier