Werner-Heisenberg-Gymnasium Garching

Kollegstufe 2006/2008

Facharbeit im Leistungskurs Biologie

über das Thema

Biometrische Personenidentifizierung

von

Marek Kubica

Kursleiter: Herr Maier

Abgabetermin: 25. Januar 2008

Punkte: _____

_____

Unterschrift des Kursleiters

Inhaltsverzeichnis

1 Was ist Biometrie?

Biometrie ist der Zweig der Biologie, der sich mit statistischen Methoden befasst. Die Erkenntnisse der Biometrie können und werden auch für medizinische und pharmazeutische Anwendungszwecke benutzt. Eine solche Anwendung ist der Test der Effektivität eines neuen Wirkstoffes, dessen Wirkung erst statistisch nachgewiesen werden muss [Cavalli-Sforza74].

Jedoch bezeichnet der Begriff „Biometrische Identifizierung“ ein etwas anderes Teilgebiet der Biometrie. [Wayman05] definiert die biometrische Identifizierung, im Folgenden als „Biometrie“ abgekürzt folgendermaßen:

> “Biometric technologies” are automated methods of verifying or recognizing the identity of a living person based on physiological or behavioral characteristic.[a]

Diese Definition ist gut geeignet um die Kernpunkte der Biometrie hervorzuheben. So geht es in der Biometrie um die Erkennung und/oder die Bestätigung der Identität von Personen. Die Biometrie grenzt sich von dem Feld der Forschung über die menschliche Identität ab, indem sie sich nur mit automatisierbaren Vorgängen befasst und sich auf die Identifizierung von lebenden Menschen spezialisiert.

1.1 Kennzeichen der Biometrie

Die Definition von Biometrie lässt zwei Arten von Identifizierung zu. Eine Möglichkeit ist die Messung von physiologischen Merkmalen, wie die Länge der Gliedmaßen oder der Struktur der Organe (Finger, Iris, Blutgefäße). Die zweite Möglichkeit ist die Messung von Verhalten, wie etwa die Art zu unterschreiben oder das Tippverhalten. Zur Erhöhung der Sicherheit sind natürlich auch Kombinationen von mehreren Verhalten denkbar.

Die Frage welches Verfahren am besten ist, lässt sich jedoch nicht endgültig beantworten, da es oft von den Anforderungen abhängt, die an ein biometrisches System gestellt werden. Es gibt fünf Kriterien für das ideale Identifizierungssystem: Beständigkeit, Einzigartigkeit, Verfügbarkeit, Messbarkeit und Akzeptanz [Petermann02].

- Beständigkeit bedeutet, dass dieses Merkmal sich während des Lebens so wenig wie möglich ändert (Fingerabdrücke verändern sich wenig, die Stimme kann sich aber beispielsweise durch Krankheit ändern)

[a] „Biometrische Technologien“ sind automatisierte Methoden die Identität einer lebenden Person zu erkennen oder zu bestätigen, die auf der Physionomie oder dem Verhalten beruhen.

- Die **Einzigartigkeit** sagt aus, dass das Merkmal in der Bevölkerung möglichst unterschiedlich ausgeprägt ist (die Iris ist sehr individuell, das Tippverhalten kann bei verschiedenen Menschen ähnlich sein)
- **Verfügbarkeit** steht dafür, dass möglichst alle zu erfassenden Menschen dieses Merkmal aufweisen (Stimme als Merkmal ist für stumme Menschen ein Problem)
- Dadurch, dass die Identifizierung automatisiert ablaufen soll ist die **Messbarkeit** durch elektronische Sensoren ein wichtiges Kriterium (die Retina zu erfassen ist schwieriger als die Handgeometrie)
- Zuletzt ist auch die **Akzeptanz** zu berücksichtigen, die besagt, wie viel Mitarbeit von dem zu identifizierenden Menschen notwendig ist (für eine Gesichtserkennung reicht ein Kamerabild, ein Irisscan erfordert Stillstehen und Geradeschauen) und wie die Menschen auf diese Authentifizierung reagieren (eine Unterschrift wird bereitwillig gegeben, Fingerabdrücke erinnern an Strafverfolgung)

1.2 Wichtige Grundbegriffe

Jedes biometrische System erfordert das Einlernen der zur Erkennung notwendigen Merkmale eines Menschen. Dieser Schritt wird **Enrollment** genannt. Dabei wird aus den Daten des zukünftigen Nutzers ein Referenzdatensatz generiert, das sogenannte **Template**. Zukünftige Identifizierungsvorgänge vergleichen die eingegebenen Daten mit diesem Template (oder auch einer ganzen Datenbank von Templates), daher ist es wichtig, dass das Template möglichst akkurat ist. Später müssen die gemessenen Merkmale so gut wie möglich mit diesem Template zusammenpassen, damit ein Nutzer identifiziert werden kann [Petermann02].

Die einzelnen Messungen unterliegen bestimmten Messungenauigkeiten. Diese Ungenauigkeiten können umweltbedingt sein, wie die Beleuchtungsverhältnisse aber auch die Person selbst kann sich verändern. Ein Beispiel dafür ist Bartwuchs, der etwa bei der Gesichteserkennung zu einem Problemfaktor werden kann. Daher müssen auch nicht hundertprozentige Übereinstimmungen der Daten und der Referenzdaten trotzdem korrekt einander zugeordnet werden, um Personen richtig zu identifizieren. Dieses bedingt das Einführen eines Schwellenwertes, der die notwendige Ähnlichkeit beschreibt, um einer Person ein Template zuzuweisen, sie also erfolgreich zu identifizieren. Dieser Schwellenwert bestimmt dadurch zwei weitere Kriterien eines biometrischen Systems: die **Rate falscher Ablehnung** (FRR[b]) die die Person nicht korrekterweise ihrem Template zuordnet, sowie die **Rate falscher Akzeptanz** (FAR[c]), die eine Person fälschlicherweise als

[b] False Rejection Rate
[c] False Acceptance Rate

eine andere in der Datenbank vorhandene identifiziert. Diese Werte beeinflussen sich gegenseitig über den Schwellenwert. Wird dieser erhöht, sinkt die FRR, die FAR jedoch steigt. Die optimalen Werte können nicht berechnet werden, man muss sie empirisch ermitteln und den Schwellenwert für den jeweiligen Anwendungszweck anpassen [Wayman05].

1.3 Überblick über ausgewählte biometrische Verfahren

Es gibt eine Vielzahl von Verfahren, die für die biometrische Identifikation genutzt werden können, daher ist es unmöglich alle umfassend vorzustellen. Die moderne Biometrie ist eine noch recht junge Wissenschaft und viele Verfahren befinden sich noch in einer sehr frühen Entwicklungsphase oder sind noch nicht ausgereift [Petermann02]. Zu diesen in Zukunft möglicherweise verwendbaren Verfahren zählt die Geruchsidentifikation, die Erkennung durch Ohrgeometrie sowie viele verhaltensbasierte Verfahren.

Es ist also sinnvoll sich auf die populärsten Verfahren zu beschränken, Abbildung 1 fasst die Nutzung der Biometrie in Deutschland zusammen. Es ist leicht zu erkennen, dass Fingerabdruck, Gesichtserkennung und Irisscan die momentan am häufigsten eingesetzten Verfahren sind. Daher wird auf diese im folgendem näher eingegangen. Zusätzlich wird die prominenteste deutsche Biometrieanwendung diskutiert – der Pass.

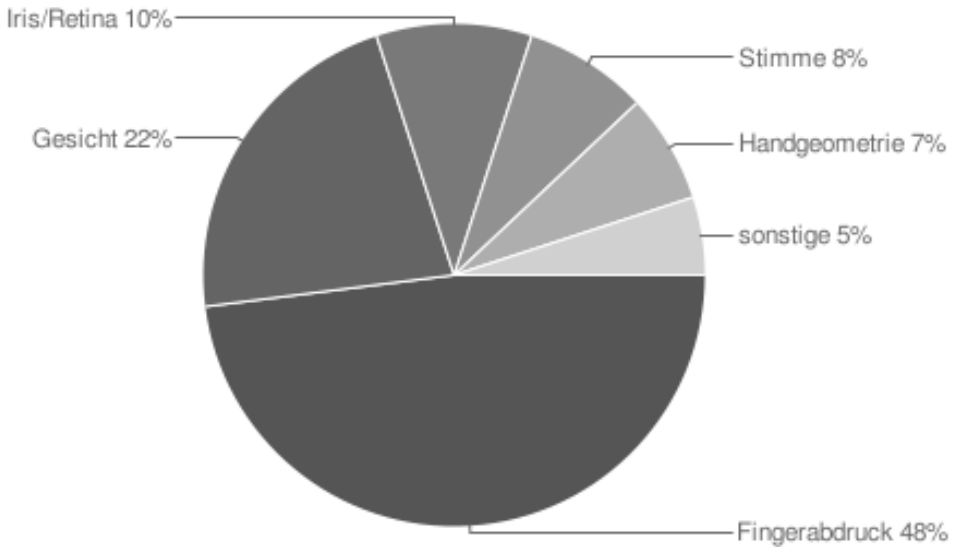

Abbildung 1: Anteil der Technologien am deutschen Biometriemarkt 2006 [Lange07]

2 Fingerabdrücke

Die Verwendung von Fingerabdrücken ist die älteste, bekannteste und sicherste Methode Menschen zu identifizieren. Sie bieten eine gute Grundlage um biometrische Verfahren unter Ausnutzung ihrer seit langem bekannten Eigenschaften anzuwenden. Möglich wird dies durch die bei allen Menschen unterschiedliche Struktur der Haut auf den Fingerkuppen die, wie auf Abbildung 2 zu erkennen ist, sehr deutlich und detailliert ist.

Abbildung 2: Zwei deutliche Fingerabdrücke [Wayman05]

2.1 Geschichtlicher Abriss

Die frühesten Zeugnisse der Nutzung von Fingerabdrücken um Personen mit bestimmten Taten zu verknüpfen stammen aus China, Babylon und Assyrien und lassen sich bis auf das Jahr 600 vor Christus zurückverfolgen. Im 17. Jahrhundert findet man die ersten Erwähnungen von den Strukturen die als Papillarlinien bekannt sind, das heißt von den Strukturen auf den Fingern, die komplizierte Linienmuster bilden. Detailliertere Beschreibungen der Strukturen, wie Wirbel, Gabelungen, Berührungen, Verzweigungen und weitere Arten findet man in wissenschaftlichen Publikationen des frühen 19. Jahrhunderts [Wayman05].

Auf die Idee Fingerabdrücke zu Identifizierungszwecken zu nutzen kam 1856 William Herrschel. Um die Fingerabdrücke zu ordnen und wiederzufinden[d] wurde in den siebziger Jahren des 19. Jahrhunderts ein Klassifizierungssystem entwickelt. Zu den Pionieren der Forschung zählt auch Francis Galton, der sich Ende des 19. Jahrhunderts mit Fingerabdrücken beschäftigt hat und

[d] in diesem Kontext spricht man von Klassifikation

die Wahrscheinlichkeit dafür, zwei identische Fingerabdrücke zu finden durch Berechnung auf 1:64 Milliarden abgeschätzt hat. Schon 1897 wurde von Edward Henry ein bis heute genutzte Klassifizierungssystem eingeführt.

2.2 Typische Einsatzgebiete der Fingerabdrücke

Durch ihren langjährigen, erfolgreichen Einsatz, die extensive Erforschung und allgemeine Akzeptanz als Beweismittel vor Gericht sind Fingerabdrücke die bekannteste Anwendung der Biometrie. Ihre Vorteile machen Fingerabdrücke für eine Vielzahl Einsatzzwecke interessant.

2.2.1 Kriminalistik

Da Fingerabdrücke schon früh für kriminologische Ziele erforscht wurden, werden sie heutzutage für eine große Zahl von Einsatzgebieten eingesetzt. Dabei werden sie nicht nur verwendet um die an einem Tatort sichergestellten Fingerabdrücke mit denen der Verdächtigen zu vergleichen, sondern auch um Personen die einen falschen Namen verwenden zu identifizieren [Wayman05]. Ebenfalls ist es möglich, verstorbene Personen anhand ihrer Fingerabdrücke zu identifizieren, doch befindet sich letzteres nicht mehr im Hauptaugenmerk der Biometrie.

2.2.2 Komerzieller Einsatz

Frühe komerzielle Systeme hatten viele Probleme und funktionierten eher schlecht. Das lag teilweise auch an den Nutzern dieser Systeme, die die Proben der Finger falsch abnahmen. So wurden den Proben von der Fingerspitze oder der Fingerseite aufgenommen, statt der präferierten Mittelregion der Fingerkuppe, was zu unbrauchbaren Templates führte. Moderne Systeme sind aber inzwischen wesentlich leistungsfähiger geworden, so dass sogar der Einsatz im Bankenwesen denkbar wäre. Ebenso sind die Anwender sind inzwischen in der Lage korrekte Templates zu erstellen. Simple Systeme zur Zugangskontrolle werden mitunter auch in Computer verbaut.

2.3 Funktionsweise

2.3.1 Scan und Digitalisierung

Anfangs wurden Fingerabdrücke mit Hilfe von Tinte auf Karten abgedrückt, die daraufhin von Menschen ausgewertet werden mussten. Mit dem zunehmenden Einsatz von Computern wurd

es nötig, diese Daten in den Computer zu übernehmen, wozu möglichst hochqualitative Scan
ner zum Einsatz kommen müssen um die feinen Details wiedergeben zu können. Solche Scann
müssen eine 1,5 x 1,5 Zoll große Fläche mit über 1.000 dpi[e] und einem Farbspektrum von 10 bis
12 Bit (entspricht 2^{10} - 2^{12} Graustufen) abtasten können [Wayman05]. Abbildung 3 zeigt einen
mit solchem Scannern aufgenommenen Abdruck. Es herrscht inzwischen aber ein Trend zu s
genanntem „Live Scan“ vor, bei dem die Fingerabdrücke ohne den Umweg über Papier direkt i
digitale Form gebracht werden können.

Diese Live-Scanner können die Fingerabdrücke auf verschiedene Weisen einlesen, das simpe
Verfahren benutzt optische CCD-Sensoren, wie sie auch in handelsüblichen Flachbettscanne
zum Einsatz kommen. Komplexere Verfahren arbeiten mit Halbleitersensoren, die die Gleich
stromkapazitäten zwischen dem Finger und der Scanneroberfläche messen sowie mit Ultraschall,
mit Hilfe dessen man den akkustischen Widerstand der Haut auf dem Finger messen kan
[Petermann02].

Abbildung 3: Ein mit Tusche abgenommener Fingerabdruck [Wayman05]

2.3.2 Bildverbesserung

Eine wesentliche Vorraussetzung, um die in der Scan-Phase gewonnenen digitalen Bilder zu
Identifizierung verwenden zu können ist die Nachbearbeitung des Bildes, um die benötigten
Strukturen der Papillarlinien (Wirbel, Verzweigungen und viele andere) stärker herauszustel-
len.

[e] Dots per inch – Punkte pro Zoll

Ein simples Verfahren zur Verbesserung des Kontrastes ist LACE[f] welches die jeweils benachbarten Bildpunkte in ein Verhältnis zum durchschnittlichen Kontrastwert des gesamten Bildes setzt [Wayman05]. Es nutzt den Kontrast-Durchschnitt und -Varianz von 15x15 Pixel großen Feldern und berechnet darüber unter Einbeziehung empirisch ermittelter Korrekturkonstanten die neue Intensität jedes einzelnen Bildpunktes. Dieses Verfahren ist nicht speziell auf die Verbesserung des Fingerabdruck-Bildes ausgelegt, es kann auch in normalen Bildbearbeitungsprogrammen zur Kontrastverbesserung von beliebigen Bildern eingesetzt werden. Im Vergleich zu seinem geringen Aufwand erreicht es jedoch recht gute Ergebnisse, die auf Abbildung 4 zu sehen sind.

Eine weitere Möglichkeit zur Verbesserung des Fingerabdruckbildes sind sogenannte Kontextuelle Filter[Wayman05]. Diese Filter erfüllen zweierlei Aufgaben: Sie füllen kleine Lücken in den Papillarlinien auf dem Bild, die auf Poren in der Haut oder Bildrauschen zurückzuführen sind. Dabei werden diese Filter Längs der Linien angewendet, um die Linien „nachzuziehen“. Die zweite Aufgabe, die bessere Unterscheidung zwischen den parallel verlaufenden Papillarlinien wird erledigt, indem die Zwischenräume der Linien, die Täler, weiß gefüllt werden. Diese beiden Ziele können mit sogenannten Gabor-Filtern erreicht werden. Diese komplizierten mathematischen Funktionen transformieren die Bildpunkte um das gewünschte Ergebnis zu erreichen. Dadurch, dass auf das Bild genau jene Transformationen angewendet werden, die im Kontext von Fingerabdrücken sinnvoll sind, ist die Qualität der so gewonnenen Bilder wesentlich besser als die der ursprünglich aufgenommenen. Abbildung 4 zeigt den Abdruck aus Abbildung 3 nach der Transformation mit Gabor-Filtern.

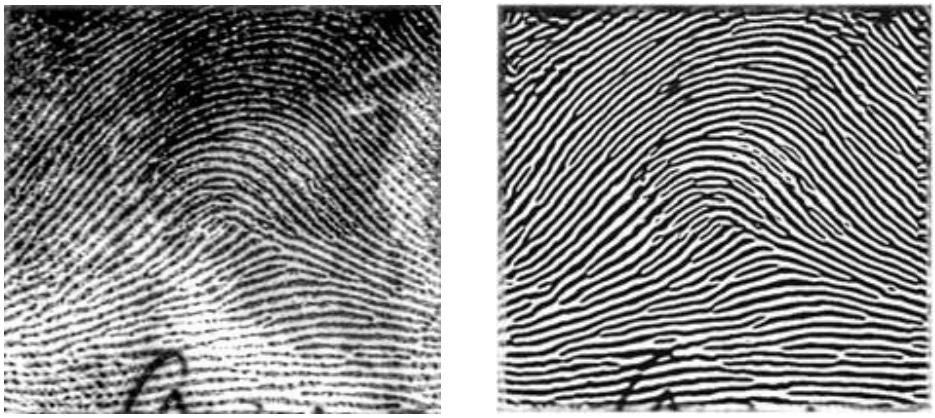

Abbildung 4: Der Fingerabdruck nach LACE- und Gabortransformation [Wayman05]

[f] local area contrast enhancement

2.3.3 Extraktion von Merkmalen

Das in der Bildverbesserungs-Phase gewonnene Graustufenbild kann in der Regel in ein Zwe farb-Bild konvertiert werden, bei dem die Linien durch schwarze Pixel und die Zwischenräume durch weiße Pixel dargestellt werden. Der nächste Schritt ist, die mehrere Pixel breiten schwar zen Linien zu 1-Pixel breiten Linien zusammenzuziehen, denn das ermöglicht daraufhin einfa chere maschinelle Verarbeitung. Diese Binearisierung genannte Vorgang kann auf verschiedene Weise erfolgen, die Methode von Rosenfeld liefert oft gute Ergebnisse. Dabei werden zu jedem Pixel die 3x3 Pixel in der Nachbarschaft analysiert um zu entscheiden, ob der Pixel in der Mitte schwarz oder weiß werden soll [Wayman05]. Abbildung 5 zeigt die jeweiligen Resultate dieser beiden Schritte.

Abbildung 5: Der binearisierte Fingerabdruck, Fingerabdruck mit verdünnten Linien [Wayman05]

Nachdem ein Bild mit 1-Pixel breiten Linien vorliegt, kann die Extraktion der Merkmale beginnen, bei der wiederum die 3x3 Pixel-Nachbarschaft der Bildpunkte ausgewertet wird. Es ist her auszufinden, ob der Pixel sich auf einer Linie befindet, der Endpunkt einer Linie ist oder an einer Linien-Gabelung liegt. Die auf diese Weise gefundenen Merkmale – die Minuzien – werden nun weiterem Gültigkeitstests unterzogen, wie der Prüfung ob die Länge der Linie zwischen den End punkten sich in bestimmten, vernünftigen Grenzen hält. Endpunkte die Teil von zu kurzen oder zu langen Linien sind, werden verworfen, da es sich bei ihnen höchstwarscheinlich um Fehler im aufgenommen Fingerabdrucksbild handelt. Ein weiterer möglicher Test ist die Invertierung der Farben und eine erneute Suche nach Merkmalen, die nun an Stelle der Gabelungen Endpunkt liefert und umgekehrt. Nur Merkmale die alle Testkriterien erfüllen, werden als gültige Merkmale des Fingerabdrucks angesehen.

2.3.4 Klassifizierung

In der Klassifizierung der gewonnenen Fingerabdrücke geht es um das Auffinden von Mustern aus den Papillarlinien und den Minuzien. Dabei wird versucht erst drei Grundformen zu erkennen: Whorl, Loop und Delta. Es wird wiederrum eine mathematische Funktion verwendet, die den Poincaré-Index berechnet, der aussagt, ob der zu prüfende Punkt Teil eines Whorls, Loops, Deltas ist oder nicht. Um das Muster zu erkennen wird die Richtung der Nachbarlinien zu Rate gezogen.

Sobald diese Grundmuster bekannt sind, ist es möglich durch einen bestimmten Regelsatz größere Muster zu konstruieren. Eine solche Regel kann besagen, dass Bögen keine Loops oder Deltas besitzen. Durch einen umfangreicheren Regelsatz lassen sich so komplexere Muster aufbauen.

2.3.5 Auffinden

Nachdem ein Fingerabdruck analysiert wurde, müssen dessen Merkmale nun mit den Merkmalen anderer in der Datenbank vorhandener Fingerabdrücke verglichen werden, damit die Person, dessen Fingerabdruck abgenommen wurde identifiziert werden kann.

Das Problem beim Auffinden von Fingerabdrücken ist, dass sie niemals absolut identisch eingescannt werden, selbst wenn es der gleiche Finger ist. Es können mehrere Komplikationen auftreten:

- **Position, Rotation, Druck, Verzerrung** Die Position an der ein Finger auf dem Sensor liegt, kann sich immer geringfügig unterscheiden, ebenso ist es möglich, dass der Finger einen unterschiedlichen Winkel zum Sensor aufweist, also nicht immer flach auf dem Sensor aufliegt. Der Druck des Fingers spielt für das Erscheinungsbild ebenfalls eine Rolle. Es tritt auch immer eine unvermeidliche, leicht variierende Verzerrung auf, wenn man die dreidimensionale Struktur des Fingers mit dem zweidimensionalen Sensor ausmisst[g]
- **Rauschen, Fehler in den Algorithmen** es ist ebenso denkbar, dass das vom Sensor gelieferte Bild Unterschiede aufweist, die auf Verschmutzung oder Abnutzung zurückzuführen sind. Die Algorithmen, die verwendet werden, um Merkmale zu extrahieren, sind ebenfalls nicht absolut fehlerfrei, also ist es möglich, dass manchmal einige Minuzien gefunden werden, die bei einer erneuten Analyse des selben Fingers nicht mehr gefunden werden oder umgekehrt.

[g] Vergleichbar mit der Darstellung der geoiden Erde in einem Atlas

Alle diese Einflüsse führen dazu, dass man Fingerabdrücke nicht mit hundertprozentiger Sicherheit zuordnen kann und somit Entscheidungsschwellenwerte definieren muss. Es müssen also fehlertolerante Methoden verwendet werden, um Fingerabdrücke zu vergleichen. Bei einem Vergleich von zwei Fingerabdruck-Bildern legt man sie übereinander und zieht um die Minuzien sogenannte Toleranzrahmen. Abbildung 7 zeigt, wie solche Toleranzen zu verstehen sind. Nun müssen die Minuzien des anderen Bildes sich in diesem Rahmen befinden, damit eine Übereinstimmung erkannt wird. Zusätzlich dazu muss sich die Ausrichtung der Minuzien sich in einem Toleranzbereich befinden. Wenn dies nicht der Fall ist, werden die Minuzien ebenso als nicht übereinstimmend befunden. Auf diese Weise werden alle Merkmale geprüft, bis eine Abschätzung gegeben kann, ob die Fingerabdrücke als übereinstimmend befunden werden können.

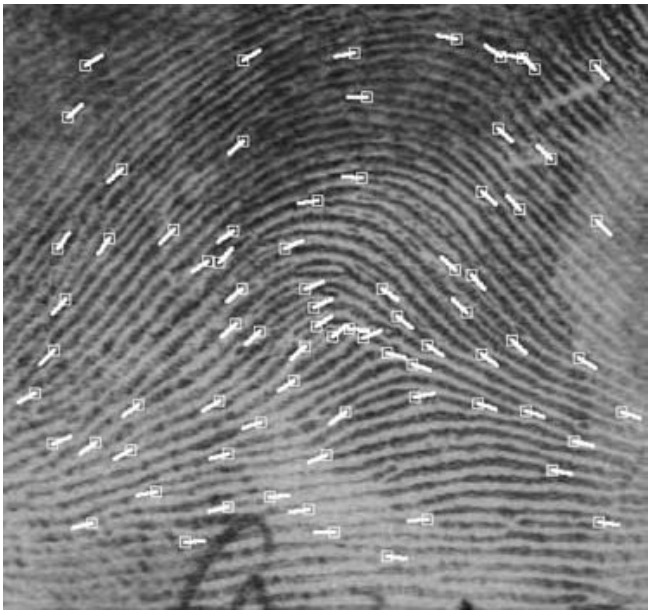

Abbildung 6: Auf dem Fingerabdruck angetrage Minuzien [Wayman05]

2.4 Fälschungen

Dass Fingerabdrücke überall hinterlassen werden ist nicht nur für die Kriminalistik wichtig, sondern führt auch dazu, dass fremde Fingerabdrücke recht simpel kopiert werden können[h]. Somit können auch recht simpel gefälscht werden.

Der Chaos Computer Club demonstriert eine Methode, die keine spezielle Ausrüstung benötigt [Guyot06]. Dennoch lassen sich auf diese Weise ausreichend gute Attrappen herstellen, um simple Fingerabdrucksysteme zu überwinden. Dabei wird ein Abdruck auf Glas mit den Ausdünstungen von Flüssigkleber bedampft, um den Abdruck besser sichtbar zu machen. Dieser

[h] Der Chaos Computer Club spricht von etwa 30 verwertbaren Abdrücken am Tag

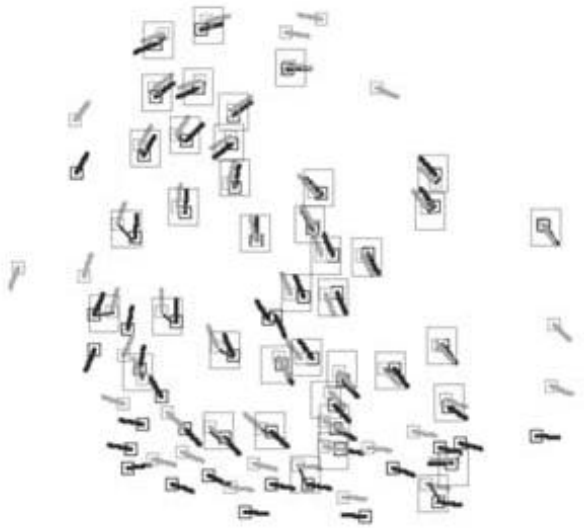

Abbildung 7: Minuzien, die gegen ein Template geprüft werden [Wayman05]

Abdruck wird fotografiert und das Bild auf den Computer übertragen, wo es mit einem Bildbearbeitungsprogramm modifiziert wird, sodass der Fingerabdruck als Negativ auf Folie ausgedruckt werden kann. Der Ausdruck wird mit einer dünnen Schicht Leim überzogen, der sich in die Mikrostruktur des Negativs anpasst und so das Fingerabdruck-Positiv bildet. Nach kurzem Aushärten kann die Leimattrappe abgezogen werden und mit hautfreundlichem Kleber auf einen Finger befestigt werden, so dass sie kaum zu sehen ist.

Dieses Verfahren funktioniert zwar nur bei optischen Sensoren, zeigt aber, dass biometrische Systeme nicht generell gegen Fälschungen gesichert sind[i].

[i] Der Lebensmittelmarkt „Edeka“ hat in Test-Supermärkten solche Sensoren eingesetzt, die sich auf diese Weise durch Attrappen verwirren ließen, wie das Magazin Plusminus herausfand

3 Gesichtserkennung

Die Identifizierung von Menschen aufgrund der Merkmale ihres Gesichtes ist ein weiteres populäres Verfahren, welches gegenüber Fingerabdrücken einige Vorteile bietet. Da es kontaktfrei arbeitet, das heißt ohne physischen Kontakt zu dem zu identifizierenden Menschen auskommt, werden Verunreinigung und starke Abnutzung der Messgeräte ausgeschlossen. In einigen, vor allem asiatischen Kulturen besteht eine Hemmung Gegenstände anzufassen die Fremde benutzt haben [Guyot06]. Daher ist die Gesichtserkennung dort aus psychologischen Gründen ganz besonders vorteilhaft.

3.1 Messung

Trotz der Vorteile, sind für eine zuverlässige Gesichtserkennung einige Hürden zu überwinden, um Menschen trotz ihrer sich ständig verändernden Mimik sowie eventuellen Bartwuchses und unvermeidlicher Alterung korrekt zu erkennen. Ein zusätzliches Problem für die richtige Erkennung sind wechselnde Lichtverhältnisse, die die Ausleuchtung eines Gesichtes verändern.

Die Erfassung verläuft in zwei Phasen [Petermann03]. In der ersten Phase muss das von einer Kamera aufgenommene Bild analysiert werden, um das Gesicht zu finden und vom Hintergrund zu extrahieren (*face detection*). Dazu gibt es verschiedene Möglichkeiten, etwa durch das Ausfinden von typischen Gesichtsbewegungen, die Suche nach gesichtsähnlichen Formen oder gar durch Verwendung von Thermogrammen, die mit Infrarotkameras aufgenommen werden. Die zweite Phase beschäftigt sich mit der Analyse des nun gefundenen Gesichtes (*face recognition*). Auch in der zweiten Phase gibt es mehrere Alternativen, die eingesetzt werden, um das Gesicht zu identifizieren.

Die einfachste Methode ist die *Gesichtsmetrik* [Wächter01], bei der die Positionen von Augen, Nase, Mund und weiteren Gesichtsmerkmalen zueinander in Verhältnis gesetzt wird. Dabei können auch die Größen der Organe sowie die Breite des Gesichtes und weitere Längen in die Messung mit aufgenommen werden. Diese Werte werden mit den Werten der Templates in der Datenbank verglichen, bis man ein Template findet, dass ähnliche Proportionen aufweist.

Eine weitere einfache Methode ist das *Template-Matching* [Wächter01], bei dem charakteristische Teile des Gesichtes wie die Nase, die Augen oder der Mund aus dem Gesichtsbild ausgeschnitten werden und jeweils einzeln gegen eine Datenbank von Gesichtsausschnitten (den Templates) verglichen werden. Dabei werden die einzelnen Teile übereinander gelegt und die Anzahl der nicht übereinstimmenden Pixel gezählt. Je niedriger die Anzahl der Pixel, desto größer die Übereinstimmung der Bilder.

Abbildung 8: Ausschnitte des Gesichtes, die für das Template-Matching verwendet werden [Wächter01]

Das Elastic Bunch Graph Matching [Wächter01] ist ein Verfahren, bei dem auf über das Gesicht ein Netz gelegt wird, der sogenannte labeled Graph. Die Knoten dieses Netzes werden auf markante Stellen des Gesichtes gesetzt, so dass das Netz nicht radial oder rechtwinklig ist, sonde aus vielen einzelnen, verbundenen Strecken besteht, die verschieden lang sind. Ein solcher labeled Graph ist auf Abbildung 9 dargestellt. Die Längen und Winkel die die Verbindungslinien zueinander bilden sind für das Gesicht individuell, können also benutzt werden um die Ähnlichkeit von Gesichtern zu vergleichen. Bei einem Vergleich der Eingangsdaten eines Gesichtes m einer Datenbank ähneln sich die Gesichter am meisten, die die meisten ähnlichen Winkel und Längen in ihren Netzen enthalten.

Eines der etabliertesten Verfahren ist die Nutzung der Eigengesichter[j] [Petermann02], dabei wird das Gesicht in 100 bis 150 einzelne Bilder zerlegt, die auf verschiedene Weisen vereinfachte V sionen des ursprünglichen Bildes sind und die nun einfacher automatisiert mit anderen, bereit sich in der Datenbank befindlichen Eigengesichtern verglichen werden können. Einige Eigengesichtereines Gesichtes sind auf Abbildung 10 dargestellt.

Ein anderes, bereits im komerziellen Einsatz erprobtes Verfahren beruht darauf, dass von de beim Enrollment aufgenommenen Gesichtsbild ein Computerprogramm über 300 verschiede ausgeleuchtete Versionen des ursprünglichen Bildes erstellt [Guyot06]. Dabei wird ein Ray-tracing genanntes Verfahren eingesetzt, dass oft bei 3D-Animationen zum Einsatz kommt um Lich zu simulieren. Zusätzlich werden weitere 400 Bilder mit geringfügig unterschiedlichen Gesichts-

[j] Eigenfaces

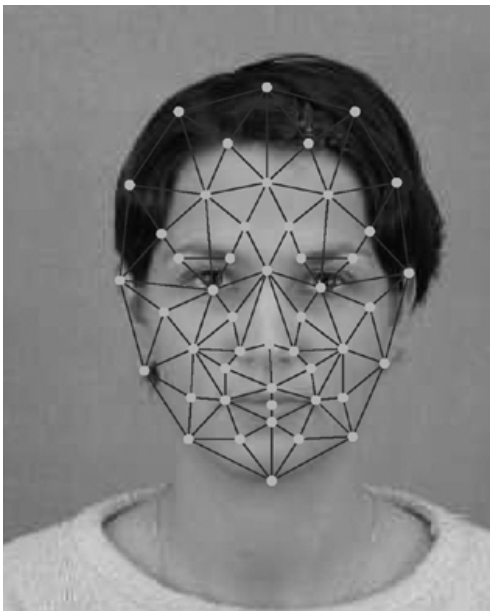

Abbildung 9: Der Labeled Graph am Gesicht angetragen [Boehringer06]

positionen generiert. Dies wird durch ein Modeling genanntes Verfahren erreicht, bei dem das Wache Bild des Gesichtes, die Textur, auf ein 3D-Modell gelegt wird. Dadurch ist es möglich, das während der Identifizierung aufgenommene Bild leicht mit den in der Datenbank vorhandenen Bildern zu vergleichen und die Person zu identifizieren.

3.2 Einsatzgebiete

Da das Gesicht recht groß ist, lässt es sich auch noch aus größerer Entfernung aufnehmen, oh dass die aufgenommene Person dies überhaupt merken muss. Somit eignet sich die Gesichts kennung perfekt zur Überwachung von Personen auch in größeren Menschenmengen.

Das Bundeskriminalamt testete von Oktober 2006 bis Januar 2007 am Mainzer Haptbahnhof d komerzielle Systeme zur Gesichtserkennung [Lange07]. Unter den täglich circa 22 000 Besuch des Bahnhofes war eine Gruppe von 200 bekannten Testpersonen, die von den Systemen erka werden sollte. Die besten Erkennungsraten wurden auf Rolltreppen erziehlt, wobei die Leute unbeweglt standen. Bei optimalen Lichtverhältnissen betrug die Erkennunsrate des besten Sy tems 70 Prozent, unter direkter Sonneneinstrahlung oder Dunkelheit sank sie jedoch auf 10 b 20 Prozent. Dieser Wert ist für automatisierte Fahndung natürlich nicht akzeptabel.

Obwohl das Bundeskriminalamt in nächster Zeit keine Pläne zur Bahnhofsüberwachung hat wäre der Einsatz eines biometrischen Überwachungsystems eine Möglichkeit die Fahnder a Bahnhof zu unterstützen. So sinkt die Aufmerksamkeit eines Fahnders, der das Bild von zwe

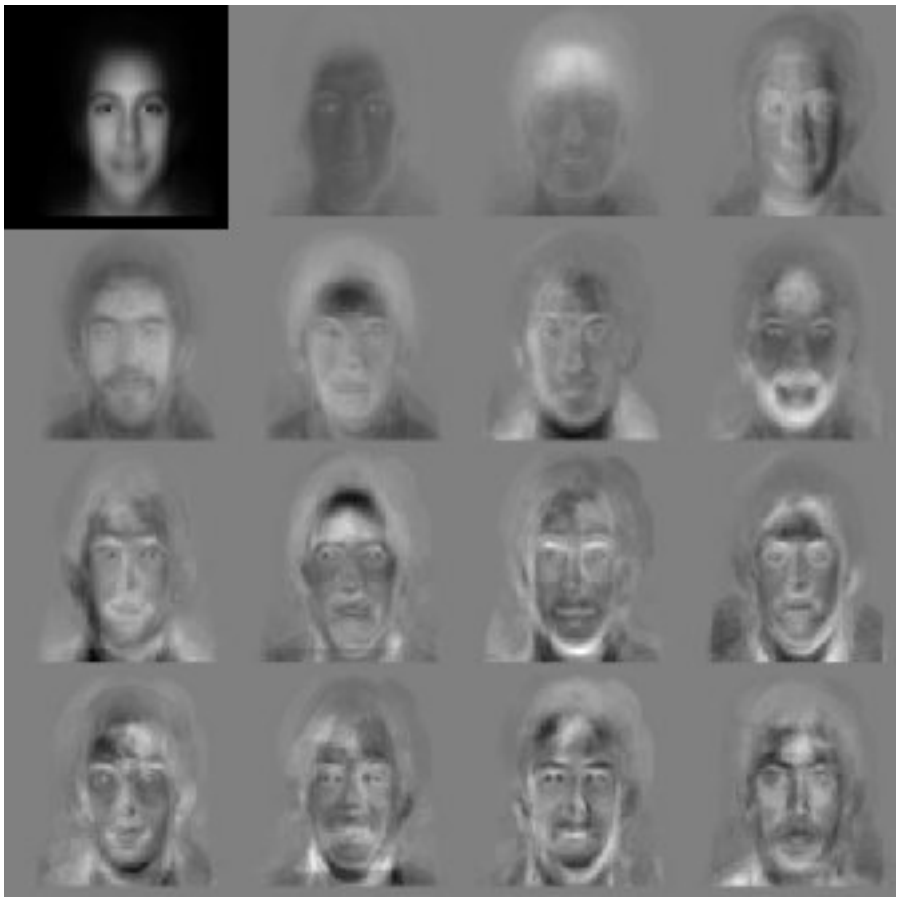

Abbildung 10: Eigenfaces [Petermann02]

Monitoren überwacht innerhalb von 12 Minuten um 50 Prozent, in 22 Minuten schon um 95 Pro-
zent. Ein halbautomatisches System mit einer großen FAR, dass bei Verdacht den Fahnder alar-
miert, so dass der er diesem Hinweis nachgehen kann könnte die Effektivität der Personensuche
stark erhöhen.

Ein weiteres Einsatzgebiet für biometrische Gesichtserkennung sind Spielecasinos [Lange0
Nach einem Urteil des Bundesgerichtshofes sind Casinobetreiber verpflichtet, Spielsüchtige am Spiel zu
hindern. Einige Casinos bieten es daher an, sich für eine „freiwillige Selbstsperrung“ biometrisch
erfassen zu lassen. Dadurch können die Überwachungssysteme des Casinos die gesperrten P
sonen im Falle eines erneuten Besuches schnell erkennen und das Personal auf diese Perso
aufmarksam machen. Das Personal kann nun die freiwillig gesperrte Person nach draußen bi
ten.

3.3 Fälschungen

Die Überwindung simpler Gesichtserkennungssysteme gestaltet sich äußerst einfach, da sich d
Systeme oft schon durch Fotos a
Vgen oder Videos von Gesichtern täuschen lassen. Daher ist es
wichtig, dass der Identifizierungsvorgang durch Personal überwacht wird oder eine Lebender-
kennung einzusetzen. Eine Lebenderkennung kann Augen- oder Lidbewegungen vorraussetze
sowie zum Schutz vor Videoatrappen die Bewegungen des Kopfes sowohl optisch als auch the
misch mit Infrarotkameras aufnehmen und feststellen, ob sie zueinander passen.

Abbildung 11: Das Thermogramm eines Gesichtes [Petermann02]

4 Iriserkennung

Von den vielen physiognomischen Möglichkeiten Menschen zu identifizieren ist die Erkennung anhand der Regenbogenhaut (Iris) die genaueste, da die Iris die komplexeste, äußerlich messbare Zufallsstruktur des Körpers ist [Guyot06]. Jedoch ist ihre Messung nicht ganz so einfach, denn die Iris befindet sich hinter der Hornhaut des Auges, wird teilweise vom Lid verdeckt und ist zudem ein kleines Detail des Körpers.

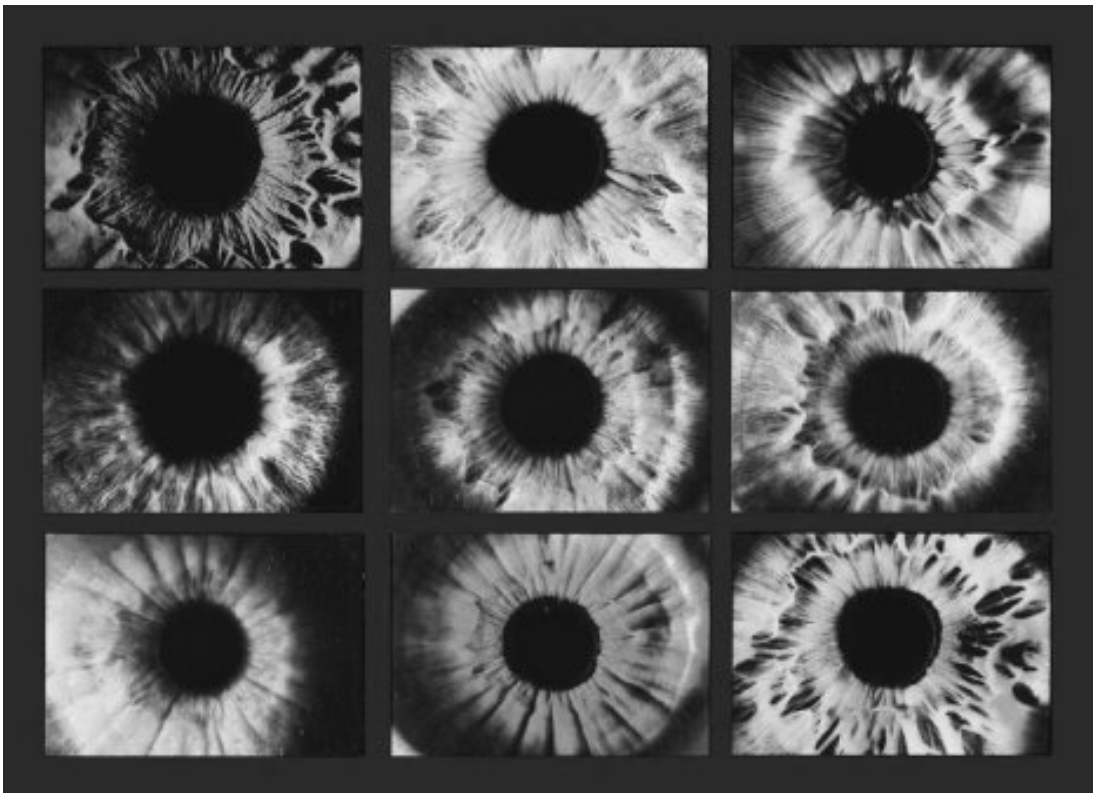

Abbildung 12: Verschiedene, sehr unterschiedliche Iriden [Petermann02]

4.1 Messung

Die Iris besteht aus einer Vielzahl von einzelnen Merkmalen, die biometrisch ausgewertet können. So werden die Corona, Krypten („Crypts“), Fasern, Flecken („Freckles“), Narben, Radiale Furchen („Radial Furrows“) und Streifen unterschieden. Die Farbe hingegen bleibt unberücksichtigt [Petermann02].

4.1.1 Bildaufnahme

Die Iris ist ein kleines Objekt mit ungefähr einem Zentimeter Durchmesser. Aufgrund dessen, dass die Iris vergleichsweise dunkel ist, muss sie zusätzlich ausgeleuchtet werden, um ein ausreichend detailreiches Bild zu bekommen. Dabei darf die Beleuchtung aus Gründen des Augenschutzes nicht zu grell sein.

Es gibt zwei Methoden Bilder der Iris aufzunehmen. Die aktive Methode erfordert, dass das Auge weniger als 50 cm von der Kamera entfernt ist – üblich zwischen 15 und 35 cm. Der passive Ansatz erfordert nur, dass der zu identifizierende Mensch ruhig in einem Abstand von 30 bis 100 cm steht und in die Kamera blickt. Das aktive System muss also zusätzlichen Aufwand betreiben, um auf dem aufgenommenene Bildausschnitt das zu analysierende Auge zu finden. Entgegen der verbreiteten Annahme benutzt man zur Iriserkennung keine Laser, sondern optische Kameras, daher sind keine Augenschäden zu erwarten.

Beide Ansätze setzen 8-Bit Videokameras[k] ein, welche auch verwendet werden können um auch eine Lebendanalyse durchzuführen. Die Lebendanalyse der Iris beruht auf der Analyse der „Hippus“-Bewegung, einer geringfügigen, periodischen Iriskontraktion die mit 0,5 Herz auftritt.

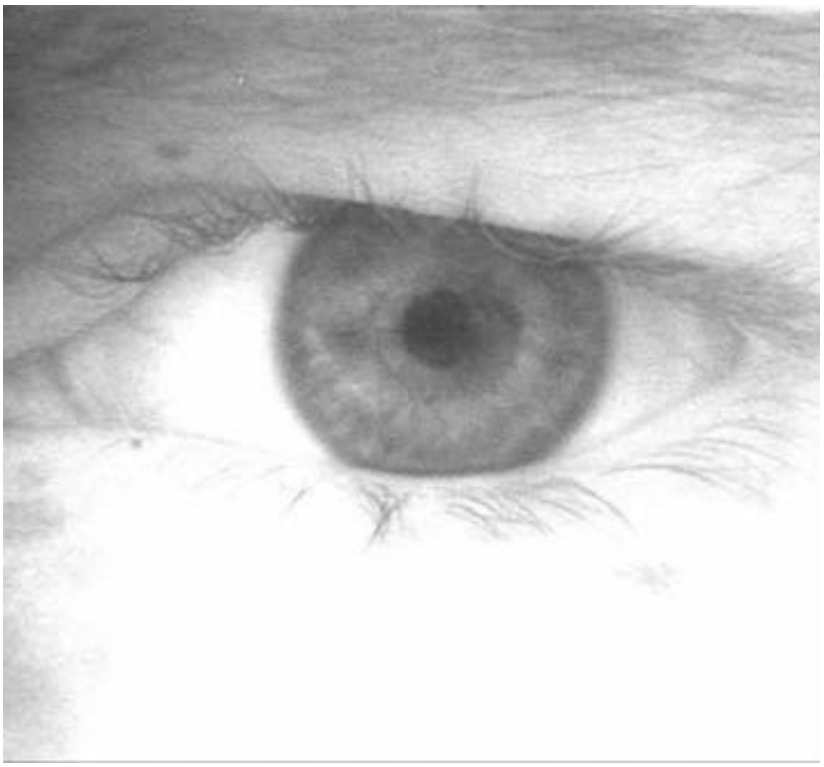

Abbildung 13: Ein aufgenommenes Auge [Wayman05]

[k] mit $2^8 = 256$ Graustufen

Unabhängig von der Aufnahmemethode wird aus einer Sequenz von Videobildern ein einzelne
Bild ausgewählt, dass weiter analysiert werden kann.

4.1.2 Irisfindung

Unabhängig davon, wie gut das aufgenommene Bild ist, beinhaltet es auch immer Teile de
Gesichtes ebenso wie die Augenlider mit Wimpern die für die Analyse irrelevant sind. Daher
müssen alle unnötigen Teile des Bildes gelöscht werden. Dazu verwendet man einen Algorith
mus, der unter Einbezug verschiedener Faktoren wie Intensität oder Kontrast bestimmen kann
ob ein Bildpunkt zur Iris gehört oder nicht. Dieses Verfahren wurde angewendet, um die Iris in
Abbildung 14 aus Abbildung 13 zu extrahieren. In dieser Phase kann auch ein als Machine Vi-
sion bekanntes Verfahren zum Einsatz kommen, welches Bildteile anhand von ihren Konturen
zu erkennen versucht. Dabei wird im Falle einer Iris die Kontur eines kleinen grob runden Kör-
pers angegeben, der gegebenfalls oben und unten wegen der Augenlider abgeflacht ist und innen
einen weiteren runden Körper enthält, die Pupille. Das Machine Vision-Verfahren kann nun die
auf dem Bild vorhandenen Konturen suchen und die Iris lokalisieren.

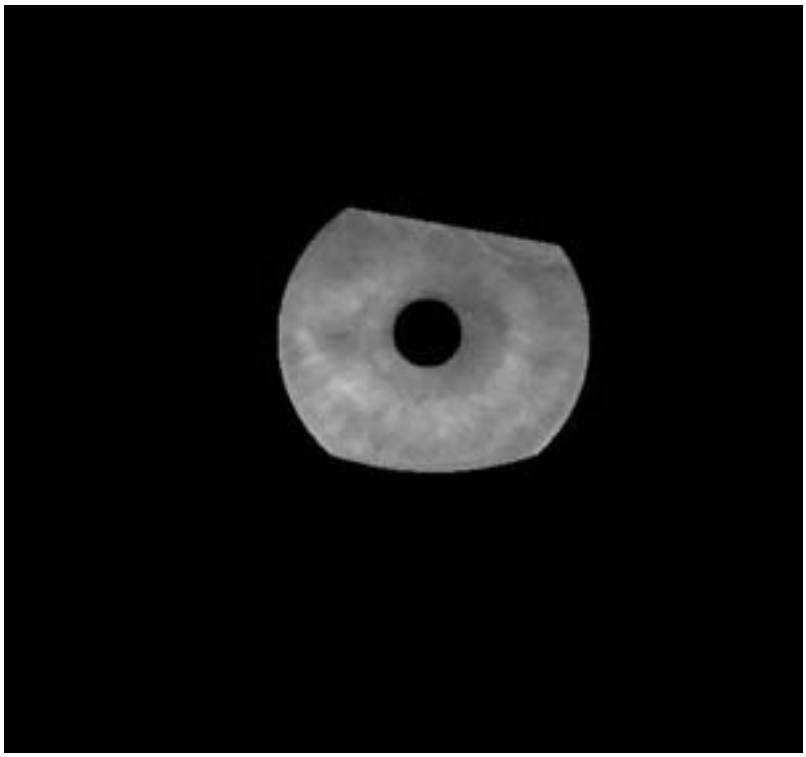

Abbildung 14: Die extrahierte Iris [Wayman05]

4.1.3 Identifikation

Nachdem die Iris gefunden wurde, ist es nötig die Iris auf eine feste Größe zu skalieren, da di
zu identifizierende Person unterschiedlich weit von der Kamera entfernt stehen konnte. Danach
wird die Anzahl der übereinstimmenden Bildpunkte zwischen dem aufgenommenen Bild und
dem Referenzbild berechnet. Dies ist der sogenannte Hammingabstand, der für ein Paar von
Bildern einen bestimmten Wert besitzt. Je niedriger der Abstand, desto ähnlicher sind sich di
Bilder und desto größer ist die Wahrscheinlichkeit einer Übereinstimmung.

Für eine effektive Identifizierung bleibt zu entscheiden, auf welchen Wert des Hammingabstan-
des die Entscheidungschwelle anzusetzen ist. Je nach Schwelle kann das System das aufgen
mene Bild der Iris mit einem in der Datenbank hinterlegtem Iris-Template als übereinstimmend
erklären oder aber es als unterschiedlich verwerfen.

4.2 Einsatzgebiete

Durch ihre hohe Individualität und ihre geringe Veränderung während des Lebens ist die Iris
ein gerne verwendetes biometrisches Merkmal um die Identität einer Person zu verifizieren.
Das größte biometrische System zur Iriserkennung ist am Flughafen in Abu Dhabi installiert
[Guyot06], wo sich jeder Reisende biometrisch ausmessen lassen muss. Dabei wurden inzw
schen schon 850 000 Templates erstellt und in die Datenbank aufgenommen. Durch die do
durchgeführten Kontrollen konnten schon mehrere tausend illegale Einwanderer mit gefälschten
Pässen an der Einreise gehindert werden.

4.3 Fälschungen

Es wurde schon oft versucht das Iriserkennungsystem in Abu Dhabi zu umgehen. Die einfachst
Möglichkeit, die Nutzung von Fotografien und Videos wird durch das Überwachungspersonal
und die Lebenderkennung verhindert. Die Lebenderkennung verhindert auch die Nutzung von
speziell bemalten Kontaktlinsen, die Irismuster tragen.

Jedoch bleibt die Möglichkeit von Manipulationen am Auge selbst. Es ist möglich, pupillenwei-
tende Augentropfen zu verwenden, um zu versuchen das System zu verwirren. Das in Abu Dhab
eingesetzte System konnte so erweitert werden, dass es geweitete Pupillen erkennt und die Ide
tifizierung verweigert [Guyot06]. Daraufhin muss die Person etwa zwei bis drei Stunden warten,
bis sich die Pupille wieder normalisiert hat, bevor sie korrekt identifiziert werden kann.

4.4 Zukünftige Entwicklung

Die Iriserkennung ist bisher weit davon entfernt vollständig ausgereizt zu sein. Das heutzutage verwendete Stop-and-Stare-Verfahren ist nur bei Kooperation der zu identifizierenden Person möglich. Daher konzentriert sich die weitere Forschung darauf die Iriserkennung schneller zu machen und vor allem die Entfernung zwischen Auge und Kamera zu vergrößern [Guyot06]. Das Projekt Iris on the Move hat sich zum Ziel gesetzt, Personen zu erkennen die sich mit 1 Meter pro Sekunde bewegen und 3 Meter von der Kamera entfernt sind.

5 Der ePass

Der vor einiger Zeit in Deutschland eingeführte Elektronische Reisepass, kurz ePass, ist die bislang größte, bekannteste und auch kontroverseste Biometrie-Anwendung in der Bundesrepublik Deutschland ist jedoch nicht das einzige Land, welches elektronische Reisepässe einsetzt. E Pionierrolle spielte bei der Einführung von elektronischen Reisepässen Malaysia, wo elektroni sche Reisepässe zum ersten Mal eingeführt wurden und wo das System schon seit einigen Jah eingesetzt wird [Starbug07].

Abbildung 15: Der RFID-Chip im ePass [BMI07]

5.1 Gründe für den ePass

Der ePass ist wie viele andere Techniken dazu gedacht, administrative und strafrechtlichen Vo gänge zu vereinfachen. Zu den offiziellen Gründen des ePasses zählen laut [Starbug05]:

- Biometrie als zusätzliches Sicherheitsmerkmal des Passes
- Bestätigung der Identität des Inhabers

- Grenzkontrolle durch Computer
- Unterstützung bei Personenfahndung

Besonders der letzte Punkt wird von den Befürwortern der ePässe als wichtigstes Argument ge
nannt. Der ePass wurde als Konsequenz und zur Vorbeugung von Terroranschlägen in mehrere
Phasen eingeführt:

- 2002: Terrorismusbekämpfungsgesetz
- 2005: Beschluss zur Einführung von Biometrie im Reisepass und entsprechende Änderung
  des Passgesetzes
- 2005: Einführung der ePässe mit biometrischen Gesichtsbild
- 2007: Einführung der ePässe mit Fingerabdrücken.

5.2 Technik

Der deutsche ePass entspricht dem vorherigen Deutschen Reisepass, der bereits gut gegen
schungen gesichert war [Starbug06]. Zusätzlich ist im ePass ein sogenannter RFID-Chip[1]
baut, auf dem biometrische Merkmale des Besitzers gespeichert werden. RFID-Chips sind m
einer Antenne ausgerüstet und beziehen ihre zur Arbeit notwendige Energie per Funk. Übe
diese Antenne sind sie auch in der Lage zu senden. Das ermöglicht das kontaktfreie Ausle
sen der darauf gespeicherten Daten. Der im ePass eingesetzte Chip arbeitet auf einer Freque
von 13,56 MHz und hat eine theoretische Reichweite von 10 Zentimeter, um das Auslesen nu
aus der Nähe zu ermöglichen. Zusätzlich besitzt der Chip einen kryptografischen Coprozessor,
welcher für die Verschlüsselung verwendet wird, sowie einen Zufallszahlengenerator. Letzte-
rer ist notwendig, um die einzigartige ID-Nummer des Chips bei jedem Auslesen zu ändern
[Starbug05]. Andernfalls ist es mittels eines RFID-Empfängers möglich, die Position des Pass
zu verfolgen und somit auch den Inhaber. Die Firma Flexilis zeigt anhand von US-Pässen, dass d
Verwendung gleicher ID-Nummern sogar den Bau automatischer Schussanlagen möglich mac
[MahaLey06].

Die auf dem Chip gespeicherten Daten sind in verschiedene Datengruppen aufgeteilt; die wich
tigsten sind:

- Datengruppe 1: Die Daten, die auch aufgedruckt sind, unter anderem Name, Staatsange
  hörigkeit, Pass-ID

[1] Radio Frequency Identification

- Datengruppe 2: Gesichtsbild
- Datengruppe 3: Fingerabdrücke
- Datengruppe 4: Irisbilder

Dabei waren die Datengruppen 1 und 2 bereits seit der Einführung des Passes verpflichtend, während Gruppe 3 hingegen erst seit dem 1. November 2007 [Starbug07]. Die Daten werden mit Hilfe eines asymetrischen Verschlüsselungsverfahrens nach ECDSA signiert, so dass Veränderungen der Daten bei einer Kontrolle sofort auffallen.

Die Passdaten werden dabei von dem Schlüssel der Bundesdruckerei signiert, der alle drei Monate geändert wird. Dieser Schlüssel wird wiederrum durch den Schlüssel des Bundesamtes für Sicherheit in der Informationstechnik (BSI) signiert, der alle drei bis fünf Jahre geändert wird. Dieser Aufbau ist vergleichbar mit bereits bewährten Systemen wie OpenPGP[m] oder TLS[n]. Die „Private Keys“[o] werden oft gewechselt, weil bei einem Bekanntwerden der Schlüssel es möglich wäre, die elektronisch gespeicherten Daten zu fälschen. Durch den Wechsel stellt man sicher, dass selbst wenn ein Schlüssel bekannt werden sollte, dass dann nur eine bestimmte Serie von ePässen gefälscht werden kann.

Da die Daten des Passes über Funk übertragen werden, ist die Übertragung symmetrisch verschlüsselt, wobei die Daten der Maschinenlesbaren Zone (Machine Readable Zone, MRZ) als Passwort verwendet werden. Die Maschienenlesbare Zone ist ein international standarisiertes Feld des Passes auf dem die Daten des Inhabers auf eine leicht für Maschinen lesbare Weise aufgedruckt sind. Abbildung 16 zeigt die MRZ eines australischen ePasses.

Das biometrische Merkmal der Datengruppe 2 ist das Gesichtsbild, für das Enrollment des Gesichtsbildes wird das Passfoto des ePasses verwendet [Starbug05]. Dazu müssen seit der Einführung des ePasses die Passfotos strengen Vorgaben genügen um die Bilder biometrisch auswertbar zu machen. So muss es sich um ein Frontalfoto handeln, auf dem das Gesicht eine bestimmte Größe haben muss, die Person nicht lächeln darf, der Kontrast und die Ausleuchtung stimmen müssen [BDR05]. Bei einer Kontrolle wird das Gesicht über Gesichtsmetrik mit dem auf dem Pass gespeicherten Referenzbild verglichen.

Die Datengruppe 3 enthält Abdrücke eines Fingerpaares, wobei bei der Erstaufnahme die Zeigefinger bevorzugt werden. Falls diese nicht verfügbar sind oder ihre Abdrücke eine zu schlechte Qualität bieten ist es auch möglich die Mittelfinger, Ringfinger oder Daumen zu verwenden.

---

[m] Open Pretty Good Privacy – Ein etabliertes, sicheres Verfahren zur Verschlüsselung von Computerdaten

[n] Transport Layer Security – auch als SSL bekannt, wird bei der Verschlüsselung von Webseiten verwendet

[o] „Persönliche Schlüssel“ – diese Schlüssel dürfen niemals öffentlich bekannt werden, da sonst das Sicherheitskonzept nicht mehr greift

Abbildung 16: Maschinenlesbare Zone in einem australischen ePass [DFAT07]

Die kleinen Finger werden von einer Aufnahme in den ePass immer ausgeschlossen, da sie e
ne zu kleine biometrisch verwertbare Fläche haben. Wenn jedoch die Qualität aller Fingerpaar
zu schlecht ist, wird das Paar mit der besten Qualität verwendet. Zur Fingerabdruckkontrolle
werden die Pappilarlinienenden und -verzweigungen – die Minuzien hergezogen.

Für die zukünftige Verwendung von Iriserkennung ist bereits die Datengruppe 4 auf dem Chip
reserviert, weitere Verfahren wie 3D-Gesichtsbilder können in Zukunft mit geringem Aufwand
in weiteren Datengruppen eingeführt werden.

5.3 Kritik am ePass

Der von den Befürwortern angegebene Grund der Terrorismusbekämpfung wird von Kritikern
mit der Aussage gekontert, dass die Terroristen durchaus gültige Pässe besaßen [Starbug0
Auch wird von ihnen hervorgehoben, dass die Sicherheitsmerkmale des normalen deutsche
Passes schon ausreichend gewesen seien um gute Fälschungen zu verhindern. Argumente ge
den ePass gibt es auch aus technischer Sicht, denn obwohl die Pässe zwar 10 Jahre gültig s
wird die Lebensdauer der RFID-Chips auf zwei bis drei Jahre geschätzt [Starbug05]. Zudem i
es möglich – sofern man die Daten der MRZ kennt oder erraten kann[p] – einen Chip sogar aus
10 Meter Entfernung auszulesen. Die Kommunikation zwischen Chip und Leser ist sogar noc
aus 30 Meter Entfernung abhörbar. Das erlaubt es wiederrum auf bestimmte Pässe programmie

[p] Aufgrund dessen dass viele Werte der MRZ wie das Geburtsdatum abgeschätzt werden können, ist es durchaus möglich die MRZ mit Hilfe von Computern schnell zu ermitteln

Bomben zu bauen. Dies funktioniert auch mit zufälliger ID-Nummer, da die Kommunikation, nachdem sich mit der MRZ als Passwort entschlüsselt wurde, alle nötigen Daten enthält, um einen Pass und somit auch die Person zu erkennen.

Auch das Enrollment der Fingerabdrücke im Meldeamt ist nicht ganz unproblematisch. In Vorversuchen in Meldeämtern kam es öfters schon zu Problemen mit circa 40 jährigen Personen, weil ihre Fingerabdrücke zu undeutlich waren um ein ausreichend gutes Template zu erstellen. Gleiches gilt für Personen, die zu Berufsgruppen gehören, die viel mit ihren Händen arbeiten [Starbug07].

Die digitale Übertragung der Daten vom Meldeamt zur Bundesdruckerei verspricht zwar schnellere Anfertigung, kann aber auch als weiterer Schwachpunkt gesehen werden. Die aufgenommenen Daten können über das Internet verschickt werden, teilweise auch in E-Mails [Starbug07]. Wenn der Mailversand nicht entsprechend absichert ist, wird es möglich diese Mails abzufangen, zu lesen oder zu verändern.

Kritiker befürchten auch, dass der ePass ein Schritt auf dem Weg zum „Gläsernen Bürger" ist, da es in Zukunft möglich wäre, die auf dem Pass gespeicherten Gesichtsbilder mit einer großen Videoüberwachung zu koppeln und somit umfassende Bewegungsprofile zu erstellen. Wie in Abschnitt 3.2 beschrieben, sind die heutzutage eingesetzten Verfahren jedoch noch nicht ausreichend zuverlässig für eine umfassende Überwachung.

Die von dem ePass zusätzlich gebotene Sicherheit ist ebenso fragwürdig, da die auf dem Pass gespeicherten Daten keinen Mindestqualitätskriterien genügen müssen. Die Pässe bleiben auch mit kaputten RFID-Chip gültig, somit kann es sein, dass die Pässe keinerlei Sicherheitsvorteile geben. In diesem Fall ist das Passbild sogar weniger sicher als das des alten Passes, da sich Grenzkontrolleure an der Form des Ohres orientieren konnten, welches auf dem biometrischen Passfoto gar nicht mehr sichtbar sein muss.

Der eigentliche Zweck des ePasses, behaupten Kritiker, ist die Förderung der deutschen Biometrieindustrie. Der Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. Bitkom schätzt, dass der biometrische Markt allein in Deutschland von 120 Millionen Euro im Jahr 2006 auf 300 Millionen Euro im Jahr 2010 steigen wird [Lange07]. Ebenso ist es noch unbekannt, wie viel der Wechsel zum ePass den Staat und den Steuerzahler insgesamt kosten wird. Somit existieren einige noch nicht geklärte wirtschaftliche Fragen, auf die es bisher noch keine Antworten gibt.

5.4 Vermeidung

Da die ePässe auch mit kaputten biometrischen Chips noch gültig sind [Starbug05] [BMI07], is es möglich den Chip vorsätzlich zu zerstören um sich vor Datendiebstahl zu schützen. Der Chi ist ein recht empfindliches Gerät, also gibt es verschiedene Möglichkeiten ihn zu beschädigen. Eine einfache aber effektive Art ist, mit einem starken Sender wie einem Mikrowellenherd genug Energie zu induzieren um den Chip zu schmelzen. Ebenso kann man durch mehrmalige Biegen des Umschlages die Antenne des RFID-Chips abbrechen[q]. Zu bedenken jedoch ist, dass der Pass Staatseigentum ist und man sich der Beschädigung von Staatseigentum schuldig mac Eine nicht-destruktive Weise den Pass vor dem Auslesen zu schützen ist das Einlegen von Alu miniumfolie in den Pass. Diese Folie stört die Funksignale ausreichend, um ein unbemerkte Auslesen zu verhindern. US-Pässe haben bereits Aluminiumfolie in dem Umschlag eingearbe tet, welche bei geschlossenem Pass das Auslesen verhindert. Für deutsche ePässe gibt es be entsprechende Schutzhüllen zu kaufen[r].

Eine nicht technische Umgehungsmethode ist die Vermeidung von ePässen. Es ist derzeit mö lich, sich temporäre Reisepässe ausstellen zu lassen die ohne biometrische Merkmale ausges werden. Diese Pässe sind jedoch nur 1 Jahr gültig.

Jedoch wird gegen die biometrische Datenerfassung auch auf Rechtswege vorgegangen, so der bochumer Rechtsanwalt Michael Schwarz eine Klage gegen die Ordnungsbehörde der Sta Bochum eingereicht [Schwarz07]. Es wird argumentiert, dass die verpflichtende Aufnahme dieser Daten gegen das Recht auf Informationellen Selbstbestimmung verstößt, das es jedem ermöglicht über die Verwendung seiner personenbezogenen Daten – in diesem Fall seiner personeng bundenen Körpermetriken – selbst zu bestimmen.

[q] Was auch unbeabsichtigt passieren kann, da der Umschlag des ePasses biegsamer ist als der des alten Passe

[r] Der Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V., FoeBuD bietet in dessen Online-Shop schon seit längerer Zeit solche Hüllen an

Quellenverzeichnis

[BDR05] Bundesdruckerei GmbH (2005), „ePass Foto-Mustertafel“, <http://www.bundesdruckerei.de/de/behoerde/epass/index.html> [Stand: 20. Januar 2008]

[BMI07] Bundesministerium des Innern: „Fragen und Antworten zum ePass allgemein“, <http://www.bmi.bund.de/cln_028/nn_1084000/Internet/Content/Themen/PaesseUndAusweise/Einzelseiten/Biometrie__FAQ.html> [Stand: 19. Januar 2008]

[Boehringer06] Boehringer, Stefan; Vollmar, Tobias; Tasse, Christiane; Wurtz, Rolf P.; Gillessen-Kaesbach, Gabriele; Horsthemke, Bernhard; Wieczorek, Dagmar (2006): „Syndrome identification based on 2D analysis software“, <http://www.nature.com/ejhg/journal/v14/n10/full/5201673a.html> [Stand 19. Januar 2008]

[Cavalli-Sforza74] Cavalli-Sforza, Luigi: „Biometrie – Grundzüge biologisch-medizinischer Statistik“, Stuttgart 1974

[DFAT07] Australian Government – Department of Foreign Affairs and Trade (2007): „The Australian ePassport“, <http://www.dfat.gov.au/dept/passports/> [Stand: 19. Januar 2008]

[Guyot06] Guyot, Laurent: „Les temps des Biomaîtres / Biometrie – Fingerprint und Irisscan“, ARTE France 2006

[Lange07] Lange, Barbara: „Aktuelle Kamera – Gesichtserkennung im Dienst der Fahndung“, iX 10/2007

[MahaUey06] Mahaley, Kevin (2006): „United States e-Passport Shield Failure Vulnerability“, <http://www.flexilis.com/epassport.html> [Stand: 22. Januar 2008]

[Petermann02] Petermann, Thomas; Sauter, Arnold: „Biometrische Identifikationssysteme – Sachstandsbericht“, Berlin 2002

[Petermann03] Petermann, Thomas; Scherz, Constanze; Sauter, Arnold: „Biometrie und Ausweisdokumente: Leistungsfähikgkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung – Zweiter Sachstandsbericht“, Berlin 2003

[Schwarz07] Schwarz, Michael: „Klage des Rechtsanwalts Michael Schwarz gegen di Ordnungsbehörde der Stadt Bochum als Passbehörde wegen Erteilung eines Reisepasses“, Bochum 2007, <http://www.foebud.org/datenschutz-buergerrechte/biometrie/klage-fingerabdruecke.pdf>

[Starbug05] starbug (2005): „Die Technik im neuen ePass / Der ePass – ein Feldtest“

[Starbug06] starbug; Kurz, Constanze (2006): „Elektronische Reisedokumente – Neue Entwicklungen beim ePass“

[Starbug07] starbug; Kurz, Constanze (2007): „Meine Finger gehören mir – Die nächste Stufe der biometrischen Vollerfassung“

[Wayman05] Wayman, James; Jain, Anil; Maltoni, Davide; Maio, Dario: „Biometric Systems – Technology, Design and Performance Evaluation“, London 2005

[Wächter01] Wächter, Carsten; Römer, Stefan (2001): „Gesichts-Erkennung I“, <http://www.informatik.uni-ulm.de/ni/Lehre/WS01/HS-Biometrische-Systeme/ausarbeitungen/Gesichtserkennung_1_block.pdf> [Stand: 11. Januar 2008]

Erklärung

Ich erkläre hiermit, dass ich die Facharbeit ohne fremde Hilfe angefertigt und nur die im Quellenverzeichnis angeführten Quellen und Hilfsmittel benutzt habe.

Ich bin damit einverstanden, dass diese Facharbeit in der Lehrer- und Kollegiaten-Bücherei veröffentlicht wird.

Neufahrn, den 24. Januar 2008

_____

Unterschrift des Kollegiaten