SEMINARARBEIT

Biometrische Systeme und Fingerabdruckerkennung

durchgeführt am

Fachbereich für Computerwissenschaften

der

Universität Salzburg

vorgelegt von

Florian Kinzinger

Rafael Heil

Betreuer: Univ.-Prof. Dr. Wolfgang Pree

Salzburg, Februar 2008

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

Ein in immer mehr Bereichen des täglichen Lebens stetig anwachsender Bedarf nach eindeutiger Identitätsfeststellung und persönlicher Authentifizierung wirft ein immer stärker werdendes Licht auf den Bereich und die Funktionsweise biometrischer Systeme. Angefangen im Bereich von Zutritts- Kontrollsystemen für sensible Bereiche in großen Firmen, haben sich biometrische Systeme mittlerweile schon in die privaten Haushalte durchgerungen, wo sie teilweise Passwörter ersetzen, um z.B. Benutzer an Computersystemen anzumelden oder verschlüsselte Daten von internen oder externen Datenträgern freizugeben. Neben solchen Authentifizierungsaufgaben werden biometrische Erkennungssysteme einstweilen auch verstärkt eingesetzt, um überwachungstechnische Aufgaben zu vereinfachen, verdächtige Personen vorzeitig zu erkennen, und darauf rechtzeitig Maßnahmen setzen zu können. Im forensischen Bereich spielt die Identifizierung anhand der Desoxyribonukleinsäure (DNA) schon länger eine große Bedeutung, um Personen eindeutig zu identifizieren.

All diese verschiedenen und breit gestreuten Anwendungsbereiche für Biometrische Systeme und Erkennungsverfahren, sowie die stetig wachsende wirtschaftliche Bedeutung dieses Teilgebietes, welches medizinische und technische Erkenntnisse verbindet, bieten eine spannende Basis für das Erstellen folgender Seminararbeit.

1.2 Aufbau und Gliederung der Arbeit

Der erste Teil dieser Arbeit gibt eine kurze Einführung in den Bereich der Biometrie und beinhaltet grundlegende Informationen zu den verschiedenen Möglichkeiten, Anwendungsbereichen und Verfahren. In dem darauffolgenden Kapitel wird genauer auf den Fingerabdruck als Identifikationsmerkmal eingegangen. Es werden die damit verbundenen Technologien, Schwierigkeiten und Chancen gelistet. Abschließend wird ein kurzer Einblick in zukünftige Systeme, noch zu lösende Problemstellungen, sowie weiterzuentwickelnde Technologien und deren Möglichkeiten gegeben.

2 Grundlagen biometrischer Systeme und Verfahren

2.1 Allgemeines

Zuverlässige biometrische Systeme und Erkennungsverfahren mit den Eigenschaften eine verlässliche Identitätsfeststellung anhand der gegebenen biometrischen Merkmale zu gewährleisten, lösen immer häufiger die im letzten Jahrhundert entwickelten Methoden und Systeme ab. War es früher üblich solche Bereiche mittels Smartcard und/oder persönlichem Zugangscode zu schützen, setzt man aktuell verstärkt auf semi- bzw. vollautomatische Systeme, welche individuell spezifische biometrische Merkmale auslesen und verarbeiten können. Mit einer solchen Identitätsprüfung anhand von körperlichen Merkmalen soll dem altbekannten Problem des Diebstahls von Zutritts-Karten, bzw. den immer populärer werdenden Methoden von Passwort Phishing und Sniffing vorgebeugt werden. Oberstes Ziel hierbei ist es, nicht berechtigten Personen den Zutritt zu verweigern. Neben dieser Hauptaufgabe muss jedoch gleichzeitig sichergestellt werden, dass autorisierte Personen mit einem hohen Prozentanteil korrekt erkannt werden.

2.2 Funktionsweise biometrischer Systeme

Grundlegend kann man die Identifikation mittels biometrischer Systeme in zwei Aufgabengebiete gliedern. Neben der „Positiverkennung“, welche die Identifikation und Verifizierung des eingelesenen Merkmals anhand eines bereits im System vorhandenen Templates durchführt, existiert die Methodik der „Falscherkennung“. Hier wird ein eingelesenes Merkmal anhand einer Datenbank abgeglichen und eine positive Falscherkennung festgestellt, sollte kein Treffer gefunden werden.

Mittels der Positiverkennung lassen sich somit Systeme realisieren, welche eine positive Wiedererkennung von im System gespeicherten Personen voraussetzen. Voraussetzung hierfür ist ein einmaliges Erstellen des sogenannten Templates und die damit verbundene Speicherung von persönlichen Daten zu diesem Template.

Die Falscherkennung ist eine Methode, welche mit herkömmlichen Mitteln nicht oder nur sehr schwer realisiert werden kann. Nur mittels Abgleichen von individuellen Merkmalen einer Person ist dies ohne große Umstände machbar. So kann z.B. ein solches System im Sozialbereich eingesetzt werden, wo es sicherstellt, dass die aktuelle Person in der Vergangenheit noch keine Leistungen bezogen hat, und somit Missbrauch verhindert. Tabelle 2.1 stellt die wichtigsten Unterscheide zwischen diesen zwei Funktionsweisen detailliert dar.

Positiverkennung	Falscherkennung
Verifiziert die Person als dem System bekannt	Verifiziert die Person als dem System unbekannt
Verhindert, dass unterschiedliche Benutzer eine einzige Identität annehmen können	Verhindert mehrfache Identitäten eines einzigen Benutzers
Weist das eingelesene Merkmal einem bereits gespeicherten Template zu (eins-zu-eins)	Abgleich des eingelesenen Merkmals mit allen, bereits im System befindlichen Templates (eins-zu-vielen)
Falsche Zuweisung führt zu einer fehlerhaften Akzeptanz	Falsche Zuweisung führt zu einer fehlerhaften Abweisung
Falsche Nichterkennung führt zu einer fehlerhaften Abweisung	Falsche Nichterkennung führt zu einer fehlerhaften Akzeptanz
Manipulation mittels Übermittlung vorgetäuschter biometrischer Merkmale einer anderen Person an das System	Manipulation durch Übermittlung keiner oder veränderter Merkmale an das System

Tabelle 2.1 Vergleich Positiverkennung vs. Falscherkennung[1]

2.3 Charakterisierung biometrischer Identifikationsmerkmale

Erst individuelle und gut charakterisierbare Merkmale ermöglichen eine biometrische Identifikation. Das wohl zur Zeit am häufigsten verwendete Merkmal ist der Fingerabdruck. Aber auch andere Systeme, die sich auf Identifikationsmerkmale wie Iris, Handfläche, Stimme oder das gesamte Gesicht verlassen, finden schon praktischen Einsatz. Um die Qualität der einzelnen biometrischen Identifikationsmerkmale zu bestimmen, ist es im Allgemeinen üblich, die Charakterisierung in fünf verschiedenen Punkten vorzunehmen. [1] [2]

Robustheit

- Eigenschaft, sich auch über längere Zeit nicht zu verändern.

Gemessen über die Nichterkennungsrate (Typ 1 Fehler) beinhaltet dieses Charakteristikum die Wahrscheinlichkeit, dass die Daten des aktuell eingelesenen Merkmals nicht mit dem vom System erzeugten Template übereinstimmen.

Unterscheidungskraft

- Einzigartigkeit, und deutliche Variationen zwischen einzelnen Individuen.

Mit der Unterscheidungskraft wird die Tatsache der fehlerhaften Zuordnung zu einem falschen Template (Typ 2 Fehler) beschrieben. Sie beinhaltet die Wahrscheinlichkeit, dass ein eingelesenes Merkmal einem Template einer anderen Person zugeordnet wird.

Verfügbarkeit

- Das Merkmal sollte möglichst bei jedem Individuum vorhanden sein. Im Idealfall kommt es sogar mehrmals vor.

Um die Identifikation mittels eines biometrischen Systems für eine gesamte Spezies (auch innerhalb der Tierwelt) zu ermöglichen, ist es notwendig, dass die zu bestimmenden Merkmale bei jedem Individuum dieser Spezies vorhanden sind. Da allerdings nicht ausgeschlossen werden kann, dass einzelne Merkmale anhand von Unfällen oder Kämpfen zerstört und unbrauchbar gemacht werden, ist ein mehrmaliges bzw. redundantes Auftreten des Merkmals wünschenswert.

Zugänglichkeit

- Einfacher Zugang, um die Merkmale elektronisch zu erfassen bzw. einzulesen.

Zur Gewährleistung eines reibungslosen Ablaufes des Identifikationsprozesses wird ein möglichst einfacher Zugang zu dem einzulesenden Merkmal vorausgesetzt. Dieser Punkt beinhaltet außerdem noch die Einfachheit sowie die Geschwindigkeit der Gewinnung von aussagekräftigen Unterscheidungsfaktoren. So unterscheiden sich Merkmale wie der Fingerabdruck oder das Irisabbild stark im Vergleich zur menschlichen DNS. Während

erstere, mit bereits entwickelt und getesteten Methoden innerhalb kürzester Zeitspannen im Millisekunden Bereich ermittelt werden können, wird für eine DNS Analyse, und die damit verbundene Suche und Ermittlung der Unterscheidungsfaktoren, eine Zeitspanne von ein bis zwei Tagen, sowie ein sehr hoher Arbeitsaufwand angegeben.

Akzeptanz

- Akzeptanz unter den Anwendern, dass diese persönlichen Daten von Dritten gespeichert und verarbeitet werden dürfen

Die Akzeptanz der Anwender und deren Einverständnis über die Speicherung persönlicher biometrischer Daten ist generell ein großes Problem. Sehr viele Personen mit wenig technischem Hintergrundwissen sind sich zum Teil der Möglichkeiten des Missbrauches dieser Daten nicht bewusst. Durch eine in letzter Zeit immer stärker aufkommende Diskussion über Datenschutz und persönliche Freiheit, wird teilweise schon jetzt mit Hilfe der Medien sehr stark polarisiert und verunsichert. Sollten zudem Merkmale ausgelesen und für die Identifizierung verwendet werden, welche Rückschlüsse auf die körperliche Verfassung, sowie Krankheiten der Person bieten, kann dies in Zukunft ein wirklich starkes Argument gegen die Verwendung biometrischer Systeme in Verbindung mit diesen Merkmalen darstellen.

2.4 Abstrakte Funktionsweise

Grundlegend lassen sich alle biometrischen Systeme in fünf unterschiedliche Teilsysteme zerlegen. Während die Datenerfassung, die Signalverarbeitung, sowie die Entscheidungsfindung Subsysteme sind, welche sequentiell ablaufen und somit auf die Ergebnisse der vorangegangenen Schritte aufbauen, bieten die Teilbereiche der Datenübertragung und der Datenspeicherung Querschnitts-Funktionen, welche parallel zu den bereits erwähnten drei Subsystemen arbeiten. Abbildung 2.1 stellt so eine allgemeine Struktur eines biometrischen Systems mit den fünf Subsystemen etwas detaillierter dar.

Datenerfassung

Der Prozess der Datenerfassung, welcher in Abbildung 2.1 in der linken waagrechten Säule dargestellt wird, beheimatet alle Funktionen über das Einlesen bis hin zur Digitalisierung des biometrischen Merkmals. Hier sind die Sensoren beheimatet, die die Merkmale vom Menschen einlesen und zur Weiterverarbeitung für den Signalverarbeitungsprozess aufbereiten.

Signalverarbeitung

Das Signalverarbeitungs-Subsystem bekommt seine Daten von zwei anderen Systemen. Auf der einen Seite die vom Sensor eingelesenen Daten, und auf der anderen Seite hat es Zugriff auf die im Datenspeicher archivierten Daten. Zuerst werden die vom Sensor übermittelten Informationen mittels verschiedener Filter so bearbeitet, dass die zu untersuchenden Eigenschaften gewonnen werden können. Begleitet wird diese Extraktion der Eigenschaften durch eine ständige Qualitätsermittlung, welche für den endgültigen Prozess der Entscheidungsfindung maßgeblich sein kann.

Nach einer erfolgreichen Ermittlung der spezifischen Eigenschaften werden diese mit den bereits in der Datenbank gespeicherten Templates abgeglichen. Mit dem am besten übereinstimmenden Template wird schlussendlich der sog. Match score in Prozent ermittelt.

Entscheidungsfindung

Hier wird die endgültige Entscheidung über Akzeptanz oder Abweisung getroffen. Dazu verwendet das System den Match score. Manche Systeme beziehen zusätzlich noch eine Qualitätskennzahl mit ein, um die gesamte Leistungsfähigkeit des Systems zu erhöhen. Detailliertere Informationen über die Verwendung und Bedeutung des Match scores und den damit verbundenen Möglichkeiten ein biometrisches System zu definieren werden in Kapitel 2.5 genauer aufgelistet.

Datenübertragung

Die Bedeutung des Subsystems für die Datenübertragung steigt mit der Ausdehnung des gesamten biometrischen Systems. Dieses muss bei der Übertragung die Integrität der Daten gewährleisten. Eine weitere Aufgabe des Übertragungssystems ist es, sicherzustellen, dass die Informationen nicht von unbefugten Dritten gelesen werden können, welche sie für spätere Angriffe auf das System verwenden könnten.

Datenspeicherung

Als Querschnittfunktion in Abbildung 2.1 rechts unten dargestellt, spielt die Datenübertragung für das gesamte biometrische System in Punkto Sicherheit aller gespeicherten Datensätze eine zentrale Rolle. Hier muss neben einer sicheren und fehlerfreien Speicherung auch definiert werden, welche anderen Teilbereiche Daten abfragen und- oder verändern dürfen.

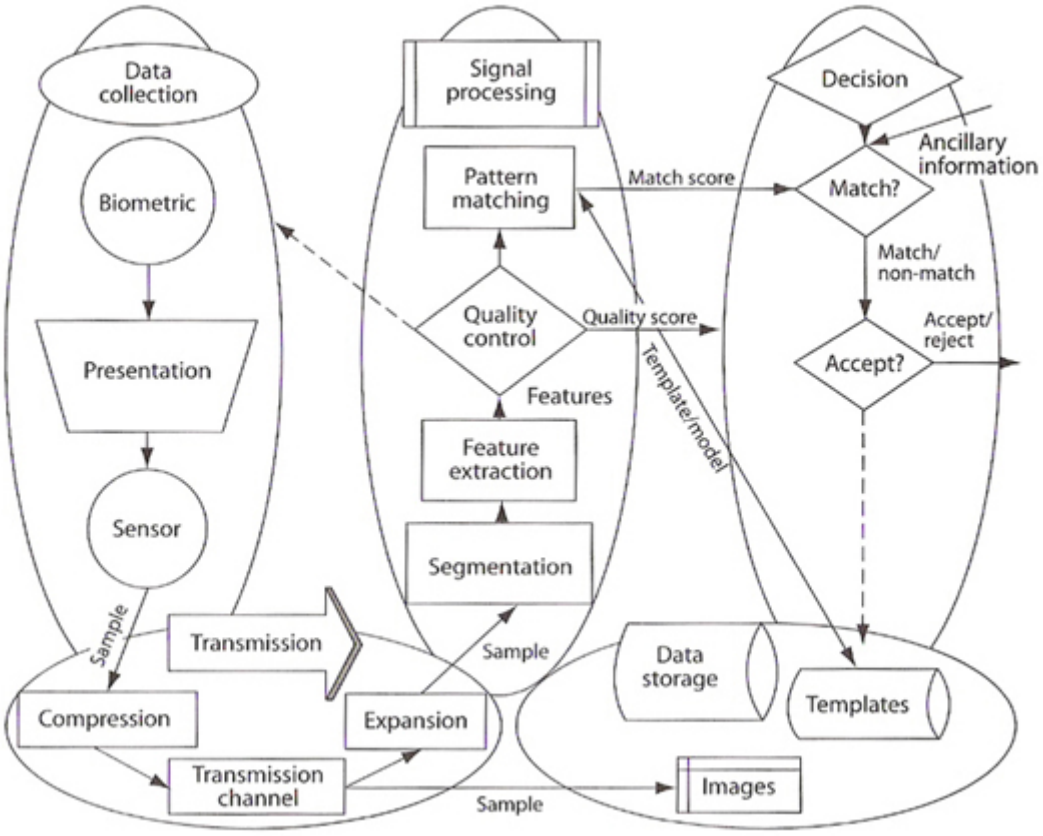

Abbildung 2.1 Allgemeine Struktur biometrischer Systeme [1]

2.5 Leistungsfähigkeit biometrischer Systeme

Durch die elektronische Verarbeitung und Digitalisierung der biometrischen Daten gehen je nach Methode und Filter unterschiedlich viele Informationen des Originalmerkmals verloren, so dass ein 100%iger Abgleich fast unmöglich wird. Aus diesem Grund wird der bereits in Kapitel 2.4 unter Entscheidungsfindung angesprochene Match score oder auch Übereinstimmungswert in Prozent ermittelt. Da man bei jedem Auswertungs- und Vergleichsvorgang, beeinflusst durch z.B. Verunreinigungen des Sensors, des Merkmals, oder sich verändernde Umwelteinflüsse wie Sonnenlicht oder Temperatur, nicht immer die zu 100% gleichen Informationen zur Verfügung hat, ergeben sich unterschiedliche Werte im Match score.

Für jedes einzelne biometrische System gilt es nun diese meist statistisch auftretenden Schwankungen zu ermitteln. Aus den daraus gewonnenen Kenntnissen über das System kann nun eine Akzeptanzschwelle für eine gültige Autorisierung gesetzt werden. Bei der Wahl dieses Schwellenwertes gibt es nun vier verschiedene Situationen, die es zu beachten gibt.

- Berechtigte Person wird zugelassen (richtige Identifikation)
- Nicht berechtigte Person abgewiesen. (richtiges Abweisen)
- Berechtigte Person wird abgewiesen (falsche Abweisung)
- Nicht berechtigte Person wird zugelassen (falsche Identifikation)

Während die ersten zwei Punkte in obiger Auflistung ein korrektes Verhalten des Systems beschreiben, ergeben sich im Fall der letzten zwei Punkte erhebliche Probleme. Hier ist allerdings noch einmal zu unterscheiden: Während eine falsche Abweisung für manche Benutzer mit dem höheren Aufwand eines erneuten Authentifizierungsversuches verbunden ist, kann im Falle einer falschen Identifikation einer nicht berechtigten Person erheblicher Schaden verursacht werden. Die zwei Bereiche, in denen in unserem Beispiel in Abbildung 2.2 solche Fehler auftreten können, sind als Falschakzeptanzrate (FAR) und Falschrückweisungsrate (FRR) gekennzeichnet. Durch Verändern des Wertes der Akzeptanzschwelle kann man nun das Verhältnis zwischen FRR und FAR bestimmen, wodurch das System maßgeblich definiert wird. [3]

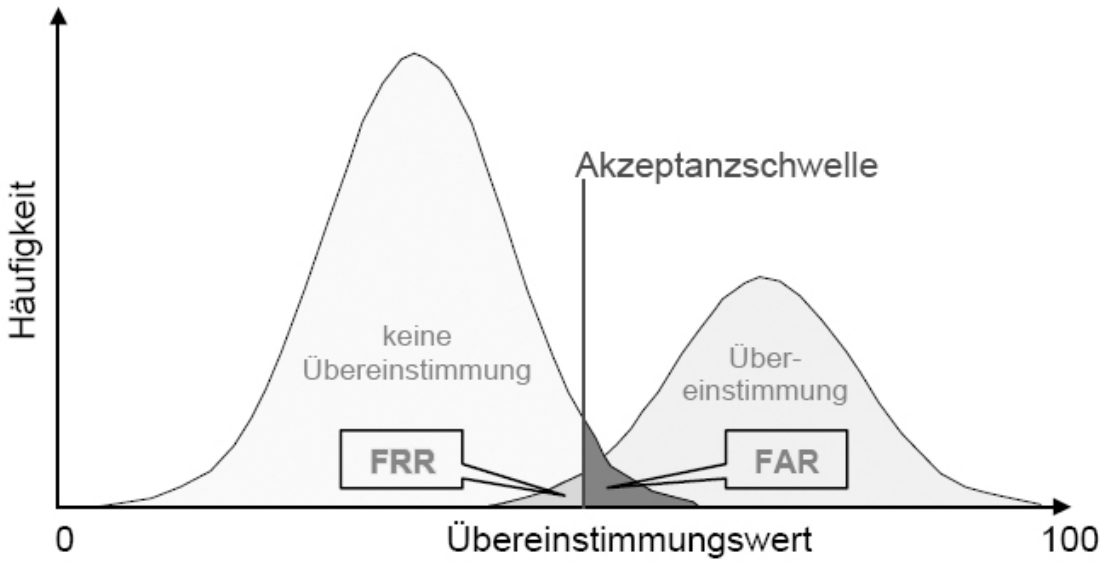

Abbildung 2.2 Systemdesign mittels statistisch auftretendem Match score und Akzeptanzschwelle[3]

2.6 Biometrische Standards

Biometrische Standards können vernachlässigt werden, wenn das Gesamtkonzept bzw. auch die Realisierung eines biometrischen Systems von einem einzigen Hersteller stammt. Gut definierte und leistungsfähige Standards werden überall dort umso dringender benötigt, wo Komponenten verschiedener Hersteller zu einem Gesamtsystem zusammengefasst, oder bereits bestehende Systeme mit biometrischen Zusatzfunktionen erweitert werden. Solch eine Vorgangsweise findet meistens bei größeren Systemen mit vielen verschiedenen Authentifizierungsterminals, eines somit auftretenden komplexen Datenübertragungssystems und mehrerer im Hintergrund verteilt arbeitender leistungsfähigen Datenverarbeitungsservern, Einsatz.

In den letzten zehn Jahren entwickelten sich mehrere Standards. Durch die Interessen verschiedener Hersteller und Konsortien getragen, wurde hier in die verschiedensten Richtungen geforscht und entwickelt. So entstanden verschiedene Normen und Spezifikationen für die verschiedensten Bereiche. Organisationen wie das International Committee for Information and Technology Standards (INCITS) in der Untergruppe INCITS M1, oder auch die International Standards Organisation (ISO) unter dem Begriff ISO/IEC JTCI SC37 arbeiten in den verschiedenste Bereichen, angefangen von der Interfacegestaltung, über die zu verwendenden Übertragungsformate, bis hin zu

Metriken, über welche ein biometrisches System beschrieben werden kann. Detailliertere Informationen darüber können im Rahmen dieser Arbeit nicht behandelt werden, lassen sich aber unter [4] (INCITS M1) bzw. [5] (ISO/IEC JTCI SC37) finden.

Neben dieser systemumfassenden Standardisierung etablierten sich andere Standards wie z.B. der ANSI X9.84, in welchem lediglich die sichere Datenübertragung, Datenspeicherung, sowie das Datenmanagement standardisiert werden, oder das Common Biometric Exchange File Format (CBEFF), in welchem ein Übertragungsformat spezifiziert wird, welches es ermöglicht, biometrische Daten zwischen Produkten unterschiedlicher Hersteller auszutauschen.

3 Fingerabdruckerkennung

3.1 Einleitung

Im Jahre 1684 veröffentlichte Nehemia Grew die erste wissenschaftliche Arbeit über biologische Charakteristika, wie Porenstruktur und Hautrillen von Fingerabdrücken (Daktylogramme). Mit dem Erscheinen dieser Arbeit stieg das wissenschaftliche Interesse in der Daktyloskopie (Personenidentifizierung mittels Fingerabdrücke) an und viele Wissenschaftler und Forscher widmeten sich dieser Thematik. Ende des 19. Jahrhunderts verfasste der britischen Naturforscher Francis Galton das Buch „Finger Prints“ welches folgende Kernaussagen beinhaltet:

- Fingerabdrücke sind unveränderlich und permanent
- Fingerabdrücke sind ein Unikum

Darüber hinaus beschreibt er darin die Klassifizierung der Papillarlinien von Fingern und formuliert somit einerseits den Grundstein für weitere Forschungsarbeiten, sowie die Grundlage für die heutige Daktyloskopie. Die Tatsache, dass Daktylogramme einen Menschen eindeutig identifizieren, als auch die Annahme, dass ein Fingerabdruck einzigartig ist, hat dazu geführt, dass der Fingerabdruck nicht nur in der Kriminalistik ein anerkanntes Beweismittel ist, sondern auch Anwendung in den unterschiedlichsten Gebieten findet. [6]

Bevor auf diverse Methoden zur Aufnahme von Fingerabdrücken eingegangen wird, werden im nächsten Kapitel die wichtigsten Merkmale eines Fingerabdruckes erläutert.

3.2 Unterscheidungsmerkmale von Fingerabdrücken

Um eine Differenzierung zwischen den einzelnen Fingerabdrücken durchführen zu können und dadurch in weiterer Folge eine Identifizierung von Personen zu ermöglichen, unterscheidet man zwischen verschieden Merkmalen, die eine Charakterisierung der Abdrücke erlauben. Dabei wird in erster Linie die Beschaffenheit und Anordnung der Papillarlinien (engl. Ridges) der Fingeroberfläche observiert. Im Allgemeinen variiert die

Breite dieser zwischen 100µm und 300µm. Die Merkmale lassen sich in drei Hauptgruppen unterteilen:

Singularitäten

Darunter versteht man die globale Struktur eines Abdrucks, welche durch die Ausrichtung der Papillarleisten festgelegt ist. Diese unverwechselbaren Topologien werden folgendermaßen klassifiziert.

- Loop (Schleife): hierbei laufen die Ridges halbkreisartig um einem Punkt
- Whorl (Wirbel): der Abdruck weißt ein strudelförmiges Muster auf
- Delta (Gabelung): dreiecksförmiger Zusammenlauf der Hautrillen

Kern

Der Kern (engl. Core) befindet sich häufig in der Nähe des Zentrums eines Fingerabbildes um welches sich die Papillarleisten anordnen. Abbildung 3.1 veranschaulicht die drei Singularitäten. Bei diesen Daktylogrammen ist der Kern durch einen weißen Punkt symbolisiert.

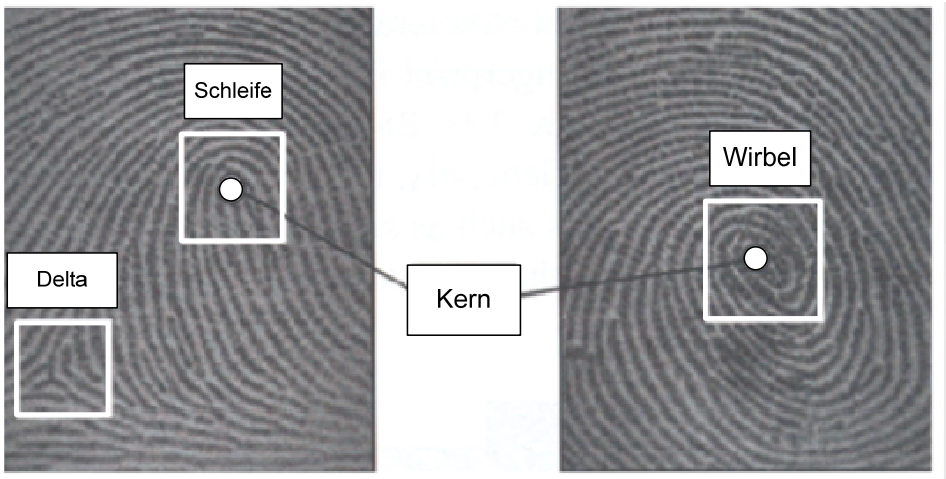

Abbildung 3.1 Darstellung der Singularitäten mit Kern [6]

Minutien

Als Minutie, oder in manchen Büchern auch als „Galton Detail“ beschrieben, wird die Endung beziehungsweise Anordnung der Papillarlinien eines Fingerabdruckes bezeichnet.

Insgesamt unterscheidet man zwischen mehr als 150 Minutien. Die wichtigsten Minutien sind in Abbildung 3.2 visualisiert.

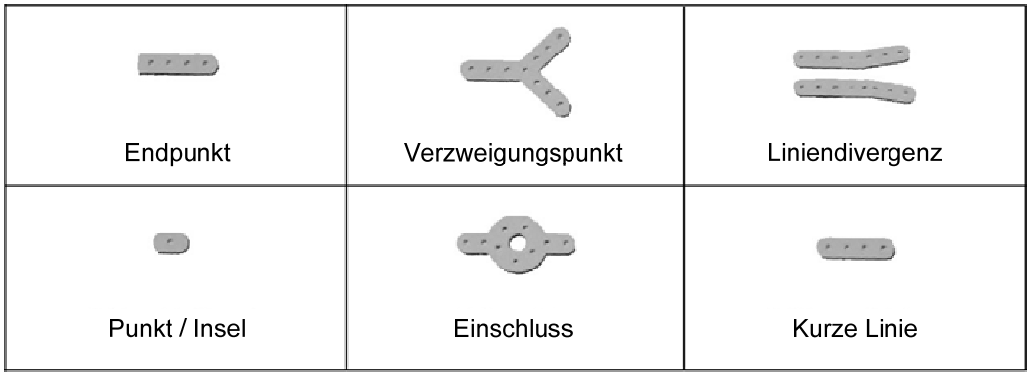

Abbildung 3.2 Exemplarische Illustration einiger Minutien

Anhand der Singularitäten teilte Edward Henry Ende des 19. Jahrhunderts die Musteranordnung der Fingerabdrücke in folgende drei Klassen ein:

- Whorl (Wirbel)
- Arch (Bögen)
- Loop (Schleife)

Das Henry - Klassifizierungssystem reduziert durch die logische Kategorisierung der Fingerabdrücke den zeitlichen Aufwand, der notwendig ist, um einen größeren Datensatz nach einem bestimmten Fingerabdruck zu durchsuchen. Aus diesem Grund kam diese Klassifizierung nicht nur früher bei manuellen Suchvorgängen zum Einsatz, sondern findet auch bei modernen Automated Fingerprint Identification Systems (AFIS) noch Anwendung. Es sei jedoch an dieser Stelle erwähnt, dass diese Kategorisierung bei Zutrittskontrollsystemen für gewöhnlich nicht eingesetzt wird. Anlehnend an den von Henry definierten Klassen wurden im Laufe der Zeit noch weitere hinzugefügt. In der Abbildung 3.3 werden neben den drei Hauptgruppen noch zwei weitere Kategorien exemplarisch aufgezeigt. Außerdem sind in den einzelnen Daktylogrammen die Deltas (Dreieck) sowie der Kern (Viereck) markiert.

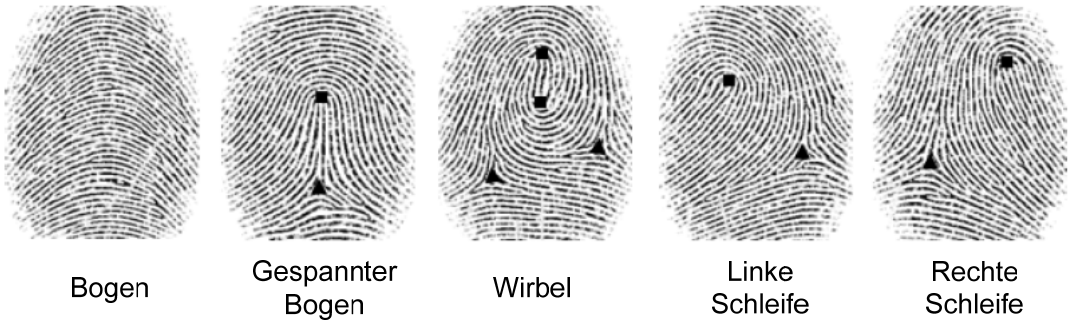

Abbildung 3.3 Fünf Klassen der Fingerabdrücke [6]

Ein weiterer wichtiger Aspekt in der Klassifizierung der Daktylogramme ist die Linienzahl. Diese Merkmalsausprägung definiert für jene Linien, welche eine imaginäre Linie zwischen dem Delta und dem Kern berühren beziehungsweise kreuzen, einen numerischen Wert, dessen Konkretisierung auf Grund des komplexen Papillarlinienmusters schwierig ist.

Nachdem im vorherigen Kapitel die wesentlichen Unterscheidungsmerkmale vorgestellt wurden, werden im folgenden Kapitel die verschiedenartigen Methoden zum Erfassen der Fingeroberfläche beschrieben.

3.3 Fingerabdruckabtastung

Bei der Fingerabdruckabtastung soll ein möglichst gutes Abbild eines Fingers erzeugt werden. Grundsätzlich kann die Abtastung der Fingerkuppel „off-line“ oder „online“ erfolgen. Neben diesen zwei prinzipiellen Abtastverfahren werden in diesem Abschnitt die grundlegenden Konzepte der verschiedenen Sensoren und der jeweiligen Abtastmethoden näher erläutert.

3.3.1 Off-line – Abtastung

Bei diesem Verfahren erhält man das Daktylogramm indem das mit Farbe überzogene Fingerbeere von einer Nagelseite zur anderen über ein Papier gerollt wird. Durch diese Vorgehensweise wird gewährleistet, dass die gesamte Unterseite der Fingerkuppel abgebildet wird. Nach dem Abrollen wird in einem weiteren Schritt das Papillarlinienmuster mittels Kamera oder Scanner digitalisiert. Ein Nachteil dieser

Methode ist, dass durch das Abrollen Qualitätsverschlechterungen (z.B.: Verzerrungen) im Abbild entstehen können. Darüber hinaus ist sie langsam und für Zutrittskontrollen unbrauchbar.

3.3.2 Online – Abtastung

Bei der Online – Abtastung, oder häufig auch Lebendabdruckabtastung (engl. Live-scan) bezeichnet, werden die Papillarlinien des aufgelegten Fingers von einem Sensor abgetastet, sowie in weiterer Folge ein Abbild des gescannten Fingers erzeugt. Eine zentrale Komponente bei der Online – Abtastung ist der Sensor, der den Finger abtastet. Je nach verwendeten Abtastverfahren kommen verschiedene Fingerabdrucksensoren zum Einsatz, welche sich in folgende Hauptgruppen kategorisieren lassen:

- Optische Sensoren
- Siliziumsensoren
- Ultraschallwellensensoren

Ein wesentlicher Unterschied dieser Variante zur Off-line Abtastung ist, dass hierbei der Fingerabdruck üblicherweise durch Auflegen des Fingers auf die Oberfläche des Sensors erhalten wird. Es existieren unterschiedliche Methoden/Sensoren, mit denen die Abtastung der Papillarlinien erfolgen kann. In den nachstehenden Unterkapiteln werden die konventionellsten Methoden bzw. Sensortechniken zum Erfassen des Lebendabdrucks näher erläutert. [3][6]

3.3.3 Optische Sensoren

Bei dieser Technik wird der Finger grundsätzlich auf eine ebene, transparente Plattform aufgelegt. Je nach Verfahren kann es sich bei der Fläche beispielsweise um ein Glasprisma, wie es beim FTIR – Verfahren (Frustrated Total Internal Reflection) verwendet wird, oder ein Fiberglas (Optical Fibers) handeln. Während die Papillarlinien direkt auf der Oberfläche aufliegen, besteht zu den Tälern eine entsprechende Distanz. Wird das Fingerbeere nun von einer Lichtquelle wie zum Beispiel einem LED (Light Emitting Diode) beleuchtet, so wird dieses von den Papillarlinien gebrochen und in weiterer Folge absorbiert. Jene Lichtstrahlen, welche auf die Grate emittiert wurden, werden komplett

reflektiert und können durch einen im Fokus befindlichen CCD (Charge-coupled Device) - oder CMOS - Sensor zur Abdruckerfassung weiterverarbeitet werden. Ein Vorteil dieser Methode ist, dass der Sensor robust gebaut ist und somit gegenüber äußerlichen Einwirkungen gut geschützt wird. Des Weiteren sind Aufnahmen mit hoher Qualität (Auflösung: 500 dpi) möglich. Eine negative Eigenschaft dieser Technologie ist, dass die Prismaoberfläche durch Schweiß und Schmutz verunreinigt wird, was zum Einen zu einer Minderung der Bildqualität führt und zum Anderen eine Erhöhung der Fehlerrate zur Folge hat. Aus diesem Grund ist eine regelmäßige Reinigung der Oberfläche essentiell. Die Abbildung 3.4 zeigt einen FTIR basierten optischen Sensors. [6]

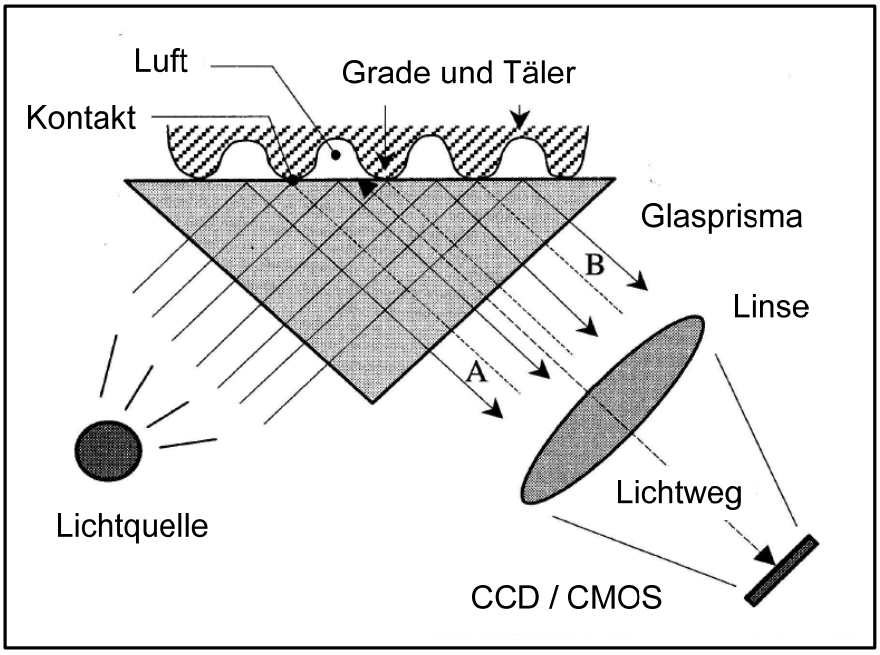

Abbildung 3.4 Schematische Darstellung eines FTIR [6]

3.3.4 Siliziumsensoren

Die Siliziumsensoren fanden Ende 1980 Einzug in den Bereich der Fingerabdruckerkennung, wobei die Entwickler das damalige Kosten- bzw. Größenproblem von Fingerabdruckerkennungssystemen mit diesem Typus lösen wollten. Heutzutage sind die Unterschiede in Bezug auf Größe und Preis, im Gegensatz zu den anderen im Einsatz befindlichen Sensoren, nicht mehr relevant. Der Sensor an sich besteht bei diesem Verfahren aus einem zweidimensionalen Array, welches wiederum in kleine Bereiche (Pixel) segmentiert ist. Jedes dieser Pixel repräsentiert dabei einen

eigenen kleinen Sensor und stellt einen Pixel im Fingerabbild dar. Erfolgt die Abtastung des Fingers unter Verwendung eines Siliziumsensors, so ist es erforderlich, dass der Benutzer den Finger auf die Sensoroberfläche auflegt. Die Sensoren erfassen anschließend je nach Art eine physikalische Größe wie Kapazität, Temperatur oder elektrische Feldstärke, wobei laut [6] kapazitive Sensoren überwiegend Verwendung finden. Ein Nachteil beziehungsweise einee kritische Komponente dieses Fingerabdruckerkennungssystems stellt die Schutzschicht, welche auf der Oberfläche der Sensoren aufgebracht ist, dar. Die Beschichtung soll die Sensoren vor elektrostatischem Aufladen des Fingers schützen, sowie eine Verunreinigung verhindern. Die Oberflächenbeschichtung darf nicht zu dick gewählt werden, da sonst die Qualität des Abbildes reduziert wird. Eine zu dünne Beschichtung hätte jedoch zur Folge, dass die Sensoren gegenüber äußerlichen Einflüssen sehr empfindlich wären. Meist beträgt die Dicke einige Mikrometer. In Abbildung 3.5 wird das Prinzip eines kapazitiven Sensors schematisch dargestellt. [6]

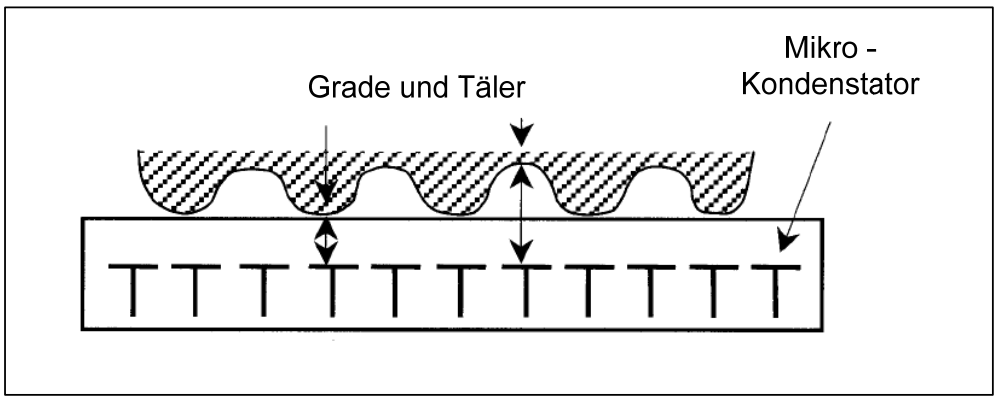

Abbildung 3.5 Kapazitiver Sensor [6]

3.3.5 Ultraschallwellensensoren

Bei diesem Verfahren sendet der Sensor gepulste Ultraschallwellen aus, welche je nach abgetasteter Oberfläche entsprechend reflektiert werden. Aus den reflektierten Ultraschallwellen, dem sogenannten Echo-Signal, lässt sich in weiterer Folge ein Abbild der Papillarlinien errechnen. Der Sensor besteht in diesem konkreten Fall aus einem Transmitter, sowie einem Receiver. Da die akustischen Wellen durch normale Unreinheiten nicht verfälscht werden, liefern diese Sensoren ein Abbild von hoher Qualität. Dessen ungeachtet findet dieses Verfahren auf Grund des hohen technischen

Aufwands bei der Installation, sowie den außerordentlichen Kosten in der Praxis kaum Akzeptanz. Abbildung 3.6 veranschaulicht das grundlegende Prinzip der Ultraschalltechnik. [6]

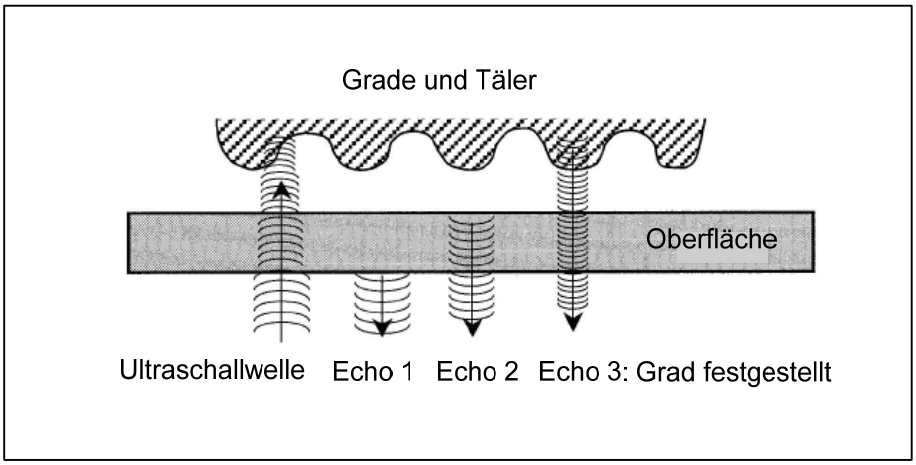

Abbildung 3.6 Grundprinzip eines Ultraschallsensors [6]

3.4 Vergleichsverfahren

Im Rahmen des folgenden Unterkapitels werden zu Beginn allgemein gültige Probleme des Matching vorgestellt. Im Anschluss daran wird näher auf das Minutienbasierte Verfahren eingegangen, da dieses laut [6] eine breite Akzeptanz aufweist und zu den verlässlichsten zählt, weshalb dieses Verfahren von Gericht und Strafverfolgungsbehörden angewendet wird. Im Allgemeinen haben die verschieden Methoden / Algorithmen die Aufgabe, zwei Fingerabdrücke, Inputfingerabdruck und Templatefingerabdruck, miteinander zu vergleichen und in weiterer Folge eine mögliche Übereinstimmung zu finden. Neben dem Minutienbasierten Ansatz gibt es noch zwei weitere, welche in der Praxis alternativ zum Einsatz kommen:

Korrelationsverfahren

Korrelationserfahren verwenden den Pixelgrauwert des Fingerabdruckbildes als Vergleichskriterium. Dabei werden über eine Ähnlichkeitsfunktion mögliche Übereinstimmungen gefunden. Im Allgemeinen sind Korrelationsbasierte Verfahren sehr rechenintensiv.

Graderkennungsverfahren

Unter Umständen, beispielsweise bei einer schlechten Qualität des Fingerabdrucks, ist eine Extraktion der Minutien schwierig, weshalb bei diesen Methoden Eigenschaften wie, lokale Orientierung, Frequenz (Dichte) oder Formteile der einzelnen Papillarlinien im Daktylogramm als Vergleichsparameter benutzt werden.

Genaue Erläuterungen sowie einzelne Algorithmen, welche auf Graderkennung bzw. Korrelation basieren, können [6] entnommen werden.

3.4.1 Grundsätzliche Probleme der Vergleichsverfahren

Wird das Papillarlienenmuster von einem Sensor aufgenommen, so ist auf die Positionierung als auch auf die Rotation des Fingers im Vergleich zu vorhergegangenen Aufnahmen zu achten. Bei großen Variationen kann es, insbesondere bei Sensoren mit einem kleinen Sensor-Array, zu unterschiedlichen Erfassungen des Fingerbeeres kommen. Folglich werden nicht akurate Ergebnisse in der Wiedererkennung geliefert. Lösungen hierfür sind Algorithmen, welche rotations- und translationinvariant sind, wie zum Beispiel die Phasenmethode von Jiang und Yau in [7].

Darüberhinaus spielt der Druck, mit dem der Finger auf die Sensoroberfläche aufgelegt wird, eine entscheidende Rolle, da dies zu linearen Verzerrungen im Daktylogramm führen kann. Außerdem führen äußerliche Einflüsse, wie verschmutzte Sensoroberflächen oder verunreinigte Fingerkuppen, zu einer Minimierung der Abdruckqualität, was eine Verfälschung der Matchingresultate zur Folge hat.

3.4.2 Minutienbasierte Verfahren

Bei diesen Verfahren wird der Inputfingerabdruck $\boldsymbol{I}$, als auch der Templatefingerabdruck $\boldsymbol{T}$, in Form eines Vektors dargestellt. Jedes Element des Vektors repräsentiert dabei eine Minutie $\boldsymbol{m}$, welche zuvor aus den Rohbilddaten extrahiert wurden.

$$\boldsymbol{T} = \{\boldsymbol{m}_1, \boldsymbol{m}_2, \dots, \boldsymbol{m}_m\},$$

$$\boldsymbol{I} = \{\boldsymbol{m}_1', \boldsymbol{m}_2', \dots, \boldsymbol{m}_n'\}$$

Die Minutien werden wiederum durch eine Reihe von Attributen, wie zum Beispiel Lage im Fingerabdruckabbild, Ausrichtung oder Typ, beschrieben. Wie im Folgenden gezeigt, wird eine Minutie für gewöhnlich als ein Tripel definiert.

$$\boldsymbol{m}_i = \{x_i, y_i, \theta_i\}, \qquad i = 1..m$$
$$\boldsymbol{m}_j^{'} = \{x_j^{'}, y_j^{'}, \theta_j^{'}\}, \qquad i = j..n$$

Dabei geben x , y die Koordinaten im Image an und über θ wird der Winkel, welcher im Intervall von 0° bis 360° liegen kann, konkretisiert.

Die räumliche Differenz sd (spatial distance) zweier Minutien wird definiert durch:

$$sd(\boldsymbol{m}_j^{'}, \boldsymbol{m}_i) = \sqrt{(x_j^{'} - x_i)^2 + (y_j^{'} - y_i)^2}$$

Die Richtungsdifferenz dd (direction difference) zwischen zwei gegeben Minutien wird folgendermaßen beschrieben:

$$dd(\boldsymbol{m}_j^{'}, \boldsymbol{m}_i) = \min\left(|\theta_j^{'} - \theta_i|, 360° - |\theta_j^{'} - \theta_i|\right)$$

Eine Minutie $\boldsymbol{m}_j^{'}$ aus $\boldsymbol{I}$ und eine Minutie $\boldsymbol{m}_i$ aus $\boldsymbol{T}$ werden als Äquivalent zueinander angenommen wenn gilt:

$$sd \leq r_0$$

$$dd \leq \theta_0$$

Dabei repräsentiert r_0 eine Toleranzgrenze, welche sich auf die räumliche Distanz bezieht und über θ_0 wird jener Grenzwert angegeben, der die maximale Richtungsdifferenz, häufig auch als Winkeltoleranz bezeichnet, definiert.

Aus den oben genannten Funktionsdefinitionen lässt sich in einem weiteren Schritt die Funktion $equal$ definierten.

$$equal(\boldsymbol{m}_j^{`}, \boldsymbol{m}_i) = \begin{cases} 1 & sd(\boldsymbol{m}_j^{`}, \boldsymbol{m}_i) \leq r_0 \quad und \quad dd(\boldsymbol{m}_j^{`}, \boldsymbol{m}_i) \leq \theta_0 \\ 0 & sonst. \end{cases}$$

Diese liefert, sofern die zwei Toleranzgrenzen nicht überschritten werden, den Wert 1 zurück. In einem ersten möglichen und allgemein formulierten Algorithmus können die einzelnen Minutien von $\boldsymbol{I}$ gegen $\boldsymbol{T}$ geprüft werden. Dabei werden die Rückgabeparameter der $equal$ – Funktion aufsummiert und in weiterer Folge gegen einen Schwellwert geprüft. Liegt der Funktionswert innerhalb eines vorgegeben Grenzwertes, typischerweise wird hier der Wert 12 (12-Punkte-Regel) gewählt [8], so kann davon ausgegangen werden, dass $\boldsymbol{I}$ und $\boldsymbol{T}$ äquivalent sind, d.h. sie „matchen“ sich. [6]

Abbildung 3.7 veranschaulicht das „Matching“ von einem Inputfingerabdruck mit dem in einer Datenbank befindlichen Templatefingerabdruck, wobei die Minutien des Inputes mit einem x und die des Templates mit einem o gekennzeichnet sind.

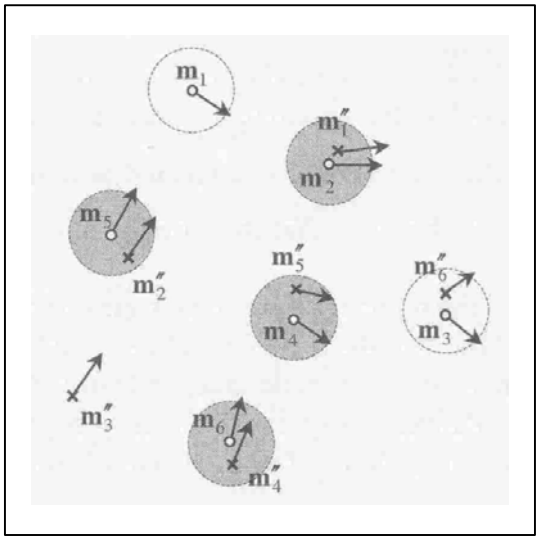

Abbildung 3.7 Matching von Minutien [6]

Der Kreis um die einzelnen Minutien charakterisiert die maximale räumliche Distanz r_0. Die Pfeile visualisieren in welche Richtung die Minutien ausgerichtet sind. Ist ein Kreis grau hinterlegt, „matchen“ sich die Orts- als auch die Richtungsparameter der jeweiligen Minutien innerhalb der Toleranz.

Weiterführende Informationen zu dieser Thematik, sowie konkret ausformulierte Algorithmen, wie dem Hough – Verfahren oder der Phasenmethode von Jiang und Yau können [6] entnommen werden.

4 Schlussbetrachtung

Nach einer kurzen Einleitung wurde im ersten Teil der Bereich der biometrischen Systeme grundlegend beschrieben und einige allgemeine Informationen gegeben. Im zweiten Teil wurde auf den Teilbereich der Fingerabdruckerkennung genauer eingegangen. Wie schon erwähnt deckt der Bereich der Fingerabdruckerkennung lediglich einen sehr kleinen Teilbereich biometrischer Systeme ab. Um die Schritte angefangen von dem Erfassen des Merkmals bis hin zur endgültigen Entscheidung über die Akzeptanz zu erklären, konnten hier Zusammenhänge erläutert werden welche sich auch auf andere Erkennungsverfahren im biometrischen Bereich wie Iriserkennung, oder Gesichtserkennung und andere übertragen lassen.

Grundsätzlich ist zu sagen, dass die Fingerabdruckerkennung das zurzeit am meisten Entwickelt und Erforsche Verfahren zur biometrischen Identifikation ist. Jedoch beinhaltet diese Technologien auch sehr viele Schwachstellen, gerade was die Sicherheit betrifft. So ist es schon bereits mit geringem Wissen, und gut dokumentierten Anleitungen einigermaßen leicht, solche Systeme zu Überwinden, bzw. den Fingerabdruck einer Person zu fälschen.

In naher Zukunft wird auf dem Sektor der biometrischen Identifikation ein weiterer enormer Fortschritt festzustellen sein. Nach dem Lösen immer komplexer werdender Probleme gerade im Bereich der Iris, sowie der Gesichtserkennung erwarten sich Wirtschaft, und Forschung großes Potential im Hinblick auf Sicherheit und Vertrauenswürdigkeit aber auch Akzeptanz dieser Systeme.

5 Literaturverzeichnis

[1]. **Wayman, J. et al.** *Biometric Systems - Technlogy, Design and Performance Evaluation.* London : Springer-Verlag London Limited, 2005.

[2]. **Ross, A. et al.** *Handbook of Multibiometrics.* New York : Springer Science+Business Media, LLC, 2006.

[3]. **Bundesamt für Sicherheit in der Informationstechnologie.** *Evaluierung biometrischer Systeme, Fingerabdrucktechnologien – BioFinger.* Bonn : s.n., 2004.

[4]. **INCITS.** M1 - Biometrics. [Online] http://www.ncits.org/tc_home/m1.htm.

[5]. **ISOTC.** ISO Standards Development. [Online] http://isotc.iso.org.

[6]. **Maltoni, D. et al.** *Handbook of Fingerprint Recognition.* New York : Springer-Verlag, 2003.

[7]. **Jiang, X. und Yau, W.** *Proc. Fingerprint Minutiae Based on the Local and Global Structures, , pages 1038-1041.* s.l. : 15th International Conference on Volume 2, 2000.

[8]. **Pankanti, S. et al.** *On the Individuality of Fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 8.* 2002.