

Dirk Labudde

2.1 Einleitung

Die moderne Tatortarbeit hat sich in den letzten Jahren deutlich verändert. Dabei sollte man nicht die in der Presse und Bevölkerung entstandene Erwartungshaltung durch den „CSI-Effekt“ aus dem Blick verlieren. Der Begriff ist von den CSI-Serien abgeleitet und vermittelt die Technikaffinität der Forensik. Im Kontext der Technikentwicklung und der Effektivität sollte der Einsatz von neuen Technologien zur Analyse von Spuren (digitalisierten Daten) behutsam diskutiert werden. Natürlich lassen neue Technologien auch neue Analysemethoden zu, jedoch sollten Aspekte der Machbarkeit im Alltag ebenfalls berücksichtigt werden. Neue Technologien sind die Grundlage für eine moderne forensische Fallarbeit. In diesem Kontext wollen wir von digitalisierten Spuren sprechen, also physische Spuren, die durch geeignete Technologien digitalisiert, analysiert und visualisiert werden können. Seit Jahrhunderten möchten Menschen andere erkennen bzw. wiedererkennen, sei es aus Gründen der Freundschaft oder Feindschaft. Hier bedient sich der Mensch erkennbarer biologischer Merkmale. Diese können physiologische Merkmale oder Verhaltenscharakteristika sein. Heute werden durch geeignete Methoden (Scanning, Capturing) aus diesen biologischen Merkmalen biometrische Merkmale. Eine weitere Abstraktionsebene wäre die biometrische Signatur (Hashfunktion). Wir unterscheiden zwei Aufgaben, Identifizierung bzw. Authentifizierung/Verifizierung einer Person, welche durch verschiedene Methoden abgedeckt werden [42].

D. Labudde (✉)

Lehrstuhl für Bioinformatik und Forensik, Leiter Forensic Science Investigation Lab (FoSIL),
University of Applied Sciences Mittweida
Technikumplatz 17, 09648 Mittweida, Deutschland
E-Mail: labudde@hs-mittweida.de

2.1.1 Die Identifikation – Wer bin ich?

Aus einem Referenzdatensatz, in dem Daten mehrerer Personen gespeichert sind, wird die zu identifizierende Person herausgesucht. Die aktuellen Daten müssen von dem biometrischen System mit dem gesamten Datenbestand verglichen werden bis in den Referenzdaten Übereinstimmungen gefunden sind. Die Genauigkeit des Verfahrens hängt von den zuvor festgelegten Toleranzschwellen ab. Es kann aber keine hundertprozentige Übereinstimmung erreicht werden, sondern nur eine hinreichende Deckung der Daten. Zur Identifizierung einer Person muss der Schwellwert bezüglich eines Referenzdatensatzes überschritten werden. Mithilfe eines $1 : n$ -Vergleichs aus dem Referenzdatensatz ist dem System die gesuchte Person bekannt und es weiß, um welche Person es sich handelt [42].

2.1.2 Die Verifikation – Bin ich der, für den ich mich ausbebe?

Damit das Verfahren herausfindet, ob eine Person die ist, für die sie sich ausgibt, müssen die Daten innerhalb von festgelegten Toleranzschränken übereinstimmen. Diese Schranken sind im Programm festgelegt. Das bedeutet, dass die gewonnenen Daten mit einem einzigen Datensatz in einem $1 : 1$ -Vergleich gegenübergestellt werden. Der Vorteil beim Abgleich der aktuellen Daten mit nur einem Referenztemplate ist der Faktor Zeit, da eine Identifikation mithilfe eines $1 : n$ -Vergleichs mit zunehmender Größe immer langsamer wird [42].

In der modernen forensischen Fallarbeit gewinnt die Biometrie (biometrische Verfahren und Systeme) immer mehr an Bedeutung. Der technologische Fortschritt erlaubt in zunehmendem Maße rasche Messungen von biologischen Charakteristika und deren Auswertung mit vertretbarem Aufwand und hoher Qualität. Der Einsatz von Biometrie ist ein vielversprechender Ansatz, das Locard'sche Prinzip auf eine neue qualitative und quantitative Ebene zu heben. Wie verbindet man die Spuren mit der Identität einer oder mehrerer Personen? Dies gilt nur, unter der Annahme, dass biometrische Systeme kreiert werden, die eine Speicherung, Analyse, Kombination und Vergleich biometrischer Daten ermöglichen. In der heutigen globalisierten Informations- und Wissensgesellschaft kommt der Lösung dieses Problems eine immense Wichtigkeit und Bedeutung zu. Analog zum menschlichen Verhalten können diese Systeme trainiert werden und so eine höhere Erkennungsrate erzielen [42].

2.2 Biometrie

Der Begriff Biometrie stammt aus dem Griechischen und bildet sich aus den altgriechischen Wörtern *bios* (*βίος*) für Leben und *metron* (*μέτρον*) für Maß. Danach ist die Biometrie die Wissenschaft der Körpermessung an Lebewesen, speziell am Menschen. Die klassische Begriffsdefinition der Biometrie beschreibt die Anwendung statistischer

Methoden in Human- und Veterinärmedizin, in Land- und Forstwirtschaft, in der Biologie sowie in verwandten Wissenschaftsgebieten. Dieser Begriff schließt das Wissen um die Merkmale von Menschen mit ein. Aus einzelnen oder einer Kombination von biometrischen Daten, welche auf diesen Merkmalen basieren, wird eine Person authentifiziert oder identifiziert.

2.2.1 Historischer Streifzug durch die Biometrie in der Forensik

Die Vermessung des Menschen zu Identifikationszwecken ist eine alte wissenschaftliche Idee. Bereits mehr als zweitausend Jahre vor Christus wurden Fingerabdrücke verwendet, um auf Tontafeln, welche zu dieser Zeit als Urkunden dienten, den Aussteller der Urkunde zu markieren. Auch zu Zeiten der Han-Dynastie, ca. 100 nach Christus, verwendete man den Fingerabdruck als Unterschrift. In Strafverfolgungsprozessen wurde der Identifizierungswert des menschlichen Fingerabdruckes vermutlich schon im zwölften Jahrhundert eingesetzt. Darauf weist ein 40-bändiger Kriminalroman des chinesischen Schriftstellers Shi nai-ngan hin, welcher beschreibt, wie man zwei Mörderinnen die „Finger einschwärzen und abdrücken“ ließ. Unter dem Titel: „Über das äußere Gefühlsorgan“ wurde im Jahre 1686 durch Marcellus Malphigius erstmals eine Schrift veröffentlicht, welche sich den Furchen und Mustern der Handflächen widmete. Der tschechische Professor Johann Evangelista Purkinje legte 1823 durch seine Definition der neun Grundmuster die Basis für die heutige Klassifizierung von Fingerabdrücken. Etwa 20 Jahre später erbrachte der deutsche Anthropologe Hermann Welker den empirischen Beweis der Unveränderlichkeit des Fingerabdrucks im Laufe eines Lebens. Ende des 19. Jahrhunderts wird durch die systematische Aufnahme verschiedener Körpermaße, wie beispielsweise der Länge und Breite des Kopfes, der Begriff der „Anthropometrie“ geprägt. Alphonse Bertillon publiziert 1885 die Farbe der Iris als Erkennungsmerkmal des Menschen. 1892 postulierte Sir Francis Galton, dass der menschliche Fingerabdruck einzigartig für jedes Individuum ist und im Laufe des Lebens weitgehend unverändert bleibt. Damit wurde der wissenschaftliche Grundstein für die Verwendung der Daktyloskopie in der Personenerkennung gelegt. Bereits fünf Jahre später wurden die ersten Straftäter durch New Scotland Yard mithilfe von Fingerabdrücken überführt. Seit 1952 erkennt der deutsche Bundesgerichtshof den Beweiswert der Daktyloskopie uneingeschränkt an. Die Einzigartigkeit der Irismusterung und deren Eignung zu Identifizierungszwecken wurden erstmals 1936 erwähnt. In den 1980er Jahren wurden dann Verfahren zur Retina- und Iriserkennung entwickelt. Im Jahr 1994 wurde der erste einsatzfähige biometrische Algorithmus von John Daugman entwickelt und zum Patent angemeldet. In den Jahren 1994 bis 1996 wurde von dem US-amerikanischen Verteidigungsministerium der erste Wettbewerb von Gesichtserkennungssystemen ausgetragen [23].

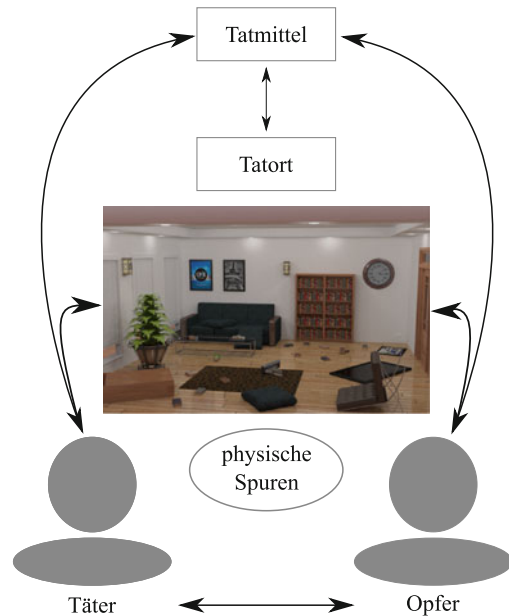
2.2.2 Biometrie und das Locard'sche Prinzip

Das Locard'sche Austauschprinzip macht die Rolle der Spur (physisch und digital) auf eine einprägsame Art deutlich. Wir werden uns hier lediglich auf die „biometrischen“ Spuren konzentrieren. Jedoch gilt das Prinzip der Ähnlichkeit auch für Werkzeugspuren oder Abdrücke von Autoreifen. Im Wesentlichen unterscheidet man vier Spurenkategorien:

- **Materialspuren.** Basieren auf den stofflichen Eigenschaften und deren Zuordnung (z. B. Spermaspuren, Blutspuren, Speichelspuren, Haare).
- **Formspuren.** Forensische Schlussfolgerungen basieren auf der Form der Spuren (z. B. Blutspritzmuster, Werkzeugabdruck auf Haut oder Knochen).
- **Situationsspuren.** Sammlung von Informationen aus der besonderen Lage von Spuren oder Gegenständen zueinander oder zur Umgebung (Stellung von Fenstern und Türen, Lage der Kleidung).
- **Gegenstandsspuren** sind beweiserhebliche Gegenstände, die vom Täter oder Opfer am Tatort (Tatortbegriff im erweiterten Sinne) zurückgelassen worden.

Opfer, Täter, Tatmittel und Tatort stehen über die Veränderungen (physische Spur) in einem nachvollziehbaren Zusammenhang (Abb. 2.1). Kein Täter kann eine Tat begehen oder einen Tatort verlassen, ohne eine Vielzahl von Spuren zu hinterlassen. Locard formulierte das so:

Abb. 2.1 Darstellung der Beziehungen zwischen Täter, Opfer, Tatmittel und dem Ort des Geschehens. Der Zusammenhang wird durch die physischen Spuren vermittelt



Tab. 2.1 Zusammenhang Spurenverursacher und Spurenräger. Dargestellt sind mögliche Übertragungen zwischen Täter, Opfer, Tatmittel und dem Ort des Geschehens [19]

Spurenverursacher	Spurenräger	Beispiel
Täter	Opfer	Würgemale
	Tatmittel	Fingerabdrücke auf Hammerstiel
	Tatort	Fußabdruckspuren im Garten
Opfer	Täter	Blutspuren auf Hemd
	Tatmittel	Hautzellen des Opfers
	Tatort	Blutspuren des Opfers
Tatmittel	Täter	Fingerabdrücke an der Waffe
	Opfer	Schussverletzungen
	Tatort	Reifenspuren
Tatort	Täter	Bodenspuren an den Schuhen
	Opfer	Botanische Spuren
	Tatmittel	Mechanische Spuren an der Tür

„Überall dort, wo er geht, was er berührt, was er hinterlässt, auch unbewusst, all das dient als stummer Zeuge gegen ihn. Nicht nur seine Fingerabdrücke oder seine Fußabdrücke, auch seine Haare, die Fasern aus seiner Kleidung, das Glas, das er bricht, die Abdrücke der Werkzeuge, die er hinterlässt, die Kratzer, die er in die Farbe macht, das Blut oder Sperma, das er hinterlässt oder an sich trägt. All dies und mehr sind stumme Zeugen gegen ihn. Dies ist der Beweis, der niemals vergisst. Er ist nicht verwirrt durch die Spannung des Augenblicks. Er ist nicht unkonzentriert, wie es die menschlichen Zeugen sind. Er ist ein sachlicher Beweis. Physikalische Beweismittel können nicht falsch sein, sie können sich selbst nicht verstellen, sie können nicht vollständig verschwinden. Nur menschliches Versagen, diese zu finden, zu studieren und zu verstehen, kann ihren Wert zunichtemachen.“[31]

Die Auswirkung oder auch Wirkung ist in den Veränderungen an den Objekten messbar. Ausgehend vom Locard’schen Prinzip sind Spurenübertragungen von Form- und Materialspuren zwischen Täter, Opfer, Tatmittel und Tatort möglich. Tab. 2.1 beinhaltet einen Überblick zu möglichen Übertragungen und Zusammenhängen zwischen Spurenverursachern und Spurenrägern [19]. So kann ein Täter seinen individuellen Fingerabdruck auf einem Tatwerkzeug hinterlassen. Durch biometrische Methoden und Systeme kann dieser Abdruck analysiert und zugeordnet werden. Das Verständnis und die Zuordnung der Spuren ermöglicht eine Rekonstruktion des Tatherganges und die Identifizierung bzw. Verifizierung des Täters und/oder des Opfers. Der Prozess der Zuordnung (Identifikation bzw. Verifikation) lässt über die Bestimmung der Ähnlichkeit zweier Merkmale bzw. deren Veränderungen am Tatort bestimmen. Biometrische Verfahren erlauben ebenso Gegenstände die mit einem möglichen Täter oder Opfer in Verbindung stehen zu analysieren und diese einer Person zu zuordnen.

Der Raum der möglichen Spuren hat sich durch das Informationszeitalter, in dem wir leben, deutlich vergrößert. Neben den von Menschen erkennbaren Merkmalen wie dem Gesicht, der Stimme, dem Gang oder der Handschrift können speziell entwickelte Ver-

fahren Parameter, die dem menschlichen Auge verborgen sind, erfassen und analysieren. Dazu gehört der sogenannte chemische Fingerabdruck [25], die Zusammensetzung der Atemluft und der Individualgeruch des Menschen [27] oder die komplexe Struktur der Iris [5]. So ist es heute denkbar, das Verhalten eines Menschen bei der Bedienung von mobilen Devices durch sein Tippverhalten zu charakterisieren. Analog dazu wurden Algorithmen entwickelt, die eine Identifizierung oder Verifizierung von Personen über die Benutzung eines Bio-Pens [49] ermöglicht. Dabei ist die Vorgehensweise mit dem Verfahren der Analyse der klassischen Handschrift vergleichbar. Die Authentifizierung von Personen über deren Handschrift ist in den letzten Jahren ein wichtiges Einsatz- und Forschungsgebiet des Sicherheitssektors geworden

Dabei wird das individuelle Schriftbild einer Person mithilfe eines Passwortes aufgenommen und anschließend mit biometrischen Algorithmen ausgewertet, um Identität festzustellen oder auszuschließen. Jüngste Untersuchungen [2] zeigten, dass dieses Verfahren auch in der Forensik genutzt werden kann. Der BiSP (Biometric Smart Pen) zum Beispiel erkennt Bewegungen in der Luft und kann die gewonnenen Daten dank vieler Nachbearbeitungsschritte besser und schneller miteinander vergleichen. Die durchweg sehr hohen Wiedererkennungsraten der einzelnen Schriftbilder (99,9 %) sprechen ganz klar für den forensischen Einsatz dieser Technik. Die aufwendigen Bearbeitungsschritte benötigen jedoch einen enormen Rechenaufwand, wodurch einzelne Berechnungen bis zu 15 Sekunden dauern können, was im Vergleich zu anderen biometrischen Untersuchungen (Fingerabdruck, IrisScan) langsam ist. Diese Problematik sollte, neben der Verbesserung der Usability der Geräte, Inhalt weiterer Forschungen auf diesem Gebiet sein.

2.3 Biometrische Merkmale

Die Biometrie beschäftigt sich mit dem Vermessen von Lebewesen nach quantitativen Merkmalen. Es handelt sich um die automatisierte Vermessung eines individuellen – physiologischen oder verhaltenstypischen – Merkmals einer Person, um eine Identifikation bzw. Verifizierung von Personen zu ermöglichen. Das Ziel der Biometrie ist die Zuordnung einer Identität und entsprechender Rechte zu einer physischen Person. Unterschieden werden biometrische Verfahren und Systeme. Ein biometrisches Verfahren ist ein auf biometrischer Erkennung basierender Mechanismus zur Authentisierung eines Menschen aufgrund seiner persönlichen, biologischen Eigenschaften mittels entsprechender Erkennungsgeräte. Unter einem biometrischen System ist eine Hard- und Software-Kombination zur biometrischen Identifikation oder biometrischen Verifikation zu verstehen, das unter Verwendung biometrischer Verfahren arbeitet. Die Grundlage aller biometrischer Verfahren basiert darauf, dass verschiedene Körper- oder Verhaltensmerkmale einem bestimmten Menschen zuzuordnen sind. Viele der für eine biometrische Erkennung verwendeten körperlichen Merkmale wie Gesicht und Finger sind offen erkennbar. Biometrische Merkmale können schließlich nicht auf anderen Menschen übertragen werden. Erkannt wird der Nutzer hier anhand seiner Individualität. Im Gegensatz zu lediglich auf

Tab. 2.2 Biometrie, Wissen und Besitz in Bezug auf Kopierbarkeit, Verlust, Diebstahl, Änderbarkeit und Weitergabe

	Biometrisches Merkmal	Persönlichen Besitz (Prinzip des Besitzes)	Geheimes Wissen (Prinzip des Wissens)
Verlust	Sehr schwer bis unmöglich	Einfach	Möglich
Änderbarkeit	Schwer bis unmöglich	Einfach	Einfach
Dublizierbarkeit	Einfach bis sehr schwierig	Einfach bis schwer	Möglich
Diebstahl	Schwierig	Möglich	Möglich
Weitergabe	Einfach bis schwierig	Einfach	Möglich
Beispiel	Iris, Papillarleisten, Gesicht, Ohr	Pass, Ausweise, Mitgliedskarten, Schlüssel	PIN, Logindaten, Schließcode

die Person bezogenen Merkmalen sind diese also direkt und nicht nur abgeleitet unmittelbar an die Person gebunden. An ein körperliches Merkmal muss sich der Merkmalsträger nicht erinnern, er trägt es untrennbar stets bei sich. Es kann im Allgemeinen auch nicht geheim gehalten werden. Im Gegensatz dazu stehen Merkmale die auf persönlichen Besitz und geheimes Wissen zurückgehen. Beispiele dafür sind der Besitz eines Ausweises und die Vergabe von Passwörtern. Derartige Merkmale können leichter verloren gehen, ausspioniert bzw. weitergegeben und verändert werden. In naher Zukunft ist von einer Durchmischung dieser Prinzipien (Biometrie, Wissen und Besitz) bzw. Kombination auszugehen. Ein Beispiel dafür ist die Einführung des ePass in Deutschland im November 2005. In der ersten Generation ist hier das Passfoto als biometrisches Merkmal im Chip gespeichert. Seit dem 1. November 2007 werden in elektronischen Pässen der zweiten Generation zusätzlich zwei Fingerabdrücke gespeichert.

Die Tab. 2.2 stellt die drei Prinzipien (Biometrie, Wissen und Besitz) in Bezug auf Kopierbarkeit, Verlust, Diebstahl, Änderbarkeit und Weitergabe.

Biometrische Merkmale sind aus biologischer Sicht schwer in Kategorien einteilbar. Zum einen enthalten sie genotypische Anteile und sind somit auch vererbbar. Zum anderen entstehen viele der biometrischen Merkmale, welche in der forensischen Fallarbeit genutzt werden, durch einen zufälligen Prozess während der Embryonalentwicklung. Andere Merkmale sind verhaltensgesteuert und damit konditioniert und anerzogen bzw. können geändert werden. Nach der Entstehung biometrischer Merkmale könnten somit drei Kategorien genutzt werden:

- genotypisch,
- randotypisch,
- konditioniert.

Oft enthält jedes einzelne biometrische Merkmal alle drei Entstehungskategorien, die mit einer unterschiedlichen Gewichtung, im Sinne einer Bewertung, eingehen. Die Stimme eines Menschen ist durch die individuelle Anatomie geprägt, jedoch unterliegt die Klangfarbe der Stimme im Prozess von Wachstum und Alterung starken Schwankungen. Dieses

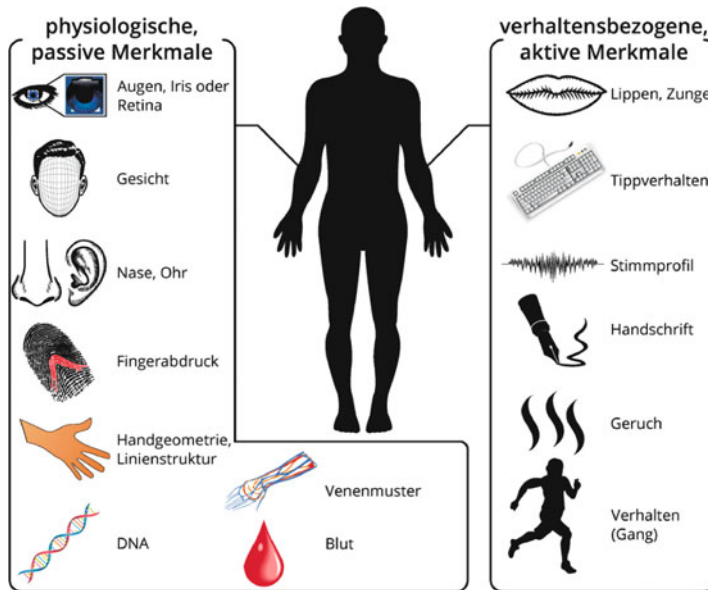


Abb. 2.2 Darstellung einer möglichen Einteilung biometrischer Merkmale auf der Grundlage ihrer Entstehung und Veränderbarkeit. Es werden die Gruppen der physiologischen bzw. verhaltensbezogene Merkmale unterteilt

Merkmal wird durch den momentanen Zustand der Person (Stress, Freude, Trauer) in einer konkreten Situation moduliert. Im Allgemeinen stellt man im Prozess der Authentifizierung und Identifizierung folgende Eigenschaften an biometrische Merkmale:

Einzigartigkeit: Merkmal muss hinreichend verschiedene Ausprägungen besitzen

Konstanz: Merkmal soll sich im Laufe der Lebenszeit möglichst wenig verändern

Verbreitung: Merkmal soll möglichst häufig in der Population vorhanden sein.

Leider sind diese Kriterien nicht immer hinreichend wissenschaftlich untersucht und dokumentiert. Biometrische Merkmale werden in der Praxis in zwei Kategorien, nach Entstehung und Veränderbarkeit, eingeteilt: physiologische (passive Merkmale) und verhaltensbezogene (aktive Merkmale). Abb. 2.2 zeigt eine Reihe biometrischer Merkmale, welche gegenwärtig in der forensischen Fallarbeit Verwendung finden. In der Literatur erfolgt oft eine andere Einteilung auf der Grundlage der angewandten Methode zur Messung der korrespondierenden Merkmale.

Die Merkmale aus Abb. 2.2 erfüllen die Anforderungen an biometrische Merkmale, jedoch besteht eine Variation in einzelnen Eigenschaften in Bezug auf Konstanz und Einzigartigkeit.

2.4 Ausgewählte Analyseverfahren

Die biometrische Erkennung basiert auf einem einheitlichen System. Trotz der hohen Individualität der verschiedenen biometrischen Systeme kann man von einem gemeinsamen Grundaufbau ausgehen. Die drei grundlegenden Phasen sind: Erfassung der biometrischen relevanten Eigenschaft, Gegenüberstellung mit einem Template-Datensatz oder Vergleichsmaterial und dem Abgleich, dem sogenannten Matching. Für den Prozess des Matchings sind sogenannte Ähnlichkeitsfunktionen erforderlich, diese ermöglichen eine genaue Abschätzung der gefundenen Ähnlichkeit bzw. Identität. Damit wird eine numerische Bestimmung im Vergleich zwischen dem Template bzw. der Vergleichsprobe und dem Original erst möglich.

2.4.1 Der Fuß als biometrisches Merkmal im Prozess der Digitalisierung

Fußabdrücke (im Gegensatz zu Schuhabdrücken), die beispielsweise an einem Tatort hinterlassen wurde, weisen neben der Fußgröße weitere spezifische Merkmale wie z. B. Länge, Breite, Ansatzfläche oder pathologische Erscheinungen, die für eine Tätersuche genutzt werden können, auf. Exemplarisch besitzen etwa 70–80 % der Erwachsenen Fußdeformitäten, die gemeinsam mit den geometrischen Fußparametern und dem Gewicht zur Eingrenzung möglicher Tätergruppen genutzt werden können. Damit stellen die Podologie und entsprechende wissenschaftliche Ansätze zur Auswertung von Fußabdrücken an einem Geschehensort ein adäquates Hilfsmittel dar.

Ähnlich wie bei der Erfassung des Fingerabdruckes sollten die messbaren Parameter eines Fußabdruckes (z. B. Clarke-Winkel, Stritzer-Guadonov-Index, Fersenwinkel) durch technische Gegebenheiten oder äußere Bedingungen so unverändert wie möglich vorliegen. Für die digitale Erfassung der Physiognomie werden Podoskope aus dem medizinischen Bereich eingesetzt. In der Medizin wird diese Form der Bildaufnahme vorwiegend zur Feststellung von Fußschwächen und Haltungsanomalien eingesetzt. Mit der Erfassung von Druckpunkten der Füße mittels polarisierten Lichts, im statischen und aktiven Zustand, stellt diese z. T. digitalisierte Aufnahmetechnik eine moderne Form, gegenüber den klassischen Tintenabdrücken in der Forensik, dar. Zur Verarbeitung der Daten können eine Reihe von Algorithmen genutzt werden [48].

Der Canny-Algorithmus wird vorzugsweise zur Kantendetektion in einem erzeugten Graustufenbild ausgehend vom Originalbild genutzt. Zur Erhaltung des Inhaltes aus dem Originalbild gliedert sich der Algorithmus in verschiedene Faltungsoperationen. An die Umwandlung in ein Schwarz-Weiß-Bild schließt die Bewertung der Pixel und deren Nachbarschaft für die Kantenfestlegung an. Problematisch bei diesem Algorithmus ist, dass durch das Bildrauschen Helligkeitsunterschiede entstehen können, wodurch die Genauigkeit des Verfahrens beeinträchtigt wird. Um diese Schwachstelle zu umgehen, wird häufig eine normalverteilte Maske angewendet. Jedoch kann es dadurch passieren, dass feinere

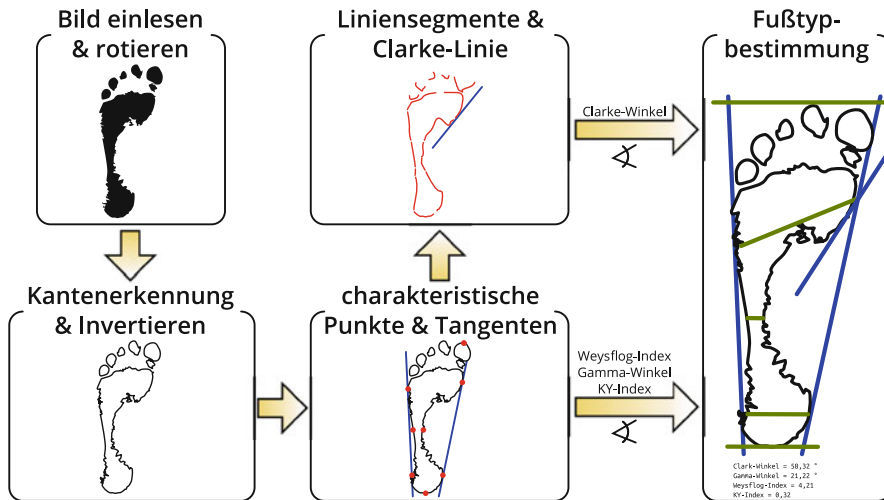


Abb. 2.3 Schritte der Fußtyperkennung

Elemente bzw. Kanten nicht als solche erkannt und folglich nicht berücksichtigt werden. Dadurch kann wiederum ein Informationsverlust im Bild entstehen [9, 21].

Mit dem Spearman-Korrelationskoeffizient wird der Grad einer linearen Abhängigkeit zwischen zwei Merkmalen bestimmt. Im Falle einer nichtlinearen Abhängigkeit würde der Wert Null resultieren. Allerdings kann zwischen den Parametern ein nichtlinearer Zusammenhang bestehen, wodurch gezeigt wird, dass der Korrelationskoeffizient kein hinreichend geeignetes Maß für die Darstellung der Merkmalsabhängigkeit ist [50].

In einer kürzlich erschienen Arbeit von Pauk et al. [37] erfolgt die Darstellung eines Systems zur allgemeingültigen computergestützten Charakterisierung diverser Fußtypen [38]. Das betreffende Verfahren teilt sich in drei grundlegende Schritte, die im Folgenden zusammenfassend erläutert werden. Im ersten Schritt werden relevante Fußparameter sowohl fotografisch als auch über ein Podoskop festgehalten. Dabei sollten die Testpersonen versuchen, eine entspannte Haltung anzunehmen. Dies hat den Zweck, dass eine annähernd regelmäßige Druckverteilung über das gesamte Fußskelett erfolgt. Des Weiteren muss in diesem Schritt eine Festlegung der Parameter im Versuchsaufbau zur Nachvollziehbarkeit und Standardisierung des Verfahrens erfolgen. Darunter eine gleichbleibende Messdistanz, homogene Kameraeinstellungen, eine horizontale Ausrichtung der Kamera, eine gleichmäßige Beleuchtung, eine voreingestellte Kameralinse und die konsistente Nutzung einer Software zur Datenakquisition und Auswertung. Der Algorithmus zur Fußtypbestimmung nach Pauk et al. (2015) (in Abb. 2.3 dargestellt) umfasst die folgenden vier Schritte:

1. Bild einlesen und rotieren
2. Kantenerkennung und Bildinvertierung

3. Detektion relevanter Messpunkte und Tangenten
4. Detektion der Liniensegmente und Clarke-Linie.

In den Schritten drei und vier werden Clarke-Winkel, Strizer-Gudonov: KY-Index, Fersenwinkel und Weysflog-Index berechnet. Die Basis hierfür bilden durch die Software erkannte signifikante parametergestützte Fußpunkte.

Zur Verifikation des Verfahrens wurden 24 männliche und weibliche Studenten ohne Verletzungen der unteren Extremität ausgewählt. Zugehörige Fußabdrücke wurden jeweils manuell sowie computergestützt erfasst und miteinander verglichen. Aus der Ergebnisgegenüberstellung wurde ersichtlich, dass keine signifikanten (Signifikanzlevel: 0,05) Unterschiede zwischen beiden Verfahren (manuell und computergestützt) zu erkennen waren. Die Studie zeigt, dass die computergestützte Analyse eine im Vergleich zu klassischen Fußabdruckverfahren nichtinvasive, schnelle und kostengünstige Alternative darstellt. Darüber hinaus zeigte sich, dass die Auswahl der Parameter ausreichend für die Analyse war. Durch den Einsatz von Algorithmen im computergestützten Verfahren wird der subjektive Einfluss des Testleiters und in Zusammenhang stehende Störvariablen minimiert. Die Autoren postulierten in der Arbeit zudem dass durch den Einsatz digitaler fotografischer Aufnahmen und einer folgenden digitalen Bildbearbeitung die Genauigkeit des Verfahrens erhöht wird [37].

Ein Fallbeispiel aus dem Jahr 1985 zeigt, dass Methoden für die Analyse von Fußabdrücken im forensischen Kontext bisher ungenügend sind und auf wissenschaftlicher, objektiver Ebene verbessert werden sollten. Mit der Schlagzeile „Spurensuche – Der ungeklärte Dreifach-Mord von Volkartshain“ beschreibt der hessische Rundfunk ein grausames Verbrechen im Jahr 1985, welches bisher noch nicht aufgeklärt ist.¹ Besonders auffällig in diesem Fall waren der unerwartete Ermittlungsablauf und die frühzeitige Präsentation von Beweisen. Die Ermittler bezogen sich in der Beweisführung auf einen blutigen Fußabdruck (Schuhgröße 44), der am Tatort gesichert wurde. Im Laufe der Untersuchungen wurden alle Männer mit der Schuhgröße 44 gebeten, einen Fußabdruck für den Zweck einer orthopädischen Analyse anfertigen zu lassen. Mit Eröffnung des Verfahrens, das überwiegend auf dem Fußabdruckvergleich der am Tatort gesicherten Spuren mit dem des Angeklagten beruhte, wurden schnell eklatante Ermittlungsfehler bemerkt. Unter anderem wurde verschleiert, dass z. B. beim Abgleich der Fußabdrücke vom Tatort mit denen vom Täter rechte und linke Abdrücke verwechselt wurden und sich laut Ergebnisstatistik eine 100 % Übereinstimmung ergab. Das Beispiel zeigt den Bedarf an objektivierten Analysemethoden in der kriminaltechnischen Arbeit und Spurenanalyse, die u. a. eine Nachvollziehbarkeit und Reproduzierbarkeit der Ergebnisse bedingen. Nur wenn eine regionalunabhängige Verfügbarkeit von Analysemethoden und technischer Ausstattung besteht, lässt sich eine objektivierte fallgebundene Darstellung der Ermittlungsergebnisse

¹ Quelle: www.hr-online.de/website/fernsehen/sendungen/index.jsp?rubrik=85159&key=standard_document_51337857

ermöglichen. Dennoch müssen die jeweiligen computergestützten Verfahrensansätze für die Analyse des biometrischen Merkmals Fuß weiter verbessert und optimiert werden.

2.4.2 Iriserkennung

Die Iris (Regenbogenhaut) wird anatomisch der Gefäßhaut des Auges zugeordnet und ist mit dem Ziliarkörper verbunden. Sie bildet eine kreisrunde pigmentierte Schicht in deren Mitte eine Öffnung – die Pupille – zu erkennen ist. Die Augenfarbe wird durch eingelagertes Melanin in der Regenbogenhaut bestimmt. In den ersten Lebensmonaten besitzen alle Menschen die gleiche Augenfarbe. Danach ändert sich diese in den meisten Fällen. Die Ausprägung des Irismusters ist ein zufälliger Prozess und ist von Ausgangsbedingungen während der embryonalen Entwicklung abhängig. Damit ist das Irismuster, entgegen der Augenfarbe, nicht genetisch kodiert. Mit einer durchschnittlichen Anzahl von über 200 Einzelmerkmalen bildet der farbige Ring um die Pupille bei jedem Menschen ein einzigartiges Muster ab. Diese Merkmale bleiben, Erkrankungen oder invasive Eingriffe ausgeschlossen, annähernd ein Leben lang erhalten. Aus den genannten Gründen ist die Iris ein sehr verlässliches biometrisches Merkmal. Selbst bei eineiigen Zwillingen ist die Irismusterung unterschiedlich ausgeprägt [14].

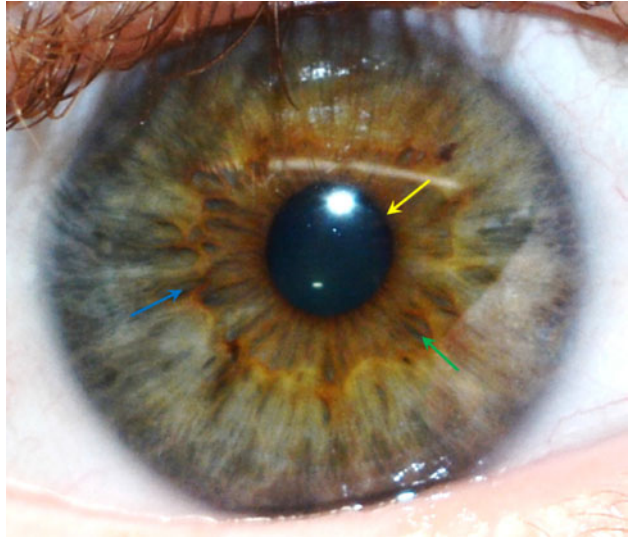
Für die Iriserkennung sind nicht die Augenfarbe, sondern die äußerlich erkennbaren Merkmale der Iris relevant. Neben dem Pupillarsaum gibt es weitere wichtige Strukturen. Zum einen wird durch den *Circulus arteriosus iridis minor* die sogenannte „Iriskrause“ gebildet, welche die Iris in zwei Bereiche einteilt. Dem Ziliarteil, welcher aus „radial gestellten Trabekeln“ [22] besteht, und dem Pupillarteil der den Sphintermuskel enthält. Zum anderen gibt es Buchten, auch Lakunen oder Krypten genannt, welche zwischen den Trabekeln angeordnet sind. In Abb. 2.4 sind diese Strukturen dargestellt [22].

Ablauf der Iriserkennung

Der dargestellte Ablauf der Iriserkennung in Abb. 2.5 ist dem patentierten Algorithmus von John Daugman nachempfunden [15]. Die Iriserkennung gliedert sich in zwei Abschnitte. Zunächst erfolgt die Aufnahme des Irisbildes während des Enrollments und die Überführung in ein Template. Daraufhin folgt der paarweise Abgleich der Templates untereinander. Während der Aufnahme wird das Auge einer Person grundsätzlich in dessen Gesamtheit aufgenommen. Um den Hintergrund in Form der Augenfarbe auszuschließen, werden die Aufnahmen im Infrarotbereich bei nahezu unsichtbarem Licht (850 nm) angefertigt, wodurch die Melaninabsorption verhindert werden soll. Bei besonders hellen Hintergründen treten oftmals Umgebungsreflexionen durch die Hornhaut auf. Dieser Effekt sollte vermieden werden, indem das Licht mit schmalen Wellenlängenbereichen bestrahlt wird. Dadurch wird lediglich das von der Kamera ausgehende Licht berücksichtigt, und ein nichtreflektierendes Bild der Iris entsteht [13].

Nachdem das Bild der Iris störungsfrei aufgenommen wurde, folgt die Segmentierung der Iris. Häufig wird hierfür die Methode einer Kreiskantenerkennung angewendet. In

Abb. 2.4 Strukturen der Iris. Äußerlich sind mehrere grobe Strukturen auf der Iris zu erkennen. Der Pupillarsaum (gelber Pfeil), welcher vom Pigmentepithel gebildet wird, die Iriskrause (grüner Pfeil), welche durch den Verlauf von Blutgefäßen entsteht und verschiedene Trabekel, die von Krypten (blauer Pfeil) unterbrochen werden. Der innere Teil der Iris wird auch als Pupillarteil, der äußere als Ziliarteil beschrieben



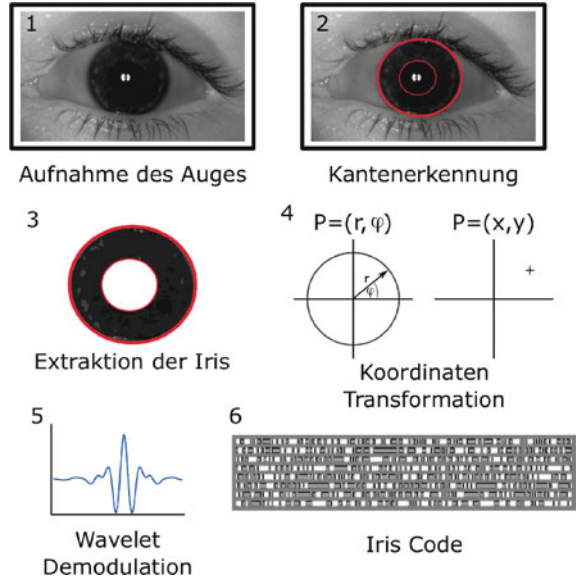
den meisten Fällen liegt jedoch, beeinflusst durch Wimpern und Augenlider, keine exakte Kreisform vor. John Daugman verwendet zur Lösung dieses Problems sogenannte Integrodifferentialgleichungen [15] (s. Gl. 2.1). Dabei wird zunächst der Irismittelpunkt bestimmt. Dies kann bereits im Schritt der Aufnahme erfolgen. Für die eigentliche Segmentierung werden im Speziellen verschiedene Übergänge, bedingt durch Helligkeitsunterschiede im Übergang von Pupille zu Iris, berücksichtigt (Abb. 2.5).

$$\max_{r, x_0, y_0} \left| G_{\sigma}(r) * \frac{\partial}{\partial r} \oint_{r, x_0, y_0} \frac{I(x, y)}{2\pi r} ds \right|. \quad (2.1)$$

Der Irismittelpunkt wird durch die Variablen X_0 und y_0 bestimmt. $I(x, y)$ beschreibt das Augenbild in Abhängigkeit der Helligkeitsintensität und wird über die Kreisfläche $ds(r)$ integriert. Mithilfe der partiellen Ableitung nach dem Radius r wird die größte Helligkeitsänderung ermittelt. Ein zu bewertender Übergang wird somit durch die maximale Änderung beschrieben. Die Rauschreduktion wird durch eine Gaußkurve G_{σ} beschrieben. Mit der Bestimmung eines neuen Startpunktes wird dann eine neue Iteration ausgeführt. Der Prozess einer Übergangsbestimmung endet, sobald die Änderung des Maximums unter einen definierten Schwellwert fällt. Aus der Segmentierung resultiert dann der aktuelle Irismittelpunkt und die Radien. Bei der Lid-Kanten-Erkennung werden parabolische Integrodifferentialgleichungen verwendet. Trotz der Komplexität überzeugen diese Operationen gerade durch deren Effizienz und Schnelligkeit [13].

Einflussfaktoren wie unterschiedlich scharfe Übergänge zwischen Sklera und Iris, nichtzirkuläre Iriskanten sowie unterschiedlich große Pupillen und Sehwinkel können eine Identifikation beeinträchtigen. Aus diesem Grund werden zur Repräsentation der

Abb. 2.5 Ablauf der Iriserkennung modifiziert nach [15]



realen Konturen der Iris sogenannte „Active Contours“ genutzt. Im Algorithmus von John Daugman wird dazu eine Fourier-Reihenentwicklung, anstelle einer Transformation, verwendet. Damit wird ein schnelles Vorgehen und eine Art Flexibilität der „Active Contours“ erreicht:

$$C_k = \sum_{\theta=0}^{N-1} r_{\theta} e^{-\frac{2\pi i k \theta}{N}}. \quad (2.2)$$

Aus M diskreten Fourier-Koeffizienten (Gl. 2.2) ergibt sich die Fourierreihe (Gl. 2.3) als Approximation der inneren oder äußeren Iriskanten:

$$R_{\theta} = \frac{1}{N} \sum_{k=0}^{M-1} C_k e^{\frac{2\pi i k \theta}{N}}. \quad (2.3)$$

Zur Bestimmung der Iriskanten werden im Daugman-Algorithmus 16–17 Fourier Koeffizienten für die inneren Kanten und 4–5 für die äußeren Kanten angewandt. Für die Wimperndetektion wird eine Verteilung der Irispixel mithilfe eines Histogramms erstellt. Sehr helle Pixel werden hierbei der Iris und dunkle Pixel den Wimpern zugeordnet. Durch einen spezifischen Schwellwert können Wimpernzugehörige Pixel eliminiert werden [15]. Für den anschließenden Schritt der Iris-Code-Erzeugung wird das zuvor bearbeitete Bild in eine Polarkoordinatendarstellung überführt (s. Gl. 2.4) [15]:

$$\begin{aligned} I(x(r, \theta), y(r, \theta)) &\longrightarrow I(r, \theta) \\ x(r, \theta) &= (1-r)x_p(\theta) + rx_s(\theta) \\ y(r, \theta) &= (1-r)y_p(\theta) + ry_s(\theta). \end{aligned} \quad (2.4)$$

Nach der Transformation folgt eine Projektion der Irisregionen auf zweidimensionale Quadratur-Gabor-Wellenpakete für die Extraktion von Phaseninformationen:

$$h_{\{Re,Im\}} = \text{sgn}_{\{Re,Im\}} \int_{\rho} \int_{\phi} e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} \rho d\rho d\phi. \quad (2.5)$$

Die Bestimmung des Phasors $h_{\{Re,Im\}}$ erfolgt nach der Gl. 2.5. Die Parameter α und β geben die Größenparameter der 2D-Wavelets (0,15–1,2 mm) an. Die Wavelet-Frequenz wird mit ω angegeben [15, 41]. Für jeden Phasor werden mithilfe von Quadranten komplexe Bits bestimmt. Dabei wird die Lage des Phasors ermittelt und Phasenkoordinaten (real, imaginär) als Paar von Nullen und Einsen ausgegeben. Aus der Iristransformation resultiert schließlich ein Iris-Code, bestehend aus 2048 Phasor-Bits bzw. 256 Bytes [15]. Den letzten Schritt der Iriserkennung bildet der bitweise Vergleich erzeugter Templates über die Bestimmung der Hammingdistanz beider Iris-Codes (Gl. 2.6 [15]). Der XOR-Operator gibt bei nicht identischen Bits eine Eins und bei Übereinstimmung eine Null aus. Störungen, die z. B. durch Reflexionen, Augenbrauen oder Augenlieder entstehen werden mit einer Und-Verknüpfung zwischen zwei Bitmustern ermittelt. Große Unterschiede zwischen zwei Iris-Codes werden mit dem Wert 1 der Hamming-Distanz beschrieben. Umgekehrt kennzeichnet ein Wert 0 eine Übereinstimmung zweier Codes. Im Allgemeinen würde das biometrische System ab 70 % Identität, d. h. einer Hamming-Distanz von 0,3, ein positives Ergebnis beim Abgleich von zwei Irismustern erbringen:

$$HD = \frac{\| (codeA \otimes codeB) \cap maskA \cap maskB \|}{\| maskA \cap maskB \|}. \quad (2.6)$$

Die Iriserkennung bietet zusammengefasst zahlreiche Vorteile, die sie als biometrisches Merkmal auszeichnet. Ähnlich wie der Fingerabdruck besitzt das Irismuster ein ähnlich hohes Maß an Variabilität und Zufälligkeit der Textur. Ein großer Vorteil gegenüber Fingerabdrucksystemen ist die berührungsfreie Aufnahmemethode der Iriserkennungssysteme. Es ist sogar möglich, aus einigen Metern Entfernung ein Augenbild aufzunehmen und die Iris zu segmentieren. Somit kann eine Personenidentifizierung völlig unbemerkt und ohne das Zutun einer Person erfolgen. Im Vergleich zu anderen biometrischen Systemen zeigt sich, dass bei der Iriserkennung die geringsten Fehlerraten vorliegen. Mit einer *FRR* von 0,45 % und einer *FAR* von 0,0001 wird nur ein geringer Teil falsch identifiziert.

2.5 Fingerabdruckanalyse

2.5.1 Der Fingerabdruck als biometrisches Merkmal

Nach wie vor gilt ein gesicherter Fingerabdruck vor Gericht und im Ermittlungsverfahren als eines der anerkanntesten biometrischen Merkmale zur Personenidentifizierung.

Zusammen mit der DNA-Analyse besitzt der Fingerabdruck vor Gericht ein hohen Beweiswert. Die Musterentstehung der Fingerabdruckmorphologie ist ein genetisch unabhängiger Prozess, d. h., notwendige Informationen sind genetisch nicht kodiert und werden nicht auf Nachfolgenerationen weitervererbt. Das Hautleistenmuster ist bereits im vierten Embryonalmonat vollständig ausgebildet und bleibt bis zum Tode erhalten. Der Bereich, der sich mit der Charakterisierung von morphologischen Besonderheiten eines Fingerabdruckes beschäftigt, wird als „Daktyloskopie“ bezeichnet. Egal ob klassische Daktyloskopie oder digitale Auswertung der Spuren, die komplexe Wissenschaft trägt eine ganz eigene Entwicklungsgeschichte, ein einzigartiges Klassifizierungssystem und eine situationsungebundene Anwendung [23].

Bis zur Rechtsprechung im Jahr 1952, durch die der uneingeschränkte Beweiswert der Daktyloskopie im Strafverfahren anerkannt wurde, erfolgte die Datenverarbeitung und -sicherung eher über eine mittlerweile überholte Variante. Fingerabdrücke wurden mit Tinte abgenommen, auf ein Zehnfingerblatt aufgebracht und die Ablage der Blätter bzw. Recherche erfolgte in großen Karteischränken. In den 60er und 70er Jahren entwickelte sich das Verfahren in Richtung einer effizienten, datenbankgestützten Speicherung der Fingerabdrücke, um den stetig wachsenden Datenbeständen gerecht zu werden. Einer der wohl bedeutendsten Qualitätssprünge wurde mit der Einführung des automatisierten Fingerabdruckidentifizierungssystems (AFIS), das im Jahr 1992 in Betrieb genommen wurde, erzielt. Dadurch ergaben sich ganz neue Perspektiven der Datenspeicherung. Mit der Implementierung der Software *MetaMorpho* vor wenigen Jahren können mittlerweile auch Handflächen Spuren digitalisiert und ausgewertet werden. Nach aktuellen Zahlen des BKA werden monatlich mehr als 40.000 neue Fingerabdruckblätter erfasst. Die AFIS-Datenerfassung erfolgt teilautomatisiert. Jedes Grundmuster wird auch heutzutage noch über das Expertenwissen eines Daktyloskopiespezialisten ausgewertet und über die Tastatur kodiert [12, 36].

Den höchsten Identifizierungswert bei der Fingerabdruckanalyse besitzen die auf der Leistenhaut befindlichen Papillarlinien des Menschen. Jeder Mensch trägt auf der Leistenhaut individuelle Muster (Schleife, Bogen, Wirbel) und zahlreiche Besonderheiten bzw. Linienunterbrechungen (Minutien), die sich von Finger zu Finger unterscheiden.

2.5.2 Technologien zur Aufnahme des Fingerabdrucks

In der IT-gestützten, automatisierten Form ist das digitale Fingerabdruckverfahren ein biometrisches Konzept mit hoher Erkennungsleistung. Für den Vorgang der Fingerabdruckanalyse sind vier grundlegende Schritte notwendig.

1. Abtastung des Fingerabdrucks,
2. Bildgenerierung,
3. Merkmalsextraktion,
4. Matching.

Abtastung des Fingerabdrucks

Bei der Erfassung des Fingerabdrucks wird zwischen Online- und Offline-Systemen unterschieden. Mittels der Abdruckvariante auf Papier wird ein Abbild durch gleichmäßiges Abrollen des Fingers mithilfe von Tinte gewonnen (Offline-System). Der Finger wird von einer Lageseite zur anderen abgerollt, um die vollständige Linienform zu erfassen. Anschließend kann der Abdruck fotografiert oder gescannt werden. Nachteile der Methode sind auftretende Verzerrungen des Bildes, die beim Auf- und Abdrücken des Fingers entstehen, und ein langsamer Verfahrensablauf. Für ein teilautomatisiertes Kontrollsystem zur Überprüfung von Zutrittsberechtigungen ist die Aufnahme auf Papier aus diesen Gründen nicht geeignet. Für die Erfassung von Lebendabdrücken wird der Finger selbst durch leichtes Auflegen auf einen Sensor abgetastet und mit dem Datenverarbeitungssystem verbunden (Online-System). Dadurch ist der Ausschnitt des Fingerabdruckes kleiner als bei der Erfassung auf Papier. Damit können die besonderen Gegebenheiten der Finger wie die verschiedenen Hauttypen, Beschädigungen, Trockenheit oder Feuchtigkeit toleriert werden.

Mit der Einführung neuartiger sensorbasierter Verfahren zur Abtastung und Aufnahme von Fingerabdrücken vor über 30 Jahren entwickelte sich ein breites Feld an zugrundeliegenden Technologien für den Einsatz in der forensischen Praxis. Die zur Abtastung üblicherweise angewandten Technologien lassen sich in die Kategorien optische Sensoren, Siliziumsensoren und Ultraschallwellensensoren einordnen.

Optische Sensoren

Häufig kommen optische Sensoren, bei denen der Finger über einen Scanner oder eine Kamera aufgenommen wird, zum Einsatz. Ein Beispiel für einen optischen Sensor ist in Abb. 2.6 dargestellt. Zunächst wird der Finger auf eine Ebene bzw. eine Glasfläche (z. B. Glasprisma, Fiberglas) aufgebracht und das ausgehende Licht beim Auflegen des Fingers zu einem CCD-Sensor geleitet. Damit eine gute Qualität des Abbildes gewährleistet ist, sollten die Oberflächen regelmäßig von zurückgebliebenen Schweiß- oder Dreckspuren gereinigt werden. Im Allgemeinen sind hier Aufnahmen mit bis zu 500 dpi möglich. Ein gravierender Nachteil dieser Technologie ist, dass sie durch Fingerprothesen oder andere Imitate relativ einfach „auszutricksen“ ist [34].

Siliziumsensoren

Die Abtastung mittels Siliziumsensoren beruht auf der Messung physikalischer Größen, wie z. B. Wärme, elektrische Feldstärke oder Kapazität. Der Finger wird nicht wie bei den optischen Sensoren auf eine Glasprismafläche aufgebracht, sondern auf eine dünne Schicht, über welche die entsprechende physikalische Größe gemessen wird. Im Aufbau des Sensors werden mehrere Sensoruntereinheiten, in Form zweidimensionaler Arrays, unterschieden. Im resultierenden Bild entspricht jede Sensoruntereinheit einem Pixel. Von Vorteil sind die geringe Sensorgröße und die niedrigen Anschaffungskosten. Allerdings ist die Schutzschicht sehr empfindlich gegenüber äußeren Einflüssen. Eine elektrostatische Entladung des Fingers reicht schon aus, um den Sensor außer Betrieb zu setzen. Mit einer

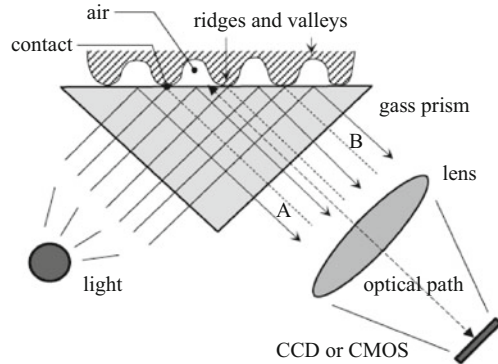


Abb. 2.6 Beispiel für einen optischen Sensor. Bestandteile des FTIR-Sensors (Frustrated Total Internal Reflection) sind: eine Lichtquelle, ein Glasprisma, eine Linse und ein CMOS- oder CCD-Sensor. Durch das direkte Aufbringen des Fingers auf das Glasprisma haben die Grate direkten Kontakt mit dem Prisma. Zwischen den Tälern und dem Prisma ist hingegen Luft. Das auf das Prisma einseitig gesendete Licht wird an den Tälern reflektiert und an den Graten absorbiert bzw. zufällig gestreut. Reflektierte Strahlen werden auf der anderen Seite durch eine Linse auf ein CMOS- oder CCD-Sensor zur Aufnahme gebündelt [34]

robusteren Schutzschicht könnte dieser Effekt umgangen werden. Jedoch würde somit die Erkennungssensitivität des Fingerabdruckes herabgesetzt werden [34].

Ultraschallwellensensoren

Vergleichsweise neuartig im Feld der Fingerabdruckerkennung ist der Einsatz von Ultraschallwellensensoren. Gemessen wird hierbei die Distanz zur Fingeroberfläche mithilfe von akustischen Ultraschallwellen, die vom Finger reflektiert werden ohne einen direkten Kontakt von Finger und Sensor. Durch Reflexion bzw. Absorption kann somit eine epidermale Mustererkennung im Abdruck erfolgen. Von Vorteil gegenüber den anderen beiden vorgestellten Technologien ist, dass die ausgesendeten Wellen unbeeindruckt von anhaftenden Schmutzpartikeln am Finger sind. Damit ist der Sensor stabil gegenüber äußeren Einflüssen. Allerdings ist die Praxistauglichkeit durch die Größe der Geräte und einen hohen Kostenfaktor gegenwärtig noch nicht ausgereift [43].

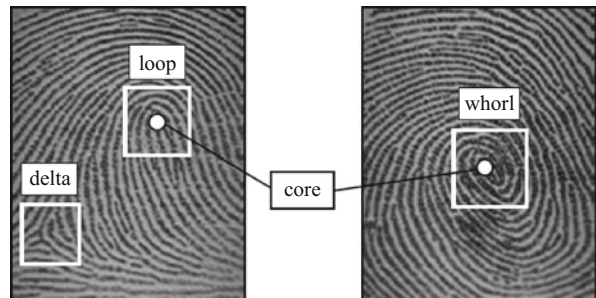
Bildgenerierung

Infolge einer sensorbasierten Aufnahme eines Fingerabdruckes resultiert ein Graustufenbild des individuellen Papillarlinienmusters. Dunkle Linien repräsentieren Grate und helle Täler. Wie gut das Endresultat der Aufnahme ist, hängt sowohl von technischen Details (z. B. Bildauflösung, mind. 500 dpi), von personenabhängigen Einflussfaktoren (z. B. ausgeübter Druck oder Platzierung des Fingers) als auch von hautabhängigen Gegebenheiten (z. B. sehr trockene oder sehr feuchte Haut) ab (Abb. 2.7). Die Erstellung eines Graustufenbildes kann über zwei Aufnahmemodi erfolgen. Im Livescan-Modus wird, wie oben beschrieben, der Abdruck über ein sensorbasiertes Verfahren detektiert. Hingegen wird



Abb. 2.7 Einfluss der Hautbeschaffenheit auf die Qualität des Bildes. **a** Fingerabdruck guter Qualität; **b** trockene Haut; **c** sehr feuchter Hautabdruck; **d** i. A. schlechter Fingerabdruck [34]

Abb. 2.8 Singularitäten und Kern [34]



beim Offline-Modus ein latenter Fingerabdruck unabhängig von einem Sensor, z. B. über fotografische Aufnahmen, erzeugt, welche dann später über einen Scanner digitalisiert werden können [34].

Merkmalsextraktion

Die Klassifikation von Eigenschaften der Gratbestandteile (engl. *ridges*) eines Fingerabdruckes erfolgt hierarchisch über drei Ebenen. In der ersten Ebene werden topologische Singularitäten (Delta, Schleife, Wirbel) (Abb. 2.8) extrahiert [34]. Diese Singularitäten werden wiederum zur Klassifikation des Abdruckes in das zugehörige Grundmuster (Abb. 2.9) genutzt. Die Extraktion von Singularitäten und dem Kern dient der Indexierung und Klassifizierung des Fingerbildes während der algorithmischen Verarbeitung des Bildes [34].

Auf der zweiten Ebene werden weitere Eigenschaften, sogenannte Minutien (lat. *minutus* = „Kleinigkeit“), im individuellen Muster zur Templategenerierung gesucht. Diese kleinen Besonderheiten im Papillarlinienverlauf entstehen durch diverse Formen von Un-

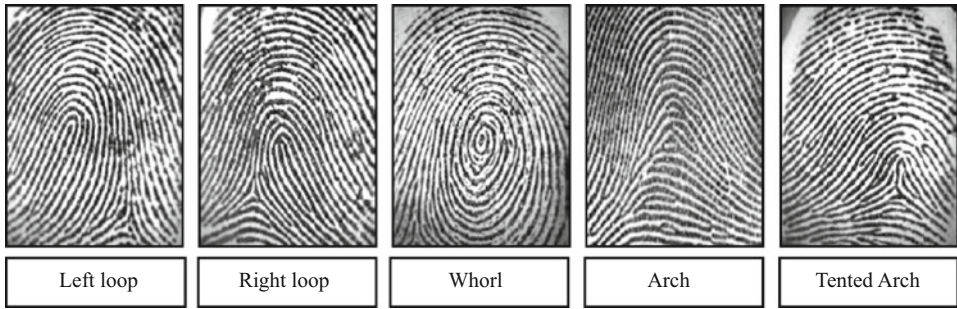


Abb. 2.9 Grundmusterklassen nach Henry (1990) [34]

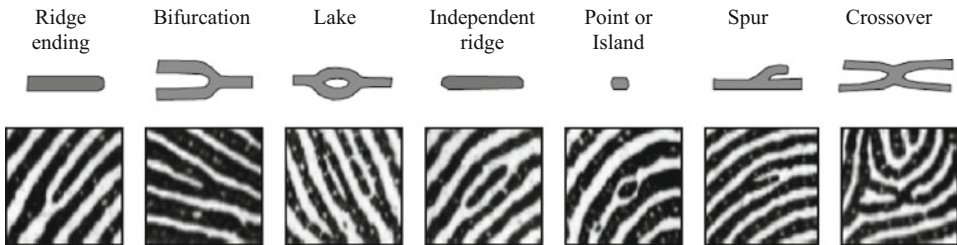
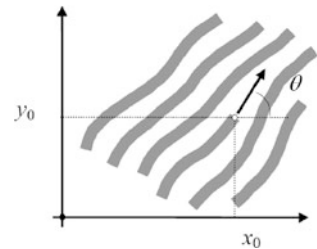


Abb. 2.10 Häufig vorkommende Minutienarten [34]

Abb. 2.11 Minutienkoordinati-
on. Eine Gratendung mit deren
Koordinaten $[x_0, y_0]$. θ ist der
Winkel, der durch die Minu-
tientangente mit der x -Achse
gebildet wird [34]



terbrechungen der Grate (Abb. 2.10). Zu Ehren von Francis Galton, der 1892 erstmals eine Klassifikationsschema für Minutien präsentierte, werden die Merkmale häufig auch „Galton details“ genannt [16, 34]. Häufig werden zur Lokalisation und näheren Beschreibung der Minutie im Graustufenbild die Position sowie ein ungefährer Tangentenwinkel im Bild angegeben (Abb. 2.11) [34].

Weitere Informationen zu den Graten, wie Breite, Form und Kontur, aber auch die Anordnung der Poren können auf der dritten Ebene der Merkmalsextraktion erhalten werden [34].

Orientierungsbilderzeugung

Grundlage der später durchzuführenden Minutienbestimmung ist die Generierung eines Orientierungsbildes aus dem originalen Fingerbild. Bei diesem Vorgehen wird zunächst

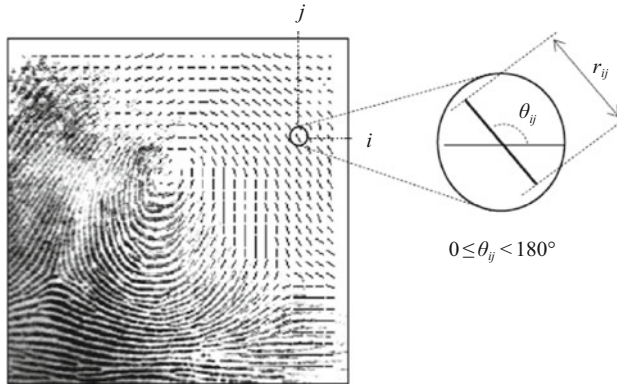


Abb. 2.12 Koordinatenvergabe und Blockorientierung zur Erzeugung eines Orientierungsbildes. Der Block $[i, j]$ aus einer 16×16 -Matrix besitzt die lokale Orientierung q_{ij} und den Zuverlässigkeitswert r_{ij} . Jedes Element bezeichnet die lokale Ausrichtung der Papillarlinien. Die lokale Orientierung ist durch die Auslenkung der Strecke zur x -Achse dargestellt und die Größe des Zuverlässigkeitswertes durch die Länge dieser Strecke [34]

das aufgenommene Muster (Fingerabdruck) in regelmäßige Blöcke unterteilt. Dabei ist es möglich, dass ein Block aus einem einzigen Pixel besteht. Anschließend erfolgt die Beschreibung jedes Blockes der Matrix über die Orientierung eines Gattes, indem eine lokale Orientierungsangabe durch den Winkel zwischen Grattangente und der horizontalen x -Achse im Muster abgebildet wird [20]. Für die Berechnung eines Orientierungsbildes aus dem Fingerabdruck können verschiedene mathematische Verfahren, wie der projektionsbasierte Ansatz nach Stock und Swonger (1969) oder die Berechnung der Gratgradienten [39, 40, 45] verwendet werden.

Durch mögliche Bildungenauigkeiten, beispielsweise ein Bildrauschen, muss die jeweilige bestimmte Blockorientierung auf Zuverlässigkeit geprüft werden. Hierzu wird das Phänomen der „Glattheit“ des Fingerabdruckes bewertet, d. h., bei geringem Bildrauschen verändert sich die lokale Orientierung direkt benachbarter Blöcke kaum. Verallgemeinert beschreibt das Zuverlässigkeitsmaß die Übereinstimmung benachbarter Orientierungen (Abb. 2.12) [34].

Aus der Gesamtheit aller Orientierungen der Teilblöcke ergibt sich dann das Orientierungsbild, wie in Abb. 2.13 zu erkennen [34].

Frequenzbilderzeugung

Nach der Erzeugung des Orientierungsbildes folgt die Erstellung eines Frequenzbildes, über welches die lokale Dichte der Grate bestimmt wird. Auf Grundlage der Dichteinformationen können sowohl eine Menge an Fingerabdrücken als auch Fingerabdruckregionen voneinander unterschieden werden. Für jeden bereits existierenden Block im Orientierungsbild $[x_i, y_i]$ wird ein weiteres Segment gewählt, welches orthogonal zum lokalen Orientierungsmittelpunkt des Blocks zentriert ist. Daraufhin wird die Anzahl der segment-

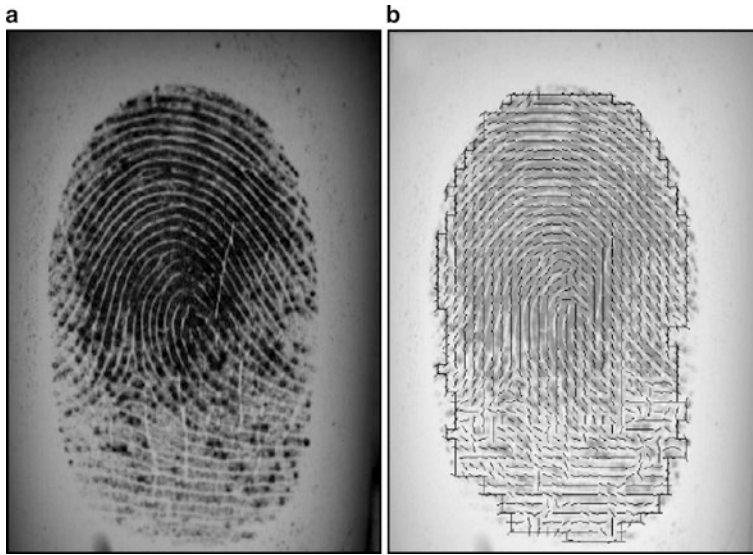


Abb. 2.13 Orientierungsbild. Von dem Fingerbild (a) wurde das Orientierungsbild (b) erzeugt [34]



Abb. 2.14 Frequenzbild von zwei Fingerabdrücken. Helle Bereiche bzw. Blöcke lassen hohe Frequenzwerte erkennen. Hingegen kennzeichnen dunkle Blöcke niedrige Frequenzbereiche [33, 34]

schneidenden Grate ausgezählt. Im Bild wird ein Grat als Graustufenspitze angenommen. Nach der Berechnung der Frequenzwerte werden die unterschiedlichen Gratdichten übergreifend in Form von Grauabstufungen dargestellt (Abb. 2.14).

Segmentierung

Der Schritt der Segmentierung beschreibt verallgemeinert die Trennung des Fingerabdruckmusters (Vordergrund) vom Bildhintergrund, um die Extraktion von Hintergrundinformationen (z. B. Bildrauschen) zu vermeiden. Eine Variante der Segmentierung stellt die Erzeugung des Orientierungsbildes dar, wobei von einer sog. „Unorientiertheit“ des

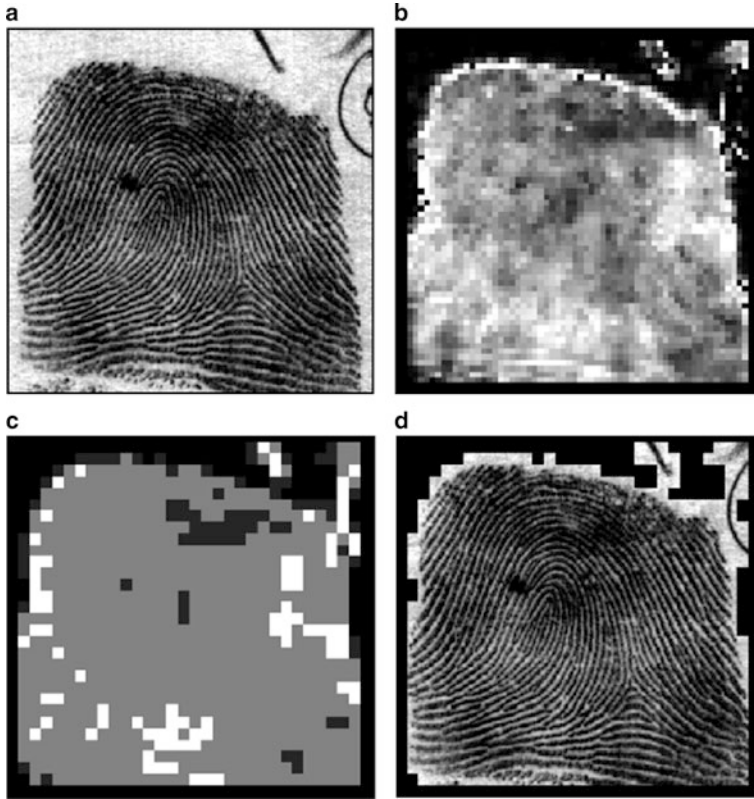


Abb. 2.15 Methoden der Segmentierung nach Ratha et al. [40]. **a** Originalbild; **b** Varianzfeld; **c** aus **b** abgeleitetes qualitatives Bild: ein Wert („gut“, „mittel“, „schlecht“ oder „Hintergrund“) für die Qualität wird in Abhängigkeit der Varianz jedem Block zugeordnet; **d** segmentiertes Bild [34]

Hintergrundes ausgegangen wird. Der Abdruck an sich ist hierbei stark orientiert (siehe Abb. 2.15). Mit problembasierten Lernmethoden für die Segmentation z. B. nach Bazen and Gerez [3], Chen et al. [10] und Zhu et al. [51] kann eine detailliertere Segmentierung im Vergleich zu z. B. Schwellwert-basierten Methoden erfolgen [3, 10, 51].

Bestimmung von Singularitäten und dem Kern

Wie bereits in der Einleitung zum Schritt der Merkmalsextraktion beschrieben, werden sowohl der Kern als auch die Singularitäten zur Indexierung und Klassifizierung des Fingerabdruckes benötigt. Ein Verfahren zur Bestimmung dieser beiden Variablen ist das Poincaré-Indexierungsverfahren nach Kawagoe und Tojo [28]. Der Poincaré Index wird wie in Gl. 2.7 dargestellt berechnet, wobei d_k , $k = 0, \dots, 7$, die acht umliegenden Blöcke von $[i, j]$ sind und jeweils die Blöcke d_k , $d_{(k-1) \bmod 8}$ benachbart sind.

$$P(i, j) = \sum_{k=0, \dots, 7} \text{angle}(d_k, d_{(k-1) \bmod 8}) \quad (2.7)$$

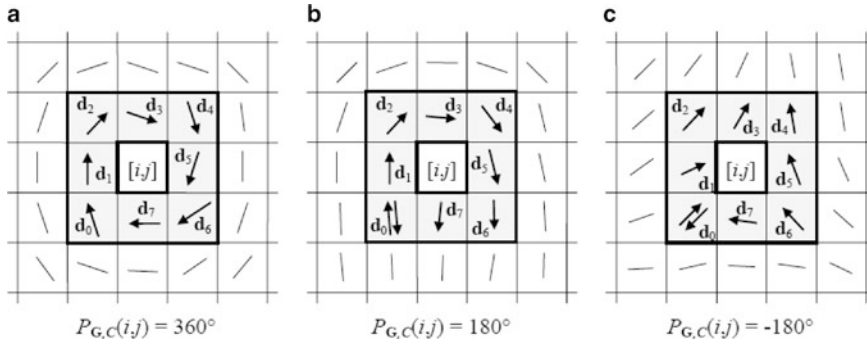


Abb. 2.16 Beispielhafte Berechnung des Poincaré-Index in der 8er-Nachbarschaft von Punkten die zu (v. l. n. r.) einer Wirbel-, Schleife-, und Delta-Singularität gehören [34]

Mit der Funktion *angle* wird der Unterschied zwischen den Winkeln beider Blockorientierungen beschrieben. Bei der Erzeugung gerichteter Orientierungen wird beim ersten Block eine der beiden möglichen Richtungen gewählt. Die direkte Nachbarschaft wird dann immer mithilfe des kleinsten Winkelunterschiedes bestimmt. Der Index wird dann gemäß Gl. 2.8 interpretiert (vgl. Abb. 2.16) [34].

$$P_{G,C}(i, j) = \begin{cases} 0^\circ & \text{if } [i,j] \text{ does not belong to any singular region} \\ 360^\circ & \text{if } [i,j] \text{ belongs to a whorl type singular region} \\ 180^\circ & \text{if } [i,j] \text{ belongs to a loop type singular region} \\ -180^\circ & \text{if } [i,j] \text{ belongs to a delta type singular region} \end{cases} \quad (2.8)$$

Minutienbestimmung

Die Bestimmung von Minutien kann über zwei Methoden erfolgen. Zum einen kann dies über das erzeugte Graustufenbild, zum anderen über ein Binärbild geschehen. Beim Einsatz des Graustufenbildes wird, ausgehend von einem lokalen Punkt, über die Grate iteriert und ein neues Bild aufgezeichnet. Vom lokalen Punkt wird in Richtung der lokalen Orientierung eines Zwischenpunktes gegangen. Daraufhin wird eine orthogonal zur Orientierung gelegene Strecke mit dem Zwischenpunkt als Ursprung betrachtet. Auf dieser Strecke wird der höchstgelegene Punkt, welcher einen neuen Punkt darstellt, gesucht. Die Schritte werden bis zu einer bereits bekannten Gratmündung oder dem Gratende wiederholt [34].

Zunächst muss das Graustufenbild in ein Schwarzweißbild, durch Umwandlung der Pixel entsprechend eines Grau-Schwellwertes, transformiert werden. Im Ergebnis wird ein Binärbild erzeugt. Die Grattendicke wird im Binärbild auf die Breite eines Pixels normiert. Mögliche Artefakte, die hierbei entstehen und zu einer fälschlichen Identifikation führen können, werden aus dem Bild gefiltert, um die tatsächlichen Minutien bestimmen zu können. (Abb. 2.17) [32].



Abb. 2.17 Minutiendetektion nach Maio und Maltoni [34]

Die Minutien können z. B. anhand der „crossing number“ $cn(p)$ eines Pixels p bestimmt werden (Gl. 2.9).

$$cn(p) = \frac{1}{2} \sum_{i=1, \dots, 8} |val(p_{i \bmod 8}) - val(p_{i-1})| \quad (2.9)$$

Wobei p_i , die acht Nachbarpixel von p und jeweils $p_{i \bmod 8}$, p_{i-1} benachbart sind. Der Farbwert des Pixels wird über die Funktion val angegeben (0 = weiß und 1 = schwarz). Generalisiert beschreibt $cn(p)$ die in p mündende Anzahl der Grate. Unechte Minutien, die in ihrer Struktur von tatsächlichen abweichen, werden in einem zusätzlichen Nachverarbeitungsschritt über die Glattheit des Fingers herausgefiltert.

2.5.3 Matching

Für den Vergleich zweier Fingerabdrücke (Input vs. Template) existieren drei Verfahren.

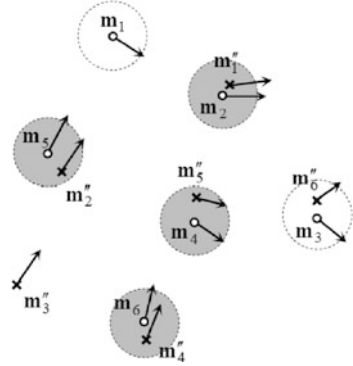
Korrelationsverfahren: Bei diesem Verfahren werden die Abdrücke über einen Vergleich der Pixel miteinander korreliert. Die Bilder werden hierbei in unterschiedlichen Positionen miteinander verglichen, um Fehlplatzierungen zu umgehen.

Minutienbasierte Verfahren: Das minutienbasierte Verfahren ist eines der etabliertesten Matching-Verfahren. Die Fingerabdrücke werden hier anhand der Minutienlage und Orientierung miteinander verglichen.

Nichtminutienbasierte Verfahren: Zum Abgleich zweier Fingerabdrücke werden hierbei Grattedichte, Orientierung und Gratform gegenübergestellt. Das Verfahren ist besonders für die Auswertung qualitativ geringer Abdrücke geeignet.

Im Folgenden wird beispielhaft die funktionsweise minutienbasierter Verfahren im Überblick dargestellt. Beide Abdrücke – Template- und Inputfingerabdrücke – lassen sich

Abb. 2.18 Matchende Minuten sind von *grau* ausgefüllten Kreisen umgeben. Hier liegen räumliche und Richtungsdivergenz unter den Toleranzwerten. Für alle übrigen Inputminuten gibt es keine matchende Templateminuterie [34]



vektoriell als $T = (m_1, m_2, \dots, m_m)$ und $I = (m'_1, m'_2, \dots, m'_n)$ beschreiben. Ein zugehöriger Vektor besitzt demzufolge eine beliebige Anzahl Minuten m_i , bzw. m_i Minuten werden als Tripel der beiden Ortskoordinaten x und y sowie ihrer Ausrichtung θ ($m_i = (x_i, y_i, \theta_i)$, $i = 1..m$; $m'_j = (x'_j, y'_j, \theta'_j)$, $j = 1..n$) beschrieben. Die räumliche Differenz sd (*spatial difference*) und die Richtungsdivergenz dd (*direction difference*) zweier Minuten werden gemäß Gl. 2.10 definiert.

$$\begin{aligned} sd(m'_j, m_i) &= \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0 \\ dd(m'_j, m_i) &= \min(|\theta'_j - \theta_i|, 360^\circ - |\theta'_j - \theta_i|) \leq \theta_0 \end{aligned} \quad (2.10)$$

r_0 und θ_0 sind die jeweiligen Toleranzwerte. Liegen räumliche und Richtungsdivergenz unter diesem Schwellwert bzw. den Toleranzwertgrenzen, kann von matchenden Minuten ausgegangen werden. In Abb. 2.18 ist der Richtungsabgleich von Minuten eines Inputfingerabdruckes mit den Minuten eines Templatefingerabdruckes dargestellt. Hier sind Minuten des Inputabdruckes mit x und die des Templates mit o bezeichnet. Die Kreise entsprechen der maximalen Entfernung, also dem Toleranzwert r_0 . Die Pfeile stellen die Ausrichtung der Minuten dar.

Damit die Anzahl an matchenden Minuten zwischen Input- und Template eruiert werden kann, müssen auf die Orts- und Richtungsparameter des Inputs verschiedene geometrische Transformationen durchgeführt werden, die eine maximale Anzahl matchender Minuten erlaubt. Dies ist zwingend, aufgrund von verschiedenen Einflussfaktoren, notwendig. So spielt z. B. die Variationsbreite bei Positionierung und Rotation, im Schritt der Fingerabdruckaufnahme, eine große Rolle. Es ist fast unmöglich, den Finger bei jeder Aufnahme identisch auf dem Sensorsystem zu positionieren, wodurch der eigentliche Erfassungsbereich des Abdruckes stark variiert. Des Weiteren kann es durch einen unterschiedlich ausgeübten Druck zu nichtlinearen Verzerrungen in der Aufnahme kommen. Ebenfalls können die im Schritt der Merkmalsextraktion entstandenen und möglicherweise nicht erkannten Artefakte zu einer Fehlinterpretation führen. Daher ist eine Qualitätsprüfung des Abdruckes während des Enrollments unerlässlich, wodurch bereit im Voraus

die genannten Einflussfaktoren beseitigt werden können. Für die geometrische Transformation existieren mehrere Möglichkeiten:

- Deplatzierung der Koordinaten x und y ,
- Skalierung,
- verzerrungstolerante Transformation,
- Rotation der Ausrichtung θ ,
- jede beliebige affine Transformation.

Die Frage nach dem „besten“ Matchingalgorithmus kann nur schwer beantwortet werden. Die Performance hängt von vielen Faktoren, wie Genauigkeit (z. B. FMR, FNMR), Effizienz (Enrollment-, Verifikationszeit), Skalierbarkeit zur $1 : N$ -Identifikation und Templategröße, ab. Des Weiteren spielt für die Entscheidung und damit auch für die Gewichtung der einzelnen Performanzmaße, natürlich das jeweilige Einsatzgebiet eine herausragende Rolle.

Am Beispiel des individuellen Papillarleistenmusters, welches sich nach der Digitalisierung als Papillarlinien-Muster darstellt, kann das Prinzip der Abhängigkeit des Informationsgehaltes eines biometrischen Merkmals von der Verwendung von Daten aus unterschiedlichen Ebenen sehr gut nachvollzogen werden. Die erste Ebene der Information stellen die Grundmuster (Schleife, Bogen, Wirbel) im Papillarlinienmuster dar. Der Informationsgehalt wird deutlich durch die Hinzunahme der anatomischen Merkmale auf der zweiten Ebene (Minutien: eingelagerte Linie, Gabelungen, Auge oder Insel) sowie durch die Lage und Form derer zueinander erhöht. Eine dritte Ebene bilden die sogenannten Erscheinungen, Zwischenlinien, Poren, Kantenverläufe und Feinstrukturen von Falten, Furchen oder Narben. Durch die Verbesserung der Aufnahmetechniken im Prozess der Digitalisierung ist der Informationsgehalt dieser Daten in der Kombination deutlich gestiegen. Eine vierte Ebene können chemische Komponenten darstellen, welche sich im Papillarleistenmuster angereichert haben. Ein solcher „chemischer Fingerabdruck“ ver-rät den Ermittlern nicht nur die Identität des Täters (aus der Analyse der ersten drei Ebenen), sondern auch, was er zuletzt in den Fingern hatte. Durch ein Analyseverfahren lassen sich Spuren von Drogen, Sprengstoff oder bestimmten Stoffwechselprodukten des Täters direkt nachweisen. Das Analyseverfahren ist die Desorptions-Elektrospray-Ionisations-Massenspektrometrie (Desi-MR). Aus den Daten wird dann der „chemische Fingerabdruck“ erzeugt und liefert zusätzlich ein klassisches Fingerabdruckbild, welches mit herkömmlich gespeicherten Dateien verglichen werden kann. Durch neuartige Methoden kann auch das feuchte Medium der Fingerbeeren analysiert werden. Beispiele dafür sind:

- Zusammensetzung [18],
- Altersbestimmung [17],
- Visualisierung [46],
- Geschlechtsbestimmung [1].

2.6 Ausgewählte Forensische Datenbanken

Der Übergang von einem biometrischen Verfahren zu einem funktionsfähigen und den Anforderungen entsprechenden biometrischen System wird durch die Suche und den Vergleich mit in Datenbanken abgelegten Datensätzen erst möglich. Nachfolgend wird eine Auswahl an gebräuchlichen Datenbanken gezeigt. In der Regel besitzen Strafverfolgungsbehörden interne, der Öffentlichkeit unzugängliche Datenbanken. Das beim Bundeskriminalamt (BKA) betriebene elektronische Informationssystem der Polizei (INPOL) dient als informationstechnisches Verbundsystem von Bund und Ländern. Zugriffsberechtigt sind neben dem Bundeskriminalamt selbst die Landespolizeidienststellen, die Bundespolizei und die Zollbehörden. INPOL besteht zum einen aus Personen- und Sachfahndungsdateien², zum anderen ist es in zahlreiche Teildatenbanken aufgeteilt, die jeweils eigene Errichtungsanordnungen, d. h. Verfahrensverzeichnisse, die u. a. die Erhebung und Weiterverwendung personenbezogener Daten regeln, besitzen. Beispiele solcher Teildatenbanken sind die DNA-Analysedatei (DAD) und das Analysesystem zur Serienzusammenführung bei Gewaltverbrechen (ViCLAS).

2.6.1 DNA-Analysedatei (DAD)

Die DNA-Analysedatei [24] ist eine zur Speicherung von DNA-Profilen eingerichtete Datenbank, die seit dem 17. April 1998 vom Bundeskriminalamt (BKA) betrieben wird. In der DAD werden durch die DNA-Analyse ermittelte genetische Fingerabdrücke von bekannten Personen (sogenannte Personendatensätze), sowie Tatortspuren von unbekannten Personen (sogenannte Spurendatensätze) eingestellt und abgeglichen. Durch die Vernetzung und den automatisierten Abgleich der DNA-Datenbanken vieler europäischer Staaten können zudem wertvolle Ermittlungshinweise bei grenzüberschreitender Kriminalität erhalten werden. Die DAD umfasste mit Ablauf des II. Quartals 2015 insgesamt 1.111.833 Datensätze, die sich aus 839.875 Personendatensätzen und 271.958 Spurendatensätzen zusammensetzen. Seit Errichtung der Datei wurden 198.644 Treffer erzielt.³

2.6.2 Violent Crime Linkage Analysis System (ViCLAS)

ViCLAS [26, 35] ist ein Analysesystem zur Serienzusammenführung bei Gewaltverbrechen. Es handelt sich also insbesondere um eine Falldatenbank, die speziell für den Bereich der besonders schwerwiegenden Gewaltkriminalität entwickelt wurde und bei Tötungs- und Sexualdelikten zum Einsatz kommt, bei denen keine familiären oder sons-

² Stand 2014: 382.597 Festnahmeersuchen, 181.794 Ausschreibungen zur Aufenthaltsermittlung und 10,6 Mio. gelistete Gegenstände.

³ nähere Informationen: http://www.bka.de/DE/ThemenABisZ/DnaAnalyse/Statistik/dnaStatistik__node.html?__nnn=true

tigen bekanntschaftlichen Vorbeziehungen zwischen Opfer und Täter bestanden. Die ViCLAS-Datenbank basiert auf der, in den 1980er Jahren durch das FBI entwickelten, Falldatei „Violent Criminal Apprehension Program (ViCAP)“ und wird durch die „Royal Canadian Mounted Police (RCMP)“ verwaltet. ViCLAS wird neben Kanada in zehn weiteren Staaten, wie Deutschland, Dänemark und Großbritannien, weltweit eingesetzt. Die Datenbank ist dazu geeignet Rückfall-, Wiederholungs- und Serientäter anhand ihrer Taten (Begehungsmuster) zu erkennen sowie Einzeltaten schnellstmöglich zusammenzuführen und bezüglich Übereinstimmungen zu anderen Fällen zu prüfen. In ViCLAS werden ausführliche Fallinformationen zu Tötungsdelikten, sexuellen Gewaltdelikten, Vermisstenfällen und verdächtigem Ansprechen von Kindern und Jugendlichen erfasst.⁴ Gerade mit dem Blick auf den CSI-Effekt ist es vorstellbar, dass alle besprochenen biometrischen Merkmale und die daraus extrahierten biometrischen Daten gespeichert und verglichen werden können. Geeignete Datenbanktechnologien stehen Entwicklern und Nutzern im ausreichenden Maße zur Verfügung.

2.6.3 Integrated Ballistic Identification System (IBIS)

Die IBIS-Datenbank [6, 47] beinhaltet Informationen über Geschoss- und Patronenhülsen sowie Schusswaffen, die an Tatorten und von Tatverdächtigen sichergestellt werden konnten. Das Ziel dieser forensischen Datenbank liegt in der Beschleunigung des herkömmlichen labor- und zeitintensiven Vergleichsvorganges von ballistischen Informationen in polizeilichen Ermittlungen. Ein wesentlicher Vorteil des IBIS liegt darin, dass Beweismittel einer laufenden Untersuchung mit ballistischen Informationen aus vorangegangenen Ermittlungen verglichen werden können, um dadurch beispielsweise Schusswaffen zu identifizieren, die bei mehreren Straftaten verwendet wurden. Um dies zu realisieren werden beispielsweise Aufnahmen von an einem Tatort asservierten Patronenhülsen in die Datenbank importiert und mit enthaltenen Daten abgeglichen. Im Falle eines Matches erfolgt dann eine zusätzliche manuelle mikroskopische Überprüfung und Auswertung der Daten durch einen Ballistik-Experten.⁵

2.6.4 Paint Data Query (PDQ)

Bei der PDQ-Datenbank [4, 8, 11] handelt es sich um eine Ansammlung chemischer Zusammensetzungen von Farben und Lacken in- und ausländischer Automobilhersteller. Die PDQ ist mit über 74.000 gespeicherten individuellen Farbschichten von Fahrzeugen die größte internationale Datenbank, die Informationen dieser Art beinhaltet und Rück-

⁴ nähere Informationen: http://www.bka.de/DE/ThemenABisZ/OperativeFallanalyse/Viclas/viclas__node.html?__nnn=true

⁵ nähere Informationen: <https://www.atf.gov/>

schlüsse auf die Marke, das Model und Fabrikationsjahr eines Fahrzeugs ermöglicht. Die Datenbank wird von forensischen Wissenschaftler aus einer Vielzahl von Ländern, wie Kanada, USA, Australien, Afrika und Deutschland verwendet. Verwaltet wird die PDQ von der „Royal Canadian Mounted Police“, der nationalen Polizei Kanadas. Die Informationen über die gespeicherten Lacke und Farben werden zum einen direkt von den Herstellern der Fahrzeuge bezogen, zum anderen aber auch von Fahrzeugen von Schrottplätzen und Karosseriewerkstätten. Typische kriminalistisch relevante Sachverhalte, in denen die PDQ Anwendung findet, sind Fahrerfluchten mit Personen- bzw. Sachschäden. Eine zur PDQ ähnliche Datenbank ist die „National Automotive Paint File“ Datenbank des FBI.⁶

2.6.5 SoleMate

„SoleMate“ ist eine kommerzielle Datenbank, die Informationen über den Hersteller, das Produktionsjahr und teilweise Fotoaufnahmen von mehr als 30.000 Sport-, Freizeit- und Arbeitsschuhen enthält. Die Datenbank findet Anwendung, um Schuhabdrücke an Tatorten hinsichtlich einer bestimmten Marke zu identifizieren und somit möglichen Tatverdächtigen oder Personen, die sich am Tatort befunden haben, zuordnen zu können. „SoleMate“ kann als Stand-Alone oder mit SICAR, dem „Shoe Print Identification and Casework Management System“, verwendet werden. Um einen asservierten Schuhabdruck mit in der Datenbank abgelegten Daten vergleichen zu können, werden typische Features, wie Kreise, Rauten und Kurven, aus dem Schuhabdruck extrahiert. Die erhaltenen Muster werden als Grundlage für einen Vergleich verwendet.⁷

2.6.6 TreadMate

Bei „TreadMate“ handelt es sich um eine ähnliche Datenbank wie SoleMate mit dem Unterschied, dass Informationen zu Fahrzeugreifen gespeichert sind. Die Datenbank enthält mehr als 5.000 Sommer-, Winter- und Allwetterreifen. Der Vergleich erfolgt ebenfalls über extrahierte Features und Matchingalgorithmen.⁸

2.6.7 Automatisches Fingerabdruckidentifizierungssystem (AFIS)

Bei AFIS [29, 30] handelt es sich um eine in Deutschland seit dem Jahr 1993 genutzte Datenbank über Fingerabdrücke. Die Datenbank basiert auf der Kodierung sogenannter

⁶ nähere Informationen: <http://www.rcmp-grc.gc.ca/index.shtm>

⁷ nähere Informationen: <http://www.fosterfreeman.com/index.php/trace-evidence/357-sicar-6-solemate-2>

⁸ nähere Informationen: <http://www.fosterfreeman.com/index.php/component/content/article/20-products/shoe-print-identification/119-treadmate>

Minuten, wie die Gabelung einer Papillarleiste oder der Beginn bzw. das Ende einer Papillarleiste. Nach dem Einscannen und der Digitalisierung der Fingerabdrücke ermöglicht AFIS eine automatische Featureberechnung basierend auf den Minuzien und den Abgleich mit in der Datenbank bereits hinterlegten Fingerabdrücken. Zurzeit umfasst AFIS ca. 2.800.000 Fingerabdruckblätter, ca. 1.900.000 Handflächenabdrücke und ca. 400.000 offene (ungelöste) Spuren. Durchschnittlich werden pro Jahr etwa 350.000 Fingerabdruckblätter, ca. 200.000 handflächenpaare und ca. 180.000 Spuren bearbeitet. Die Zahl der Identifizierungen pro Jahr liegt bei ca. 20.000 Personen- und ca. 24.000 Spurenidentifizierungen.

2.6.8 Eurodac-System

Das Eurodac-System [7, 44] dient Mitgliedstaaten der Europäischen Union seit dem Jahr 2000 zur Identifizierung von Asylbewerbern und Personen, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen wurden. Die Grundlage bilden unter anderem wie bei AFIS Fingerabdrücke der jeweiligen Personen. Bei Aufgreifen eines Verdächtigen kann überprüft werden, ob dieser in einem anderen EU-Mitgliedsstaat Asyl beantragt hat oder womöglich bereits zum wiederholten Male illegal eingereist ist, d. h., es soll verhindert werden, dass Asylbewerber in mehreren Mitgliedsstaaten zeitgleich mehrere Asylverfahren betreiben können. Neben Fingerabdrücken werden in der Datenbank zusätzliche Informationen, wie Geschlecht der Person, Herkunftsland und der Zeitpunkt der Abnahme der Fingerabdrücke, gespeichert.

Literatur

1. Badawi, A.M., Mahfouz, M., Tadross, R., Jantz, R.: Fingerprint-based gender classification. In: IPCV, S. 41–46. Citeseer (2006)
2. Bashir, M., Scharfenberg, G., Kempf, J.: Person authentication by handwriting in air using a biometric smart pen device. BIOSIG **191**, 219–226 (2011)
3. Bazen, A.M., Gerez, S.H.: Segmentation of fingerprint images. In: Proc. Workshop on Circuits Systems and Signal Processing (ProRISC 2001), Bd. 276280. Citeseer (2001)
4. Bowen, R., Schneider, J.: Forensic databases: paint, shoe prints, and beyond. NIJ Journal **258**, 34–38 (2007)
5. Bowyer, K.W., Hollingsworth, K.P., Flynn, P.J.: A survey of iris biometrics research: 2008–2010. In: Handbook of iris recognition, S. 15–54. Springer (2013)
6. Brinck, T.B.: Comparing the Performance of IBIS and BulletTRAX-3D Technology Using Bullets Fired Through 10 Consecutively Rifled Barrels. Journal of Forensic Sciences **53**(3), 677–682 (2008)
7. Brouwer, E.: Eurodac: Its limitations and temptations. European Journal of Migration and Law **4**(2), 231–247 (2002)

8. Buckle, J., MacDougall, D., Grant, R.: PDQ – Paint Data Queries: The History and Technology Behind the Development of the Royal Canadian Mounted Police Forensic Laboratory Services Automotive Paint Database. *Canadian Society of Forensic Science Journal* **30**(4), 199–212 (1997)
9. Canny, J.: A computational approach to edge detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **PAMI-8**(6), 679–698 (1986)
10. Chen, X., Tian, J., Cheng, J., Yang, X.: Segmentation of fingerprint images using linear classifier. *EURASIP Journal on Advances in Signal Processing* **2004**(4), 1–15 (2004)
11. Christy, B.B.: The use of the PDQ (Paint Data Query) database along with other resources to provide vehicle information for hit and run fatalities within Virginia. In: *Proceedings of the Trace Evidence Symposium*, August, S. 13–16 (2007)
12. Cole, S.A., et al.: *Suspect identities: A history of fingerprinting and criminal identification*. Harvard University Press (2009)
13. Daugman, J.: Iriserkennung. In: *Biometrische Identifikation*, S. 129–158. Springer (2001)
14. Daugman, J.: The importance of being random: statistical principles of iris recognition. *Pattern recognition* **36**(2), 279–291 (2003)
15. Daugman, J.: How iris recognition works. *Circuits and Systems for Video Technology*, *IEEE Transactions on* **14**(1), 21–30 (2004)
16. Galton, F.: *Finger prints*. Macmillan and Company (1892)
17. Girod, A., Ramotowski, R., Lambrechts, S., Misrielal, P., Aalders, M., Weyermann, C.: Fingerprint age determinations: Legal considerations, review of the literature and practical propositions. *Forensic science international* **262**, 212–226 (2016)
18. Girod, A., Ramotowski, R., Weyermann, C.: Composition of fingerprint residue: a qualitative and quantitative review. *Forensic science international* **223**(1), 10–24 (2012)
19. Grassberger, M., Schmid, H.: *Todesermittlung. Befundaufnahme & Spurensicherung: Ein praktischer Leitfaden für Polizei, Juristen und Ärzte*. Springer Wien (2009)
20. Grasselli, A.: On the automatic classification of fingerprints. *Methodologies of Pattern Recognition* S. 253–273 (1969)
21. Green, B.: *Canny edge detection tutorial* (2002)
22. Grehn, F.: *Augenheilkunde*. Springer (2006)
23. Herrmann, B., Saternus, K.S.: *Biologische Spurenkunde: Bd. 1: Kriminalbiologie*, Bd. 1. Springer (2007)
24. Hohoff, C., Brinkmann, B.: Trends in der forensischen Molekulargenetik. *Rechtsmedizin* **13**(4), 183–189 (2003)
25. Ifa, D.R., Manicke, N.E., Dill, A.L., Cooks, R.G.: Latent fingerprint chemical imaging by mass spectrometry. *Science* **321**(5890), 805–805 (2008)
26. Johnson, G.: VICLAS: Violent crime linkage analysis system. *RCMP Gazette* **56**(10), 9–13 (1994)
27. Kanakam, P., Rao, K., Hussain, S.M.: Olfactory biometric technique: An emerging technology. *Journal of Advancement in Robotics* **1**(1), 1–11 (2015)
28. Kawagoe, M., Tojo, A.: Fingerprint pattern classification. *Pattern Recognition* **17**(3), 295–303 (1984)

29. Khanna, R., Shen, W.: Automated fingerprint identification system (AFIS) benchmarking using the National Institute of Standards and Technology (NIST) Special Database 4. In: Security Technology, 1994. Proceedings. Institute of Electrical and Electronics Engineers 28th Annual 1994 International Carnahan Conference on, S. 188–194. IEEE (1994)
30. Komarinski, P.: Automated fingerprint identification systems (AFIS). Academic Press (2005)
31. Locard, E.: Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden. Berlin (1930)
32. Maio, D., Maltoni, D.: A structural approach to fingerprint classification. In: Pattern Recognition, 1996., Proceedings of the 13th International Conference on, Bd. 3, S. 578–585. IEEE (1996)
33. Maio, D., Maltoni, D.: Ridge-line density estimation in digital images. In: Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on, Bd. 1, S. 534–538 (1998)
34. Maltoni, D., Maio, D., Jain, A., Prabhakar, S.: Handbook of fingerprint recognition. Springer Science & Business Media (2009)
35. Martineau, M.M., Corey, S.: Investigating the Reliability of the Violent Crime Linkage Analysis System (ViCLAS) Crime Report. Journal of Police and Criminal Psychology **23**(2), 51–60 (2008)
36. Nogala, D., Mittendorf, V.: Fingerabdrucksysteme. In: Wörterbuch zur Inneren Sicherheit, S. 87–92. Springer (2006)
37. Pauk J. Kuzmierowski, T.T.S.J., Ostaszewski, M.: Computer-aided system for foot type assessment based on photos taken by the podoscope (2015)
38. Pauk J. Kuzmierowski, T.T.S.J., Ostaszewski, M.: Computer-aided system for foot type assessment based on photos taken by the podoscope (2015)
39. Rao, C.K.: On fingerprint pattern recognition. Pattern Recognition **10**(1), 15–18 (1978)
40. Ratha, N.K., Chen, S., Jain, A.K.: Adaptive flow orientation-based feature extraction in fingerprint images. Pattern Recognition **28**(11), 1657–1672 (1995)
41. Reimer, H.: Biometrische Identifikation – eine aussichtsreiche Innovation. In: Biometrische Identifikation, S. 1–7. Springer (2001)
42. Samir Nanavati Michael Thieme, R.N.: Biometrics: Identity Verification in a Networked World, 1st edn. Wiley (2002)
43. Schneider, J.K.: Ultrasonic fingerprint sensors. In: Advances in Biometrics, S. 63–74. Springer (2008)
44. Schröder, B.: Das Fingerabdruckvergleichssystem EURODAC. ZAR (2), 71–75 (2001)
45. Stock, R., Swonger, C.: Development and evaluation of a reader of fingerprint minutiae. Cornell Aeronautical Laboratory, Technical Report CAL no. XM-2478-X-1 S. 13–17 (1969)
46. Su, B.: Recent progress on fingerprint visualization and analysis by imaging ridge residue components. Analytical and bioanalytical chemistry **408**(11), 2781–2791 (2016)
47. Thompson, R.M.: Automated firearms evidence comparison using the Integrated Ballistic Identification System (IBIS) (1999)
48. Urry, S.R., Wearing, S.C.: A comparison of footprint indexes calculated from ink and electronic footprints. J Am Podiatr Med Assoc **91**(4), 203–209 (2001)
49. Wickramaarachchi, W., Vasanthapriyan, S.: Multi-layer framed offline signature recognition algorithm. Journal of Image and Graphics **3**(1) (2015)

-
50. Zar, J.H.: Significance testing of the Spearman rank correlation coefficient. *Journal of the American Statistical Association* **67**(339), 578–580 (1972)
 51. Zhu, E., Yin, J., Hu, C., Zhang, G.: A systematic method for fingerprint ridge orientation estimation and image segmentation. *Pattern Recognition* **39**(8), 1452–1472 (2006)

Forensik in der digitalen Welt

Moderne Methoden der forensischen Fallarbeit in der
digitalen und digitalisierten realen Welt

Labudde, D.; Spranger, M. (Hrsg.)

2017, XXIV, 326 S. 115 Abb., Softcover

ISBN: 978-3-662-53800-5