Multimedia-Forensik als Teildisziplin der digitalen Forensik

Rainer Böhme,[†] Felix C. Freiling,[‡] Thomas Gloe,[†] Matthias Kirchner[†]

[†] Technische Universität Dresden, Institut für Systemarchitektur, 01062 Dresden
[‡] Universität Mannheim, Lehrstuhl Praktische Informatik 1, 68131 Mannheim

Abstract: Die Vielzahl neuer Publikationen zum Thema Multimedia-Forensik verlangt nach Reflexionen über die Definition dieses neuen Forschungsgebietes und dessen Beziehung zu bereits etablierteren Disziplinen. Dieser Aufsatz entwickelt eine Strukturierung forensischer Disziplinen anhand der Natur der ausgewerteten Beweismittel. Demnach zählen sowohl Computer-Forensik als auch Multimedia-Forensik zur Klasse der digitalen Forensik. Nichtsdestotrotz unterscheiden sich beide Gebiete angesichts ihres zugrunde liegenden Beobachtermodells, welches den Blick des Forensikers auf die Realität (oder Teile davon) beschreibt. Durch die nur eingeschränkt beobachtbare Realität ergeben sich für die in der Multimedia-Forensik analysierten Sensordaten wichtige Implikationen hinsichtlich der Zuverlässigkeit gewonnener beweiserheblicher Tatsachen. Während eine perfekte Verschleierung von Straftaten im Bereich der Computer-Forensik prinzipiell möglich ist, kann bei Anwendung von multimediaforensischen Techniken nicht erwartet werden. Die im Aufsatz ausgeführten Argumente stützen sich auf konkrete Beispiele und nehmen Bezug auf etablierte Verfahren.

1 Kriminalistik im digitalen Zeitalter

Fortschritte in der Informations- und Kommunikationstechnologie haben in den vergangenen beiden Jahrzehnten zu einer digitalen Revolution geführt, die unsere Welt in ihren Grundfesten verändert hat und noch immer verändert. Digitale Daten und die Computer, auf denen sie gespeichert werden, durchdringen und definieren immer stärker alle Bereiche unseres Alltags und werden damit zu einem nicht mehr wegzudenkenden Teil unserer Realität. Interpersonale soziale Interaktionen werden zunehmend durch computervermittelte ersetzt, die in virtuellen Räumen stattfinden. Folgerichtig gelten Rechtsnormen auch in diesen digitalen Räumen, was deren Durchsetzung im Sinne einer Verfolgung von Straftaten einschließt. Um dies zu gewährleisten, besteht die unmittelbare Notwendigkeit, Abfolgen von Handlungen in der digitalen Welt in einer wissenschaftlich fundierten und zuverlässigen Art und Weise rekonstruieren zu können. Nur so können kausale Zusammenhänge aufgedeckt (oder zumindest angenähert) werden und damit potenzielle Täter für ihre Handlungen verantwortlich gemacht, sowie mögliche Nachahmer abgeschreckt werden.

Systematische wissenschaftliche Ansätze zur Gewinnung beweiserheblicher Tatsachen aus in Kriminalfällen sichergestellten Beweismitteln werden im Allgemeinen unter dem Begriff „Forensik“ zusammengefasst. Der Begriff hat seinen etymologischen Ursprung in dem lateinischen Wort *forum*, was soviel bedeutet wie Marktplatz, dem Schauplatz frü-

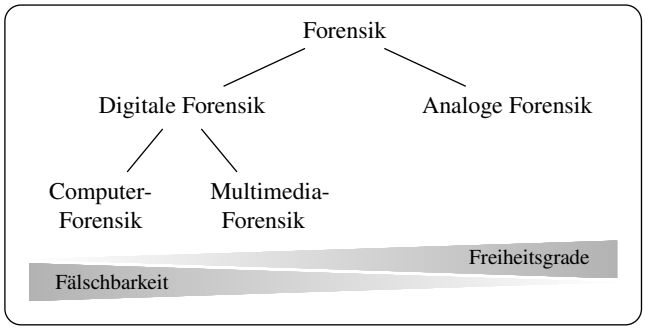

Abbildung 1: Strukturierung der in diesem Aufsatz besprochenen forensischen Disziplinen.

herer Gerichte. Als Reaktion auf die zentrale Rolle des Computers in unserer heutigen Welt beschreibt der Begriff der „Computer-Forensik“ all jene forensischen Techniken, die zum Einsatz kommen, wann immer Computer in eine kriminelle Handlung verwickelt sein könnten. Bislang gibt es keine klare Definition dieses Zweigs der Forensik, vermutlich weil Computer in vielfältiger Weise in Beziehung zu begangenen Straftaten stehen können: Sie können einerseits lediglich Werkzeug für kriminelle Handlungen in der herkömmlichen, materiellen Welt sein, oder andererseits erst einen digitalen, immateriellen Raum schaffen, in dem Straftaten begangen werden. In beiden Fällen ist es die Aufgabe der Computer-Forensiker, beweiserhebliche Tatsachen aus den betroffenen Computern zu gewinnen.

Fügt man den bisherigen Betrachtungen einen *Sensor* als mögliche Quelle digitaler Daten hinzu, so wird die Situation noch komplizierter. Sensoren bilden die Realität, also die materielle Welt (oder Teile davon), ab und transformieren diese in digitale Repräsentationen, die dann auf Computern gespeichert und weiter verarbeitet werden. Solche digitalisierte Versionen der Realität können selbstverständlich auch Teil von forensischen Untersuchungen sein. Sie können jedoch nur als beweiserhebliche Tatsache dienen, wenn ihre Authentizität gesichert ist. Dies kann als Aufgabe der „Multimedia-Forensik“ verstanden werden. Mit dieser Arbeitsdefinition wird die Teildisziplin im vorliegenden Aufsatz abgegrenzt.

Ziel dieses Aufsatzes ist es, einen Vorschlag zur Abgrenzung und Strukturierung der neu entstandenen forensischen Teildisziplinen zu unterbreiten. Dabei werden insbesondere die den Teildisziplinen zugrunde liegenden Annahmen im Vergleich zur klassischen Forensik in der materiellen Welt berücksichtigt. Abb. 1 stellt die vorgeschlagene Ordnung der Teildisziplinen dar. Zunächst bietet sich eine Unterscheidung der verschiedenen forensischen Wissenschaften hinsichtlich der Natur der von ihnen ausgewerteten Beweismittel an. Die klassische (analoge) Forensik beschäftigt sich mit der Analyse materieller Beweismittel, wohingegen die digitale Forensik auf digitale Beweismittel beschränkt ist. Während wir für den Begriff des materiellen Beweismittels aufgrund seiner langen Tradition in der Kriminalistik im Allgemeinen klare Vorstellungen haben, erscheint das digitale Beweismittel als etwas Immaterielles und damit deutlich abstrakter. Im Rahmen dieses Aufsatzes verstehen wir digitale Beweismittel als endliche Folgen von diskreten und uneingeschränkt beobachtbaren Symbolen, meist Elemente eines binären Alphabets, wie sie beispielsweise

aus dem Arbeitsspeicher oder von der Festplatte eines Computers gelesen werden können. Somit basieren sowohl die Computer-Forensik als auch die Multimedia-Forensik auf der Analyse von digitalen Beweismitteln und ordnen sich in dem Gebiet der digitalen Forensik unter.

Ausgehend von der klassischen, analogen Forensik (Abschnitt 2) gehen wir im weiteren Verlauf auf jeden der in Abb. 1 gezeigten Zweige näher ein. In Abschnitt 3 werden grundlegende Konzepte der Computer-Forensik besprochen, um dann in Abschnitt 4 Unterschiede zur Multimedia-Forensik herauszustellen. In Abschnitt 5 wechseln wir schließlich die Perspektive und betrachten mögliche Gegenmaßnahmen und Herausforderungen für das Feld der digitalen Forensik. Der abschließende Abschnitt 6 widmet sich der in der Praxis vermutlich häufig auftretenden Überschneidung und Kombination einzelner forensischer Teildisziplinen. Diese lassen die wichtigen Unterschiede zwischen den einzelnen Teilen leicht in den Hintergrund treten und unterstreichen somit die Notwendigkeit einer klaren Strukturierung, zu der dieser Aufsatz einen Beitrag leisten möchte.

2 Klassische (analoge) Forensik

Die 'klassische' Forensik subsumiert all jene Verfahren, die darauf abzielen, beweiserhebliche Tatsachen aus materiellen Beweismitteln zu extrahieren. Sie hat ihre Wurzeln im Locard'schen Austauschprinzip, das zu Beginn des 20. Jahrhunderts von dem französischen Wissenschaftler Edmond Locard postuliert wurde. Die Kernannahme des Prinzips besagt, dass bei jedem Kontakt zwischen zwei Objekten unvermeidbar auch physische Spuren des Kontakts am jeweils anderen Objekt hinterlassen werden [Saf00, Cas04, u. a.]. Derartiger Austausch kann beispielsweise in Form von Finger- und Fußabdrücken, Haaren, Stofffasern, Kratzern, Wunden, Ölspuren, usw. geschehen.

Akzeptiert man die im Locard'schen Prinzip gemachte Annahme als gegeben,[1] ist nachstehende Aussage des Chemikers Paul L. Kirk nur folgerichtig:

> "Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

Der entscheidende Punkt hierbei ist, dass ein uneingeschränkter Forensiker die Realität zumindest theoretisch aus unendlich vielen Perspektiven betrachten kann. Damit existiert immer eine nicht völlig vernachlässigbare Wahrscheinlichkeit, dass selbst noch so subtile Spuren gefunden werden. Die moderne Erkenntnistheorie räumt jedoch ein, dass die menschliche Wahrnehmung der Realität in vielerlei Hinsicht eingeschränkt ist. Zuallererst vermitteln die menschlichen Sinnesorgane nur ein unvollständiges Bild der Realität. Diese Einschränkung kann in gewisser Weise als eine Art Filter verstanden werden, dessen Wirkung mit technischen Hilfsmitteln abgeschwächt werden kann (beispielsweise vergrößern Mikroskope die Auflösung des menschlichen Sehvermögens). Nichtsdestotrotz bleibt die Heisenberg'sche Unschärferelation, die besagt, dass allein durch die Beobachtung der

[1] Zumindest auf Ebene einzelner Elementarteile bleibt die Gültigkeit des Prinzips fragwürdig.

Realität diese verändert wird. Das Heisenberg-Prinzip steht dabei nicht im Widerspruch zum Locard'schen Prinzip, das nicht explizit zwischen Täter und Forensiker als Teil der gleichen Realität unterscheidet.

Da sich dieser Aufsatz primär der digitalen Forensik widmet, soll hier nicht weiter auf die Analyse materieller Beweisstücke eingegangen werden. Wichtig für die folgende Argumentationskette ist lediglich die Frage nach der prinzipiellen Vertrauenswürdigkeit von aus materiellen Beweisstücken gewonnenen beweiserheblichen Tatsachen. Wie schwierig ist es für einen Täter, seine Spuren tatsächlich vollständig zu verwischen, oder, sogar noch schlimmer, neue Spuren so zu legen, dass sie zu Falschbezichtigungen führen? Letztlich entspricht beides dem Versuch, die Realität derart zu ändern, dass diese mit einer alternativen Version seiner Handlung im Einklang steht. Da sowohl Forensiker als auch Täter selbst Teil der gleichen Realität und damit an ähnliche physische wie kognitive Einschränkungen gebunden sind, kann selbst der sorgfältigste Täter niemals völlig sicher sein, ob seine Version der Realität tatsächlich vollkommen konsistent mit der (imaginären) Realität ohne dessen Handlungen ist. Insofern ist das „perfekte Verbrechen", welches alle Spuren zu Genüge verwischt und damit eine konsistente Realität vorgibt, in der Tat ein unglaublich schwieriges bis unmögliches Unterfangen. Entsprechend bleibt die gängige Meinung, dass sorgfältige Untersuchungen von materiellen Beweisstücken mit hoher Wahrscheinlichkeit entweder vertrauenswürdige oder keine beweiserheblichen Tatsachen liefern. (Abgesehen von Ermittlungsfehlern, die natürlich niemals ganz ausgeschlossen werden können.[2].)

3 Computer-Forensik

Betrachten wir Computer als Maschinen mit gewissen materiellen Eigenschaften, dann sind sie zweifelsohne Teil unserer Realität. Folgt man dem Locard'schen Prinzip, sollte es demnach gleichermaßen auch auf die Computer-Forensik zutreffen. Häufig wird hier jedoch die implizite Annahme gemacht, dass sich die forensische Analyse lediglich auf die digitalen Symbole beschränkt, die den Zustand des in jedem Computer implementierten deterministischen, endlichen Automaten beschreiben. Dem Computer-Forensiker wird damit lediglich ein stark eingeschränktes Beobachtermodell mit einem sehr begrenzten Blick auf die Realität zugestanden. Bits und Bytes stellen an sich nur ein theoretisches und abstraktes, immaterielles Konzept dar, dass keine weiteren Informationen über deren Vergangenheit und Entstehung beinhaltet. Die gängige Praxis, auf einem Rechner gefundene digitale Beweismittel auf einen *read-only* Massenspeicher zu kopieren und diesen für alle weiteren Untersuchungen zu nutzen, setzt das beschriebene Beobachtermodell direkt um [Cas04].

Eine derartige Beschränkung führt zu Konsequenzen bezüglich der Vertrauenswürdigkeit der aus digitalen Beweismitteln gewonnenen beweiserheblichen Tatsachen. Durch die endliche Anzahl von Zuständen in einem geschlossenen System bleibt immer eine echt positive Wahrscheinlichkeit, dass ein sorgfältig agierender Täter den Computer in einen Zustand

[2] In einem aktuellen Beispiel führte die Verunreinigung von Wattestäbchen zu einer europaweiten Suche des so genannten „Phantoms von Heilbronn". An 40 verschiedenen Tatorten wurden fälschlicherweise DNA-Spuren der gleichen Person „gefunden". Siehe z. B. `www.stern.de/phantom`

versetzt, der *alle* Spuren verwischt. Davon ausgehend, dass der persistente Zustand eines Rechners zur Gänze auf der Festplatte gespeichert ist, kann dies etwa durch das Booten des Computers mit Hilfe einer Live-CD erreicht werden (wobei selbstverständlich kein schreibender Zugriff auf die Platte stattfinden darf).

In der Praxis gestaltet sich das Vermeiden *aller* Spuren natürlich oft etwas komplizierter. Die Anzahl möglicher Zustände steigt bei heutiger Rechentechnik schnell ins Unermessliche. Eine Platte mit 100 GB Speicherkapazität entspricht $2^{10^{11}}$ Zuständen. Zum Vergleich: Die Anzahl von Atomen im Universum wird mit einer Größenordnung von 2^{10^3} angegeben. Bei den heutigen, aus vielen Softwarekomponenten bestehenden und mit aller Art von Hardwareschnittstellen versehenen, komplexen Systemen ist es somit wenig erstaunlich, dass Täter oft eben nicht alle Bereiche des Zustandsraums unter ihre Kontrolle bringen können. Jedoch haben sie die Möglichkeit, sich weiterer Technik zu bedienen, um ihre Ziele zu erreichen. Durch Zuhilfenahme eines Zweitsystems, das den betreffenden Computer virtualisiert, kann ein gültiger und plausibler Zustand mit geringerem Aufwand (wieder)hergestellt werden. Im Allgemeinen ist dabei nur ein äußerst kleiner Anteil aller möglichen Zustände für die Suche nach gültigen Zuständen relevant. Dieser Ansatz der Spurenvermeidung impliziert jedoch einen Beobachter, der selbst blind für Teile des Zustandsraumes ist und die zusätzliche Technik zum Aufsetzen des „sauberen“ Systems ignoriert. In der Praxis ist es für den Computer-Forensiker jedoch ohnehin oftmals schwierig, die Grenzen des zu untersuchenden Systems zu markieren, insbesondere wenn Netzwerkverbindungen bestehen.

Selbst mit einem Beobachtermodell, das faktisch das gesamte System einschließt, bleibt mit den oben angebrachten Einschränkungen digitaler Beweismittel jedoch stets die theoretische Möglichkeit, dass ein sorgfältiger Täter tatsächlich sämtliche digitalen Spuren perfekt verwischen kann. In der Praxis mögen solche Fälle rar sein, eine gewisse Skepsis scheint aber angebracht, wenn mittels Computer-Forensik gewonnene beweiserhebliche Tatsachen vor Gericht zum Einsatz kommen.

Es stellt sich somit die Frage, ob das Locard'sche Prinzip auch in der Computer-Forensik seine Berechtigung hat. Viele Praktiker werden dies aus ihren Erfahrungen heraus bejahen: Jeder Täter begeht Fehler. Nichtsdestotrotz macht die Natur digitaler Beweismittel ein perfektes Verbrechen möglich. Hinzu kommt, dass, anders als bei den praktisch bedingten Einschränkungen bei der Analyse von Spuren in der materiellen Welt, der Täter den blinden Fleck des Forensikers genau kennt. Er kann seine Handlungen entsprechend anpassen und leicht falsche bzw. in die Irre führende Spuren legen. Die Vorteile einer kostengünstigen (da automatisierten) und bequemen[3] forensischen Analyse gehen jedoch mit einer verminderten Vertrauenswürdigkeit der beweiserheblichen Tatsachen einher. Von nicht unwesentlicher Bedeutung ist in diesem Zusammenhang, wie die begrenzten öffentlichen Mittel zur Kriminalitätsaufklärung in einer zunehmend computervermittelten Informationsgesellschaft zwischen der Analyse materieller und digitaler Beweismittel verteilt werden sollen.

Abschließend sei darauf hingewiesen, dass Computer-Forensik auch in einem weiteren

[3] Die wohl größte Schwierigkeit bei heutigen Untersuchungen digitaler Beweismittel liegt vermutlich in der schieren Menge von Daten auf beschlagnahmten Computern.

Sinne verstanden werden könnte als bislang in diesem Aufsatz. Wenn neben digitalen auch materielle Beweismittel zur Analyse zugelassen werden, ergibt sich eine völlig andere Situation. Solch zusätzliche Merkmale, wie Verschleißspuren, Messungen von elektromagnetischer Abstrahlung [Kuh03] oder Temperatur [ZM08], sowie jegliche Form von analogen Spuren auf Speichermedien [WKS08], sind zwar oftmals nur mit vergleichsweise hohem Aufwand zu gewinnen. Sie können aber Anhaltspunkte über vergangene Zustände eines Computers geben und stellen somit ein geeignetes Mittel dar, um die Wirksamkeit der Verschleierung rein digitaler Spuren zu mindern. Selbst digitale Beweismittel auf anderen Computern oder Datenträgern können hier nützlich sein, solang ihre Integrität gesichert ist (etwa mittels *secure logging* [SK98]). Beispielsweise konnte der US-Agent Oliver L. North im Zusammenhang mit der Iran-Contra-Affäre 1986 überführt werden, indem Beweismittel auf getrennt aufbewahrten Sicherungsbändern ausgewertet wurden.

4 Multimedia-Forensik

Eine wichtige Kategorie von Daten, die im Rahmen einer Analyse von digitalen Speichermedien häufig auftritt, sind digitale Bild- oder Audioaufnahmen. Solche digitalen Mediendaten durchdringen unser alltägliches Leben heute in nahezu allen Bereichen. In letzter Zeit sind jedoch verstärkt Stimmen zu vernehmen, die auf die leichte Manipulierbarkeit solcher Daten hinweisen. Ausgereifte Bearbeitungssoftware ermöglicht es selbst unerfahrenen Benutzern, digitale Mediendaten mit wenig Aufwand hochqualitativ zu bearbeiten und zu verändern. Die Echtheit aller Mediendaten ungewisser Herkunft muss damit erst einmal prinzipiell infrage gestellt werden. Dies gilt insbesondere dann, wenn folgenreiche Entscheidungen an sie geknüpft sind, beispielsweise wenn digitale Bilder als Beweismittel vor Gericht verwendet werden [Kno08].

Bedingt durch Relevanz und technische Möglichkeiten hat sich die Multimedia-Forensik in den letzten Jahren zu einem äußerst aktiv betriebenen Forschungsgebiet an der Schnittstelle zwischen Multimedia-Sicherheit, Computer-Forensik sowie Bild- und Signalverarbeitung entwickelt. Ähnlich zur Computer-Forensik wertet die Multimedia-Forensik lediglich digitale Daten aus. Diese entstammen hier jedoch einem Sensor und stellen dessen Abbildung der Realität in die digitale Welt dar. Dieser grundlegende Unterschied hat einige Auswirkungen auf die Zuverlässigkeit und Aussagekraft der mittels Multimedia-Forensik gewonnenen beweiserheblichen Tatsachen, die im Folgenden näher ausgeführt werden sollen.

4.1 Überblick zum aktuellen Stand der Multimedia-Forensik

Verfahren der Multimedia-Forensik verfolgen im Allgemeinen das Ziel, Spuren möglicher Manipulationen aufzudecken oder Rückschlüsse auf das zur Aufnahme verwendete Eingabegerät zu ziehen. Für diese beiden prinzipiellen Szenarien, Manipulationsdetektion und Quellenidentifikation, wird davon ausgegangen, dass dem Forensiker keinerlei Wis-

sen zu einem etwaigen Original vorliegt. Derartige Methoden werden dementsprechend als „blind“ bezeichnet [NCLS06] und sie bedienen sich typischerweise zweierlei Arten von digitalen Spuren:

- **Charakteristika des Eingabegerätes** können sowohl auf Vorhandensein (Quellenidentifikation) als auch auf Konsistenz (Manipulationsdetektion) geprüft werden.
- **Manipulationsartefakte** weisen auf durchgeführte Bearbeitungsoperationen hin.

Das Entstehen von Spuren der ersten Art ist untrennbar mit dem Aufnahmeprozess digitaler Mediendaten verbunden [KMM+06]. Fertigungsbedingt variieren verschiedene Eingabegeräte systematisch darin, wie sie die Realität in digitale Abbilder transformieren. Darauf basiert die Annahme, dass in jedem digitalen Medium charakteristische Merkmale des zur Aufnahme verwendeten Gerätes zu finden sind. Dabei ist zu unterscheiden, ob derartige Charakteristiken zur Identifikation der Geräteklasse [KCAD08, MSGW08], des Modells [KSM04, BW05, OVD07, KODL07, BSM08, Far08, GBW09], oder eines tatsächlichen Gerätes [GBK+01, CFGL08, DSM08] geeignet sind. Bisherige multimediaforensische Techniken dienen zu einem Großteil der Analyse von digitalen Bildern, wobei das in diesem Fall vermutlich am besten untersuchteste Gerätemerkmal das CCD/CMOS-Sensorrauschen ist, welches in praktisch allen Digitalkameras [CFGL08] oder Flachbettscannern [GFW07] auftritt. Eine Abschätzung der systematischen Rauschanteile, der sogenannten *photo response non-uniformity* (PRNU), dient als „digitaler Fingerabdruck“, der es erlaubt, Bilder einzelner (auch baugleicher) Eingabegeräte zu unterscheiden.

Gerätecharakteristische Spuren können jedoch nicht nur zur Identifikation des Aufnahmegerätes eingesetzt werden, sondern finden auch Anwendung bei der Manipulationsdetektion [PF05b, JF06, MCP+07, CFGL08]. Hierfür wird auf ein konsistentes Vorhandensein derartiger Spuren im gesamten Medium getestet, um auf diese Weise örtliche Abweichungen vom Original aufzudecken. So kann beispielsweise ein örtlich begrenztes Nicht-Vorhandensein des zu erwartenden PRNU als Hinweis für eine entsprechende Nachbearbeitung nützlich sein.

Neben fehlenden Gerätecharakteristika können auch die Spuren der durchgeführten Bearbeitungsoperationen an sich zu forensischen Zwecken genutzt werden [PF04, PF05a, WF07, JF07]. Hierbei dient demnach nicht das Fehlen spezieller Merkmale sondern explizit deren Vorhandensein als Indiz. Typische Spuren dieser Kategorie sind etwa periodische Korrelationsmuster zwischen einzelnen Pixeln in skalierten Bildern [PF05a] oder (nahezu) identische Bildregionen nach sogenannten *copy & paste* Operationen [PF04]. Abbildung 2 zeigt ein aktuelles Beispiel für letztere Spurenart. Die nachträglich duplizierten Raketen im Bild eines iranischen Raketentests konnten mittels eines *copy & paste* Detektors als Fälschung erkannt werden.[4]

4.2 Verhältnis zur Computer-Forensik

Wie eingangs angemerkt, basieren Computer-Forensik und Multimedia-Forensik auf der Analyse digitaler Daten. Im Unterschied zur Computer-Forensik stammen die in der Multi-

[4] Die Fälschung ist jedoch so schlecht gemacht, dass sie auch mit bloßem Auge als solche erkennbar ist.

Abbildung 2: Typische Bildmanipulation und deren Detektion mittels Multimedia-Forensik. Vermutliches Originalbild eines iranischen Raketentests mit einer nicht gezündeten Rakete (links, Quelle: Online-Ausgabe JameJam Daily) und dessen manipulierte Version (Mitte, Quelle: Iranische Revolutionsgarden). Der *copy & paste* Detektor [PF04] markiert Regionen, die mit hoher Wahrscheinlichkeit übereinstimmen (rechts).

media-Forensik untersuchten diskreten Symbole jedoch von einem Sensor, der die Realität (oder Teile davon) in ein digitales Abbild transformiert. Dies rechtfertigt eine Unterscheidung der beiden Disziplinen, da die Multimedia-Forensik mit der Analyse digitaler Repräsentationen einer nicht (vollständig) wahrnehmbaren Realität eher als empirische Wissenschaft aufgefasst werden muss. Diese Perspektive auf die Multimedia-Forensik hat starke Gemeinsamkeiten mit dem erkenntnistheoretischen Zugang zu anderen Techniken der Multimedia-Sicherheit, so etwa der Steganographie [Böh09]. Letztlich kann sich der Multimedia-Forensiker nie endgültig sicher sein, ob ein ihm vorliegendes Medium tatsächlich einem gültigen Abbild der Realität (bzw. Teilen davon) entspricht oder nicht. Gleiches gilt jedoch auch für dessen Gegenspieler: Ein Fälscher kann niemals mit absoluter Sicherheit davon ausgehen, dass seine Manipulation keine detektierbaren Spuren hinterlassen hat. Anders als bei der Computer-Forensik leiten sich die fraglichen digitalen Daten von der Welt außerhalb des abgeschlossenen Computer-Systems ab und sind somit technisch nicht effizient reproduzierbar. Während das Locard'sche Prinzip, wie oben ausgeführt, nicht direkt auf die Computer-Forensik (im engeren Sinne) übertragen werden kann, scheint es demnach im Bereich der Multimedia-Forensik gültig zu sein.

Wie andere empirische Wissenschaften auch, arbeitet die Multimedia-Forensik im Allgemeinen mit Modellen der Realität. Auch wenn diese selten explizit als solche bezeichnet werden, dienen Modelle der Vereinfachung der überaus komplexen Realität sowie deren digitalen Abbilds. So bedient sich etwa die PRNU-basierte Kameraidentifikation der Annahme, das gesuchte Sensorrauschen folge einer bestimmten Wahrscheinlichkeitsverteilung, die mit hinreichender Genauigkeit als Normalverteilung approximiert werden kann. Auf diese Weise lässt sich das Problem der Kameraidentifikation als Hypothesentest beschreiben, für den ein optimaler Detektor abgeleitet werden kann [CFGL08]. Auch die Erkennung von *copy & paste* Operationen bedient sich implizit eines Modells der Realität. Der Detektor basiert auf der Annahme, dass Regionen identischer (jedoch nicht konstanter) Pixelwerte nur mit sehr geringer Wahrscheinlichkeit in originalen Bildern auftreten [PF04]. Die beiden Beispiele verdeutlichen, dass typische Modelle die Funktion einer Dimensionalitätsreduktion übernehmen (zusätzlich zu der bereits im Sensor vorgenommenen Reduktion beim Übergang von der materiellen Welt auf das digitale Abbild) und damit nur einen stark vereinfachten Blick auf die Realität geben können.

Die Güte der mit Multimedia-Forensik gewonnenen beweiserheblichen Tatsachen hängt offensichtlich von der Qualität der verwendeten Modelle ab. Je besser ein Modell die Realität (oder Teile davon) erklären und vorhersagen kann, umso belastbarer sind die darauf basierenden Entscheidungen. Ein Modell des Sensorrauschens, das die Möglichkeit verschiedener Bildausrichtungen einbezieht, reduziert die Falschrückweisungsrate und ist somit stets zu bevorzugen. Gleichermaßen kann die Falschakzeptanzrate durch das Entfernen sogenannter *non-unique artifacts*, etwa Spuren von Farbinterpolation, vermindert werden [CFGL08].

Neben dem empirischen Charakter von Methoden der Multimedia-Forensik existiert ein weiterer wichtiger Unterschied zur Computer-Forensik. Die Transformation von Realität auf digitales Abbild bringt zusätzliche Freiheitsgrade auf der Ebene des Sensors mit sich. Insbesondere das Ausmaß der Quantisierung ist eine wichtige Einflussgröße für alle Verfahren der Multimedia-Forensik; im Allgemeinen gilt dies aber für jede Form von Signalverarbeitung innerhalb des Aufnahmegerätes. Per Definition verursacht Quantisierung einen gewissen zusätzlichen Informationsverlust und bringt damit neue Unsicherheit in die forensische Analyse. Dabei muss Quantisierung nicht nur auf verlustbehaftete Kompressionsalgorithmen wie JPEG bezogen werden, sondern kann beispielsweise auch die Auflösung der Sensorausgabe einschließen. Bei der Frage danach, wie breit der Begriff des Sensors aufgefasst werden soll („Welche Nachbearbeitungsoperationen gehören genuin zur Transformation von Realität auf digitales Abbild?“), stößt man unweigerlich auf den Aspekt der „legitimen“ Nachbearbeitung. So stellen beispielsweise Scans von abgedruckten und gerasterten Bildern aus Zeitungen nur eine sehr grobe digitale Repräsentation der Realität dar, können aber nichtsdestotrotz bei einer Analyse von inkonsistenter Beleuchtung nützlich sein [JF07]. Im Allgemeinen zeigt sich, dass die für eine sinnvolle forensische Analyse benötigte Ausgabequalität des Sensors stark von den eingesetzten Methoden abhängt. Eine vergleichbare Abhängigkeit ist für Verfahren der Computer-Forensik (im engeren Sinne) nicht bekannt, da die zu untersuchenden digitalen Symbole in keinem direkten Bezug zur Außenwelt stehen.

Wird der Begriff der Computer-Forensik weiter gefasst, wie im letzten Absatz von Abschnitt 3 angedeutet, dann lassen sich grundlegende Parallelen zur Multimedia-Forensik nicht von der Hand weisen. Praktisch wird jeder Computer zu einem Sensor, wenn er Daten seiner Umgebung, also der Realität, aufnimmt. Solche Aufnahmen können aus ganz verschiedenen Gründen geschehen. So verwenden etwa Pseudo-Zufallszahlengeneratoren den Tastaturanschlag als eine mögliche Eingabe. Gleichzeitig enthält der Tastaturanschlag jedoch auch Informationen über den Schreiber [JG90], dem wohl niemand seine Zugehörigkeit zur Realität absprechen wird.

5 Techniken zur Vereitelung forensischer Erfolge

Kenntnisse der digitalen Spurensicherung in Theorie und Praxis sind nicht der speziellen Gruppe der Forensiker vorbehalten. Der wesentliche Stand der Technik ist in öffentlich verfügbaren Konferenzbänden oder wissenschaftlichen Fachzeitschriften publiziert. Während diese Transparenz im Allgemeinen ein wünschenswertes Sicherheitsprinzip um-

setzt [Ker83], erleichtert sie es gleichzeitig potenziellen Tätern, ihre Strategie zu verbessern und Techniken zur Vereitelung forensischer Erfolge zu entwickeln. Solche Gegenmaßnahmen zielen darauf ab, die Entstehung von Beweismitteln im Ansatz zu verhindern oder ihre Verfügbarkeit und Aussagekraft bei der forensischen Analyse stark einzuschränken [Har06].

Die horizontale Anordnung der Teildisziplinen in Abb. 1 wurde bewusst gewählt, um graduelle Unterschiede in der Zuverlässigkeit der beweiserheblichen Tatsachen abzubilden. Dies kommt auch in den beiden Skalen zum Ausdruck. Das Maß *Freiheitsgrade* beschreibt die Anzahl unterschiedlicher (zumindest theoretischer) Möglichkeiten eines Forensikers, Beweismittel am Tatort zu erheben. Es ist am größten bei der analogen Forensik (materielle Beweismittel) und am geringsten bei der Computer-Forensik, bedingt durch das stark beschränkte Beobachtermodell. Je eingeschränkter und vorhersehbarer das Beobachtungsmodell, desto leichter fällt es einem raffinierten Täter, die Tatsachen unerkennbar zu manipulieren. Dies kann man auch durch den Grad der *Fälschbarkeit* ausdrücken, der sich entgegengesetzt zu den Freiheitsgeraden verhält und im direkteren Bezug zu Techniken zur Vereitelung forensischer Erfolge steht. Im Folgenden werden wir die Ordnung der Teildisziplinen mit Blick auf die zu erwartende Fälschbarkeit genauer erörtern.

Folgt man dem Locard'schen Prinzip in der **klassischen Forensik**, dann kann es keine Vereitelungstechniken geben, die das Entstehen von beweiserheblichen Tatsachen vollständig vermeiden. Selbst der raffinierteste Täter kann lediglich mit den Forensikern wetteifern, wer von ihnen die beste Abstraktion der Realität findet und so viele Quellen von Spuren wie möglich bei seinen Handlungen berücksichtigt. Zum Beispiel könnte ein Täter versuchen, Fingerabdrücke zu entfernen, indem er alle berührten Oberflächen reinigt. Dies führt jedoch zu neuen Spuren des Reinigungsmittels bzw. -tuchs. Wie geschickt er sich auch anstellt, der Versuch, die „transitive Hülle" aller Spuren zu verwischen, wird höchst wahrscheinlich in einem infiniten Regress enden. Deshalb kann in der materiellen Welt nur menschliches Versagen durch Nicht-Finden von beweiserheblichen Tatsachen zum Erfolg des Täters führen (siehe Abschnitt 2).

Eine grundlegend andere Situation ergibt sich in der **Computer-Forensik**. Diskrete und endliche Computersysteme erlauben es vorausschauenden Tätern, erstens, gültige Zustände zu finden, und zweitens, ein System von einem ungültigen (d. h. verdächtigen) Zustand in einen vorher aufgezeichneten gültigen Zustand zurückzuversetzen (siehe Abb. 3). Um beispielsweise einen Datendiebstahl von einem Standard-PC zu verstecken, speichert der Täter den ursprünglichen Zustand, überträgt alle für ihn relevanten Daten, und setzt schließlich den PC zurück in den gespeicherten Urzustand. Während der Erfolg dieses Vorgehens typischerweise auf Tathergänge begrenzt ist, in denen keine Spurensicherung stattfinden kann bevor die Spuren vernichtet sind, versuchen andere Vereitelungstechniken, erkennbare Spuren gar nicht erst entstehen zu lassen. Ein einfaches Beispiel ist das Booten von CD-ROM, bei dem anschließend die lokale Festplatte nur im *read-only*-Modus eingebunden wird. Abbildung 3 illustriert diese beiden skizzierten Vorgehensweisen.

Nicht näher eingegangen sei hier auf Versuche, Spuren nicht vollständig zu verwischen, sondern lediglich die Zuordnung zum Täter zu verhindern. Dies käme etwa einem Täter gleich, der auf der Flucht durch Wasser läuft, um Spürhunde abzuhängen. Eine digitale Analogie dazu wäre bspw. das Löschen oder Verschlüsseln von Datenträgern nach der Tat.

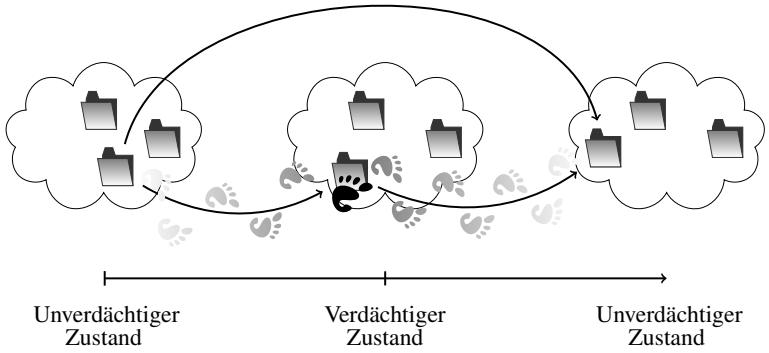

Abbildung 3: Kriminelle Handlungen hinterlassen Spuren, indem der Computer in einen verdächtigen, „ungültigen“ Zustand versetzt wird. Techniken zur Vereitelung forensischer Erfolge tilgen entweder alle Spuren in einem zweiten Schritt (unterer Pfad) oder vermeiden sie von vornherein (oberer Pfad).

Bei der **Multimedia-Forensik** lassen sich zwei mögliche Ziele unterscheiden, die ein Täter erreichen wollen könnte:

- Täuschung von Quellenidentifikation durch Unterdrücken der wahren Quelle oder durch Vorgeben einer bestimmten anderen Quelle, sowie
- Vertuschen von Nachbearbeitungsschritten durch Synthese authentisch wirkender Charakteristiken der Quelle bzw. durch Unterdrücken von Nachbearbeitungsartefakten.

Praktische Beispiele für den ersten Fall sind Versuche, das gerätespezifische Sensorrauschen in einem gegebenen Bild durch das einer anderen Kamera zu ersetzen [GKWB07]. Beim zweiten Fall sind Verfahren zum nicht nachweisbarem Skalieren [KB08] zu nennen, sowie Ansätze um authentisch wirkende CFA-Interpolationsmuster in beliebige, möglicherweise manipulierte Digitalfotos einzubringen [KB09]. Die beiden in Abb. 3 dargestellten Vorgehensweisen treffen auch auf die Multimedia-Forensik zu [KB08]: Das Generieren von gültigen CFA-Interpolationsmustern kommt dem Tilgen von Spuren gleich, während die Anwendung nicht nachweisbarer Skalierung Spuren von vornherein vermeidet.

Das Tilgen und Vermeiden von Spuren ist jedoch bei Mediendaten nicht immer ganz einfach. Der Grund dafür ist, dass die von einem Sensor ausgegebenen diskreten Symbole mit der dargestellten Szene zusammenhängen, die ein Teil der Realität ist. Obwohl die Anzahl der möglichen Zustände auch hier endlich ist (anders als in der materiellen Welt), sind es zu viele, um gültige Zustände effizient zu finden. Im Gegensatz zur Computer-Forensik mit ihren deterministischen, endlichen Automaten ist es zwecklos, das Problem durch „Virtualisierung der Realität“ in einem größeren System lösen zu wollen. Deshalb besteht ein Wettlauf um die besten Modelle zwischen raffinierten Tätern und Forensikern. Wer es eher schafft, Zusammenhänge zwischen realer Szene und digitaler Repräsentation besser zu beschreiben, kann Fälschung entweder zuverlässiger erkennen oder plausibler erstellen.

Techniken zur Vereitelung forensischer Erfolge funktionieren in Laborumgebungen hauptsächlich deshalb, weil die gegenwärtigen forensischen Verfahren sehr einfache Modelle verwenden und ihre Entscheidungen auf niedrig-dimensionalen Kriterien beruhen. Mit anderen Worten, sie vereinfachen die Realität sehr stark. Es ist dagegen kaum zu erwarten, dass heute bekannte Vereitelungstechniken auch dann noch erfolgreich sind, wenn sie in der Praxis gegen Kombinationen mehrerer forensischer Verfahren bestehen müssen, so dass sich die Dimensionalität der Entscheidungskriterien erhöht. Inwieweit derartige Kombinationen mit zukünftigen oder noch unbekannten Verschleierungstechniken überlistet werden können, bleibt eine offene Forschungsfrage. Ungeachtet dessen können Täter weiterhin versuchen, die Aussagesicherheit von forensischen Analysen zu reduzieren, indem sie verlustbehaftete aber unverdächtige Nachbearbeitungsoperationen auf digitale Beweismittel anwenden (z. B. Informationsreduktion durch Verkleinern oder verlustbehaftete Kompression). Hierbei ist entscheidend, welche Nachbearbeitungsoperationen als „zulässig“ (also unverdächtig) angesehen werden. Dies scheint ein Zwillingsproblem zur Frage nach legitimer Nachbearbeitung in Abschnitt 4.2 zu sein. Beide Antworten hängen letztendlich von den etablierten Gewohnheiten und Konventionen ab, die selbst wiederum kontextspezifisch sein können und sich vermutlich im Lauf der Zeit ändern.

6 Zusammenfassung und Ausblick

In diesem Aufsatz haben wir eine Struktur vorgeschlagen, die die verschiedenen Teildisziplinen der Forensik nach ihrer jeweiligen Natur der Beweismittel einordnet. Wir halten eine solche Unterscheidung für sinnvoll, um die zugrunde liegenden Annahmen und die Logik der Schlussfolgerungen klarer herauszustellen. Ein wichtiges Ergebnis ist, dass es im Bezug auf die Zuverlässigkeit von beweiserheblichen Tatsachen entscheidend ist, ob digitale Beweismittel ein mit Sensoren erstelltes Abbild der Realität darstellen, oder lediglich den internen Zustand eines abgeschlossenen und deterministischen Systems repräsentieren: Es ist schwerer, Mediendaten unerkennbar zu verfälschen als andere digitale Beweismittel. Außerdem hat sich der Begriff eines Beobachtermodells als hilfreich erwiesen, um die beiden Extrema – Computer-Forensik und klassische (analoge) Forensik – voneinander zu unterscheiden.

Man mag einwenden, dass diese Unterscheidungen ziemlich artifiziell und theoretisch wirken, vermutlich weil die hier vorgenommenen Abgrenzungen in der Praxis oft verschwommen sind. Zum Beispiel könnte bei einer Hausdurchsuchung ein Festplatten-Image erstellt worden sein, auf dem mit Methoden der Computer-Forensik Digitalfotos gefunden werden. Auf diese werden dann Techniken der Multimedia-Forensik angewandt, um die Bilder einer spezifischen Kamera zuzuordnen, die an anderer Stelle beschlagnahmt wurde. Fingerabdrücke auf dieser Kamera führen schließlich zum Täter. In diesem Beispiel interagieren alle forensischen Teildisziplinen, verwenden sowohl materielle als auch digitale Beweismittel, und bilden zusammen eine vollständige Indizienkette, die hoffentlich zur Verurteilung des wahren Täters führt. Derartige Kombinationen führen in der Praxis dazu, dass die subtilen Unterschiede zwischen den verschiedenen Ansätzen untergehen. Diese Unschärfe verkompliziert damit den Versuch, jede Teildisziplin separat zu betrachten.

Wir sehen den Beitrag dieses Aufsatzes in einem Versuch, das Feld zu strukturieren und über die (oft nur impliziten) Annahmen und Modelle expliziter und kritisch zu reflektieren. Unser Strukturierungsvorschlag und die zugehörige Terminologie (auch in Englisch [BFGK09]) sollte als Ausgangspunkt für weitere fruchtbare Diskussionen verstanden werden. Einen lohnenswerten Ansatz für weitere Forschung sehen wir unter anderem im Versuch einer Formalisierung der informellen Argumente. Dies hat vermutlich zur Folge, dass die überwiegend possibilistische (da einfachere) Perspektive zugunsten einer probabilistischen Theorie von Hypothesentests aufgegeben werden muss.

Danksagung

Wir bedanken uns herzlich bei Michael Knopp, der uns die Beweiswürdigung vor Gericht erläuterte und uns bei der Wahl der Begriffe für Beweismittel behilflich war, sowie bei unseren Dresdner Kollegen Benjamin Kellermann, Stefan Köpsell, Stefanie Pötzsch und Dagmar Schönfeld für ihre Diskussionsbeiträge und Anmerkungen zum Text.

Literatur

[BSM08] Sevinç Bayram, Husrev T. Sencar und Nasir Memon. Classification of digital camera-models based on demosaicing artifacts. *Digital Investigation*, 5:46–59, 2008.

[Böh09] Rainer Böhme. An Epistemological Approach to Steganography. *Angenommen bei Information Hiding 2009, 7.–10. Juni 2009, Darmstadt*, 2009. Erscheint in der Reihe *Lecture Notes in Computer Science*.

[BW05] Rainer Böhme und Andreas Westfeld. Feature-based Encoder Classification of Compressed Audio Streams. *Multimedia Systems Journal*, 11(2):108–120, 2005.

[BFGK09] Rainer Böhme, Felix C. Freiling, Thomas Gloe und Matthias Kirchner. Multimedia forensics is not computer forensics. In Z. Geradts, K. Y. Franke und C. J. Veenman, Hrsg., *Proc. of IWCF*, Bd. 5718 der Reihe *Lecture Notes in Computer Science*, Seiten 90–103, Berlin, Heidelberg, 2009. Springer Verlag.

[Cas04] Eoghan Casey. *Digital evidence and computer crime*. Academic Press, 2. Aufl., 2004.

[CFGL08] Mo Chen, Jessica Fridrich, Miroslav Goljan und Jan Lukáš. Determining Image Origin and Integrity Using Sensor Noise. *IEEE Transactions on Information Forensics and Security*, 3(1):74–90, 2008.

[DSM08] A. Emir Dirik, Husrev T. Sencar und Nasir D. Memon. Digital Single Lens Reflex Camera Identification From Traces of Sensor Dust. *IEEE Transactions on Information Forensics and Security*, 3(3):539–552, 2008.

[Far08] Hany Farid. Digital Image Ballistics from JPEG Quantization: A Followup Study. Bericht TR2008-638, Department of Computer Science, Dartmouth College, Hanover, NH, USA, 2008.

[GBK+01] Zeno J. Geradts, Jurrien Bijhold, Martijn Kieft, Kenji Kurosawa, Kenro Kuroki und Naoki Saitoh. Methods for Identification of Images Acquired with Digital Cameras. In Simon K. Bramble, Edward M. Carapezza und Lenny I. Rudin, Hrsg., *Proc. of SPIE: Enabling Technologies for Law Enforcement and Security*, SPIE Vol. 4232, Seiten 505–512, 2001.

[GBW09] Thomas Gloe, Karsten Borowka und Antje Winkler. Feature-Based Camera Model Identification Works in Practice: Results of a Comprehensive Evaluation Study. *Angenommen bei Information Hiding 2009, 7.–10. Juni 2009, Darmstadt*, 2009. Erscheint in der Reihe *Lecture Notes in Computer Science*.

[GFW07] Thomas Gloe, Elke Franz und Antje Winkler. Forensics for Flatbed Scanners. In Edward J. Delp und Ping Wah Wong, Hrsg., *Proc. of SPIE: Security and Watermarking of Multimedia Content IX*, SPIE Vol. 6505, 2007.

[GKWB07] Thomas Gloe, Matthias Kirchner, Antje Winkler und Rainer Böhme. Can we Trust Digital Image Forensics? In *MULTIMEDIA '07: Proc. of the 15th international conference on Multimedia, September 24–29, 2007, Augsburg, Germany*, Seiten 78–86, New York, NY, USA, 2007. ACM Press.

[Har06] Ryan Harris. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, 3:44–49, 2006.

[JF06] Micah K. Johnson und Hany Farid. Exposing Digital Forgeries through Chromatic Aberration. In *MM&Sec'06, Proc. of the Multimedia and Security Workshop 2006, September 26-27, 2006, Geneva, Switzerland*, Seiten 48–55, New York, NY, USA, 2006. ACM Press.

[JF07] Micah K. Johnson und Hany Farid. Exposing Digital Forgeries in Complex Lighting Environments. *IEEE Transactions on Information Forensics and Security*, 2(3):450–461, 2007.

[JG90] Rick Joyce und Gopal Gupta. Identity Authentication Based on Keystroke Latencies. *Communications of the ACM*, 33:168–176, 1990.

[KB08] Matthias Kirchner und Rainer Böhme. Hiding Traces of Resampling in Digital Images. *IEEE Transactions on Information Forensics and Security*, 3(4):582–592, 2008.

[KB09] Matthias Kirchner und Rainer Böhme. Synthesis of Color Filter Array Pattern in Digital Images. In Edward J. Delp, Jana Dittmann, Nasir D. Memon und Ping Wah Wong, Hrsg., *Proc. of SPIE-IS&T Electronic Imaging: Media Forensics and Security XI*, SPIE Vol. 7254, 2009.

[KCAD08] Nitin Khanna, George T.-C. Chiu, Jan P. Allebach und Edward J. Delp. Forensic techniques for classifying scanner, computer generated and digital camera images. In *Proc. of the 2008 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2008)*, Seiten 1653–1656, 2008.

[Ker83] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–38, 161–191, 1883.

[KMM+06] Nitin Khanna, Aravind K. Mikkilineni, Anthony F. Martone, Gazi N. Ali, George T.-C. Chiu, Jan P. Allebach und Edward J. Delp. A survey of forensic characterization methods for physical devices. *Digital Investigation*, 3(Supplement 1):17–28, 2006.

[Kno08] Michael Knopp. Digitalfotos als Beweismittel. *Zeitschrift für Rechtspolitik*, 41(5):156–158, 2008.

[KSM04] Mehdi Kharrazi, Husrev T. Sencar und Nasir Memon. Blind Source Camera Identification. In *Proc. of the 2004 IEEE International Conference on Image Processing (ICIP 2004)*, Seiten 709–712, 2004.

[KODL07] Christian Kraetzer, Andrea Oermann, Jana Dittmann und Andreas Lang. Digital audio forensics: A first practical evaluation on microphone and environment classification In *MM&Sec'07, Proc. of the Multimedia and Security Workshop 2007, September 20-21, 2007, Dallas, TX, USA*, Seiten 63–74, 2007.

[Kuh03] Markus G. Kuhn. *Compromising emanations: eavesdropping risks of computer displays*. Dissertation, University of Cambridge Computer Laboratory, 2003.

[MCP+07] N. Mondaini, R. Caldelli, A. Piva, M. Barni und V. Cappellini. Detection of malevolent changes in digital video for forensic applications. In Edward J. Delp und Ping Wah Wong, Hrsg., *Proc. of SPIE: Security and Watermarking of Multimedia Content IX*, SPIE Vol. 6505, 2007.

[MSGW08] Christine McKay, Ashwin Swaminathan, Hongmei Gou und Min Wu. Image acquisition forensics: Forensic analysis to identify imaging source. In *Proc. of the 2008 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2008)*, Seiten 1657–1660, 2008.

[NCLS06] Tian-Tsong Ng, Shih-Fu Chang, Ching-Yung Lin und Qibin Sun. Passive-blind Image Forensics. In W. Zeng, H. Yu und C.-Y. Lin, Hrsg., *Multimedia Security Technologies for Digital Rights*, Kapitel 15, Seiten 383–412. Academic Press, 2006.

[OVD07] Andrea Oermann, Claus Vielhauer und Jana Dittmann. Sensometrics: Identifying pen digitizers by statistical multimedia signal processing In R. Creutzburg, J. Takala und J. Cai, Hrsg., *Proc. of SPIE: Multimedia on Mobile Devices*, SPIE Vol. 6507, 2007.

[PF04] Alin C. Popescu und Hany Farid. Exposing Digital Forgeries by Detecting Duplicated Image Regions. Bericht TR2004-515, Department of Computer Science, Dartmouth College, Hanover, NH, USA, 2004.

[PF05a] Alin C. Popescu und Hany Farid. Exposing Digital Forgeries by Detecting Traces of Re-sampling. *IEEE Transactions on Signal Processing*, 53(2):758–767, 2005.

[PF05b] Alin C. Popescu und Hany Farid. Exposing Digital Forgeries in Color Filter Array Interpolated Images. *IEEE Transactions on Signal Processing*, 53(10):3948–3959, 2005.

[Saf00] Richard Saferstein. *Criminalistics: An Introduction to Forensic Science*. Prentice Hall, 7th. Auflage, 2000.

[SK98] Bruce Schneier und John Kelsey. Cryptographic support for secure logs on untrusted machines. In *SSYM'98: Proc. of the 7th USENIX Security Symposium*, Berkeley, CA, USA, 1998. USENIX Association.

[WF07] Weihong Wang und Hany Farid. Exposing Digital Forgeries in Video by Detecting Duplication. In *MM&Sec'07, Proc. of the Multimedia and Security Workshop 2007, September 20-21, 2007, Dallas, TX, USA*, Seiten 35–42, 2007.

[WKS08] Craig Wright, Dave Kleiman und Shyaam Sundhar. Overwriting Hard Drive Data: The Great Wiping Controversy. In R. Sekar und A. K. Pujari, Hrsg., *Proc. of ICISS*, Bd. 5352 der Reihe *Lecture Notes in Computer Science*, Seiten 243–257, Berlin, Heidelberg, 2008. Springer Verlag.

[ZM08] Sebastian Zander und Steven J. Murdoch. An Improved Clock-skew Measurement Technique for Revealing Hidden Services. In *SSYM'08: Proc. of the 17th USENIX Security Symposium*, Berkeley, CA, USA, 2008. USENIX Association.