FAKULTÄT FÜR !NFORMATIK

Didaktische Konzepte für die Lehre zum Thema 'Digital Rights Management' an postsekundären Bildungseinrichtungen

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Magister der Sozial- und Wirtschaftswissenschaften

im Rahmen des Studiums

Informatikmanagement

ausgeführt von

Rainer Poisel
Matrikelnummer 0725183

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: O. Univ. Prof. Dipl.-Ing. Dr.techn. Dietmar Dietrich

Wien, 20.01.2010

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Rainer Poisel, Dr. Theodor Körnerstraße 22/11, A-3100 St. Pölten

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

St. Pölten, 5. Februar 2010 Rainer Poisel

Kurzfassung

"Digital Rights Management" (DRM) versucht die mit dem Vertrieb und der Generierung analoger Medien verbundenen Rechte auf digitale Medien umzulegen. Der Verwendungskontext digitaler Medien steht dabei im Kontrast zu jenem von analogen Medien. So kann selbst beim Einsatz effektiver Verschlüsselungstechnologien der digitale Datenstrom oft problemlos in brauchbarer Form verbreitet werden. Einmal in ein analoges Format umgewandelt wird nahezu jeder Kopierschutzmechanismus unwirksam.

Seitens der Medienindustrie erhofft man sich durch den Einsatz von "Digital Rights Management" eine Eindämmung der durch die illegale Vervielfältigung von rechtlich geschützten Werken verursachten finanziellen Verluste. Dem gegenüber steht die Nutzerschaft, die sich in ihren Nutzungsrechten eingschränkt sieht.

Die zuvor dargestellte Thematik soll an postsekundäre Bildungseinrichtungen gelehrt werden. Die Vermittlung des Wissens erfolgt dabei unter Berücksichtigung der persönlichen Meinungsbildung der Kursteilnehmer. Forschungsleitende Fragestellung für das vorliegende Dokument war die Ermittlung der didaktischen Konzepte, sowie deren Einsatzmöglichkeiten, um die angeführten Lehrinhalte erfolgreich zu vermitteln.

Zur Beantwortung der Forschungsfrage wurde eine Literaturrecherche durchgeführt, um geeignete Studienpläne, Lehrinhalte und Lehrmethoden zu eruieren. Ergebnis dieser Diplomarbeit sind die zum Einsatz kommenden Lehrkonzepte, sowie die entsprechend aufbereiteten Inhalte. Die Praxistauglichkeit wurde in Form einer Lehrveranstaltung an der Fachhochschule St. Pölten im fünften Semester des Studienganges "IT Security" erprobt. Das Feedback seitens der Teilnehmer war durchwegs positiv. Daraus lässt sich schließen, dass die im Unterricht angewandten didaktischen Konzepte für die Vermittlung dieser Lehrinhalte geeignet sind.

Abstract

"Digital Rights Management" (DRM) tries to apply rights which users are accustomed to from the distribution and generation of analog media to digital media. The context of usage of digital media is different to that of analog media. Even by using effective modes of encryption the duplication of the digital media stream in a usable form can be accomplished easily sometimes. Once converted to an analog format, almost every mechanism of copy protection is rendered ineffective.

By using "Digital Rights Management" the media industry aims at the reduction of illegal distribution of copyright protected works. In comparison to that user groups see their usage rights restricted.

The topic presented before is to be taught in postsecundary educational establishments. The transfer of knowledge happens with consideration of personal opinion making by the course participants. The scientific problem for the present document includes to find out didactic concepts as well as application possibilities for the insemination of the content of teaching presented before.

To answer the research question adequate literature research has been performed to identify convenient degree programmes, content of teaching and methods of instruction. Results of this diploma thesis are the applied teaching methods and the refined content of teaching. For determining the practical feasibility these concepts were applied in the form of a lecture in the fifth semester of the program of study "IT Security" at the university of applied sciences in St. Pölten. The feedback given by the participants was positive consistently. This shows that the didactic concepts used in class were adequate for teaching the given subject.

Vorwort

Die Idee zum Thema der vorliegenden Diplomarbeit entstand aus den praktischen Überlegungen zu den Vorbereitungen der durch mich durchgeführten Lehrveranstaltung zur Thematik der Verwaltung digitaler Rechte - Digital Rights Management - im Bachelor-Studiengang IT Security an der Fachhochschule St. Pölten.

Die Intention der Studiengangsleitung an der Fachhochschule in St. Pölten zur Ausarbeitung des nun vorliegenden Konzepts war die Erweiterung des Wissenskompetenzbereiches der Steganographie des Lehrpersonals. Wie in späteren Kapiteln ausgeführt, ist die digitale Rechteverwaltung eng mit den technischen Prinzipien der Steganographie verknüpft, sodass diese wünschenswerten Synergien durch das gebotene Umfeld wirken konnten. Der Prozess der Unterrichtsvorbereitung konnte in den Kontext der Wissenschaft gestellt und entsprechend ausgearbeitet werden. Überlegungen zur Durchführung, sowie das Einbringen von am Studiengang neuartiger Lehrmethoden konnten unmittelbar in die Praxis umgesetzt werden.

Die vorliegende Diplomarbeit gliedert sich inhaltlich in mehrere Teile:

- Einleitung, in der die gelehrte Thematik definiert und in der die in der vorliegenden Diplomarbeit zu beantwortenden Forschungsfragen gestellt werden,
- Unterrichtsplanung mit Jahresplan und Unterrichtsentwurf, sowie der Zielgruppe und einer Einordnung der Lehrveranstaltung in die bereits existierenden Studienpläne an der Fachhochschule und der Technischen Universität Wien,
- Erläuterung der Wissens- und Wirklichkeitsbildung durch das menschliche Individuum und Vorstellung der dazu angewandten didaktischen Konzepte und Methoden,
- Beschreibung der im Vorlesungsteil gelehrten Lehrinhalte samt ihrer didaktischen Aufbereitung mit den vorgestellten Konzepten und Überlegungen sowie
- Beschreibung der im Übungsteil durchgeführten Konzepte, und eine Sammlung an durch die Studenten auszuarbeitende Themevorschläge.

Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung, wie z.B. Teilnehmer/Innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

Danksagungen

Zahlreiche der zum Verfassen dieser Arbeit notwendigen Tätigkeiten konnten während meiner beruflichen Tätigkeit als Assistent angestrengt werden. Weiters war es mir durch die Durchführung der Lehrveranstaltung möglich die didaktischen Konzepte in die Praxis umzusetzen und die damit verbundene Praxistauglichkeit zu ermitteln. Der Studiengangsleitung des zuvor erwähnten Studienganges sei aufgrund dessen an dieser Stelle mein Dank ausgesprochen.

Besonderen Dank möchte ich auch Dipl.-Ing. Albert Treytl, Dipl.-Ing. (FH) Thomas Turek und Univ. Ass. Dipl-Ing. Dr. techn. Friedrich Bauer aussprechen. Sie waren neben ihrer Tätigkeit des Mitwirkens an der Betreuung meiner Diplomarbeit als die unmittelbaren fachlichen Ansprechpersonen vorgesehen und konnten mir in dieser Position wertvolle Tipps sowohl fachlicher, als auch formeller Natur geben.

Nicht zuletzt möchte ich mich auch bei meinen Eltern, Schwestern, meiner Freundin und bei meinen Freunden bedanken. Sie haben mich während der Zeit der Recherche und des Schreibens moralisch unterstützt und mir so den Rücken gestärkt.

"Der Künstler bezahlt etwaige Mängel
des sozialen Verhaltens durch sein Werk.
Was er dem Werk zum Opfer bringt,
und das ist meistens unendlich viel mehr,
als was der brave Durchschnittsbürger
zu opfern fähig wäre,
das kommt allen zugut."

–Hermann Hesse (1877 - 1962)

Inhaltsverzeichnis

Kapitel 1

Einleitung

Der Inhalt der in der vorliegenden Arbeit beschriebenen Lehrveranstaltung dreht sich um die Thematik der Rechteverwaltung im Umfeld digitaler Medien. Neben der Definition des Begriffes "Digital Rights Management" wird zu Beginn die forschungsleitende Fragestellung entwickelt und die Methodik zur Beantwortung dieser, die Forschungsstrategie, erläutert.

1.1 Problemstellung

Thematik der Lehrveranstaltung wird "Digital Rights Management", kurz "DRM", sein. Arnold Picot definiert den Begriff wie folgt (S. 3 [Pic05]): "Digital Rights Management zielt darauf ab, für digitalisierbare Inhaltsprodukte die Voraussetzung zu schaffen, damit auch in der digitalen Welt die Rechte, die jemand solchen Produkten geltend machen kann, definiert und durchgesetzt werden können."

Im Idealfall können hierbei die aus der analogen Welt bekannten Rechte direkt abgebildet werden. Dies entspricht jedoch in beinahe allen Fällen nicht der Realität. Bei digitalen Medien ist bereits der Bezug zum gehandelten Objekt durch den Nutzer ein ganz anderer, als bei physikalischen Daten- bzw. Medienträgern, die durch den Nutzer greifbar sind, war. Gerald Fränkl erläutert (vgl. S. 13 [Fra05]) die im Sachverhalt aufeinander prallenden Fronten. Konkret sind das:

- maßlos kopierende Verbraucher, die Urheberrechtsverletzungen begehen und
- Medien- und Technologieunternehmen mit sehr restriktiven Nutzuntsvorstellungen, die unabhängig von Datenschutzrichtlinien agieren.

Weiters wird in derselben Literatur auf die Problematik der digitalen "Welt" im Vergleich zu ihrem analogen Pendant eingegangen. Analoge Medien sind demnach vom Generationsverlust betroffen. Dabei weist die Kopie eines Mediendatenträgers eine geringere Qualität als das Original auf. Bei Kopien, die von einer Kopie gemacht werden, ist die Qualität weiter vermindert. Naturgemäß gibt es daher eine Grenze, ab der sinnvoll keine weiteren Kopien mehr erstellt werden.

Kürzlich veröffentlichte Statistiken zeigen (vgl. [20]) die Auswirkungen und Ursachen der Piraterie im Softwarebereich. So liegt die weltweite Rate an unrechtlich eingesetzter Software bei ca. 40%. Kapitel 4.1 geht auf die statistischen Methoden zur Ermittlung der Zahlenwerte ein. Die folgen

der hohen finanziellen Verluste ist nur schwer überschaubar, da weite Schichten der Bevölkerung betroffen sind. Auch die Sozialsysteme der Industriestaaten leiden unter den Verlusten, da alleine zur Inbetriebnahme der Software eine Vielzahl an Menschen beteiligt ist (vgl. [7]).

Der Einsatz der hier vorgestellten Maßnahmen erfordert, dass alle Geräte die technischen Vorgaben der Medienanbieter erfüllen. Gegner der Technologie kritisieren auch die Inkompatibilität der mobilen Wiedergabegeräte und die damit verbundene Kundenbindung an das Anbietersystem, die steigenden Kosten für Computer und Komponenten, sowie die mangelhafte Umsetzung der Datenschutzrichtlinien und die Verkomplizierung der Benutzung. Auch die Erstellung von Privatkopien ist von Einschränkungen betroffen. Aus den genannten Gründen steht die Benutzergemeinschaft diesen Systemen eher ablehnend gegenüber. Außerdem wurden DRM-Systeme von der Gemeinschaft bereits technisch umgehbar gemacht, wie Berichte aus den Medien belegen. Informationsplattformen (z. B. [5]) unterrichten die Medienkonsumenten über die möglichen weitreichenden Folgen, die durch die Integration der technologischen Erweiterungen in die Endgeräte entstehen können.

Die Durchführung der Lehrveranstaltung erfolgt an postsekundären Bildungseinrichtungen in Österreich. Dies umfasst Bildungseinrichtungen mit akademischen Niveau. Seitens der Studierenden wird Maturaniveau erwartet. Weiters wird vorausgesetzt, dass in den ersten Semestern die Grundlagen der prozeduralen Programmierung, sowie die mathematischen Grundlagen zur linearen Algebra erlernt wurden. In der vorliegenden Arbeit sind die didaktischen Konzepte zur Durchführung an Universitäten und Fachhochschulen ausgelegt.

Das Publikum der in dieser Arbeit beschriebenen Lehrveranstaltung wird erfahrungsgemäß jünger oder, anders ausgedrückt, im Bereich der Medienkonsumenten anzutreffen sein. Die durch individuelle Erfahrungen geprägte Meinung, vielleicht sogar vorherrschende skeptische, ablehnende Haltung gegenüber der Thematik, jedes einzelnen Studierenden soll durch den Besuch der Lehrveranstaltung unangetastet bleiben. Die Lehrveranstaltung soll unterstützend eingreifen und helfen, die Meinung zur Thematik seitens der Studierenden durch eine begründete Argumentation zu untermauern. Deswegen wird bei der Ausarbeitung der Antworten auf die Forschungsfragen die Wirklichkeits- und Meinungsbildung besonders berücksichtigt.

Zur Wirklichkeitsbildung und in weiterer Folge auch zur Meinungsbildung trägt (vgl. S. 1 [Fri06]) zufolge maßgeblich die Beeinflussung der Menschheit durch die Medien bei. Der Verarbeitung von Eindrücken wird dabei mehr Einfluss als den Eindrücken selbst zugesprochen. Reale, mediale aber auch die virtuelle Welt werden dabei durch das menschliche Individuum verschränkt. In Kapitel 3 wird näher auf die Zusammenhänge im Kontext der Lehrmethoden eingegangen.

Kersten Reich gilt als einer der populärsten Verfechter der konstruktivistischen Didaktik. In dieser Theorie wird das Einsehen des Sinnes im Kontext des zu lehrenden Stoffes als wesentliche Motivation im Lernprozess verstanden (vgl. S. 95 [Rei06]). So wird weiters darauf eingegangen, dass zum Lernen durch die Studierenden eine Selbststeuerung unerlässlich ist. Selbst bei der Übernahme vorgefertigter Gedankenmuster wurd durch den Verstand des menschliche Individuums Wirklichkeit

konstruiert. Das Kapitel über den Konstruktivismus 3.1.1 geht näher auf die Thematik der Wissenskonstruktion ein.

Absolventen des Studienganges IT Security an der Fachhochschule St. Pölten sollen als Spezialisten im Bereich der digitalen Rechteverwaltung arbeiten können. Der Studienplan und die in der Lehrveranstaltungen durch die Lehrbeauftragten zu vermitteltenden Lehrinhalte sind bereits im sogenannten Modulhandbuch (vgl. [32]) geregelt. Von der Studiengangsleitung ist im Rahmen der Durchführung der Lehrveranstaltung auch eine Einführung in und ein grober Überblick über die Steganographie vorgesehen. Neben einer theoretischen Darstellung sind Versuche mit entsprechend aufbereitetem Material vorbereitet.

So ist es mit geringem Aufwand möglich, die Sachverhalte in verständlicher Weise greifbar zu machen. Ein grundlegendes Verständnis der steganographischen Verfahren ist für das zuvor erwähnte Berufsbild von unbedingter Notwendigkeit. Es wird als Grundlage für das Masterstudium erachtet.

1.2 Forschungsleitende Fragestellung

Die bei den Studierenden vorherrschende skeptische, ablehnende Haltung gegenüber der Thematik soll auch im Rahmen des Unterrichts und dessen zugrundeliegenden Vorbereitung unberührt bleiben, was die konstruktivistische Didaktik als für diesen Zweck als geeignet erscheinen lässt. Auf die hierfür sprechenden Gründe wird im Kapitel 3 eingegangen.

Die Studierenden sollen daher nach Besuch der Lehrveranstaltung die Für und Wider der Technologie abwägen, sowie Kriterien zum oder gegen den Einsatz je nach Anwendungsgebiet begründen können. Ergebnis des ersten Teils ist daher eine Auswahl der geeigneten Lernkonzepte nach den Vorgaben der konstruktivistischen Didaktik. Neben der Auswahl geeigneter didaktischer Methoden werden die wesentlichen Merkmale dieser und Einsatzszenarien erläutert, um zu ermitteln, wie sich diese zur Vermittlung der Lehrinhalte eignen.

Die erste Forschungsfrage ergibt sich daher wie folgt: Welche didaktischen Konzepte lassen sich aus der Problembenennung ableiten?

Da die konkrete Unterrichtsplanung ein zentrales Ergebnis dieser Arbeit ist, gilt es die Thematik des "Digital Rights Managements" in den Kontext der erwähnten didaktischen Methoden zu stellen.

Als zweite Forschungsfrage sei somit folgende zu nennen: Welche Kriterien rechtfertigen den Einsatz dieser didaktischen Konzepte zur Vermittlung der Lehrinhalte an postsekundären Bildungseinrichtungen in Österreich und wie können diese zur Vermittlung der Lehrinhalte eingesetzt werden?

Bei der Beantwortung der zweiten Forschungsfrage werden daher die zu lehrenden Inhalte, sowie die zur Lehre eingesetzten Methoden dargestellt. Abbildungen und Vorlesungsfolien selbst werden eingebracht, sofern dies im Kontext der vorliegenden Arbeit sinnvoll erscheint.

1.3 Forschungsstrategie

Zu den didaktischen Methoden gibt es bereits umfangreiche Forschungen. Entsprechend reichhaltig ist das Literaturangebot zur Thematik. Vor allem im Bereich des klassischen Frontalvortrages gibt es wahre Kataloge an alternativen Lehrmethoden, wie z. B. den von Kersten Reich moderierten konstruktiven und systemischen Methodenpool der Unterrichtsmethoden (vgl. [45]). Deswegen wird zur Beantwortung der ersten Forschungsfrage die klassische Inhaltsanalyse herangezogen. Die Recherche in wissenschaftlichen Publikationen, Papers, sowie von Internetressourcen gibt Aufschluss über die zu vermittelnden Fachinhalte. Außerdem ermöglicht diese Vorgangsweise die Ausarbeitung und Ermittlung der für die Lehrveranstaltung geeigneten didaktischen Konzepte. Ein wesentliches Kriterium bei der Wahl der Lehrmethoden ist die Möglichkeit der Wissenserarbeitung durch die Studierenden selbst.

Im Zuge der Fragenbeantwortung wird auch auf die Aspekte der Unterrichtsplanung eingegangen, um einen Arbeitsplan bzw. Stoffverteilungsplan zu erarbeiten. Dies ist notwendig, um die exakten Zeitvorgaben im Lehrplan einzuhalten. Hauptziel dieser Ausarbeitung ist Aufteilung des zu lehrenden Stoffgebietes in klar abgrenzbare Einheiten. Peterßen geht im “Handbuch Unterrichtsplanung” (vgl. S. 205ff [Pet00]) auf die einzelnen Schritte in der Planungsphase ein.

Kapitel 2

Planung der Lehrveranstaltung

Dieses Kapitel behandelt die Planung zur Lehrveranstaltung "Digital Rights Management", welche an postsekundären Bildungseinrichtungen abgehalten wird. In Abhängigkeit der Bildungseinrichtung wird auf den vorliegenden Studienplan eingegangen. Sieht dieser eine Lehrveranstaltung über Digital Rights Management nicht vor, so werden Vorschläge abgegeben, wo eine Durchführung sinnvoll durchführbar ist.

2.1 Durchführung an Fachhochschulen

Exemplarisch wird die Durchführung an Fachhochschulen (FHs) beschrieben. Der Lehrplan, und damit der Durchführungskontext, liegt hier bereits fest. Zur Durchführung an Universitäten werden Vorschläge gemacht.

2.1.1 Zielgruppe

Zielgruppe sind zum Verfassungszeitpunkt dieser Arbeit Studierende des technischen Studienganges "IT Security", der mit dem Grad des Baccalaureus abschließt. Erfahrungsgemäß umfasst ein Jahrgang in dieser Studienrichtung 25 Studierende. Demnach sind die in dieser Publikation vorgestellten didaktischen Konzepte und Durchführungsstrategien auf Gruppengrößen bis zu 30 Studierende ausgelegt.

Die praktischen Übungen werden in Gruppen zu je drei bis vier Studenten durchgeführt. Eine Aufteilung des Jahrgangs in die Kleingruppen erfolgt gemäß den Regeln für das Gruppenpuzzle unter den in den Kapiteln 3.2.4 und 5 gelieferten Gesichtspunkten.

2.1.2 Bezug zum Studienplan

Dem Modulhandbuch zu Folge (vgl. S. 3ff [32]) ist der Studienplan nach §3/2/1 Fachhochschul-Studiengesetz (FHStG) aufgebaut. Demnach ist eine Aufteilung in vier Schwerpunkte vorgesehen:

- Netzwerktechnik,

- IT-Betrieb,
- Sicherheitstechnologien, sowie
- Sicherheitsmanagement und Organisation.

Jeder Schwerpunkt ist in Modulen organisiert. "In den Modulen werden Stoffgebiete zu thematisch und zeitlich abgerundeten, in sich abgeschlossenen und überprüfbaren Einheiten zusammengefasst." Module wiederum sind in Lehrveranstaltungen aufgeteilt. Um im Wissenserwerb die Eigeninitiative der Studenten zu fördern, wird beim Einsatz didaktischer Konzepte in Abhängigkeit der Lehrinhalte der jeweiligen Lehrveranstaltungen differenziert vorgegangen.

Der Unterricht der Lehrveranstaltungen zur Thematik des Digital Rights Management ist dem Modul "Digital Rights Management" im Schwerpunkt "Sicherheitstechnologien" zuzuordnen. Dieses ist im Curriculum[1] im fünften Semester vorgesehen und umfasst neben den Lehrveranstaltungen zur Thematik des "Digital Rights Management" auch Lehrveranstaltungen zum Urheberrecht. Die DRM-Lehrveranstaltung ist in eine Vorlesung (VO) und eine Übung (UE) im Umfang von jeweils einer Semesterwochenstunde (SWS) unterteilt. Bei einer Wochenzahl von 15 je Studiensemester beläuft sich die Gesamtstundenzahl sowohl für die Vorlesung, als auch für die Übung auf 15.

Da sich der organisatorische Aufwand zur Trennung in Vorlesungs- und Übungsteil als nicht praktikabel erwies, wurde eine Zusammenlegung zu einer integrierten Lehrveranstaltung (ILV) beim Fachhochschulrat beantragt.

2.1.3 Unterrichtsplanung der Vorlesung

Bei der Unterrichtsplanung wird nach den im "Handbuch Unterrichtsplanung" von Wilhelm H. Peterßen (vgl. S. 206 [Pet00]) vorgestellten Stufen der Unterrichtsplanung vorgegangen. Die Durchführungsstrategie wird mit Hilfe der Werkzeuge der Unterrichtsplanung, wie z. B. Jahresplan und Arbeitsplan, ausgearbeitet.

Lehrplan/Curriculum, Jahresplan

Die Eingliederung in den Studienplan (Lehrplan) bzw. der Lehrplan mit den durch ihn definierten Lehrinhalten ist durch die Studiengangsleitung bereits vorgegeben. Die wesentlichen Lehrinhalte werden wiederum im Modulhandbuch (vgl. S. 32 [32]) aufgezählt

- Einführung, Terminologie, Gründe zum Einsatz,
- Erscheinungsformen (Musik, Film, Buch, Software),
- Steganographie, sowie
- Softwareschutz.

[1] auch als "Lehrplan" bekannt

Da die Lehrinhalte bereits mit der Verfassung des Modulhandbuches festgelegt wurden und die Thematik des DRMs starken Änderungen und Weiterentwicklungen unterliegt, wurden diese entsprechend dem Zeitgeist aktualisiert und angepasst. Ein von der Zeit unabhängiges Kriterium bei der Unterrichtsdurchführung ist jedoch die Unterstützung der Studierenden bei der Meinungsbildung zu DRM, sowie in der Unterstützung zur Untermauerung des jeweiligen Standpunkts durch eine entsprechende Argumentation.

Arbeitsplan, mittelfristige Unterrichtseinheiten

Der Arbeitsplan bricht den Jahresplan in Blöcke auf. Diese Blöcke werden durch die jeweils zur Vermittlung notwendige Anzahl an Lehreinheiten abgedeckt und spiegeln die durch den Lehrplan gesteckten Ziele ab:

- Block 1 über Terminologie, Digital Rights Management Systeme,
- Block 2 über Metadaten,
- Block 3 über Medienverwertung und Gebührenmanagement,
- Block 4 über Einführung in die lineare Algebra,
- Block 5 über visuelle und auditive Steganographie und
- Block 6 über Trusted Computing.

Der Unterrichtsentwurf beschreibt im Folgenden die konkrete Aufteilung in Unterrichtseinheiten.

Unterrichtsentwurf

Der Unterrichtsentwurf gibt einen Überblick über die Inhalte der jeweiligen Vorlesungseinheiten. Bei der Durchführung werden zwei bzw. drei Unterrichtseinheiten zu einem Unterrichtsblock zusammengelegt. Dadurch ergeben sich für das gesamte Studiensemester siebeneinhalb Blöcke. Tabelle 2.1 zeigt den Unterrichtsentwurf im Überblick.

2.1.4 Unterrichtsplanung der Übung

Die Durchführung der Übung kann zum Vorteil der Studenten und einer flexibleren Zeiteinteilung zu großen Teilen in Heimarbeit ohne Answesenheitspflicht erledigt werden. Ein Treffen zwischen Studenten und Lehrbeauftragtem erfolgt an drei Terminen im Laufe des Semesters. Tabelle 2.2 zeigt zusammenfassend die Planung des Übungsteiles der Lehrveranstaltung.

Eine detailliertere Beschreibung der der Übung zugrundeliegenden didaktischen Konzepte finden sich in Kapitel 3.2.4 über das Konzept des Gruppenpuzzles, eine Übersicht über die Themen, sowie den Durchführungskontext für die vorgestellten didaktischen Konzepte findet sich in Kapitel 5, das die Kriterien für den Übungsteil der Lehrveranstaltung beschreibt.

Dauer	Inhalte	Methode	Materialien
90 Min.	Block 1		
	Willkommen, Organisatorisches, Beschreibung der Inhalte, Terminologie	Präsentation und kurze Videosequenzen	Folien, Handouts und Videosequenzen
90 Min.	Block 2		
	Terminologie, DRM Systeme	Präsentation	Folien
90 Min.	Block 3		
	Metadaten	Präsentation	Folien
60 Min.	Block 4		
	Medienverwertung und Gebührenmanagement	Präsentation	Folien und Videosequenzen
30 Min.	Einführung in die lineare Algebra	Präsentation, Frontalvortrag an der Tafel	Folien, Tafel
90 Min.	Block 5		
	Einführung in die visuelle Steganographie (I)	Präsentation und Beispiel in MATLAB	Folien und Computer mit vorinstalliertem MATLAB
60 Min.	Block 6		
	Einführung in die visuelle Steganographie (II)	Präsentation und Beipsiel in MATLAB	Folien und Computer mit vorinstalliertem MATLAB
30 Min.	Einführung in die auditive Steganographie	Präsentation	Folien
90 Min.	Block 7		
	Trusted Computing	Präsentation und kurze Videosequenzen	Folien und Videosequenzen
90 Min.	Block 8		
	Prüfungsvorbereitung	Präsentation	Folien

Tabelle 2.1: Unterrichtsplanung der Vorlesung

2.2 Durchführung an Universitäten

Die Durchführung an Universitäten wird exemplarisch am Studienplan der TU-Wien (vgl. [19]) erläutert. Da die Lehrveranstaltung bislang nicht im Katalog der angebotenen Lehrveranstaltungen enthalten ist, können ausschließliche Empfehlungen betreffend den Durchführungskontext gegeben werden.

Dauer	Inhalte	Methode	Materialien
45 Min.	Starttermin		
	Gruppeneinteilung der Stammgruppen, Festlegung der Expertengruppen durch die Studenten, Auswahl der Themen durch die Expertengruppen	Frontalvortrag	Handouts
10 Min. je Gruppe	Kontrolltermin		
	Präsentation der Ergebnisse in den Expertengruppen	-	-
15 Min.	Auswahl der Themen durch die Stammgruppen	Frontalvortrag	Handouts
10 Min. je Gruppe	Schlusstermin		
	Präsentation der Ergebnisse in den Stammgruppen	-	-

Tabelle 2.2: Unterrichtsplanung für die Übung

Grundsätzlich sind Jahresplan, Arbeitsplan, und Unterrichtsentwurf an den der Durchführung an Fachhochschulen angelehnt. Im Folgenden wird die Zielgruppe, sowie der Bezug zum Studienplan beschrieben.

2.2.1 Zielgruppen

Als Zielgruppen an der technischen Universität in Wien sind folgende Studiengänge angedacht:

- Medieninformatik (vgl. S. 14ff [19]),
- Software & Information Engineering (vgl. S. 25ff [19]) und
- Technische Informatik (vgl. S. 31ff [19]).

Wie bei den Fachhochschulen ist die Lehrveranstaltung an der Technischen Universität in Wien bis Gruppengrößen zwischen 20 und 30 Studierenden sinnvoll durchführbar. Entsprechend muss diese Begrenzung der Lehrveranstaltungsteilnehmerzahl bei der Eröffnung zur Anmeldung berücksichtigt werden.

Für die Übungsdurchführung kommen dieselben Rahmenbedingungen, wie bei der Durchführung an Fachhochschulen, zur Geltung.

2.2.2 Bezug zum Studienplan

Die Studienpläne der drei zuvor erwähnten Studiengänge geben Aufschluss über die bereits vorgesehenen Lehrveranstaltungen. Als weitere Untergliederung der Einteilung in die allgemeinen Prü-

fungsfächer, sowie in die Schwerpunkte lässt sich die Lehrveranstaltung des Digital Rights Management in die Untergruppe "Informatik und Gesellschaft" einordnen. Die Lehrveranstaltung wird als "Vorlesung kombiniert mit Übung" (VU), dem Pendant zur integrierten Lehrveranstaltung (ILV) an den Fachhochschulen, abgehalten.

Hinsichtlich der Lage in den jeweiligen Semesterempfehlungen ist das Absolvieren der Lehrveranstaltung durch die Studenten nach dem Grundstudium im vierten Semester sinnvoll. Gewichtet wird die Kombination aus Vorlesung und Übung zusammen mit 3 ECTS[2]-Punkten, was einem Durchführungsaufwand von 2 Semesterwochenstunden (SWS) gleicht.

[2] European Credit Transfer and Accumulation System

Kapitel 3

Didaktische Konzepte und Methoden

Bei der im Rahmen dieser Diplomarbeit entwickelten Lehrveranstaltung über das digitale Rechtemanagement handelt es sich um eine in Vorlesungs- und Übungsteil untergliederte Lehrveranstaltung mit Fernstudienelementen. Der Übungsteil wird weitestgehend mit reduzierter Anwesenheitspflicht als Gruppenarbeit in Heimarbeit durchgeführt. Der Vorlesungsteil hingegen erfolgt nach einem vorgegebenen Stundenplan mit zuvor definierten Inhalten, sowie ausgewählten Anwendungsszenarien an zuvor festgelegten Orten.

3.1 Didaktische Konzepte

Digital Rights Management ist eine sehr kontrovers diskutierte Thematik. Auf der einen Seite erhofft sich die Medienindustrie eine Eindämmung der durch unerlaubte Vervielfältigung, so genannte Raubkopien, verursachten Verluste (hierzu siehe z. B. (vgl. S. 23ff [Pic05])). Konnten vor der Zeit der flächendeckenden Versorgung mit kostengünstigen Internetanschlüssen Verluste durch die mechanische Vervielfältigung mit Hilfe pauschalierter Abgaben ausgeglichen werden, stellt die einfache Bedienung, sowie ein breites Angebot in Online-Tauschbörsen zusehends ein Problem dar. Auf der anderen Seite stehen dem gegenüber die Nutzer, die ihre Rechte zur Nutzung digitaler Inhalte durch diverse Schutzmechanismen eingeschränkt sehen. Die Entwicklung von kritischen Informationsplattformen durch Betroffene waren die Folge. Beispielsweise wird im Portal "Digital Restrictions Management" geschrieben [5]: "As much of the information on this web site explains, large media and technology companies are the main beneficiaries of Digital Restrictions Management (DRM). Because both groups have considerable market power combined with disproportionate direct and indirect influence on all media, critical review of DRM technologies and their effect on all areas of society has been sadly lacking throughout the past years." Die Entwickler technischer Lösungen, sowie die Medieninhabern werden hier als Hauptgewinner beim Einsatz von DRM-Technologien angesehen. Begründet wird dies in deren beachtlichen Markteinfluss, dem Einfluss auf die Medien selbst und dem Einfluss auf alle Bereiche der Gesellschaft.

Dieses Kapitel erläutert die Herangehensweise an das gewählte didaktische Konzept des Konstruktivismuses. Dazu wird in den Unterkapiteln auf die theoretischen Grundlagen zur Meinungsbildung durch die Studierenden eingegangen. Weiters werden die Grundzüge der konstruktivistischen Didaktik ausgeführt und in den Kontext des Digital Rights Management gestellt.

3.1.1 Wirklichkeitsbildung

Das Wirklichkeitsbild der Studierenden zur Thematik des digitalen Rechtemanagements kann aufgrund der unterschiedlichen Erfahrungen weitgehend differieren. Kersten Reich postuliert, dass es in diesem Kontext nicht möglich ist (S. 82 [Rei06]), "den einen richtigen didaktischen Ansatz für alle zu finden und zu begründen. Wir können allenfalls ein Angebot unterbreiten, das möglichst vielen als passend erscheinen kann und das eine zahlenmäßig große Verständigungsgemeinschaft anspricht, orientiert, motiviert." Aus Sicht des Lehrenden ergibt sich die Herausforderung Vorurteile auszuräumen und die Meinungsbildung der Studierenden zu unterstützen, nicht jedoch zu lenken. Im Unterricht soll vorwiegend das techniche Verständnis dahingehend beeinflusst werden, dass die Studierenden in den Argumenten zu ihrem Standpunkt bestärkt werden.

Aufgrund dieser starken Medienpräsenz und der weiten Verbreitung von Abspielsoftware und -geräten besteht die Möglichkeit, dass sich die Studierenden bereits vor Beginn des Unterrichts eine Meinung zur Thematik gebildet haben. Das verpflichtende Berufspraktikum an Fachhochschulen, sowie die unter Umständen vorhandene berufliche Erfahrung der Studierenden generell, bieten Potenzial seitens der Studierenden für einschlägige Erfahrungen mit der Thematik im Bereich der Produktion und der Verwertung digitaler Medien.

Ziel der Lehrveranstaltung ist dem im Modulhandbuch (vgl. [32]) vorgestellten Lehrplan zu Folge die Ausbildung von Digital Rights Management ExpertInnen. Um den Studierenden die Bildung einer eigenen Meinung zu ermöglichen, wird versucht, ein möglichst von allen Seiten beleuchtetes Bild der Thematik zu vermitteln und Standpunkte aufzuzeigen. Die philosophische Ausrichtung des Unterrichts legt dann fest, wie dieser gestaltet werden muss, um die Studierenden im Prozess der Meinungsbildung zu unterstützen. Eine Klassifizierung der Ausrichtungen soll anhand der Wirklichkeitsbildung durch das menschliche Wesen erfolgen.

Konstruktivismus

Bei einer Definition des Konstruktivismusses wird von einer aktiven Einbindung der Studierenden in den Vermittlungsprozess ausgegangen [23]: "Constructivism is the label given to a set of theories about learning which fall somewhere between cognitive and humanistic views. If behaviourism treats the organism as a black box, cognitive theory recognises the importance of the mind in making sense of the material with which it is presented. Nevertheless, it still presupposes that the role of the learner is primarily to assimilate whatever the teacher presents. Constructivism – particularly in its 'social' forms – suggests that the learner is much more actively involved in a joint enterprise with the teacher of creating ('constructing') new meanings." Die Erklärung fällt hier anhand eines Vergleiches zwischen Behaviorismus und Konstruktivismus aus. Letzterer bezieht die Präsentation der zu erlernenden Inhalte in den Zusammenhang mit der Aufnahme durch die Studierenden. Neue Ansichten und Meinungen werden gemeinsam mit dem Lehrer kreiert.

In weiterer Folge untergliedert die oben referenzierte Publikation den Konstruktivismus in zwei Teilbereiche.

- Der kognitive Konstruktivismus macht Abhandlungen über das Verstehen von Dingen aus Sicht des Studierenden in Form von Entwicklungsstadien und Lernstilen.
- Der soziale Konstruktivismus schafft Wissen über Bedeutungen und Verständnis, sowie deren Entstehen aus sozialen Begegnungen.

Beide Teilbereiche werden im Rahmen der Lehrveranstaltung eine tragende Rolle spielen, da neben der Vermittlung der Lehrinhalte auch die Zusammenarbeit in Kleingruppen von je drei bis fünf Studenten und die Vermittlung der Argumentation der jeweils anderen Zielgruppe (z. B. Befürworter des Einsatzes der Technologie und Endnutzer, der gegen den Einsatz ist) vorgesehen ist.

Peter Hubwieser geht auf den Konstruktivismus im Kontext des Studierenden (vgl. S. 10 [Hub03]), den kognitiven Konstruktivimsus, ein. Die Thematik wird im Kontrast zum radikalen Konstruktivismus gestellt. Letzterer (vgl. S. 85 [Rei06]) "... überbetont die Relativität der subjektiven Erkenntnis als Ausdruck von Wirklichkeitskonstruktionen." Die Formen der radikalen Konstruktivismen zeichnen sich durch eine starke subjektivistische Orientierung aus. Das gelehrte Wissen selbst wird dabei in einer relativierenden Sicht dargestellt. Aufgrund der ausschließlich subjektiven Wahrnehmung ist beim radikalen Konstruktivismus daher keine Übereinstimmung zwischen wahrgenommenen Bild und der objektiven Wirklichkeit möglich. Deswegen wird im Kontext des gemäßigten Konstruktivismus gelehrt. Dieser zeichnet sich durch folgende Prozessmerkmale aus:

- Lernen setzt die aktive Beteiligung der Studierenden voraus; so müssen diese z. B. motiviert sein und Interese haben oder entwickeln für das was sie tun.
- Selbststeuerung ist Voraussetzung für jedes Lernen, die Studierenden müssen also Steuerungs- und Kontrollaufgaben übernehmen und diese je nach Situation variieren.
- Kognitiven Prozessen gehen eigene Interpretationen je nach individuellem Erfahrungs- und Wissenshintergrund voraus; Lernen ist somit in jedem Fall konstruktiv.
- Lernprozess finden situativ statt; das hängt damit zusammen, dass Lernen stets in spezifischen Kontexten stattfindet.

Im Zusammenhang mit dem sozialen Konstruktivismus wird erwähnt, dass Studierende und deren Aktivitäten stets soziokulturellen Einflüssen ausgesetzt sind, und dass das Lernen ein interaktives Geschehen ist.

Konstruktion der Wirklichkeit

Fritz trifft die Annahme (S. 1 [Fri06]), "dass Wirklichkeit nicht per se existiert, sondern nach Maßgabe neuronal bedingter Konstruktionen, die das menschliche Gehirn auf der Grundlage von Wahrnehmungen vornimmt. Dabei sind nicht die Eindrücke selbst das Entscheidende, sondern deren Verarbeitung. In zunehmendem Maße verschränken sich reale, mediale und auch virtuelle Welt,

was zu andersartigen Erfahrungen führt, die die Bildung der Persönlichkeit beeinflussen." Dies geht einher mit der Wissensbildung durch das menschliche Individum. Schon der deutsche Philosoph Imannuel Kant hielt fest [38]: "Alles Wissen stammt aus der Erfahrung." Der menschliche Verstand erlaubt das Ziehen von Schlussfolgerungen. In Abhïgigkeit neuer Situationen werden gemachte Erfahrungen aus bisherigen Situationen angewandt. Aufgrund der instinktiven Grundhandlung ist in der Tierwelt der Einfluss durch Erfahrungen weitaus weniger ausgeprägt und äußert sich nur durch eine Konditionierung (vgl. S. 197ff [Zim08]).

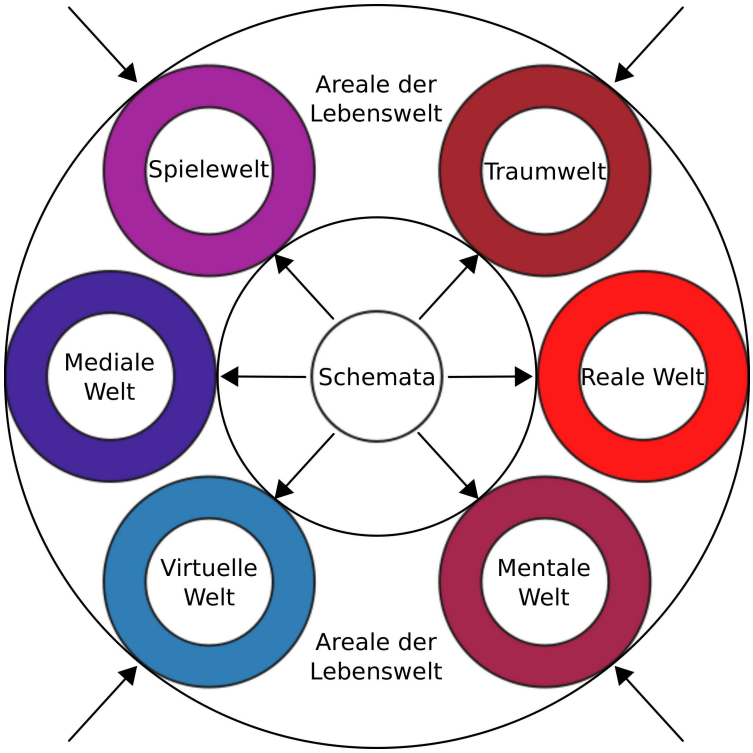

Abbildung 3.1: Netzwerk der Lebenswelt [Fri06, vgl. S. 5]

Abbildung 3.1 zeigt die weiteren Welten, die der Mensch in die reale Welt einbettet. Sie erweitern den Gesamtkomplex der Lebenswelt und verfügen über keine eigenen Grenzen, sondern bezeichnen Orte (S. 5 [Fri06]), "in denen spezifische Umgehensweisen mit den Reizeindrücken stattfinden." Fritz zitiert (vgl. S. 12 [Fri06]) weiters aus Schmidt drei Annahmen über die Wirkung der medialen Welt auf die Sichtweise des Menschen (vgl. S. 267ff [Sch94]):

- Bei Jugendlichen und Kindern führt die Mediennutzung dazu, dass die Unterscheidung zwischen Fiktion und Tatsachen schwieriger getroffen werden können.
- Bei Jugendlichen führt die Mediennutzung zu einem verzerrten Bild der realen Welt.
- Allgemein bewirkt die Mediennutzung, dass die Erfahrung der realen Welt vermindert wird.

Die individuelle Wahrnehmung der Wirklichkeit beeinflusst die Meinungsbildung durch das menschliche Individuum wesentlich. Der Einfluss der Medien in diesem Prozess wird durch Weber

untersucht (vgl. S. 1ff [Web02]). Die Publikation stellt im ersten Teil die Begriffe des Realismus und des Konstruktivismus gegenüber:

- "Der Realismus geht davon aus, dass es eher oder überhaupt nur die Wirklichkeit ist, die auf die Instanz ein-wirkt (und nicht umgekehrt); während
- der Konstruktivismus behauptet, dass es eher oder überhaupt nur die Instanz ist, die im Akt des Erkennens die Wirklichkeit erzeugt."

Da das Thema des digitalen Rechtemanagements (DRM) in zahlreichen Medien präsent ist, stellt der Einfluss durch diese einen nicht unwesentlichen Faktor dar. In den folgenden Überlegungen wird davon ausgegangen, dass die Meinungsbildung zur Thematik im Wesentlichen Meldungen aus den Medien entnommen wurden. Es liegt in der Natur des Menschen, sich eine Meinung zu bilden, selbst für eine Übernahme von vorgefertigen Gedankenmustern bemüht man als menschliches Wesen den Verstand: man kann "nicht nicht" konstruieren, da das im Laufe der Geschichte immer so geschehen ist. (S. 13 [Web02]) "In der Tat ist die Aussage 'Medien konstruieren immer mehr, häufiger oder öfter Wirklichkeit' eher mit dem Realismus vereinbar, da Konstruktion dann eher als bewusste Strategie verstanden wird." Die weite Verbreitung von Tauschbörsen und Internetplattformen zum Austausch digitaler Medien, sowie der Verbund von Informationsplattformen im Internet unterbreiten ihren Nutzern durch etwaige integrierte Mitteilungs- und Nachrichtendienste u. U. ein einseitiges Bild über die Thematik.

Wie folgt lässt sich festhalten (S. 12 [Web02]): "Dementsprechend liest sich die konstruktivistische Denkweise auch als Antipode des realistischen Begriffsfelds." Die Frage, die sich durch die Existenz der Medien auftut lautet der Publikation zufolge: "Bilden wir Wirklichkeit ab, oder bauen wir sie auf." An späterer Stelle wird an zuvor zitierter Stelle die Ansichten des radikalen Konstruktivismusses eingegangen. Diese lauten: "'Medien konstruieren Wirklichkeit' per se und immer schon, weil es eben gar nicht anders gehen kann, weil die Weltanschauung und das Wirklichkeitsverhältnis von Medien an sich konstruktiv sei." Kapitel 3.1.1 erläutert die Argumente, die gegen den radikalen und für einen gemäßigten Konstruktivismus sprechen.

Eine wesentlich plausiblere Variante ist der empirische Konstruktivismus. Sein Leitsatz lässt sich wie folgt zusammenfassen (S. 3 [Web02]): "'Medien konstruieren Wirklichkeit' kann aber auch ergänzt werden um: immer mehr oder immer weniger." In Zuge der Erklärungen wird die dualistische Redeweise eingeführt. Grundsätzlich wird dabei unterschieden zwischen:

- dem konstruktivistischen Anteil (Beobachter, Subjekt, Instanz, Erzeuger der Welt) und
- dem realistischen Anteil (Beobachtetes, Realismus, Wirklichkeit, Welt die auf die Instanz wirkt).

Die Wirklichkeit wird dann mit "Eher-Tendenzen" aus den beiden Anteilen (konstruktivistisch, realistisch) gebildet. So kann anhand der Makro-Trends der Medialisierung, wie etwa Entertainisierung, Fiktionalisierung, sowie z. B. Kommerzialisierung erkannt werden, dass der konstruktivistische Anteil einen konkreten Trend darstellt. Als Beispiele hierfür werden u.a. Kujaus Hitler-Tagebücher

und Michael Borns Spielfilm-Fakes, sowie die unter dem Begriff "Militainment" bekannte Unterhaltung genannt. Letzterer Begriff zeichnet sich Weber zu Folge durch live Kriegsberichterstattung in "Hollywood-Optik" aus (vgl. S. 4 [Web02]).

3.1.2 Konstruktivistische Didaktik

Wie im letzten Kapitel dargestellt ist der Konstruktivismus ein mit der Didaktik eng verknüpfter Begriff. Boudourides geht auf die Entwicklung des und den Zusammenhang mit dem Konstruktivismsus in der Didaktik ein (vgl. [25]).

Reich erläutert den Grundsatz der konstruktivistischen Didaktik wie folgend (S. 95 [Rei06]): "Jeder Sinn, den ich selbst für mich einsehe, jede Regel, die ich aus Einsicht selbst aufgestellt habe, treibt mich mehr an, überzeugbt mich stärker und motiviert mich höher, als von außen gesetzter Sinn, den ich nicht oder kaum durchschaue und der nur durch Autorität oder Nicht-Hinterfragen oder äußerlich bleibende Belohnungssysteme gesetzt ist." Außerdem wird an selber Stelle erläutert, dass sich die Konstruktion von Intentionen, sowie die Auswahl von Inhalten selbst dann, wenn sie bereits als Lehrplan fixiert und markiert wurden, neu zu konstruieren ist. Genügend Spielraum vorausgesetzt kann mit den Studierenden diskutiert werden, was die von anderen getroffene Zielsetzung für uns zu bedeuten hat.

Die Definition der konstruktivistischen Didaktik von Kersten Reich deckt sich mit den von Hsiao getroffenen Aussagen [36]: "In sum, the contemporary constructivist theory of learning acknowledges that individuals are active agents, they engage in their own knowledge construction by integrating new information into their schema, and by associating and representing it into a meaningful way. Constructivists argue that it is impractical for teachers to make all the current decisions and dump the information to students without involving students in the decision process and assessing students' abilities to construct knowledge. In other words, guided instruction is suggested that puts students at the center of learning process, and provides guidance and concrete teaching whenever necessary."

Bezogen auf die differierenden Ansichten des Einzelnen zur Thematik des Digitalen Rechtemanagements wird die Methodik der Wissenskonstruktion zur Bildung des eigenen Standpunkts der Studierenden angewandt. Aussagen über naturwissenschaftliche, technische, mathematische, usw. Tatsachen, sogenannte "hard facts", haben generell Gültigkeit, bis sie der Forschungsstand überholt. Im Kontrast dazu können bei interagierendes Systemen, sowie bei Beziehungsgeflechten Teilnehmer oder Akteure rein aus ihrer eigenen Positionen nur unklar darlegen, welche die beste bzw. letzte Beobachtung ist, die dauerhafte Gültigkeit hat (vgl. S. 74ff [Rei06]).

Die Thematik des Digital Rightsmanagements kann dahingehend als interagierenden System verstanden werden in dem sich mehrere Benutzergemeinden gegenüberstehen:

- Produzenten, Künstler, sowie alle anderen Urheber digitaler Inhalte,

- Distributoren, die die Vermarktung der digitalen Inhalte vornehmen,
- Hersteller von Abspiel- und Aufnahmegeräten und
- Konsumenten der digitalen Inhalte.

Die hier getroffene Auflistung spiegelt die in (vgl. S. 6 [30]) vorgestellte Wertschöpfungskette wieder. Zum Schutz digitaler Inhalte muss ein Digital Rights Management System (zur Begriffsdefinition siehe Kapitel 4.1.1) alle Akteure in diesen Kategorien berücksichtigen. Distributoren werden die Technologie möglichst restriktiv einsetzen wollen, um aus ihrem Medienangebot den erzielbaren Profit zu maximieren. Dem gegenüber steht die Gemeinschaft der Nutzer, die an einem möglichst ungehinderten Zugang zu digitalen Inhalten interessiert sind.

Als Vertreter der ersten, zweiten und dritten Kategorie in der oben angeführten Aufzählung versucht die Medienindustrie Konsumenten der digitalen Inhalte von der Notwendigkeit der Technologie zu überzeugen. Häufiges Argument ist die langfristige und faire Vergütung von allen an der Wertschöpfungskette Beteiligten. Fränkl erläutert, dass sich geschützte Inhalte im besten Fall wie ihre Pendants aus der analogen, physikalisch greifbaren Welt verhalten (vgl. S. 14 [Fra05]). Gegenargumente aus der Nutzerschaft sind wiederum, dass Entscheidungen seitens der Industrie ohne Einflussnahme getroffen werden.

Im Kapitel über die praktischen Zugänge zur konstruktivistischen Didaktik ("Learning by Doing" gemäß John Dewey) geht Reich auf drei wesentliche Perspektiven im Blick auf alle Lehr- und Lernprozesse ein (vgl. S. 138ff [Rei06]):

- Die Lehre sollte grundsätzlich so ausgerichtet sein, dass die Studierenden die Möglichkeit zur Selbsterfahrung, zum Ausprobieren, Untersuchen und Experimentieren haben. Ihr Grundmotto sollte daher "Wir sind die Erfinder unserer Wirklichkeit." sein. Dies wird unter dem Kriterium der "Konstruktion" zusammengefasst.
- Das Motto der Perspektive der "Rekonstruktion" lautet "Wir sind die Entdecker unserer Wirklichkeit.". Demzufolge wird immer mehr Zeit dafür aufgewendet, die Erfindungen anderer für uns nachzuentdecken. Außerdem führen Unübersichtlichkeit, Bedeutungslosigkeit, sowie Ohnmacht vor dem Wissen anderer dazu, dass die eigene Entdeckungs- und Erfindungsgabe vernachlässigt werden.
- Die Perspektive der Destruktion hängt unter dem Motto "Es könnte auch noch anders sein! Wir sind die Enttarner unserer Wirklichkeit!". Damit gemeint ist allerdings nicht zynisches Besserwissertum, sondern (S. 141 [Rei06]) "viel mehr um Auslassungen, die möglichen anderen Blickwinkel, die sich im Nachentdecken oder Erfindungen anderer oder in der Selbstgefälligkeit der eigenen Erfindung so gerne verstellen".

Neben den drei Perspektiven der Didaktik sollen Reich zu Folge Lehrende im Rahmen ihrer Tätigkeit auch drei Rollen einnehmen, um didaktische Prozesse zu reflektieren (vgl. S. 137 [Rei06]): Beobachter nehmen wahr, wie didaktische und andere Handlungen ablaufen, Teilnehmer sind in bestimmte Vorverständigungen eingebunden und als Akteure sind sie Handelnde im didaktischen Prozess.

Die Unterscheidung in diese Rollen kann den Gestaltungsraum erweitern. Außerdem können didaktische Prozesse intensiver auf Aspekte der Selbst- und Fremdbeobachtung und wechselseitige Interaktionen im Lernprozess untersucht werden.

Die Meinungsbildung zur Thematik wird hier de-, als auch konstruktiv gebracht. Aussagen über die technischen Teilgebiete werden von den Studierenden im Rahmen der Lehrveranstaltung rekonstruiert.

In den weiter unten angeführten didaktischen Methoden wird die Einbringung der eigenen Meinung berücksichtigt. Während des Praxisteils wird (siehe dazu Kapitel 5) bei der Themenwahl darauf geachtet, den Studierenden die Freiheit zu lassen, ihren Standpunkt wahrzunehmen und durch fundierte, konstruierte Argumente zu untermauern.

3.2 Didaktische Methoden

In diesem Kapitel werden die im Unterricht eingesetzten didaktischen Methoden erläutert und in den Kontext des Unterrichtsfaches gestellt. Der von Reich im Internet vorgestellte Methodenpool (vgl. [45]) dient als Grundlage zur Auswahl der eingesetzten didaktischen Konzepte.

3.2.1 Frontalvortrag

Unter Frontalunterricht versteht die Fachliteratur meist die klassische Präsentation mittels Folienkonzept (z. B. Beamer, Overhead-Projektor, etc.) oder Referate.

Die Methodik des Frontalunterrichts deckt sich nur bedingt mit den Prinzipien der konstruktivistischen Didaktik. Trotzdem will die konstruktivistische Didaktik frontale Phasen im Lernen und Lehren nicht abschaffen (vgl. [45]). Vielmehr will man bestimmte Handlungsphasen mit den frontalen Phasen kombinieren. Genannt werden in der zuvor referenzierten Ressource folgende:

- frontale Präsentation von Ergebnissen, Material, Medien in der Gruppe, das Vorbereiten,
- Einführung in Problemstellungen durch Referat, Präsentation, das Informieren,
- Präsentation von Zwischenergebnissen und Zusammenfassungen, das Durchführen,
- Vortrag, Präsentation vor dem Plenum, Referat, das Präsentieren und
- die Präsentation von erarbeiteten Ergebnissen vor dem Plenum oder vor anderen, das Evaluieren.

Glorian nennt konkret mehrere Schwächen der Methodik (vgl. [34]). Vielen Schülern wird sie nicht gerecht, da sie über- oder unterfordert. Außerdem ist sie für die Lehrenden anstrengend, wird schnell als langweilig empfunden und ist am gemessenen "Output" nicht effektiv. Viel Zeit geht auch für Disziplinierung verloren. Während dem letzten Argument in der Erwachsenenbildung weniger Bedeutung beigemessen werden kann als beim Unterrichten von schulpflichtigen Kindern, treffen die restlichen Argumente ungeachtet des Alters zu.

Frontalunterricht wird im Rahmen der Digital Rights Management Lehrveranstlatung überwiegend im Vorlesungsteil eingesetzt. Das Kapitel 4 geht auf die Gestaltung der Präsentationsunterlagen ein.

3.2.2 Fragend-entwickelnde Methode

Der Methodenpool definiert die Methode wie folgt [45]: "Die darstellend-entwickelnde Methode setzt sich aus Vortrag (Frontalunterricht) mit Zwischenfragen zusammen. Ein fragend-entwickelnder Unterricht baut hingegen auf Fragen der Lehrkraft auf, die möglichst von vielen Lernern beantwortet werden, um im Unterricht voranzukommen. Dabei sind die Ziele und Fragestellungen in die Hand der Lehrkraft gelegt."

In weiterer Folge wird im zuvor zitierten Methodenpool Kersten Reichs die Vorgangsweise der fragend-entwickelnden Inhaltsaufbereitung stark kritisiert. Vom Lehrenden wird vorausgesetzt, dass er sympathisch ist und die Studierenden seinem interessanten und anspruchsvollen Vortrag folgen können. In der Praxis ist das Bild dieses Meisterlehrers meist nicht anzutreffen. Außerdem wir die Schwierigkeit der gestellten Fragen dadurch, dass sie einerseits nicht so schwierig sein dürfen, dass das Durchhaltevermögen der Studierenden durch lange Frage- und Antwortspiele überstrapaziert und auf der anderen Seite die Antwort nicht suggestiv vorgeben oder bloß rhetorisch den Studierenden die Fragen letztlich selbst beantworten lassen.

Selbst ältere Publikationen weisen auf die Schwierigkeit der Methode hin (S. 13ff [Gau09] zitiert aus (S. 46 [Gau69])): "Die Frage des Lehrers ist das fragwürdigste Mittel. An eine Gesundung des deutschen Schulwesens vermag ich nicht eher zu glauben, ehe nicht der Despotismus der Frage gebrochen ist. Wenn man wenigstens anfinge, den Wert der Frage in Frage zu ziehen!". Der letztgenannten Publikation zu Folge liegen die Kritikpunkte Gaudig's in verkürzter Darstellung darin:

- Die Denkarbeit geht vom Lehrenden und nicht vom Studierenden aus.
- Bereits die Fragestellung alleine zwängt den Schüler in eine Denkrichtung und unterdrückt damit die geistige Entfaltung.
- Die Frage des Lehrers erstickt die Motivation der Studierenden[1] zu fragen, jugendlicher Intellekt kann auf diese Art nicht gefordert werden.
- Die Frageform wird in ihrem ursprünglichen Sinne vorwiegend dazu eingesetzt, damit der Fragende Dinge erfährt, die dieser nicht weiß; in diesem Fall will uns der Fragende etwas wissen lassen, was der Befragte (noch) nicht weiß.

Gaudig schlussfolgert die Gestaltung des Unterrichts mit Hilfe der fragend-entwickelnden Methode durch folgendes Zitat (S. 46 [Gau69]): "Sonach ist die Frage der ärgste Feind der Selbsttätigkeit." Hat sich der Studierende im Lernprozess gefügt, so wurde dieser durch die Methodik geführt, im Falle einer Widersetzung wurde der Studierende durch den Unterricht gezerrt.

[1] in der Publikation liegt der Schwerpunkt auf jugendlichen Lernern

3.2.3 Referate

Dem Methodenpool kann folgende Definition entnommen werden [45]: "Ein Referat (lat. von referre: berichten) ist ein Vortrag über ein Thema, der in einer begrenzten Zeit gehalten wird. Dabei geht es in schulischen und universitären Kontexten meist um die Wiedergabe von Tatsachen, Gedanken und Ideen, die zusammengefasst und einem Plenum vorgetragen werden." Die Wichtigkeit von Referaten im Unterricht an Hochschulen heben Bromme und Rambow durch drei Gründe (vgl. [26]) hervor:

- Lehrinhalte werden durch die Studierenden aktiv erarbeitet. Diese Erarbeitung kann bei der Gelegenheit der konstruktiven Kritik durch den Hochschullehrer und durch andere Studierende gestellt werden.
- Den anderen Studierenden wird Unterrichtsstoff dargeboten. Pädagogisch-psychologische Forschung zum allgemeinbildenden Schulunterricht hat ergeben, dass die Qualität des Unterrichts nicht nur durch Betrachtung der Beiträge des Lehrenden beurteilt werden kann.
- Das Halten von Referaten ermöglicht den Studierenden das Vortragen als zusätzliche Fähigkeit, die in vielen Berufen, für die an Hochschulen ausgebildet wird, erforderlich ist. Dieses Merkmal ist auch unter dem Namen der "Vortragskunst" bekannt.

Der Konstruktivistische Methodenpool von Reich (vgl. [45]) erläutert neben der grundlegenden Definition der Methode auch Hinweise zum Aufbau und zur Erstellung von Referaten. Ersteres lässt sich in drei Teilen beschreiben: Einleitung, Hauptteil und Schlussteil.

Die Einleitung macht die Audienz aufmerksam, motiviert sie zum Zuhören und lässt sie für das Thema interessieren. In der Ressource wird empfohlen zum Einstieg einen brisanten Anlass zu wählen. Weiters sollte das Thema abgegrenzt werden, und eine Gliederung gibt an, in welcher Reihenfolge die behandelten Punkte dargelegt werden.

Im Hauptteil werden Themen je nach Komplexität in mehrere, meist drei bis vier, Blöcke zusammengefasst. Beim Vortrag der Blöcke sollte darauf geachtet werden, dass diese deutlich getrennt von den Bewertungen zu bringen sind. In diesem Teil des Referats sollte sich den Ausführungen im Methodenpool zu Folge der Referent auf das Wichtigste konzentrieren. Zu viel Stoff ermüdet allerdings die Zuhörer. Deswegen ist es wichtig Orientierungshilfen zu bieten. Dies kann beispielsweise durch ein wiederkehrendes Einblenden der Gliederung erfolgen. Weiters können interessante Überschriften in diesem Zusammenhang je nach Plenum eine geeignete Hilfestellung bieten.

Den Schluss des Referats sollte eine Zusammenfassung bilden. Die Wichtigkeit der Kerngedanken kann in diesem Teil nocheinmal besonders betont werden. So ist die Beantwortung, mit der ein Referat beispielsweise begonnen wurde in diesem Teil richtig aufgehoben. Diskussionen können durch provokative Fragen des Referenten bewusst initiiert und gesteuert werden. Auch Fragen seitens des Plenums können hier aufgenommen werden.

3.2.4 Gruppenpuzzle

Das ZUM-Wiki beschreibt diese didaktische Methode wie folgt [51]: “Als Gruppenpuzzle bezeichnet man eine Methode des kooperativen Lernens. Dabei werden die Teilnehmer von gleich großen Arbeitsgruppen abwechselnd zu Stamm- und zu Expertengruppen zusammengesetzt. Die Analogie zum Puzzle besteht darin, dass eine Stammgruppe in ‘Puzzleteile’ ‘zerschnitten’ und dann die Puzzleteile zu einem neuen ‘Bild’, der Expertenrunde, und schließlich wieder zur Stammgruppe zusammengesetzt werden.” Abbildung 3.2 stellt diese Zusammenhänge graphisch dar.

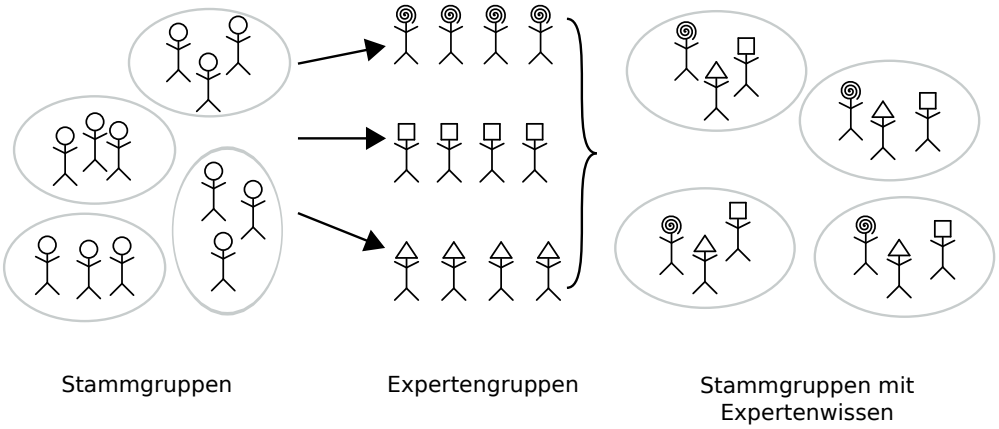

Abbildung 3.2: Bildliche Darstellung des Gruppenpuzzles (vgl. [51])

Der erwähnten Publikation zufolge soll Gruppenarbeit die Eigenständigkeit und Eigenverantwortung des Studierenden fördern. Oft aber läuft Arbeit in der Gruppe nicht so ab, dass die Präsentation der Gruppenergebnisse den Wissensstand der einzelnen Gruppenmitglieder widerspiegelt. Die sogenannten “Trittbretfahrer” können i.R. darauf vertrauen, dass der ihnen zugewiesene Teil der Arbeit zumindest auch zum Teil von den anderen Gruppenmitgliedern erledigt wird.

Als Lösungsvorschlag wird das Gruppenpuzzle angeführt. Es werden dabei generell zwei Gruppen unterschieden:

- Expertengruppen, die ein spezielles Thema erarbeiten. Mitglieder in diese Gruppe wurden aus den Stammgruppen entsandt.
- Stammgruppen, die das in den Expertengruppen erarbeitete Wissen zu einem Gesamtbild zusammensetzen.

Jedem Teilnehmer kommt bei dieser Methode die Rolle des Experten und des Wissensvermittlers zu. In der Beschreibung des Gruppenpuzzles in (vgl. [29]) werden weitere Anweisungen zur Dimensionierung der Gruppengröße, sowie zur Stoffaufteilung angegeben:

- Die Gruppenanzahl richtet sich nach der Anzahl der zu behandelnden Stoffbereiche.
- Am Ende der Expertenrunde wird ermittelt, ob sich die Teilnehmer ausreichend mit den ihnen zugewiesenen Themenbereichen auskennen.

- Der Zeitraum für die individuelle Recherche durch die Experten variieren je nach Stoffumfang und können auch so organisiert sein, dass sie 30 bis 60 Minuten nicht überschreiten.

Anwendung findet das Gruppenpuzzle in Martin Lehners Publikation mit Beispielen zu guter Lehre an Fachhochschulen (vgl. S. 49ff [Mar08]). Das Gruppenpuzzle wird hier anhand einer integrierten Lehrveranstaltung (Kombination aus Vorlesung und Übung) erläutert. Besonderheit an der hier präsentierten Variante ist der Durchführung der Leistungsbeurteilung durch die Studierenden selbst. Jede Stammgruppe ist einmal im Semester mit der Erstellung, der Beaufsichtigung, der Korrektur und der Beurteilung einer Leistungsüberprüfung beauftragt. Die Leistung der Stammgruppe wird anhand folgender Kriterien beurteilt:

- der Abdeckung des Stoffgebiets, einer adäquaten Wahl des Schwierigkeitsgrades, die Qualität der Angabe,
- die Durchführbarkeit der Absolvierung der Leistungsbeurteilung in 15 bis 20 Minuten, der Umgang mit dem Zeitbudget,
- der Qualität der Korrektur und
- das Aufstellen eines Gesamtpunktebudgets, welches nur nach Absprache mit den Lehrbeauftragten überschritten werden darf, der Fairness der Beurteilung.

Im Jigsaw Classroom (vgl. [22]) wird die Methode des Gruppenpuzzles positiv dargestellt, da mit ihr rassische Konflikte vermieden werden können.

Die im Kapitel 3.2.3 beschriebene Methode der Referate wird als zu erarbeitende Leistung des Gruppenpuzzles eingesetzt. Zur Leistungsüberprüfung werden die erarbeiteten Inhalte im Klassenrahmen den Kollegen präsentiert und im Anschluss sowohl von diesen, als auch vom Lehrpersonal evaluiert.

3.2.5 Mindmapping

Im Methodenblatt zum Mindmapping wird erläutert, dass diese Methode von Tony Buzan entwickelt wurde, um Aufzeichnungen und Notizen zu machen und um gezielt nachzudenken, zu planen oder Ideen zu finden (vgl. [44]). Weiters lassen sich aus Mindmaps sehr gut Gliederungen für längere Arbeiten entwickeln. Die Grundregeln der Mind-Map-Technik sind daher:

- Der zu beschreibende Begriff wird in der Mitte des Blattes platziert. Vor allem Bilder prägen sich gut ein und regen kreatives Denken an.
- Bilder können auch in den weiteren Verzweigungen zum Einsatz kommen.
- Wörter sollten in Großbuchstaben geschrieben werden. Druckschrift gibt zur Nachlese ein fotografischeres, unmittelbareres und verständlicheres Bild.
- Wörter sollen auf den Linien geschrieben und Linien mit anderen Linien verbunden werden.
- Wörter sollen weiters in Einheiten angeordnet sein, ein Wort je Linie.

- Der Einsatz von Farben erhöht die Übersichtlichkeit und lasst die Zusammenhänge deutlicher erkennen.
- Alles, was im Zusammenhang mit der Zentralidee steht sollte unmittelbar, spontan in der Mindmap festgehalten werden.

3.2.6 E-Learning

Gusenstätter definiert den Begriff des E-Learnings wie folgt (S. 11 [35]): "E-Learning findet statt, wenn Lernprozesse in Szenarien ablaufen, in denen gezielt multimediale und (tele-) kommunikative Technologien integriert sind."

Im ITB-Forschungsbericht zu eLearning (vgl. S. 4ff [Fis03]) wird der Rahmen beschrieben, der E-Learning ausmacht. Der materielle Ausgangspunkt ist demnach ein mikroprozessorgesteuertes Gerät, mit dem der Lernprozess mittels Aktion und Reaktion vollzogen wird. Durch die Interaktion ist sowohl eine Individualisierung, als auch eine Kollektivierung von Lernprozessen möglich. Steuerung der Lerngeschwindigkeit, des Lernweges, der Lehrinhalte und Lehrergebnisse durch den Studierenden sind Auszeichnungen der Individualisierung. Die Kollektivierung von Lernprozessen beinhaltet, dass die Ergebnisse und die Wege unter den Studierenden selbst wahrgenommen und reflektiert werden. Die Medienauswahl und die Richtlinien generell für Distancelearning werden durch den "Media Selection Guide" (vgl. [Jol06]) beschrieben. Demnach wird bei der Einteilung der Lernumgebungen zwischen zwei großen Gruppen unterschieden:

- Synchrone Lernumgebungen die auch als "Live-Systeme" bekannt sind. Zwischen Lehrer und Studierenden findet eine zwei-wege Kommunikation statt. Diese Umgebung ördert ein dialektisches Lernumfeld mit hoher Interaktivität. Neben der vorherseh- und kontrollierbaren Sitzungszeit spielt der Lernort eine untergeordnete Rolle. Drei wesentliche Systeme kommen zum Einsatz:
  - Audio-Systeme,
  - Interaktive-Keypad-Systeme,
  - Videokonferenz-Systeme.
- Asynchrone Lernumgebungen, bei denen die Kommunikation zwischen Lehrer und Studierenden nicht in Echtzeit[2] stattfindet. Typische Beispiel für solche Umgebungen sind textbasierte Materialien, sowie Diskussionsplattformen, die genutzt werden können, um auf Fragen vom Lehrpersonal oder von anderen Studierenden zu antworten. Dies regt i. R. mehr zum Überdenken vor der Bekanntgabe der eigenen Meinung an. Das Umfeld ist weder durch Zeit, noch durch den Ort abhängig.

E-Learning geht aus Sicht des Studierenden mit einer größeren Flexibilität und Variabilität von Lernzeiten und Lernorten einher. So muss man nicht am Ort des Lerngeschehens sein und die Unterrichtsmaterialien sind zu jedem Zeitpunkt und über größere Zeitdauer verfügbar. Das ermöglicht

[2] Abläufe, die in "Echtzeit" passieren sind unmittelbar oder innerhalb einer vorgegebenen Zeitspanne abgeschlossen; im Englischen unter "real-time" bekannt (vgl. S. 66 [Roe05])

sonst ausgeschlossenen Personenkreisen, wie z. B. Alleinerziehenden, Schichtarbeitenden, Kranken, usw. am Unterricht teilzuhaben. Die Nachteile liegen darin, dass die berufliche und die private Sphäre zunehmends verschmelzen.

Fischer et al. erwähnt (vgl. S. 14 [Fis03]), dass das Berufsbildungspersonal in seiner überwiegenden Mehrheit von E-Learning nicht begeistert ist. Das ist auf die hohen zusätzlich notwendigen Anforderungen bei der Entwicklung und Anwendung von E-Learning Systemen zurückzuführen.

Im Rahmen der hier dokumentierten Lehrveranstaltung wird die E-Learning Plattform "moodle" (vgl. [9]) zum Einsatz kommen. Die zum Betrieb notwendige Infrastruktur wird seitens der Bildungseinrichtung zur Verfügung gestellt. Diese Lernumgebung lässt sich nach der oben erfolgten Defnition in die Gruppe der asynchronen Lernumgebungen eingliedern. Den Kursteilnehmern werden im wesentlichen neben den Vortragsfolien und weiterführenden Links die Möglichkeit zum Austausch über ein Forum zur Lehrveranstaltung geboten.

3.3 Leistungsbeurteilung

Rheinberg definiert den Begriff der konventionellen Leistungsbeurteilung im Schulalltag (vgl. S. 1ff [Rhe01]). Hierzu wird in zwei Teilbegriffe untergliedert:

- Leistungsmessung macht die Aussage, dass nur ein Ergebnis, das qualitativ (beispielsweise die Aussprache von gelernten Vokabeln) und/oder quantitativ (beispielsweise die Menge der gewussten Vokabeln) erfasst werden kann.
- Leistungsbeurteilung hingegen beschreibt, dass ein Ergebnis nur dann aussagekräftig ist, wenn es mit einem Maßstab verglichen werden kann.

Die Beurteilung der Studierenden erfolgt bei dieser Lehrveranstaltung durch zwei Leistungsnachweise:

- Beim Vorlesungsteil erfolgt die Leistungsmessung sowohl quantitativ, als auch qualitativ. Bei einer mehrteiligen Prüfung über die im Unterricht durchgenommenen Themengebiete wird der momentane Kenntnisstand der Studierenden ermittelt. Die Anzahl der beantworteten Fragen machen eine quantitative und die Detailliertheit der gegebenen Antworten eine qualitative Aussage über die von den Studierenden erbrachte Leistung.
- Beim Übungsteil erfolgt die Durchführung des unter 3.2.4 vorgestellten Gruppenpuzzles. Pro Studierendem und Durchgang wird dabei ein Dokument im Umfang von ca. 4 A4-Seiten ausgearbeitet und in Form einer Präsentation vor den anderen Studierenden vorgetragen. Die Leistungsmessung erfolgt in diesem Falle daher rein qualitativ.

Die Leistungsbeurteilung in Form einer Gesamtnote ergibt sich dann durch eine arithmetische Mittelung. Sowohl der Übungsteil, als auch der Vorlesungsteil werden je mit 50% gewichtet. Beim

Übungsteil machen bei einer Gleichgewichtung die einzelnen Ausarbeitungen und Präsentationen jeweils 25% von der Gesamtnote aus.

Kapitel 4

Vorlesungsteil der Lehrveranstaltung

Folgendes Kapitel beschreibt die zu lehrenden Theoriegebiete der digitalen Rechteverwaltung. Im Studiumsleitfaden für den Studiengang IT Security an der Fachhochschule St. Pölten wird als mögliches berufliches Einsatzszenario der Absolventen die Tätigkeit als ExpertIn für Digital Rights Management genannt. Da die Lehrveranstaltung einen Rahmen von zwei Semesterwochenstunden umfasst kann diese jedoch nur als eine Einführung in die Thematik verstanden werden.

Bei der hier vorliegenden Ausarbeitung liegt der Schwerpunkt auf einem möglichst breit gefächerten Überblick im Gegensatz zu einer detaillierten Behandlung eines Einzelthemas.

4.1 Block 1: Grundlagen des Digital Rights Managements

Im ersten Block des Vorlesungsteiles wird auf die Terminologie, sowie auf den grundsätzlichen Aufbau von Digital Rights Management Systeme eingegangen. Das hierbei vermittelte Wissen ermöglicht den Studierenden die richtige Wortwahl bei Abhandlungen, wie z. B. Diskussionen, zur Thematik.

Picot definiert den Begriff auf folgende Weise (S. 3 [Pic05]): "Digital Rights Management (DRM) zielt darauf ab, für digitalisierbare Inhaltsprodukte die Voraussetzungen zu schaffen, damit auch in der digitalen Welt die Rechte, die jemand mit solchen Produkten geltend machen kann, definiert und durchgesetzt werden können."

An dieser Stelle wird im Unterricht Zeit für eine Diskussion eingeräumt, da möglicherweise Teilnehmer der Lehrveranstaltung bereits Erfahrungen mit der Thematik des Digital Rights Managements (DRM) machen konnten. Dadurch soll erreicht werden, dass Kompetenzen mit der Thematik nicht nur erkannt, sondern auch an die anderen Studenten weitergegeben werden können.

Einher geht diese Diskussion mit der Berücksichtigung der Kritik an der Frage-entwickelnden Methode. Die Antwort der Frage kann nicht als ultimativ verstanden werden. Genauso wenig soll die Fragestellung den Studierenden durch den Unterricht führen oder gar zerren. Ziel dieser Vorgangsweise ist, den Studierenden möglichst viele Sichtweisen darzulegen und diese im Kreise der anderen Studenten im Jahrgang zu vertreten bzw. im Kritikfalle durch Argumente zu untermauern oder diese zu ändern.

Um die Motivation der Industrie zur Entwicklung von DRM-Konzepten zu verstehen, werden Statistiken der Business Software Alliance (BSA), sowie von der International Data Corporation (IDA) gezeigt. Der Studie zufolge liegt die weltweite Piraterierate bei Software im Jahr 2007 bei 38% (vgl. S. 2 [20]). Die Rate im Asien-Pazifischen Raum ist relativ niedrig, da in diese Region auch Länder, wie Japan, Australien und Neuseeland, also Länder mit einer sehr niedrigen Rate, fallen. Am Endverbrauchermarkt ist die Rate in der Regel höher als in Firmen. Unter den Firmen entscheidet im Wesentlichen die Firmengröße über die Rate: größere Firmen setzen demnach eher legal erworbene Software als Klein- und Mittelbetriebe ein (vgl. S. 4 [20]).

Der Verlust in den am Bruttoinlandsprodukt (BIP) gemessenen wohlhabenderenden Ländern größer, da hier der Markt am größten ist. Indiens lokaler Softwaremarkt ist mit dem eines Entwicklungslandes vergleichbar, da Software zu einem Großteil exportiert wird. In einigen Staaten der ehemaligen Sowiet-Union fördern staatliche, sowie Programme der Hersteller die Akzeptanz von Software als geistiges Eigentum (vgl. S. 6 [20]).

Zwei Faktoren beeinflussen die Softwarepiraterierate wesentlich (vgl. S. 8 [20]):

- Internetanschlüsse treiben die Rate in die Höhe, da die Verteilung von Software vereinfacht wird.
- Die Globalisierung hingegen senkt die Rate, da große Konzerne, die vorwiegend lizenzierte Software einsetzen, mit der Zeit multinationaler tätig werden und so auch in weniger entwickelten Ländern den Anteil an legaler Software erhöhen.

Die in Abbildung 4.1 gezeigte Methode zur Berechnung der illegal kopierten Softwareinheiten gestaltet sich wie folgt: die Anzahl an installierten Softwareinheiten ergibt sich aus der Multiplikation von verkauften Hardwareinheiten mit den installierten Softwareeinheiten pro Hardwareeinheit. Die Anzahl der verkauften Softwareeinheiten ergibt sich aus der Division von den Gesamteinnahmen durch Verkäufe von Software und dem Durchschnittspreis für eine Softwarelizenz. Um die Softwarepiraterierate zu bestimmen wird die Anzahl der installierten Softwareeinheiten mit der Differenz aus installierten Softwareeinhaiten mit den verkauften Softwareeinheiten ins Verhältnis gesetzt (vgl. S. 14 [20]). In Abbildung 4.1 wird die Folie mit dem Blockschaltbild dargestellt, nach dem die Berechnung der unzulässig kopierten Softwareeinheiten erfolgt.

Das Kopieren analoger Medien ist zeitaufwändig, teuer und mit einem Qualitätsverlust behaftet. Man spricht in diesem Zusammenhang auch vom Generationsverlust (vgl. S. 14 [Fra05]). Mit der Entwicklung der Digitaltechnik gingen leistungsfähige, an das Anwendungsgebiet angepasste, Kompressionsalgorithmen hervor. Breitband-Internetanschlüsse, billige Massendatenträger, einfach zu bedienende Software zum Tauschen digitaler Medien, sowie das verlustlose Kopieren digitaler Daten begünstigen die illegale Distribution urheberrechtlich geschützter Inhalte (vgl. S. 16 [Fra05]).

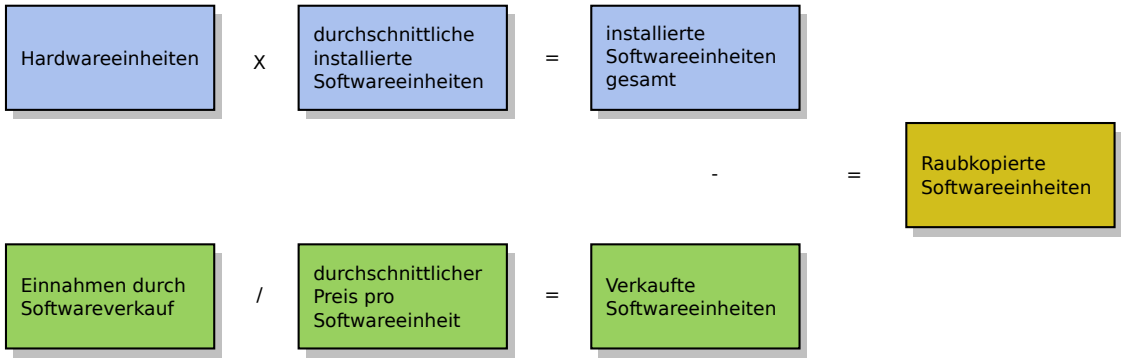

Abbildung 4.1: Folie zur Verdeutlichung der Berechnung [20, vgl. S. 12]

Hauptsächlich betroffen sind die Bereiche

- Audio,
- Video,
- Print,
- Software.

Die Verteilung digitaler Medien kann auf unterschiedlichen Wegen erfolgen. Neben der zuvor angesprochenen Verteilung mittels Massendatenträgern oder über Breitbandinternetanschlüsse besteht auch die Möglichkeit zur Superdistribution. Das aus Japan stammende Modell sieht vor, dass das Kopieren der Software auf legalem Weg möglich und sogar erwünscht ist. Die Verteilung erfolgt damit nur in der Anfangsphase auf Kosten des Distributors. Die Verwendung der Software ist jedoch immer noch an den Erwerb einer Lizenz gebunden (vgl. S. 57ff [30]).

Der kommerzielle Vertrieb digitialer Inhalte kann durch bestimmte Maßnahmen verbessern. Diese Maßnahmen werden an dieser Stelle in drei Kategorien eingeteilt (vgl. [Pil86]):

Der rechtliche Schutz lässt sich in die folgenden Teilbereiche einteilen (vgl. S. [jSB02]):

- Durch das Urheberrecht soll dem Urheber eines Werkes der Lohn für seine Arbeit garantiert werden. Probleme ergeben sich beim Urheberrecht noch im Detail (vgl. S. 148 [jSB02]). So ist beispielsweise nicht klar, wie die rechtliche Situation im Falle von Kopien der digitalen Inhalte im Arbeitsspeicher[1] eines Computers zur Laufzeit von Programmen aussieht (vgl. S. 151 [jSB02]).
- Durch Zustimmen des Medien-Nutzers zu sogenannten Nutzungsverträgen bindet sich dieser an die Vorgaben des Medieninhabers (z. B. Durchsetzung von rechtlichen Bestimmungen zur Abspielhäufigkeit). Durch die Distribution digitaler Medien über das Internet ergeben sich dadurch Massenverträge (vgl. S. 154 [jSB02]).
- Einen weiteren Schutz bieten Technologie-Lizenzverträge (S. 178 [jSB02]): “Viele technische Komponenten von DRM-Systemen sind durch Patente geschützt. Daneben hüten DRM-Entwickler zahlreiche Komponenten als Geschäftsgeheimnis. So werden bei Verschlüsselungssys-

[1] auch als RAM bekannt

temen die verwendeten Schlüssel nicht veröffentlicht, sondern als Geschäftsgeheimnis geheim gehalten, da ansonsten das Verschlüsselungssystem nicht mehr sicher wäre."

- Außerdem sind technische DRM-Komponenten geschützt (S. 196 [jSB02]): "In den letzten Jahren haben auch die Gesetzgeber auf nationaler wie in- ternationaler Ebene erkannt, daß technische Schutzmechanismen zum Schutz von Urhebern und Leistungsschutzberechtigten immer wichtiger werden. Daher finden sich zunehmend gesetzliche Regelungen, durch die technische DRM-Komponenten spezifisch reguliert werden. Am bedeutendsten sind dabei Vorschriften, die die Umgehung technischer Schutzmaßnahmen verbieten (Schutz durch Umgehungsvorschriften). Daneben finden sich Vorschriften, die in bestimmten Fällen die Verwendung von DRM-Komponenten gesetzlich vorschreiben (Obligatorischer Einsatz von DRM-Komponenten)."

Weiters Maßnahmen, die sich in Form von Zusatzangeboten für den Konsumenten digitaler Medien präsentieren fallen in die Kategorie des organisatorischen Schutzes. Beispiele hierfür sind:

- gute Dokumentation für registrierte Kunden,
- Zusendung von Unterlagen,
- Anpassung der Software an spezielle Kundenwünsche und
- eine individuelle Preispolitik.

Schließlich gibt es technische Elemente zum Schutz digitaler Medien (vgl. S. 23ff [jSB02]). Dem zu Folge sind dies folgende Hilfsmittel:

- (S. 23 [jSB02]) "Mit Verschlüsselungstechniken können digitale Inhalte derart modifiziert werden, daß sie nur für Nutzer brauchbar sind, die über einen entsprechenden Schlüssel zum Entschlüsseln des digitalen Inhalts verfügen. Selbst wenn ein Nutzer den verschlüsselten Inhalt kopieren kann, ist dieser für ihn ohne einen entsprechenden Schlüssel nutzlos."
- (S. 75 [jSB02]) "DRM-Systeme wollen ein umfassendes Sicherheitskonzept für den Vertrieb digitaler Inhalte bieten. Dabei muß sichergestellt sein, daß die in einem DRM-System übertragenen Inhalte nicht von einem Angreifer verändert werden können. Dies ist als Schutz der Integrität bekannt."
- (S. 75 [jSB02]) "Auch muß sichergestellt sein, daß die Inhalte tatsächlich von derjenigen Instanz stammen, die sich als Absender der Inhalte ausgibt." Dies bietet der Schutz durch Authentizität.

Fränkl geht auf mögliche Kritikpunkte des DRMs ein (vgl. S. 39 [Fra05]). Der Autor des Buches plädiert dabei, dass das "R" in der Abkürzung nicht seinem Anspruch der "restriction" gerecht werden solle. Beispielhaft wurden kopiergeschützte CDs erwähnt. Die Kopierschutzmechanismen greifen in diesem Fall oft so schlecht, dass selbst Originaldatenträger nicht mehr in den Wiedergabegeräten abgespielt werden können. Weiters wird noch auf die Umsetzung von "Trusted Computing" Mechanismen durch die "Wintel-Allianz" hingewiesen. Diese sollen den Benutzer in die Lage bringen, nur noch "guten" Programmcode auf den PCs ausführen zu lassen. In diesem Falle wird zwar der Virenschutz erhöht, Nebeneffekt dieses Schutzes kann aber durchaus eine sehr Starke Kontrolle von Inhalten am jeweiligen PC sein.

Als Beispiel für die Umsetzung eines DRM-Systems wird das Produkt “Fairplay” der Firma “Apple” herangezogen. Im Falle dieses Systems werden die Schlüssel zur Dechiffrierung der digitalisierten Musikstücke auf der Hardware des Endnutzers selbst gespeichert. Diverse Projekte, die sich mit der Umgehung dieses Kopierschutzes beschäftigen, knacken das zur Speicherung genutzte, lokale Key-Repository, um die geschützten Musikstücke zu entschlüsseln und anschließend ungehindert zu verbreiten (vgl. S. 46 [30]).

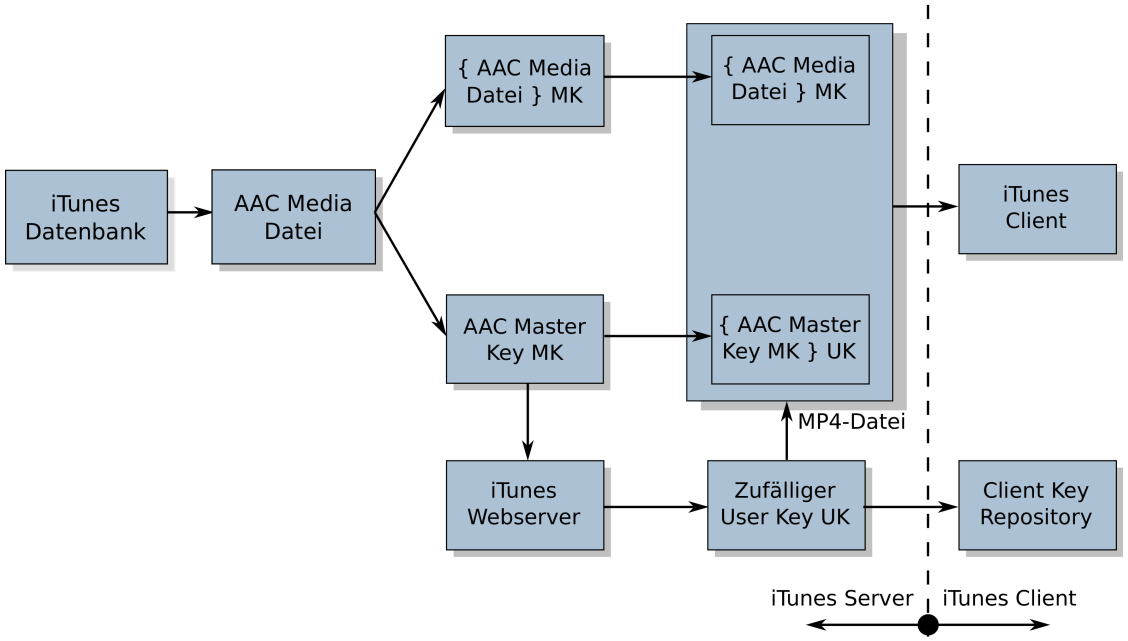

Abbildung 4.2: Schema von Apple’s Fairplay (vgl. S. 45 [30])

Das Schema von Apple’s Fairplay wird präsentiert. Vor der Nutzung des Systems wird eine eindeutige Systemkennung, der “System Key” generiert. Dieser wird bei der Verbindungsaufnahme mit dem iTunes-Store übermittelt und zur Generierung des “User Keys” herangezogen. Weiters wird erwähnt, dass die Verschlüsselung der Musikstücke zweistufig erfolgt. Zuerst werden Musikstücke symmetrisch mit dem sogenannten “Master Key” chiffriert. Der zum Dechiffrieren benötigte Schlüssel befindet sich auch in der MPEG-4 Datei. Der als “Atom” bezeichnete Speicherbereich zur Speicherung des “Master Keys” wird mit dem “User Key” verschlüsselt. Die durch den “System Key” gesicherte Datenbank der “User Keys” kann nicht ohne Weiteres von einem System auf ein anderes übertragen werden, da sich ersterer Verschlüsselungsparameter von System zu System unterscheidet. Die Herleitung basiert auf eindeutigen Systemparametern, wie z. B. der CPU-ID und der BIOS-ID. Auf mobilen Endgeräten, wie z. B. dem iPod wird der “System Key” von der “Hardware ID” abgeleitet.

Nachdem die Komponenten im Zusammenspiel, sowie die Parameter für die Verschlüsselungsstufen erklärt wurden, werden die Studierenden vor die Aufgabe gestellt aufzuzeigen, worin die Schwachpunkte des Systems liegen.

Als Ausweg aus dem Dilemma der Entwicklung und der Umgehung von Schutzmaßnahmen wurde bereits öfter die Einführung einer Pauschalvergütung erdacht. Auf diese wird auch unter dem

Begriff der "Kulturflatrate" referenziert. In Form einer Diskussion werden die Für und Wider der Pauschalvergütung erarbeitet.

Fränkl erwähnt in diesem Zusammenhang, dass durch die Pauschalvergütung auch jene Personen bezahlen müssen, die gar keine digitalen Medien in Anspruch nehmen (vgl. S. 81ff [Fra05]). Beispielhaft sei hier die Nutzung eines CD-Brenners zur ausschließlichen Nutzung als Sicherungsgerät erwähnt. Im Zeitalter der durch den Generationsverlust behafteten Geräte war die Pauschalvergütung ein adequater Weg, um die Verluste durch Kopien auszugleichen.

Secure Digital Media Initiative

Das Digital Media Manifesto (DMM), das unter der Leitung von Leonardo Chiariglione im Jahre 2003 entstand, ging aus der Secure Digital Media Initiative (SDMI) hervor. Die SDMI hatte, wie das DMM, das Finden eines Konsens für DRM zum Ziel. Das SDMI-Projekt wurde im Jahre 2001 auf Eis gelegt (vgl. S. 10 [30]).

Der Geschäftsführer der SDMI, Leonardo Chiariglione, kommentierte das Ende der Initiative mit folgenden Worten [40]: "Unfortunately it turned out that none of the technologies submitted could satisfy the requirements set out at the beginning, e.g. of being unnoticeable by so-called 'golden ears'. SDMI has then decided to suspend its work and wait for progress in technology."

Die im Rahme des Projekts entwickelten Technologien waren demnach nicht den Anforderungen gewachsen. Edward W. Felten präsentierte auf dem zehnten USENIX Security Symposium unter heftigem Protest seitens der SDMI Wege, um die Kopierschutzmechanismen zu umgehen (vgl. [33]).

4.1.1 Digital Rights Management Systeme

Die in diesem Kapitel dargelegten Inhalte über die Digital Rights Management Systeme werden auf den Vorlesungsfolien sowohl in Auflistungsform, als auch in Form von Mindmaps präsentiert, um den Studierenden mehrere Möglichkeiten zur Internalisierung zu geben.

DRMS (Digital Rights Management Systeme) haben als oberstes Ziel die unkontrollierte Weitergabe von Inhalten zu unterbinden. Als Kombination aus Soft- und Hardware verfolgen DRMS daher im engen Sinn eine vollständige Kontrolle über Verbreitung und Nutzung von Content (vgl. S. 15 [Pic05]). Weiters verfügen einige DRMS noch über Funktionen zur Unterstützung von Abrechnungen (vgl. S. 18 [Pic05]).

Fränkl definiert den Begriff der Digital Rights Management Systeme (DRMS) wie folgt (S. 21 [Fra05]): "Digital Rights Management Systeme (DRMS) sind technische Lösungen zur sicheren

zugangs- und nutzungskontrollierten Distribution, Abrechnung und Verwaltung von digitalem und physischem Content."

An dieser Stelle wird im Unterricht die Thematik der DRMS durch eine Mindmap dargestellt. Kapitel 3.2.5 geht auf die wesentlichen Kriterien des Mindmappings ein. Als Werkzeug zur Unterstützung des Lernprozesses bei visuellen Lerntypen wird im Frontalvortrag diesem Umstand Rechnung getragen. Abbildung 4.3 zeigt die Folie mit der Übersichts-Mindmap. Exemplarisch wird in Abbildung 4.4 gezeigt, wie Details dargestellt werden. Um den Bezug zum Gesamtthema, hier konkret die DRM Systeme, zu erhalten, wird auch dieses in Form eines Zweiges dargestellt.

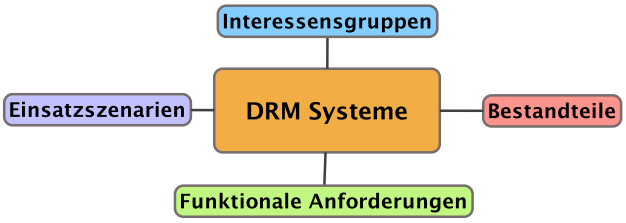

Abbildung 4.3: Mindmap zur Thematik "Digital Rights Management Systems"

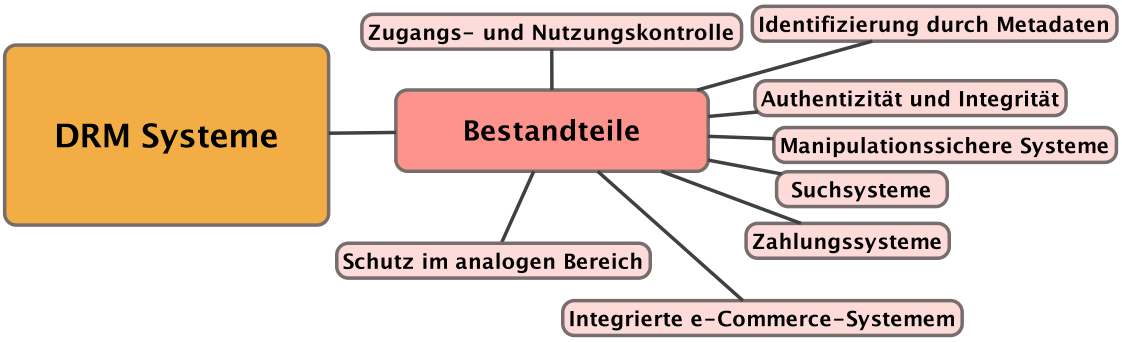

Abbildung 4.4: Mindmap zur Thematik "Digital Rights Management Systems"

Wesentliches Element der in Abbilung 4.3 gezeigten Folie sind die 4 Unterpunkte zur Beschreibung von Digital Rights Managemen Systemen: Interessensgruppen, Funktionale Anforderungen, Einsatzszenarien und Bestandteile. Informationen zu den ersten drei Punkten wurden dem Tagungsband der TU München entnommen (vgl. S. 6-7 [30]), die Bestandteile werden in (vgl. S. 23ff [jSB02]) abgehandelt.

Einsatzgebiete

Die Einsatzgebiete von Digital Rights Management (DRM) werden in Fachliteratur häufig auch als die "logischen Funktionen" klassifiziert. Im Kontext des Rechteschutzes für DRMS bedeutet dies (vgl. S. 16-17 [Pic05]):

- Durch Nutzungskontrolle erhalten ausschließliche Berechtigte Zugang zum geschützten Content. Die Randbedingungen können nach Termin (Zeitpunkt, Periode), Nutzungshäufigkeit,

Ort der Nutzung, spezielle Endgeräte, sowie die erlaubte Art der Weiterverarbeitung gegeben sein.

- Durch Abrechnung sollen alle Arten von Erlösformen unterstützt werden. Das Einbinden von neuen Geschäftsideen muss flexibel möglich sein, Beispielhaft wird im Zusammenhang das Öffnen eines digitalen Dokuments erläutert. So wird hierbei ein bestimmter Betrag abgerechnet. Bei pauschalvergüteten Dokumenten wird das Vorhandensein eines Abos geprüft.
- Die Detektion und Verfolgung von Rechteverletzungen, da im Falle einer Rechteverletzung sowohl Authentizität (Zurechenbarkeit der Informationen zu deren Urheber), als auch die Integrität (Wahren eines definierten Zustands der digitalen Daten) gewährleistet sein müssen, um eine Strafverfolgung zu unterstützen

Interessensgruppen

Die von DRM betroffenen Interessensgruppen lassen sich (vgl. S. 7 [30]) zu Folge in die zwei Gruppen der Marktteilnehmer und der Konsumenten gliedern. Erstere Gruppe umfasst einerseits die Autoren, Künstler, die die schützenswerten Inhalte erzeugen. Die Bündelung erfolgt meist durch Medienunternehmen, die auch diesem Zweig der Interessensgruppen angehören. Weiteres gehören dieser Gruppe die Systemanbieter an, die ihren Kunden aus einer breiten Palette von Funktionen ein maßgeschneidertes DRMS aus einem Guss bieten. Letztere, die Gruppe der Kunden und Konsumenten umfasst private Endnutzer. die DRMS, um geschützte Inhalte abzuspielen. Ein wesentliches Merkmal liegt hier in einer einefachen Bedienung des Systems. Gewerbliche Endnutzer unterscheiden sich von den privaten Endnutzern durch die gezielte Weiterverarbeitung der erworbenen Inhalte (z. B. Bilddatenbanken für Redaktionssysteme).

Anforderungen an Digital Rights Management Systeme

Damit Digital Rights Management Systeme von ihren Nutzern akzeptiert werden, stellen die Rechtebesizter folgende Anforderungen:

- Betrachtung der gesamten Wertschöpfungskette; von der Generierung der Inhalte über die Distribution zum Kunden bis hin zum Austausch zwischen den Kunden.
- Betrachtung der Bedienbarkeit der Endnutzerschnittstelle. Akzeptanz durch die Endnutzer setzt voraus, dass DRMS einfach zu bedienen sind.
- Die Standardisierung sichert, dass DRMS möglichst unabhängig von eingesetzter Plattform, Geräten, usw. eingesetzt werden können.
- Die Verarbeitung von Medien unabhängig vom Medientyp und Content-Format (Audio, Video, Texte, Bilder) soll mit ein und demselben DRMS möglich sein.
- Durch die Sicherheitsstufe oder, anders ausgedrückt, der Anpassung des Schutzes an den jeweiligen Anwendungszweck unter dem Gesichtspunkt der Wirtschaftlichkeit (z. B. Contentwertigkeit $\Leftrightarrow$ Transaktionskosten).

Bestandteile von Digital Rights Management Systemen

Die Bestandteile von Digital Rights Management System werden durch (vgl. S. 23ff [jSB02]) aufgezählt. Auf die als Bestandteil zählende Thematik der Identifizierung durch Metadaten wird in Kapitel 4.2.2 eingegangen.

Restriktionen im Zugang und zur Nutzung von digitalen Inhalten beschäftigen sich im Wesentlichen damit, deren Verwendbarkeit an Vorgänge, wie z. B. den Einsatz von zusätzlichen Geräten, zu binden:

- Digitale Inhalte werden zur Gewährleistung des Schutzes in Form von digitalen Containern so lange verschlüsselt gehalten, wie möglich. Sobald das Medium in analoger Form vorliegt, ist ein technischer Schutz nur sehr bedingt möglich. Weitere Ausführungen zur Thematik siehe weiter unten.
- Teilweise Verschlüsselung ermöglicht eine "grobe" Einsicht, solange der Nutzer nicht über die erforderlichen Zugangsmittel verfügt. Dies kann auch als "Vorschaudienst" verstanden werden. Bei Bildern beispielsweise könnten verkleinerte Ansichten unverschlüsselt vorliegen, während die tatsächlichen Daten mit einem Zugangschlüssel veschlüsselt wurden.
- Portabilität und Beständigkeit von Nutzerrechten, denn diese müssen an den Nutzer selbst, und nicht an Abspielsoftware oder -geräte gebunden sein. Diese Überlegungen stammen aus der analogen "Welt", in denen der Mediennutzer neben der gewährten Mediennutzung das Trägermedium tatsächlich besaß.
- Die Verschlüsselung wird (vgl. S. 27.ff [Kun04]) zu Folge in symmetrische, asymmetrische und hybride Verfahren eingeteilt. Ersteres Verfahren zeichnet sich durch Verwendung desselben Schlüssels zur Ver- und Entschlüsselung aus. Die asymmetrische Verschlüsselung verwendet sogenannte Schlüsselpaare. Hierbei werden die Inhalte mit einem anderen Schlüssel entschlüsselt, als jener mit dem sie verschlüsselt wurden. Hybride Verfahren stellen eine Kombination aus symmetrischen und asymmetrischen Verfahren dar. Die Nutzdaten werden symmetrisch, und die Schlüssel für die symmetrische Verschlüsselung wiederum asymmetrisch verschlüsselt. Dieses Verfahren kommt deswegen oft zum Einsatz, weil sich die sensiblen Schlüsseldaten über die asymmetrische Verschlüsselung sicherer übertragen lassen. Die gesamt benötigte Rechenzeit ist geringer als beim Austausch sämtlicher Daten über die asymmetrische Variante. Die asymmetrisch ausgetauschten Schlüsseldaten wiederum werden als jene für den Datenaustausch, der symmetrisch verschlüsselt wird, herangezogen.

Authentizität und Integrität untergliedert sich in (vgl. S. 75ff [jSB02]) in die Gruppe der Schutzobjekte:

- Bei digitalen Inhalten stellt die Authentizität die Herkunft des digitalen Materials sicher, Integrität hingegen sichert, dass der Inhalt nicht verändert bzw. bearbeitet wurde.
- Metadaten setzen bei deren Einsatz in DRM Systemen voraus, dass die beschreibenden Inhalte zuverlässig und korrekt sind.

- Nutzer und Systemkomponenten: berechtigte Nutzer dürfen dem System nicht vorgetäuscht werden (Authentizität), weiters darf es nicht passieren, dass nicht-authentifizierte Geräte in das System eingebracht werden, sowie dass diese nicht manipuliert wurden (Integrität)

Weiters werden noch Schutzverfahren als weiteres Untergliederungsmerkmal angeführt. Sie umfassen:

- Hashfunktionen, die auch unter dem Begriff der Prüfsummen bekannt sind. Alle Bits des Eingangsmediums fließen in die Berechnung ein und beeinflussen das Ergebnis maßgeblich. Der Empfänger der digitalen Daten berechnet seinerseits auch die Prüfsumme. Stimmt diese mit der empfangenen überein, so kann mit sehr hoher Wahrscheinlichkeit davon ausgegangen werden, dass die Daten korrekt übertragen wurden.
- Digitale Signaturen werden als Kombination aus Prüfsummenberechnung und asymmetrischer Verschlüsselung beschrieben (S. 31 [Kun04]): "Der Message Digest[2] wird anschließend mit dem privaten Schlüssel des Senders verschlüsselt und zusammen mit der (ebenfalls verschlüsselten) Nachricht übertragen. Der Empfänger entschlüsselt nun den übertragenen Hash-Wert mit dem öffentlichen Schlüssel des Senders, wodurch die Authentizität des Senders gewährleistet wird. Anschließend berechnet er aus der erhaltenen Nachricht einen eigenen Message Digest und vergleicht diesen mit dem von dem Empfänger erhaltenen. Stimmen beide überein, verfügen Sender und Empfänger über dieselbe Nachricht."
- Auf das Teilgebiet der fragilen Wasserzeichen wird im Kapitel 4.5.2 explizit eingegangen.
- Challenge-Response-Verfahren werden zur gegenseitigen Authentisierung der Komponenten eines DRM Systems eingesetzt. Dadurch kann sichergestellt werden, dass kein Teil des Systems kompromiert oder gar ausgetauscht wurde.

Manipulationssichere Systeme werden aufgeteilt in Hardware, die beispielsweise in Computern, DVD-Abspielgeräten, eBook-Lesegeräten, sowie in Set-Top-Boxen verbaut sein kann.

- Dongles, Geräte, die an die Schnittstellen von Computer angesteckt werden, und lizenzpflichtige Software mit Schlüsselmaterial versorgen. Meist ist auch eine eingeschränkte Programmnutzung möglich, sofern kein Dongle angeschlossen wurde (z. B. Testversion).
- Smartcards (S. 82 [jSB02]) "...enthalten eine integrierte Schaltung, die über Elemente zur Datenübertragung, -speicherung und -verarbeitung verfügt. Auf diesen Chips können dauerhaft Daten gespeichert werden, die auch ohne Stromzufuhr erhalten bleiben.". Grundsätzlich kann eine Einteilung in zwei Gruppen erfolgen: Speicherkarten und Mikroprozessorkarten (vgl. S. 7 [Ran02]). Während erstere ausschließlich zum Speichern von kleinen Datenmengen herangezogen wird, können auf letzteren auch diverse Kryptoalgorithmen implementiert werden. Gemeinsam ist beiden Ansätzen jedoch das hohe Sicherheitsniveau. Anwendung finden Smartcards beispielsweise in Mobiltelefonen, Krankenversicherungskarten (z. B. eCard), Pay-TV-Systemen, sowie in Zugangskontrollsystemen. Auch im täglichen Zahlungsverkehr findet diese Technologie ihre Anwendung. Eine Besonderheit liegt darin, dass der Chip gegen

[2] digitaler Fingerabdruck; wird durch eine Einweg-Hash-Funktion ermittelt (vgl. S. 31 [Kun04])

einige Angriffe resistent ist. Unter bestimmten Umständen ist es möglich eine automatisierte Abschaltung oder Zerstörung der Hardware zu implementieren.

Software als weiterer Bestandteil von manipulationssicheren Systemen kommt im Zusammenhang mit schützenswerten Inhalten zum Einsatz:

- allgemeines Szenario eines Angreifers ist es, ein Softwareprogramm und die von ihm belegten Speicherbereiche zu untersuchen, um Informationen über die Funktionsweise zu erlangen. Bislang wurde der vollständige Schutz in Hardware noch nicht ausreichend umgesetzt. Deswegen wird auch auf Software-Schicht ein ausreichender Schutz favorisiert. Dieser kann beispielsweise durch das Einführen einer zusätzlichen Abstraktionsebene zur Integritätsprüfung des ausgeführten Codes erreicht werden. Auch Verschlüsselung kann zur Verbesserung der Sicherheit eingesetzt werden: Teile des auszuführenden Codes werden hierbei verschlüsselt und erst kurz vor der Ausführung entschlüsselt um eine Manipulation zu erschweren (vgl. S. 87-88 [jSB02]).
- Unter Code-Obfuscation versteht man (S. 1 [Mat06]) "Code obfuscation makes it harder for a security analyst to understand the malicious payload of a program. In most cases an analyst needs to study the program at the machine code level, with little or no extra information available, apart from his experience." Eng im Zusammenhang mit der Code-Obfuscation steht das sogenannte "Reverse-Engineering", bei dem versucht wird, die Funktionsweise eines Mechanismuses aus dem Endprodukt zu erkennen (vgl. S. 89 [jSB02]). Bei der Code-Obfuscation erfüllt das Endprodukt (Maschinencode) den gleichen Zweck, wie das unveränderte Original. Versucht man jedoch das bewusst modifizierte Endprodukt in eine höhere Programmiersprache zurückzuführen, so ist dies nicht ohne weiteres möglich, da Variablennamen verändert wurden, zusätzliche Abstraktionsebenen, sowie zusätzliche Programmierklassen, usw. eingefügt wurden, um den Code komplizierter erscheinen zu lassen.

Suchsysteme werden in zwei Gruppen eingeteilt (S. 91 [jSB02]): "pre-infringement control" und "post-infringement control". Erstere verhindern die Erstellung unberechtigter Kopien, während letztere die Suche nach bereits erstellen Kopien ermöglicht.

- Bei der Suche zur Feststellung rechtswidriger Kopien, wird das Internet systematisch nach unberechtigt erstellen Kopien von z. B. Bildern durchsucht. Oft basieren die Suchkriterien auf digitalen Wasserzeichen, die in das Material eingebracht wurden und so eine eindeutige Zuordnung zum Rechteinhaber ermöglichen. In diesem Zusammenhang sei das System "Marc-Spider" der Firma "DigiMarc" erwähnt (vgl. S. 3 [Rac03]).
- Bei der Suche zur Feststellung von Integritätsverletzungen handelt es sich um Systeme, die nach fragilen Wasserzeichen suchen. Sind diese vorhanden, so wurde der Inhalt mit großer Wahrscheinlichkeit nicht modifiziert. Fehlt es, so kann davon ausgegangen werden, dass Änderungen durchgeführt wurde (vgl. S. 30 [Dit00]).
- Im Zusammenhang mit der Suche zur Nutzungsregistrierung werden die eingebrachten Wasserzeichen für Zählvorgänge benutzt. Dies ist auch unter dem Begriff des "broadcast monitorings" bekannt (S. 3 [A. 07]): "In this case, the interested party is the broadcaster who wants to get informa- tion about his broadcasts ratings. This is accomplished again by monitoring

stations that decode the watermark which contains in- formation about the identification of the broadcaster and of the broadcast content, as well as the time of broadcast and sometimes the receiver's location."

Integrierte e-Commerce-Systeme:

- Electronic Data Interchange (EDI) wird wie folgt definiert (S. 1 [Kar00]): "EDI is defined as the exchange of data between heterogeneous systems to support transactions. This is not simply the exportation of data from one system to another, but the actual interaction between systems. Companies that have implemented EDI rave about the various benefits. In fact, these benefits can be expanded to a chain of suppliers." Im referenzierten Dokument wird noch darauf eingegangen, dass die Lücke zwischen den angesprochenen Vorteilen und der tatsächlichen Implementierung in der Realität sehr groß ist, weil die Interoperabilität schwer herstellbar ist. Auch ein Verbinden über ein einheitliches Netzwerk (Internet) führte nicht zur gewünschten Lösung, da viele Faktoren außer Acht gelassen wurden. So bestimmen z. B. unterschiedliche Plattformen, Anwendungen, Datenformate, usw. auch weiterhin die tatsächlichen Bedingungen zur Zusammenarbeit.
- Auch XML-basierte Systeme kommen im Zusammenhang mit DRM zum Einsatz (vgl. S. 98 [jSB02]). Es handelt sich bei XML um eine Meta-Beschreibungssprache, die zum standardisierten Nachrichtenaustausch eingesetzt werden kann. Außerdem stellt sie die Grundlage für die im WWW eingesetzte Auszeichnungssprache HTML dar. Für DRM wurde das IOTP (Internet Open Trading Protocol) entwickelt. Das Protokoll soll das Austauschen von Vertragsangebot und -annahme standardisieren.

Zahlungssyteme werden in Modelle des "pay per use" und des "pay per subscription" eingeteilt (vgl. S. 1ff [Pet99]). Eng zusammenhängend damit geht die Pauschalvergütung einher. Eine finanzielle Abgeltung kann beispielsweise durch die elektronische Bezahlung per Kreditkarte oder durch Werbeeinblendungen erfolgen.

Beim Schutz im analogen Bereich kommen eigene Technologien zum Einsatz, bei denen veränderte NTSC/PAL-Signale nicht mehr durch Videorekorder (VCRs) aufgenommen werden können (vgl. S. 1268 [Jef99]). Darunter fällt z. B. namentlich "APS" der Firma Macrovision. Da auf DVDs nicht direkt NTSC- oder PAL-Signale gespeichert werden, wird im Header des MPEG-Streams festgelegt, wie und ob APS zur Anwendung kommen soll. Der digitale Content (in verschlüsselter Form) soll so lange, wie möglich vorliegen, damit die Schutzmechanismen, die auf digitale Informationen ausgerichtet sind, greifen können (vgl. S. 100 [jSB02]).

Weitere Einteilungsmöglichkeiten

Während die Bestandteile der DRMS vom organisatorischen und technischen Standpunkt aus dargestellt werden können (vgl. S. XI [jSB02]), gehen (vgl. [30]) und (vgl. S. 10 [Gas08]) auch auf die logische Darstellung ein. Demnach besteht ein DRM System aus den folgenden drei Komponenten:

- Inhalteanbieter,
- Lizenzanbieter und
- Clientanwendung.

Erstere beide erscheinen aus Sicht des Mediennutzers als ein einziges Element. Das Zusammenspiel wird durch eine einfach handhabbare Anwendung gewährleistet.

Im Tagungsband der TU München (vgl. S. 37 [30]) werden die Komponenten kommentiert. Bevor die Daten über ein öffentlich zugängliches Kommunikationsmedium übertragen werden können, werden sie mit einem geheimen Schlüssel verschlüsselt. Zugang zum Schlüssel erhalten nur Lizenznehmer durch Verbindungsaufnahme mit dem Lizenzserver. Worin die Schwächen eines solchen Systems liegen zeigt das Kapitel 4.1.

4.2 Block 2: Metadaten

Im zweiten Block des Vorlesungsteiles wird auf die Beschreibung des Inhaltes eingegangen. Dies ermöglicht eine Indizierung der vorliegenden Inhalte. Weiters wird erläutert, wie die Rechte im digitalen Umfeld formalisiert werden.

4.2.1 Inhaltsbeschreibung

Gasser erwähnt (vgl. S. 16 [Gas08]), dass Metadaten formale Angaben zum Inhalt in DRM-Systemen machen. Die Verarbeitung kann daher automatisiert erfolgen. Drei bekannte Metadatensysteme werden angeführt:

- Der Digital Object Identifier (DOI) wird wie folgt definiert (S. 1 [Ceu]): “The Digital Object Identifier (DOI) system provides a framework for the persistent identification of content in its broadest interpretation.” Ein DOI ist eine unmissverständliche und persistente Zeichenkette, die auf ein einzelnes Element verweist und auf einem Nummerierungsschema beruht. Der referenzierte Inhalt ist somit vom Speicherort losgelöst und kann unter einer eindeutigen Adresse erreicht werden. Das DOI System wird von der International DOI Foundation (IDF) betrieben. Sie ermöglicht die Zuordnung zu den aktuellen Standorten.
- Dublin Core (DC) wird wie folgt definiert: “Dublin Core (DC) ist ein aus wenigen Metadatenelementen bestehender Standard, der ursprünglich für die Beschreibung von Text-Dokumenten im Internet entwickelt wurde, aber für sämtliche unterschiedliche digitale Ressourcen (also auch Musikstücke) eingesetzt werden kann, um Sie auf einfache Art zu beschreiben und wieder auffindbar zu machen (S. 4 [28], zitiert aus [50]): ”DC besteht aus 15 Elementen: das Dublin Core Metadata Element Set (DCMES). Bekannt sind diese Elemente durch ihren Einsatz in den Kopfdaten von HTML-Dokumenten. Als Beispiel seien der Titel des Dokuments, der Ersteller, eine Beschreibung, das Erstellungsdateum, sowie die Sprache, in der das Dokument verfasst wurde, zu nennen.

- Das Resource Description Framework (RDF) wird definiert als eine graph-basierte Sprache, die schemenlos und selbstbeschreibend ist. In anderen Worten kann festgehalten werden, dass die Beschriftungen der Graphen innerhalb eines Graphen die enthaltenen Daten beschreiben (vgl. S. 1, Übersetzung vom Verfasser der vorliegenden Arbeit [Har05]).

4.2.2 Rights Expression Languages

Der Begriff der Rights Expression Languages (REL) kann wie folgt definiert werden (S. 9 [Kar03]): "It seems obvious, but it's a language that expresses rights, that says what rights you have in relation to this file. You could argue that we have a perfectly good rights expression language in our copyright laws ... The problem is that the copyright laws are written in legal language, a language that requires some interpretation and some judgment as it is put into practice. An REL in the digital rights management sense is a different kind of language; it is a formal language like mathematics or like programming code; it is language that can be executed as an algorithm. A rights expression language is not open to interpretation but must be rendered precisely through software."

Dies lässt sich wie folgt übersetzen: Rechtebeschreibungssprachen drücken jene Rechte aus, die bei der Nutzung bestimmter digitaler Inhalte zum Tragen kommen. Wenn auch sich festhalten lässt, dass die perfekte Rechtebeschreibungssprache bereits durch das Urheberrecht gegeben ist, ... ist das Urheberrecht in einer Sprache verfasst, die menschliche Intelligenz zur Interpretation voraussetzt. Rechtebeschreibungssprachen, im Vergleich, ähneln in ihrem Aufbau einer formalen Sprache, wie das z. B. bei Mathematik oder Programmiersprachen der Fall ist: eine Sprache, die sich als Algorithmus ausführen lässt. Rechtebeschreibungssprachen können nicht frei interpretiert werden, sie müssen prezise ausformuliert werden, sodass sie durch Software umgesetzt werden können.

Digitale Rechtebeschreibung

Abbildung 4.5 zeigt die wesentlichen Elemente einer Rights Expression Language (vgl. S. 9 [Kar03], zitiert aus (vgl. [37])):

- Berechtigungen (Permissions) oder "was" gemacht werden darf,
- Bedingungen (Constraints) oder der rechtliche Vorbehalt,
- Verbindlichkeiten (Obligations) oder das, was im Gegenzug geboten werden muss und
- Rechteinhaber (Rights Holders) oder "wer" erlaubt ist, etwas zu tun.

Als Beispiel sei genannt, dass ein bestimmtes Video bis zu 10 mal (Zählkriterium) abgespielt werden kann (Benutzungserlaubnis) zu jedem Zeitpunkt (Zeitkriterium) zum Preis von 10$ (Zahlungsverpflichtung). Jedes Mal, wenn das Video abgespielt wird, erhalten John, Mary und Sue (die Rechteinhaber) einen Prozentanteil der Abspielgebühr). Normalerweise ist ein Recht, das nicht explizit ausformuliert wurde, nicht zugesichert und kann somit durch den Mediennutzer nicht in Anspruch

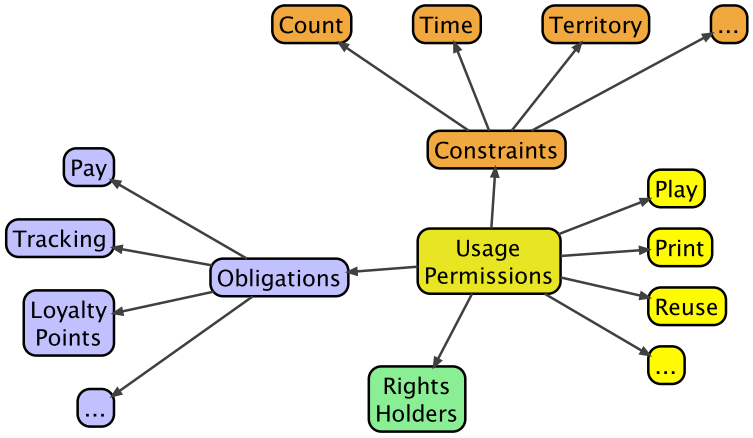

Abbildung 4.5: Das Rights Expression Model, angelehnt an [37, vgl.]

genommen werden. Dies ist eine kritische Annahme bei der Implementierung von Rechtsbeschreibungssprachen und sollte allen Mediennutzern unmissverständlich kommuniziert werden (vgl., Übersetzung vom Verfasser der vorliegenden Arbeit [37]).

Auszeichnungssprachen zur Rechtebeschreibung für das DRM

Zwei wesentliche Konzepte für digitale Rechtebeschreibungssprachen können genannt werden (vgl. S. 6 [Che03]): deklarative und Logik-basierte Sprachen. Im Rahmen des Unterrichts wird nur auf erstere eingegangen. Zwei XML-basierte Rechtebeschreibungssprachen werden näher erläutert (vgl. S. 11 [Kar03]):

- Renato Ianella entwickelte basierend auf dem in Abbildung 4.5 präsentierten Rechtebeschreibungsmodell die “Open Digital Rights Language” (ODRL). Ausgehend von den Elementen des Modells wurden Terme festgelegt, die die Nutzung beschreiben. So sind beispielsweise die Rechte “play”, “print”, “sell”, “move”, “lend”, . . . definiert.
- Die “eXtensible rights Markup Language” (XML) ist ein Produkt der Firma ContentGuard. Im referenzierten Dokument wird angegeben, dass die Sprache komplexer ist als ODRL. Sie kann als Sprache zur Entwicklung von Rechtebeschreibungssprachen angesehen werden. Als Beispiel wird Absatz 5.5.2.1 “Authorization of Located Bits” aus dem Standard der “Motion Picture Experts Group” (MPEG) genannt: “Let g be any authorized Grant containing a Resource d which is a DigitalResource. Let b be the sequence of bits which is the result of any execution of the location algorithm of d. Then the Grant g’ which is identical to g except that d is replaced by a DigitalResource which contains a child binary element which contains a base64 encoding of b is also authorized.” XrML ist demnach nicht semantisch, im Sinne der menschlichen Sprache, Aussagen werden als Formeln mit mathematischer Genauigkeit ausgedrückt.

Die ODRL ist eine offene Standardisierungsinitiative, die als Ziel eine freierhältliche REL für DRM Systeme hat. Die Entwicklung wurde maßgeblich von den Firmen RealNetworks und Nokia vor-

angetrieben. Einfluss übte der Standard auf die Entwicklung von IBMs EMMS[3] aus.

Die Wurzeln von XrML liegen weiter zurück. Die Sprache wurde in ihrer ersten Fassung von der Firma Xerox PARC entwickelt und 1996 veröffentlicht. Syntaktisch und semantisch erfolgte eine Auszeichnung der Rechte durch die Programmiersprache Lisp. Mittlerweile wurde das Sprachformat auf XML geändert. Einsatz findet die XrML in Produkten der Firma Microsoft.

Die beiden Ansätze konkurrieren. Sie unterscheiden sich im Wesen und in der Verfügbarkeit. Während der erste Ansatz, ODRL, in open-source Applikationen Anwendung findet, ist der zweite Ansatz, XrML, grundsätzlich für den Einsatz in kopiergeschützten Anwendungen konzipiert. Weiteres Unterscheidungsmerkmal findet sich in den unterstützenden Firmen (vgl. S. 4 [STW04]).

4.3 Block 3: Verwertung und Gebührenmanagement

Im dritten Block erfahren die Studierenden, wie geistiges Eigentum geschützt werden kann und welche organisatorische Maßnahmen seitens der einzelnen Staatsapparate zur Verfügung stehen. Außerdem wird auf die Deckung der durch den Betrieb von Rundfunkanstalten entstandenen Kosten eingegangen.

4.3.1 Medienverwertung

In den Online-Ressourcen der österreichischen Bundesregierung wird die Aufgabe der Verwertungsgesellschaften wie folgt definiert [4]: “Diese erfüllen vor allem die Aufgabe der Wahrnehmung von Rechten und Ansprüchen, die wegen der Vielzahl der Verwertenden einzeln nicht wirksam geltend gemacht werden können. Sie verwerten also nicht selbst, sondern erteilen den eigentlichen Verwertenden, nämlich den Veranstalterinnen und Veranstaltern, Hörfunk- und Fernsehsendern, CD- und Videoproduzentinnen und -produzenten, Gastwirtschaften usw. Lizenzen zur Nutzung einer Vielzahl von urheberrechtlich geschützten Werken.”

Weiters erläutert die oben zitierte Referenz, dass das “Urheberrecht den Berechtigten ausschließliche Nutzungsrechte und Vergütungsansprüche” zusichert. Je nach Verwendungsfall können folgende Entgeltansprüche geltend gemacht werden:

- Leerkassettenvergütung bei privaten Überspielungen von Ton- und Bildtonträgern,
- Bibliothekstantieme bei Entlehnungen in öffentlichen Büchereien und Bibliotheken,
- Schulbuchtantieme bei Abdrucken in Schul- und Lehrbüchern und
- Reprografievergütung bei Vervielfältigungen im eigenen bzw. privaten Gebrauch mittels reprografischer oder ähnlicher Verfahren.

Unter anderen bestehen in Österreich folgende Verwertungsgesellschaften:

[3] Electronic Media Management System

- Staatlich genehmigte Gesellschaft der Autoren, Komponisten und Musikverleger (AKM) zuständig für Aufführungs- und Senderechte an Werken der Musik und den mit ihr verbundenen Texten,
- Literar-Mechana bei mechanischer Vervielfältigung von Sprachwerken und
- Austro-Mechana bei Verwertung und Auswertung mechanisch-musikalischer Urheberrechte.

Bei der AKM handelt es sich der Homepage (vgl. [2]) zu Folge um eine im Jahre 1897 gegründete Urheberrechtsgesellschaft. Sie ist aus dem Zusammenschluss von Autoren, Komponisten und Musikverlegern entstanden. Der Firmensitz der AKM ist in Wien, Geschäftsstellen gibt es in jedem Bundesland. Ihre Tätigkeiten beschreibt die Gesellschaft mit [1]: "Die AKM sorgt dafür, dass die musikalischen Urheber zu ihren Tantiemen kommen. Gleichzeitig bietet die AKM den Musiknutzern den zentralen Rechteerwerb." Zwei Teilbereiche lassen sich demnach festlegen:

Lizenzierung bei öffentlicher Aufführung (z. B. im Supermarkt, Diskothek, Gaststätten, etc.) trägt die AKM dafür Sorge, dass die Veranstalter dieser Aufführung eine Lizenz von der AKM erwerben und das Aufführungs Entgelt an die AKM bezahlen. Auch Sendeunternehmer und Diensteanbieter müssen eine Lizenz von der AKM erwerben. Im Sendebereich gibt es Gesamtverträge mit dem ORF, mit den zuständigen Fachverbänden und der Wirtschaftskammer Österreich.

Tantiemenabrechnung bedeutet, dass alle Einnahmen nach Abzug des entstandenen Verwaltungsaufwandes zur Gänze an die AKM-Mitglieder und an die inländischen und ausländischen Verwertungsgesellschaften abgerechnet. Die AKM ist ein nicht-gewinnorientiertes Unternehmen.

Außerhalb Österreichs übernehmen andere Unternehmen die Verwertung der Medien:

- in Deutschland die "Gesellschaft für musikalische Auffürungs- und mechanische Vervielfältigungsrechte" (GEMA), sowie die VG Wort im Zusammenhang mit der Verwaltung von Zweitverwertungs- und -nutzungsrechten für Autoren und Verlage (vgl. [18]),
- in der Schweiz die "Swiss Society for the Rights of Authors of Musical Works" (SUISA),
- in Großbritannien die "Artists Collecting Society" (ACS) und die "Authors Licensing and Collecting Society" (ALCS) und
- in den USA die "American Society of Composers, Authors and Publishers" (ASCAP) und "Broadcast Music, Inc." (BMI).

4.3.2 Gebührenmanagement

Die Rundfunkgebühren sind in Österreich gesetzlich im Rundfunkgebührengesetz [12] geregelt. Die Erklärung zur Notwendigkeit liest sich auf der Homepage des "Gebühren Info Service" wie folgt [10]: "Streng nach dem Rundfunkgebührengesetz. B. trachtet, müssen alle Rundfunkempfangseinrichtungen, die in einer Wohnung, einem Haus oder anderen Räumlichkeiten (z. B. Bürogebäuden, Geschäftslokalen, etc.) zum Empfang bereitgehalten werden gemeldet werden. ... Und: Der ORF

als öffentlich-rechtliches Rundfunkunternehmen hat einen klaren gesetzlichen Auftrag, der unter anderem die Vollversorgung, den Betrieb der neun Landesstudios (in den neun Bundesländern) und einen umfassenden Programmauftrag beinhaltet. Ob Fernsehen, Radio oder Internet - der ORF bietet ein breitgefächertes Angebot an Information, Wirtschaft, Bildung, Wissenschaft, Kultur, Religion, Sport und Unterhaltung. Das kostet Geld ."

An mehreren Stellen wird die weitere Notwendigkeit des Digital Rights Managements in Zeiten der Pauschalvergütung durch die GEMA postuliert (vgl. S. 81 [Fra05]). Demnach beruft sich der Autor auf den Qualitätsverlust, der beim Anfertigen einer analogen Kopie einhergeht. Von Musikkassetten waren 1-2 weitere Kopien möglich, bis die Qualitätseinbußen ein wahrnehmbares Maß überschritten hatten. Man spricht in diesem Zusammenhang vom Generationsverlust. Die Pauschalvergütung wurde (in Deutschland) für jeden verkauften, bespielbaren Tonträger an die GEMA abgeführt. Es gab Überlegungen, dass mit jedem Kauf eines PCs Urheberrechtsabgaben gezahlt werden müssen. Dies stieß bei Nutzern die ihre Geräte ausschließlich zur Produktion, sowie zur Sicherung von Daten nutzen möchten teils auf Widerstand.

Im Folgenden wird auf das Gebühren Info Service, kurz GIS, eingegangen. Hier werden Informationen über die Struktur der Gesellschaft zum Management der Rundfunkgebühren in Österreich geliefert (vgl. [11]). Demnach wurde das Unternehmen 1998 als 100%ige Tochter der österreichischen Post AG gegründet. 1999 erfolgte eine 50%ige Beteiligung durch den ORF. Seit 2001 ist das GIS eine 100%ige Tochter des Österreichischen Rundfunks (ORF).

Das Volumen der Transaktionsentgelte betrug im Jahr 2007 rund 644 Millionen Euro. Ungefähr 66% davon erhält der ORF um seine Rundfunk- und Fernsehprogramme, sowie die Landesstudios zu betreiben, der Rest wird zwischen Bund und Ländern aufgeteilt. Das Unternehmen wird durch eine Einhebungsvergütung von 3,25% finanziert. Dadurch ergibt sich ein Jahresumsatz von ca. 36 Millionen Euro.

Das “Gebühren Inkasso Service” wurde in “Gebühren Info Service” umbenannt, um das “Image” des reinen Inkasso-Unternehmens abzulegen. Das Unternehmen möchte seine Kunden auch darüber informieren, was mit den Gebühren geschieht und was bei Nichtleistung der Entrichtung passiert. In Österreich wird in ca. 3% der Haushalte “schwarzgesehen”. Dadurch entgehen dem ORF, dem Bund, sowie den Ländern jährlich ungefähr 60 Millionen Euro. Die Aufgabenbereiche des GIS stellen sich der Informationsmappe wie folgt dar:

- Öffentlichkeitsarbeit zur Bewusstseinsschaffung,
- Erfassung der Rundfunktteilnehmer auf Grundlagen von Meldedaten,
- Aufforderung zur Abgabe einer Mitteilung über die Inanspruchnahme des öffentlichen Rundfunkangebots,
- Veranlassung der Einbringung von Gebühren im Verwaltungsweg,
- Abrechnung und Weiterleitung der eingehobenen Gebühren, Abgaben und Entgelte und
- Entscheidung über Antrge auf Befreiung, Zuschussleistung.

Außerhalb Österreichs wird das Gebührenmanagement jeweils durch eigene Unternehmen durchgeführt. Als Beispiel seien hier ein paar genannt:

- in Deutschland die "Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland" (GEZ), eine Gemeinschaftseinrichtung des ARD, ZDF und Deutschlandradio,
- in der Schweiz die Billag, eine 100%ige Tochter der Swisscom und
- Großbritannien die "TV Licensing", eine Tochtergesellschaft der BBC.

4.4 Block 4: Einführung in die lineare Algebra

Die lineare Algebra bietet die mathematischen Grundlagen zur digitalen Steganographie. Im Zuge in Kapitel 4.5 vorgestellten und durchgeführten Experimente wird davon ausgegangen dass die Studierenden mit den Grundzügen der Thematik vertraut sind.

4.4.1 Begriffserklärung

Die Thematik wird oft als die Summe aus seinen Einzelteilen bestehendes Hauptwort dargestellt (vgl. S. 2 [24]).

Linear referenziert demnach auf etwas, das „straight"[4] oder „flat"[5] ist. Dem Dokument zufolge messen die angeführten Beispiele der Lösung linearer Gleichungen große Bedeutung bei. Die Potenzen von unbekannten Variablen nehmen in linearen Gleichungssystemen stets den Wert 0 oder 1 an. Zur Verdeutlichung sei an dieser Stelle ein kurzes Beispiel angeführt (Gleichungen 4.1 und 4.2).

$$2x + 3y - 4z = 13 \tag{4.1}$$

$$4x_1 + 5x_2 - x_3 + x_4 + x_5 = 0 \tag{4.2}$$

Algebra hingegen wird im Zusammenhang mit der Algebra von realen Zahlen[6] betrachtet (vgl. S. 3 [24]). Der zum Erlernen notwendige Aufwand kommt der angegebenen Quelle zufolge in etwa dem zum Erlernen einer neuen Sprache gleich. Die Algebra kann auch als ein Bereich der Mathematik verstanden werden (vgl. [Pra08]). Wenn auch die Wurzeln des Teilgebiets in der Theorie über reelle und komplexe Zahlen liegt, ist sie auf keinen speziellen Bereich der Mathematik festgelegt. Vielmehr lässt sie sich auf fast alle Domänen der Mathematik anwenden.

[4] glatt bzw. gerade, aus dem Englischen
[5] flach, aus dem Englischen
[6] auch unter dem Namen „Elementare Algebra" bekannt (vgl. [Pra08])

Weiters ein Zusammenspiel der linearen Algebra mit der Geomtrie (vgl. S. 3 [24]). Aufgabenstellungen im zwei- und dreidimensionalen Raum können der Quelle zu Folge oft auf geometrische Problemstellungen rückgeführt werden.

4.4.2 Terminologie

Dieses Kapitel eräutert die Vermittlung des zur Durchführung der in Kapitel 4.5 vorgestellten Experimente notwendigen Fachvokabulars. Im Zuge dessen wird auf die Sonderformen der Matrizen eingegangen.

Reelle Matrizen

Im Kontext der linearen Algebra versteht man (vgl. S. 2ff [Lot01]) "unter einer reellen Matrix A vom Typ (m,n) ein aus $m \cdot n$ reellen Zahlen bestehendes rechteckiges Schema mit m waagrecht angeordneten Zeilen und n senkrecht angeordneten Spalten." Die Definition einer Matrix wird weiters in Gleichung 4.3 dargestellt.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & \cdots & a_{1n} \\ a_{21} & a_{21} & \cdots & a_{2k} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} & \cdots & a_{mn} \end{pmatrix} \tag{4.3}$$

a_{ik} Matrixelemente ($i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, n$)

i, k Zeilen-, Spaltenindex

m, n Zeilen-, Spaltenzahl

Spezielle Formen der Matrizen sind die Nullmatrix 0, deren Elemente sämtlich verschwinden, die Spaltenmatrix $A_{m,1}$, einer Matrix mit nur einer Spalte[7] und die Zeilenmatrix $A_{1,n}$, einer Matrix vom Typ (1,n). Spaltenmatrizen werden auch Spaltenvektoren und Zeilenmatrizen als Zeilenvektor bezeichnet.

Quadratische Matrizen

Sonderform, gleiche Zeilen- wie Spaltenanzahl, ... Diese Sonderform der Matrizen zeichnet sich durch eine gleiche Zeilen- und Spaltenzahl aus. Sie "spielen in naturwissenschaftlich-technischen Anwendungen eine besondere Rolle (S. 7 [Lot01])." Weiters wird festgehalten, dass die Diagonalelemente $a_{ii}, i = 1, 2, \ldots, n$ miteinander verbunden werden. Im Gegensatz dazu verläuft die Nebendiagonale von rechts oben nach links unten. Außerdem gibt es weiters spezielle quadratische Matrizen, wie beispielsweise Diagonalmatrizen (vgl. S. 7 [Lot01]).

[7] entspricht einer Matrix vom Typ (m,1)

4.4.3 Gleichheit von Matrizen

Es ist definiert, dass "zwei Matrizen $A = (a_{ik})$ und $B = (b_{ik})$ vom gleichen Typ (m, n) gleich $(A = B)$ heißen, wenn $a_{ik} = b_{ik} \forall\ i, k$[8] (vgl. S. 2ff [Lot01])" gilt. Anders ausgedrückt stimmen gleiche Matrizen in ihrem Typ und sämtlich einander entsprechenden Elementen überein.

4.4.4 Rechenregeln

Addition und Subtraktion

Diese Rechenoperationen werden mit den folgenden Worten beschrieben (S. 12 [Lot01]): "Zwei Matrizen $A = (a_{ik})$ und $B = (b_{ik})$ vom gleichen Typ (m, n) werden addiert bzw. subtrahiert, indem man die entsprechenden, d.h. gleichstelligen Matrixelemente addiert bzw. subtrahiert."

$$C = A + B = (c_{ik})\ mit\ c_{ik} = a_{ik} + b_{ik} \tag{4.4}$$

$$D = A - B = (c_{ik})\ mit\ c_{ik} = a_{ik} - b_{ik} \tag{4.5}$$

Auch hier nehmen die Laufvariablen wieder den bekannten Wertebereich an $(i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n)$.

Multiplikation mit einem Skalar

Die Multiplikation mit einem Skalar genügt der folgenden Definition (S. 13 [Lot01]): "Eine Matrix $A = (a_{ik})$ vom Typ (m, n) wird mit einem reellen Skalar λ multipliziert, indem man jedes Matrixelement a_{ik} mit dem Skalar λ multipliziert." Gleichung 4.6 stellt die Zusammenhänge in der mathematischen Schreibweise dar.

$$\lambda \cdot A = \lambda \cdot (a_{ik}) = (\lambda \cdot a_{ik})\ \forall\ i, k \tag{4.6}$$

Auch hier nehmen die Laufvariablen den bekannten Wertebereich an $(i = 1, 2, \ldots, m; j = 1, 2, \ldots, n)$.

Multiplikation von Matrizen

Die Multiplikation von Matrizen ist nur unter bestimmten Voraussetzungen möglich. Ist nun $A = (a_{ik})$ eine Matrix vom Typ (m, n) und $B = (b_{ik})$ eine Matrix vom Typ (n, p), dann heißt die Matrix $C = A \cdot B = (c_{ik})$ das Produkt der Matrizen A und B, sofern die Kriterien, gegeben durch die Gleichung 4.7, erfüllt sind (vgl. S. 15 [Lot01]).

[8] $i = 1, 2, \ldots, m;\ k = 1, 2, \ldots, n$

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk} \tag{4.7}$$

Das Matrizenprodukt $A \cdot B$ ist dann vom Typ (m, p). Die Laufvariablen nehmen wieder den bekannten Wertebereich an $(i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n)$.

4.4.5 Einsatz von MATLAB

In der Lehrveranstaltung soll zur Verdeutlichung der gelehrten Inhalte die Software "MATLAB" eingesetzt werden. Der Produkthomepage zufolge wird das Werkzeug wie folgt beschrieben [15]: "MATLAB ist eine hochentwickelte Sprache für technische Berechnungen und eine interaktive Umgebung für die Algorithmenentwicklung, die Visualisierung und Analyse von Daten sowie für numerische Berechnungen. Mit MATLAB lassen sich technische Probleme schneller lösen als mit herkömmlichen Programmiersprachen wie C, C++ und Fortran."

Vor allem die Eigenschaft zur schnelle Prototypenentwicklung macht das Werkzeug hervorragend geeignet(vgl. [41]), Konzepte anschaulich darzustellen, da die zur Programmierung in weniger entwickelten Sprachen erforderlichen Eigenheiten, wie z. B. Speichermanagement und Plattformabhängigkeit außer Acht gelassen werden können. Weiters stehen für eine Vielzahl an Problemstellungen bereits fertige "Toolboxen" (vgl. [14]) mit weiteren, problemspezifischen Werkzeugen zur Verfügung.

4.4.6 MATLAB als Werkzeug

Der Produktname MATLAB stellt eine Zusasmmensetzung der Wörter "Matrix Laboratory" dar (vgl. [31]). Der Interpreter läuft offiziell unter Microsoft Windows, Linux, MacOS X und Solaris. Da es sich um eine numerische Software handelt, ist sie mit Mathematika oder Maple, als jeweils algebraische/symbolischer Software, nicht zu vergleichen.

Als interpretierte Sprache weist MATLAB die Vorteile der komfortablen Bedienung, einem einfachen Debugging, großer Absturzsicherheit, sowie einer vergleichsweise geringen Entwicklungszeit auf. Als Nachteile hingegen wäre die langsamere Ausführung, insbesondere bei Schleifen, zu vermerken (vgl. S. 1 [31]).

Weitere Informationen bietet sowohhl die Produkthomepage http://www.mathworks.com, als auch die Newsgroup comp.soft-sys.matlab.

4.4.7 Praktischer Einstieg in MATLAB

Sämtliche Listings finden sich im Anhang (siehe A) dieser Arbeit. Im Text wird auf die entsprechende Stelle verwiesen, die wesentlichen Sprachelemente werden auf Basis von geeigneter Literatur (vgl. [47]) behandelt. Allen voran wird das integrierte Hilfesystem vorgestellt (Listing A.1).

Analog zu den in Kapitel 4.4 gezeigten Matrizentypen und Rechenvorschriften, werden Beispiele durchgeführt. So zeigt das Listing A.2, wie man grundsätzlich Daten definiert. Prinzipiell erfolgt nahezu jede Definition in einer Matrix (vgl. S. 2 [31]). Zeile 1 und der in Zeile 5 erfolgte `whos`-Aufruf zeigen, dass selbst einzelne Elemente in einer Matrix vom Typ (1,1) abgelegt werden.

Zeile 3 von Listing A.2 zeigt eine Zeilenmatrix. Dieser Matrizentyp wurde in Kapitel 4.4.2 vorgestellt. Die Besonderheit liegt darin, dass die Anzahl der Zeilen höchstens `1` (eins) beträgt. Elemente unterschiedlicher Dimensionen werden bei mehrdimensionalen Matrizen durch Semikolons getrennt (vgl. S. 3 [31]). Dieser Umstand wird in Zeile 4 dargelegt.

Gleich darauffolgend werden die Grundrechnungsarten mit Matrizen praktisch erläutert. Sowohl die Multiplikation, als auch die Division erfolgen bei Matrizen entsprechend den Vorschriften der linearen Algebra nicht elementweise (siehe dazu Kapitel 4.4.4). Da es aber Algorithmen gibt[9], die von elementweisen Operationen abhängen (siehe dazu auch Kapitel 4.5.3), stellt MATLAB es dem Benutzer frei, elementweise oder nach Vorschrift zu multiplizieren bzw. dividieren (vgl. S. 1 [47]).

Listing A.3 zeigt die elementweise Multiplikation von Matrizen. Die auf Zeile 14 durchgeführte Multiplikation nach Vorschriften der linearen Algebra ist nicht möglich, da die Spaltenzahl der Matrix `a` nicht mit der Zeilenzahl der Matrix `b` übereinstimmt (vgl. S. 14ff [Lot01]).

Built-In Commands

Die built-in[10] commands erlauben es, Matrizen und deren Speicherbereich vorzureservieren. So zeigt Zeile 1 in Listing A.4, wie man mit Hilfe des `zeros(4)` Kommando eine quadratische Matrix mit einer beispielhaften Breite von 4 Elementen anlegen kann.

Will man eine Matrix vom Typ m, n mit dem Wert `0` vorblegen, so benutzt man das Kommando `zeros(m,n)`, wobei `m` durch die jeweilige Zeilen, sowie `n` durch die jeweilige Spaltenzahl zu ersetzen ist. Mit `ones()` können Matrizen analog zu `zeros()` mit dem Wert `1` vorbelegt werden. Um die Dimensionen und deren Elementezahlen einer Matrix zu ermitteln, wird das `size()` Kommando verwendet (vgl. [49]).

Im Rahmen der Lehrveranstaltung werden auch die zur Durchführung notwendigen Bit-Operatoren vorgestellt:

[9] z. B. JPEG-Kompressionsalgorithmus
[10] "eingebaut", aus dem Englischen

- `bitand`, die logische UND-Verknüpfung von Bits mit gleichem Index,
- `bitor`, die logische ODER-Verknüpfung von Bits mit gleichem Index,
- `bitshift` zum verschieben eines Elements um eine beliebige Anzahl an Bitstellen nach links[11] und
- `bitcmp`, das bitweise Komplement des gegebenen Elements.

Zeile 1 in Listing A.5 zeigt, wie die Funktion `sprintf()` genutzt werden kann, um Zahlen in unterschiedlichen Formaten darstellen zu können. In diesem Fall, wurde das hexadezimale System verwendet. Hierbei entspricht jede Stelle vier Bits. `0x0F` im hexadezimalen System (Basis 16) notiert man somit mit `00001111` im binären (Basis 2), sowie mit `15` (Basis 10) im dezimalen System.

`bitand()` und `bitor()` erwarten als Parameter die zu verknüpfenden Elemente, `bitshift()` sowohl das Element, als auch die Anzahl der Stellen, um die die Zahl nach links verschoben werden soll. `bitcmp()` nimmt als Parameter die zu behandelnde Zahl, sowie die Anzahl der Stellen in der binären Representation des Rückgabewerts (vgl. [49]).

Die Bit-Operatoren können auch auf alle Elemente einer Matrix angewandt werden. MATLAB iteriert über alle Elemente, falls es sich bei dem übergebenen Parameter um eine Matrix handelt (vgl. zum jeweiligen Befehl [49]).

Kontrollstrukturen

Bedingte Ausführung kann durch die `if` Bedingung bewirkt werden. Listing A.6 zeigt die Zusammenhänge. Das `sprintf()` Statement wird nur ausgeführt, falls die Bedingungen auf Zeile 2 erfüllt ist.

Listing A.7 zeigt, wie eine `for`-Schleife gebildet wird. Im Beispiel wird die Range-Notation verwendet[12], um einen Wertebereich zu erhalten (in diesem Fall von 1 bis 3). Die Kontrollstrukturen sind in (vgl. [31]) dokumentiert .

Funktionen

Funktionen können dazu benutzt werden, um Anweisungen zusammenfassen zu können. Die Definition erfolgt in eigenen Textdateien, üblicherweise mit der Endung ".m", deren Name gleich dem Funktionsnamen ist. Listing A.8 zeigt, wie eine Funktionsimplementierung aussehen kann. In Listing A.9 zeigt, wie der Funktionsaufruf erfolgen kann. Die Funktionsdatei wurde im Arbeitsverzeichnis[13] angelegt. Die Funktion ist durch die einzelne `for`-Schleife ausschließlich für eindimensionale Matrizen geeignet (vgl. S. 9ff [31]).

[11] das entspricht einer Multiplikation mit $2^{Anzahl\ der\ Bitstellen}$
[12] `Variable = anfang:ende`
[13] Current Working Directory

Visualisieren von Daten

Daten können in sogenannten Plots visualisiert werden. Dazu werden beispielsweise zwei Wertemengen herangezogen, um die Koordinaten für die Funktionspunkte zu bilden. Listing A.10 zeigt anhand einer Geradengleichung den Einsatz der `plot()` Funktion (vgl. S. 13ff [31]).

4.5 Block 5: Steganographie

Informationen zur eindeutigen Identifizierung, sowie Aussagen über den Inhalt sollen durch den Mediennutzer im digitalen Datenstrom nicht unmittelbar wahrnehmbar sein. Das erschwert einerseits das Entfernen dieser zusätzlichen Daten, weiters ist eine möglichst geringe Beeinträchtigung der Qualität der zu übergringenden Information wünschenswert. Das folgende Kapitel beschäftigt sich mit der Steganographie. Sie bildet die Grundlage für digitale Wasserzeichen, die als Zusatzinformation den zuvor angesprochenen Kriterien an die Unentdeckbarkeit gerecht werden.

4.5.1 Terminologie

Jana Dittmann definiert den Begriff der Steganographie mit den folgenden Worten (S. 14 [Dit00]): "In einigen Anwendungsfällen jedoch kann es von Interesse sein, die Präsenz der Kommunikation, der Nachricht selbst, zu verbergen. Dieses Problem wird von steganographischen Verfahren behandelt."

Es gibt aber noch weitere Definitionen der Steganographie. Als Beispiel sei hier die um 1644 festgehaltene Definition von "Jean Robert du Carlet" genannt: Bei Steganographie handelt es sich um "Eine selbst einem Meister verborgene Kunst". Im anglikanischen Sprachraum definiert Richard Popa den Begriff wie folgt (S. 8 [Pop98]): "Steganography is an ancient art of embedding private messages in seemingly innocuous messages in such a way that prevents the detection of the secret messages by a third party." und "In other words, steganography means establishing covert channels." Cachin hingegen beschreibt die Steganographie mit den Worten (S. 1 [Chr98]) "Steganography is the art and science of hiding information such that its presence cannot be detected."

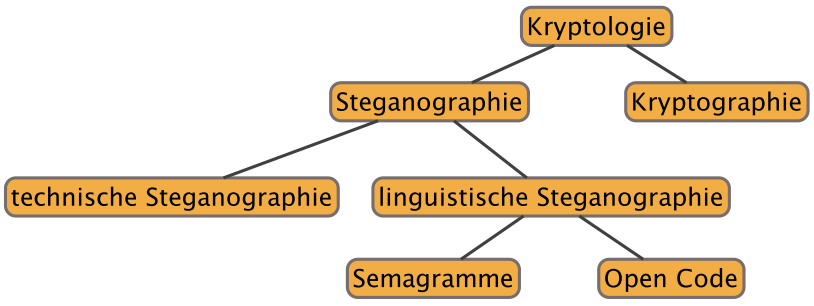

Abbildung 4.6: Einteilung der Steganographie (vgl. [Bau00])

Abbildung 4.6 zeigt die Einordnung der Steganographie in das Themengebiet der Kryptologie (vgl. [Bau00]). Während sich die Steganographie mit dem Verbergen der Existenz von Nachrichten

beschäftigt, wird die Kryptographie zum Verbergen von Nachrichteninhalten eingesetzt (vgl. S. 1 [Ros98]).

Das Themengebiet der Steganographie lässt sich in zwei große Teilbereiche gliedern (vgl. S. 8ff [Seu04]):

- "Im Bereich der linguistischen Steganografie versucht man geheime Informationen in scheinbar harmlosen Texten oder Zeichnungen unterzubringen. Hierbei haben sich im Laufe der Jahre zwei verschiedene Verfahren entwickelt:"
  - Semagramme, bei denen der Geheimtext mittels grafischer Elemente in das Trägermedium integriert wird. Das Semagramm erfüllt seinen Zweck dann optimal, wenn die verwendete Grafik oder der verwendete Text Dritten harmlos und unscheinbar erscheint. Ein Beispiel für diese Methode kann das Hervorheben von Buchstaben in einem unscheinbaren Text sein (vgl. S. 11 [Seu04]).
  - Open Code, bei dem die geheime Nachricht unverfänglich und offen verständlich dargestellt wird. Dabei werden wiederum zwei Klassen unterschieden. Bei der Maskierung wird bestimmten Handzeichen, Floskeln, Symbolen, etc. wird eine bestimmte Bedeutung zugeordnet. Bei der Verschleierung wird eine geheime Nachricht wird in eine andere, offene Nachricht eingebettet. Zwei Konzepte werden in der oben zitierten Publikation erwähnt: Sender und Empfänger vereinbaren ein System, bei dem nur jeder x. Buchstabe, das x. Zeichen nach einem Leerzeichen oder der x. Buchstabe nach einem Interpunktionszeichen zum Einbetten von geheimen Nachrichten verwendet wird. Beim zweiten Konzept werden in die Nachricht sogenannte Füllzeichen eingefügt. Als Beispiel sei hier die B-Sprache genannt. Im Internet wird die Sprache wie folgt beschrieben (vgl. [3]): Jeder Vokal oder Umlaut wir mit einem vorangestellten 'b' wiederholt (hallo ⇒ haballobo), Ausnahme: vor 'ei', 'au', 'eu', 'äu', 'öu' wird ein 'ab' vorangestellt (bauer ⇒ baueber), Ausnahme: vor 'ie' wird nur ein 'i' vorangestellt (dieb ⇒ dibieb)
- "Die technische Steganografie befasst sich im Gegensatz zur linguistischen Steganografie nicht mit der Unterbringung von Geheimnachrichten in Text oder Zeichnungen, sondern mit althergebrachten Methoden, wie zum Beispiel physischen Verstecke, und dem Einsatz der Steganografie im Zeitalter der digitalen Technik (vgl. S. 18 [Seu04])."
  - Traditionell werden hier physische Verstecke, wie Verstecke in hohlen Schuhsolen, Zauberhüte mit doppelten Boden, etc., Geheimtinte und der vorwiegend im zweiten Weltkrieg eingesetzte Mikrofilm verwendet (vgl. S. 18ff [Seu04]).
  - In der Digitaltechnik gibt es weitere Untergliederungen:
    * Die pure Steganographie nutzt die Leistungsfähigkeit heutiger Computersystem aus, um Information in Bild, Ton oder Filmen einzuBetten. Die Informationen werden im Rauschen eingebracht. Das Rauschen lässt sich wie folgt definieren (S. 20 [Seu04]): "Rauschen ist Teil unseres Lebens und findet sich in der Natur, sowie in allen modernen technischen Geräten wieder. Es beschreibt das Vorhandensein minimaler Abweichungen von eigentlich exakten Werten."

* Die verschlüsselte Steganographie zeichnet sich dadurch aus, dass Daten vor ihrer Einbettung mit einem kryptografischen Verschlüsselungsalgorithmus kodiert werden. Nachteile dieses Verfahrens liegen darin, dass der Empfänger über zwei (kryptografischer und steganografischer) Schlüssel verfügen müssen. Außerdem verursachen symmetrische Verschlüsselungsverfahren, wie beispielsweise AES oder DES eine absolute Gleichverteilung der Daten (weißes Rauschen), was Angriffe erleichtert. Deswegen hat sich in diesem Fall der Einsatz von Verschlüsselungsverfahren mit öffentlichen Schlüsseln bewährt (vgl. S. 22 [Seu04]).

Die Komponenten eines steganographischen Systems werden an dieser Stelle erläutert:

- Cover Image oder die Trägernachricht, in sie wird eingebettet,
- Secret Image, die geheime Botschaft, sie gilt es verdeckt zu übermitteln bzw. in das "Cover Image" einzubetten,
- Stego Object, das "Cover Image" mit dem eingebettetn "Secret Image",
- Encoder / Decoder, das Einbettungs- bzw. Entpackwerkzeug und
- Key, der zum Veschlüsseln der Botschaft herangezogene Schlüssel.

In Abbildung 4.7 wird das Zusammenspiel der soeben definierten Elemente gezeigt (vgl. [Kah67]). Hierbei wird in das "Cover Image" durch den "Encoder" das "Secret Image" eingebracht. Dadurch entsteht das sogenannte "Stego Object", welches über den Kommunikationskanal zum Empfänger transportiert wird. Dieser entpackt mit dem "Decoder" die versteckten Informationen. Manche verfahren setzen dazu das "Cover Image" (in der Abbildung mit "Original Cover" bezeichnet) voraus. Erfolgt die Einbettung bzw. werden die Einbettungspositionen verschlüsselt, so wird dem "Encoder" und dem "Decoder" der "Key" zugeführt (vgl. S. 5 [Cum04]).

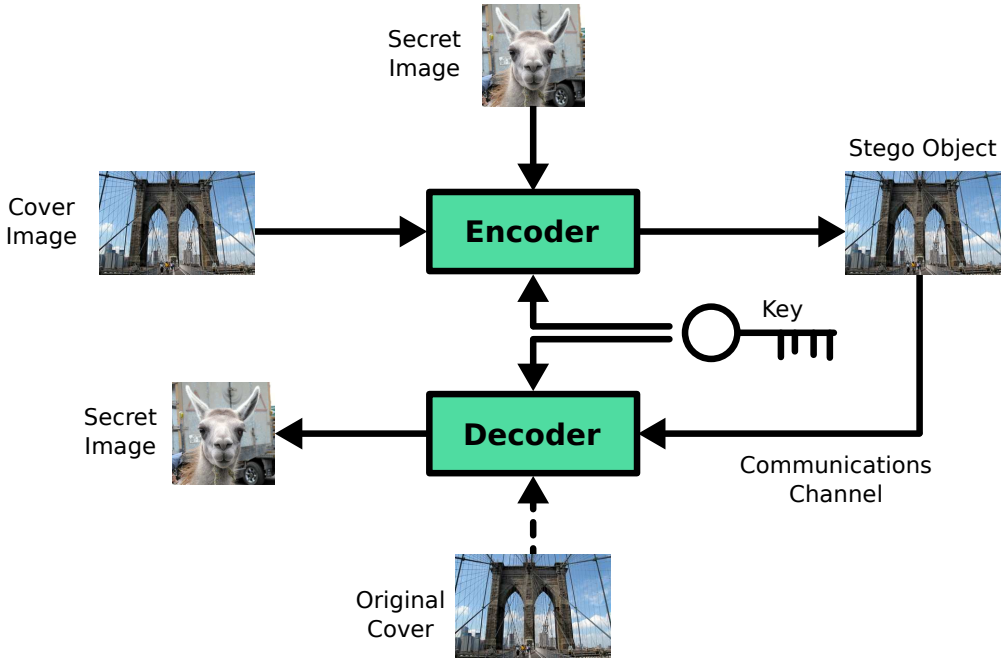

Abbildung 4.7: Generische Vorgangsweise der Steganographie (vgl. [Kah67])

Anforderungen

Es lassen sich die drei wesentlichen Kriterien für das Trägermedium erläutern (vgl. S. 7 [Seu04]):

- Robustheit beschreibt die Widerstandsfähigkeit eines Trägermediums gegen äußere Einflüsse bzw. Transformationen. Im zitierten Dokument werden dabei als Beispiele Einflüsse durch verlustbehaftete Kompressionsalgorithmen oder durch Transformationen (Rotation, Skalierung, Ab- und Ausschneiden von Datenbereichen, etc.) des Stegoobjekts bei der digitalen Steganographie genannt. Die Robustheit mach Aussage darüber, wie gut die versteckten Informationen erhalten bleiben, wenn das Trägermedium äußeren Einflüssen ausgesetzt wird.
- Kapazität macht Aussage über die Menge der versteckbaren Zusatzinformation im Trägermedium.
- Wahrnehmbarkeit beschreibt, wie sehr die Veränderung je nach Betrachter (z. B. menschlicher Organismsus, Hard- und Software, etc.) sichtbar sind, da die in ein Trägermedium eingebrachte Information dieses ändert.

Die Anforderungen an Trägermedien im steganographischen Umfeld widersprechen sich teilweise. So steigt mit der Menge der versteckten Information die Wahrscheinlichkeit, dass diese entdeckt wird. Analoges geschieht mit robuster Information, die u. U. mehrmals in das Trägermedium eingebracht wurde, um bei Transformation an den durch diese veränderten Stellen an anderen Stellen im weiters verfügbar zu sein. Diese multiple Verfügbarkeit erhöht die Chance des Entdecktwerdens für versteckte Information. Entsprechend der Anforderungen an den Verwendungszweck muss entschieden werden, welches der drei Kriterien jenes mit der größten Wichtigkeit ist.

Rahmenbedingungen

Das Kerckhoff Prinzip Dieses sagt aus, dass Sicherheit ausschließlich von der Wahl des Schlüssels abhängen darf. Umgelegt auf steganographische Systeme bedeutet dies, dass ein Beobachter, der die Funktionsweise des Systems versteht, ohne Kenntnis des Schlüssels nicht nachweisen kann, ob verdeckte Kommunikation stattgefunden hat (vgl. S. 1 [Sha07]).

Informations-Theoretisches Modell nach Cachin Das in (vgl. S. 2ff [Chr98]) vorgestellte Modell lässt sich zusammenfassen (vgl. S. 33 [Pro03]). Der Gegenspieler hat vollständige Kenntnis über die Funktionsweise des Codierungs-Prozesses, besitzt jedoch den geheimen Schlüssel nicht. Das Ziel besteht darin, die Wahrscheinlichkeitsverteilung für alle möglichen Trägermedien P_C und für alle in P_C enthaltenen, möglichen steganographischen Medien P_S gegenüberzustellen und daraus ein Modell zu entwickeln.

In weiterer Folge kann die Signalentdeckungstheorie eingesetzt werden, um zwischen zwei Hypothesen zu unterscheiden:

- Hypothese C, laut der die Nachricht keine versteckte Botschaft beinhaltet,

- Hypothese S, laut der die Nachricht eine versteckte Botschaft beinhaltet.

Ein System ist dann perfekt sicher, solange keine Entscheidungsregel existiert, die besser als zufälliges Raten ist.

4.5.2 Digitale Wasserzeichen und digitales Fingerprinting

Die Sicherheit in Hinsicht auf die versteckten Informationen lässt sich bei der Steganographie im Zusammenhang mit digitalen Wasserzeichen und digitalen Fingerabdrücken in zwei große Gruppen einteilen: Sicherheit gegen Entdecktwerden und Sicherheit gegen das Entferntwerden (vgl. S. 2 [Pop98]). Letztere der beiden Kategorien kann als das Hauptanwendungsgebiet der beiden Verfahren Watermarking und Fingerprinting angesehen werden.

An digitale Wasserzeichen und Fingerabdrücke werden folgende Anforderungen gestellt (vgl. S. 4 [Cum04]):

- Integrität der versteckten Information muss erhalten bleiben; an die geheime Botschaft darf keine Information hinzugefügt oder entfernt werden.
- Das Stegoobjekt darf durch die menschlichen Sinne nicht vom Originalobjekt unterscheidbar sein.
- Änderungen am Stego-Objekt dürfen keine Auswirkungen auf das Wasserzeichen haben.

Digitale Fingerabdrücke steht für das Einbringen einer Seriennummer in digitale Dokumente; dadurch kann z. B. der Erwerber einer Lizenz für ein digitales Dokument gekennzeichnet werden

Digitale Wasserzeichen bezeichnen das Einbringen von Markierungen in digitale Dokumente, analog zu Wasserzeichen auf Banknoten; dadurch können beispielsweise Informationen über den Urheber oder die Medienproduktion in digitalen Dokumenten eingebracht werden

Wasserzeichen und Fingerabdrücke können in zwei große Gruppen eingeteilt werden (vgl. S. 30ff [Dit00]), die sich wie folgt unterscheiden:

- das Anwendungsgebiet, das wiederum untergliedert werden kann:
  - Verfahren zur Urheberidentifizierung,
  - Verfahren zur Kundenidentifizierung,
  - Verfahren zur Annotation des Datenmaterials,
  - Verfahren zur Durchsetzung des Kopierschutzes, sowie
  - Verfahren zum Nachweis der Unversehrtheit.
- Die Verfahrensparameter hingegen werden eingeteilt in:
  - Wahrnehmungsaspekt,

- Robustheit,
- Verifizierbarkeit der Markierung,
- Verwendung des Originals beim Abfrageprozess und die
- Kapazität.

Weitere Einteilungen der Wasserzeichen

Digitale Wasserzeichen lassen sich hinsichtlich der Robustheit in zwei Gruppen einteilen (vgl. S. 7 [Cum04]):

- fragile Wasserzeichen, die zur Integritätsprüfung herangezogen werden und
- robuste Wasserzeichen, die eingesetzt werden, um beispielsweise den digitalen Fingerabdruck eines Mediennutzers zu verstecken.

Weiters kann eine weitere Einteilung in

- wahrnehmbare und
- nicht-wahrnehmbare Wasserzeichen erfolgen (vgl. S. 13ff [Cum04]).

Bei letzterer Einteilung kann unter den wahrnehmbaren Wasserzeichen beispielsweise das Einspielen einer Hintergrundmusik bei auditive Medien und das einblenden eines Logos bei visuellen Medien verstanden werden. Auf die nicht-wahrnehmbaren Wasserzeichen wird in den jeweiligen Kapiteln zur visuellen Steganographie bzw. zur Steganographie in auditiven Medien eingegangen.

4.5.3 Steganographie in visuellen Medien

Um das durch ein visuelles steganographisches System zu verarbeitende Datenaufkommen zu verstehen, wird die Leistungsfähigkeit des menschlichen visuellen Systems durch die aus der Digitalfotografie bekannten Zahlenwerte beschrieben. Die Auflösung des "Human Visual System" lässt sich mit 576 Megapixeln[14] angeben, die Lichtempfindlichkeit beträgt zwischen 1 und 800, der dynamische Bereich in Abhängigkeit von den Lichtverhältnissen 1 zu 10^6 und die Brennweite umfasst einen Bereich zwischen 22 und 24 Millimetern (vgl. [27]). Die Bitrate wird mit ca. 875 Kilobits pro Sekunde angegeben (vgl. S. 4 [Bal06]). Der dynamische Bereich der annehmbaren Werte, z. B. der der unterscheidbaren Leistungswerte, liegt generell niedriger als bei jenen des menschlichen Gehörsinnes. Siehe hierzu auch Kapitel 4.5.4.

[14] Millionen Bildpunkten

Technologien in der "spatial domain"

Man spricht in diesem Zusammenhang auch von den Verfahren, die im Bildbereich operieren (vgl. S. 44ff [Dit00]). Änderungen am Originalobjekt werden hierbei durch direkte Bildmanipulationen herbeigeführt. Da sie direkt auf den Bildpunkten arbeiten, sind sie in Hinsicht auf die Wahrnehmbarkeit und die erzielbare Datenrate etwas schlechter als die später vorgestellten Frequenzraumverfahren (vgl. S. 49 [Dit00]). Man spricht bei Methoden nach diesem Prinzip von additiven Verfahren (vgl. S. 136 [Pan04]).

Technologien in der "transform domain"

Im Gegensatz zu den zuvor erläuterten Techniken der "spatial domain" lässt sich für die "transform domain" festhalten (S. 44 [Dit00]): "Verfahren im Frequenzraum bringen ein Wasserzeichenmuster auf die Frequenzen des Bildes ein. Die Energie liegt abhängig vom konkreten Verfahren in den niedrigen oder hohen Frequenzen." Die Aufteilung in die Frequenzbestandteile erfolgt dabei in Pixelblöcken, auf die eine Transformationsfunktion (z. B. die diskrete Kosinustransformation, DCT) angewendet wird. Verfahren, die die niederfrequenten Bildanteile modifizieren sind robust gegenüber Transformationen, wie z. B. Kompression und Filterung. Sie betreffen die niederen Frequenzbereiche nicht. Wasserzeichen werden hingegen meist in die mittleren und hohen Frequenzen eingebracht, da sie auf diese Weise für das menschliche Auge unsichtbar bleiben und robust gegen das Hinzufügen von Rauschen, nicht-linearen Transformationen in Grauwerten, wie z. B. Gammakorrekturen und Helligkeitsveränderungen sind.

Im Zusammenhang mit Verfahren in der "transform domain" spricht man auch von multiplikativen Verfahren (vgl. S. 148 [Pan04]).

Least Significant Bit Hiding im Bildbereich

Das Verstecken von Information in den niederwertigsten Informationsträgern in Bildern lässt sich mit den folgenden Worten erklären (S. 1020 [Cha01]): "Here you embed the message into the least significant bit plane of the image. Since this will only effect each pixel by ± 1, if at all, it is generally assumed with good reason that the degradation caused by this embedding process would be perceptually transparent." Demnach wird bei diesem einfachen Ansatz die Information in die niederwertigsten Bits der Bildinformation des Trägermaterials eingebracht. Da die Veränderung dieses Datenteils nur eine geringfügige Änderung der Ursprungsinformation zur Folge hat (Pixelwerte werden um ± 1 verändert), kann auf diese Weise eingebrachte steganographische Information durch die menschlichen Sinne kaum wahrgenommen werden.

Mit steigender Bitzahl, die zum Verstecken herangezogen wird, nimmt die Qualität des Hostbildes ab (vgl. S. 13 [Cum04]). Zur Verdeutlichung werden Beispielgrafiken, wie in Abbildung 4.8 dargestellt, gezeigt. Die Tabellen 4.1 und 4.2 zeigen die zum Verstecken notwendigen Bitoperationen.

Diese werden von den Teilnehmern der Lehrveranstaltung im Rahmen einer Projektarbeit in die Praxis umgesetzt:

- Verwendung der jeweils höchstwertigen Bits vom Trägerbild und vom zu versteckenden Bild.
- Ersetzen der niederwertigsten Bits im Trägerbild durch die hochwertigsten Bits des zu versteckenden Bildes (Embedding Process).
- Wiederherstellen des versteckten Bildes durch Extraktion der niederwertigsten Bits im Stegoobjekt und verwenden dieser als höchstwertige Bits (Extraction Process).

Host Pixel:	10110001
Secret Pixel:	00111111
New Image Pixel:	10110011

Tabelle 4.1: Einbringen der Information bei LSB

Host Pixel:	10110011
Bits used:	4
New Image Pixel:	00110000

Tabelle 4.2: Extrahieren der versteckten Information bei LSB

Abbildung 4.8 stellt die Qualität von Stegoobjekt dem extrahierten versteckten Bild gegenüber. Während bei 7 verwendeten Bits die versteckte Information in guter Qualität wiederhergestellt werden kann, scheint diese im Stegoobjekt bereits, für das menschliche Auge sichtbar, durch. Werden weniger Bits zur Einbettung der zu versteckenden Information herangezogen, so nimmt die Bildqualität der geheimen Nachricht ab, sie kann schlechter wiederhergestellt werden und das Stegoobjekt gleicht eher der Trägernachricht. Im Falle von unkomprimiert vorliegenden Rastergrafiken nimmt die Zahl der darstellbaren Farben der geheimen Nachricht mit den zur Einbettung verwendeten Bits, und damit auch deren Bildqualität, zu. Die Beispiele sind an die aus (vgl. S. 13 [Cum04]) entnommenen angelehnt.

Im Rahmen des Unterrichts wird eines der LSB-Verfahren im Bildraum exemplarisch mit Hilfe von MATLAB ausprogrammiert. Die Beispielprogramme finden sich im Anhang A. Das Ergebnis dieser Übung zeigt die Gegenüberstellung des Fotomaterials[15] in Abbildung 4.8.

Steganographie im Frequenzraum

Analog zu der unter Punkt 4.5.3 vorgestellten Vorgangsweise eignen sich die Least Significant Bit Verfahren auch dazu, um im Frequenzbereich Information zu verstecken. Der Unterschied in der Vorgangsweise liegt darin, dass vor Einbringen der Information eine Transformation erfolgt. Beim verlustbehafteten JPEG-Verfahren erfolgt eine Transformation in den Frequenzbereich. Grundlage zum Verständnis dieses Ansatzes ist das Verständnis des Algorithmusses. Die Transformation in

[15] privat durch den Verfasser der vorliegenden Arbeit zur LV-Durchführung zur Verfügung gestellt

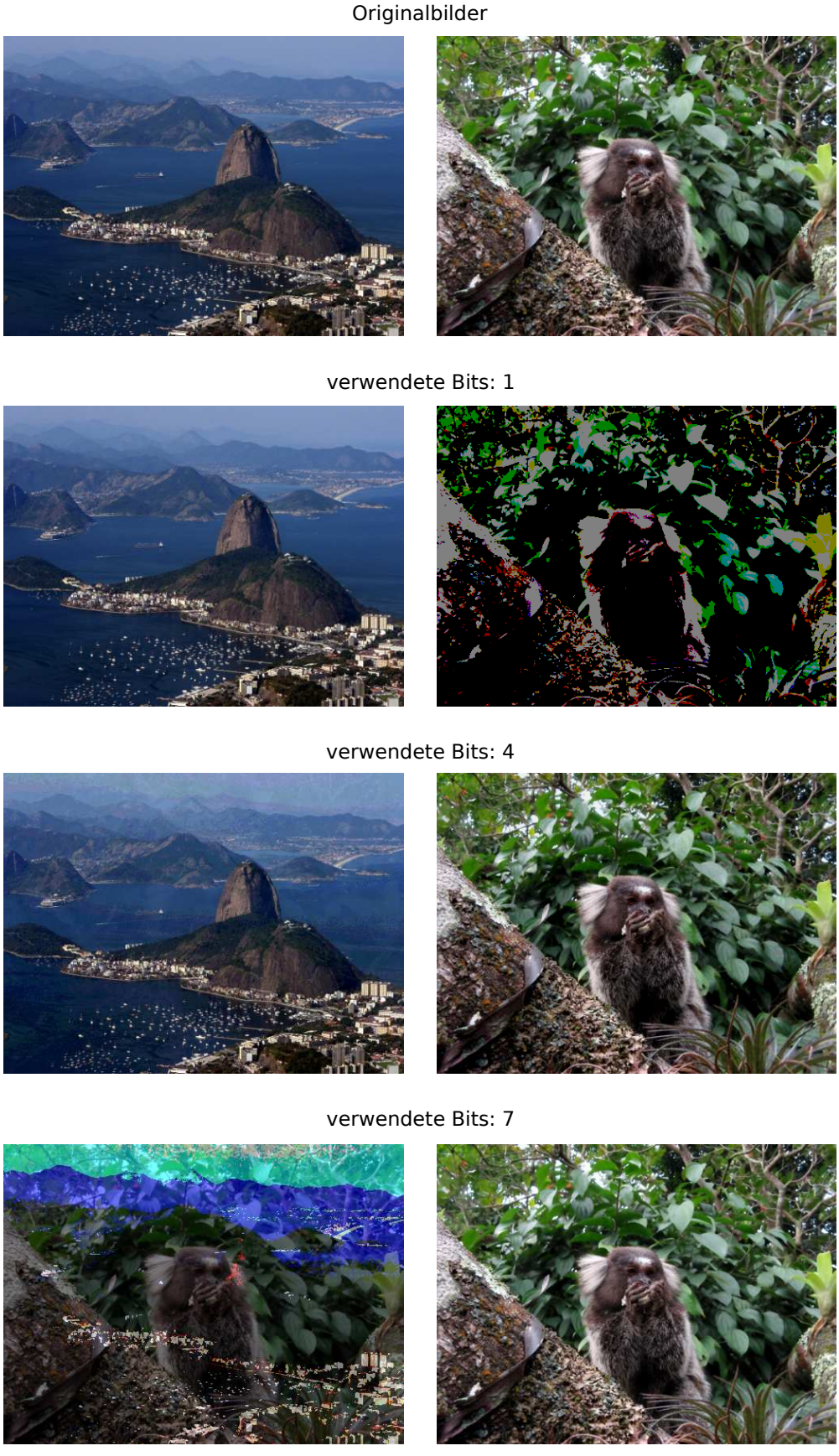

Abbildung 4.8: Auswirkungen der verwendeten Hostbits (vgl. S. 13 [Cum04])

den Frequenzraum lässt sich präziser erklären, als hier angeführt. Das JPEG-Verfahren ist jedoch im Kontext der Bildverarbeitung weit verbreitet und deshalb motivationsfördernd.

Die Kompression erfolgt in sechs Schritten:

1. Bei der Farbraumtransformation werden im Rot-Grün-Blau-Schema (RGB-Schema) gespeicherte Pixelwerte in einen Helligkeits- und zwei Farbkanäle aufgeteilt (vgl. [6]). Die Helligkeit wird in Fachliteratur auch oft als "Luminanz" bezeichnet. Bei den Farbanteilen spricht man von der "Chrominanz". Der resultierende Farbraum wird entsprechend der Abkürzungen "YCbCr"-Farbmodell genannt.
2. Tiefpassfilterung, Downsampling (verlustbehaftet) nach dem ersten Schritt. Die Farbraum-Transformation nutzt bestimmte Eigenschaften des menschlichen Auges aus (vgl. S. 4 [Han05a]). Einerseits können die menschlichen Sinne nur eine sehr begrenzte Anzahl an Helligkeitswerten unterscheiden und andererseits ist die Fähigkeit zur Unterscheidung ähnlicher Farbwerte benachbarter Pixel schlecht ausgeprägt. Demnach werden die Helligkeits- und Farbwerte von Pixeln in Blöcken zusammengefasst, die in weiterer Folge gemittelt werden.
3. Block splitting nach erfolgtem Downsampling und der Tiefpassfilterung. Hierbei werden die Pixel des Bilder zu Blöcken von je 8x8 Pixeln zusammengefasst (vgl. S. 6 [Han05a]). Die Blockgröße wurde hierbei willkürlich gewählt.
4. Diskrete Kosinustransformation nutzt die Darstellung der Informationen im Frequenzraum. Dies ermöglicht eine weitere Speicherreduktion. Während die niederen Frequenzen die graduellen Änderungen über das gesamte Bild repräsentieren, stellen die hochfrequenten Anteile die Farbänderungen von Pixel zu Pixel dar. Diese decken sich mit den unter dem zweiten Punkt (Tiefpassfilterung, Downsampling) getroffenen Annahmen und ermöglichen eine weitere Reduktion nicht-wahrnehmbarer Daten. Diese diskrete Transformation in den Frequenzraum ist nicht verlustbehaftet.
5. Bei der Quantisierung (verlustbehaftet) wird eine elementweise Division durchgeführt. Grundlage für die Divsion ist die Wahl eines geeigneten Divisors zur Elimination der hochfrequenten Anteile. Dieser Schritt ist verlustbehaftet. Die durch die menschlichen Sinne nicht-wahrnehmbaren Anteile werden unwiederbringlich weggeschnitten.
6. Im letzten Schritt, der Entropieenkodierung, werden die durch die Quantisierung ermittelten Koeffizienten umgeordnet. Die hier zum Einsatz kommenden Verfahren sind die RLE (run-length encoding)- und die Huffman-Codierung. Diese Verfahren komprimieren die visuellen Daten verlustlos.

Verlustbehaftete Operationen verändern die das Bild repräsentierende Information auf unumkehrbare Weise. Da hierbei auch davon ausgegangen werden muss, dass die Bereiche, in denen die Information eingebracht wurde, modifiziert wurden, eignen sich nur Schritte nach den verlustbehafteten zum Einbringen von geheimer Information.

Exemplarisch wird im Unterricht das unter (vgl. [8]) auffindbare Projekt "`JSTEG`" vorgestellt. Hier werden steganographische Daten in die niederwertigsten Bits der quantisierten Koeffizienten einge-

bettet (nach Schritt 5 in der oben angeführten Beschreibung). Abbildung 4.9 zeigt die Zusammenhänge. Die verschiedenen Teile des in der `README`-Datei beschriebenen Protokolls werden in der Grafik durch unterschiedliche Farben dargestellt. Das erste Feld ist fünf Bits lang und beschreibt die Länge, das zweite Feld, des Längenfelds, welches wiederum die Länge der eingebetteten Daten in Bytes beschreibt und das dritte Feld darstellt. Dieses Verfahren kann aufgrund der Änderung der niederwertigsten Bits der DCT-Koeffizienten als LSB-Hiding im Frequenzraum betrachtet werden.

Image without anything Quantized DCT coefficients	Image with text hidden Quantized DCT coefficients	Image with text hidden Least Significant Bits of the quantized DCT coefficients
D6 69 13 05 03 15 F2 EB FF 04 01 00 FA FB F9 FF 06 02 FE FF 00 00 00 FF 01 03 02 01 01 FF 00 00 01 00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00	D6 69 12 05 03 15 F3 EA FE 04 01 00 FA FB F8 FE 06 03 FE FF 00 00 00 FE 01 02 03 01 01 FE 00 00 01 00 00 00 00 00 00 00 00 FE FF 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00	00 01 00 01 01 01 01 00 00 00 01 00 00 01 00 00 00 01 00 01 00 00 00 00 01 00 01 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00

Abbildung 4.9: Modifikation der quantisierten DCT-Koeffizienten durch `JSTEG` [6, vgl.]

4.5.4 Steganographie in auditiven Medien

Steganographie mittels auditiver Medien stellt eine größere Herausforderung dar, als Steganographie im Umfeld der visuellen Medien. Dies lässt sich auf den größeren dynamischen Bereich des menschlichen Gehörsinnes (in englischsprachiger Literatur auch als "HAS", "Human Auditive System" bezeichnet) zurückführen (vgl. S. 11 [Cve04]). Das Leistungsspektrum des menschlichen Gehörsinnes beträgt 10^9 : 1 und das Frequenzspektrum 10^3 : 1. Die Empfindlichkeit gegenüber Gauss'schem Rauschen bezogen auf Umgebungsniveau beträgt $70dB$ (vgl. S. 28 [Ben96]). Weiters weißt das menschliche Gehör einen niedrigen differentiellen Bereich auf. Laute Geräusche blenden leise Geräusche aus, im Extremfall ignoriert der Sinn aus Gewohnheit bestimmte Geräusche und Einflüsse (vgl. S. 26 [Pop98]).

Die Digitalisierung von analogen, auditiven Medien stellt im Wesentlichen eine Reduktion der unendlichen Auflösung des analog vorliegenden Signals auf eine durch Computersysteme verarbeitbare endliche Zahl an endlichen, konkreten Zahlenwerten je Zeiteinheit. Analogsignale sind Zeit- und Wertkontinuierlich, Digitalsignale hingegen sind Zeit- und Wertdiskret. Der Umwandlungsprozess erfolgt in zwei bzw. drei Schritten (vgl. S. 5ff [Bur04]):

1. Unter Sampling versteht man das Abtasten eines zeitkontinuierlich vorliegenden Signales. Die Häufigkeit, mit der die Messwertnahme erfolgt, wird Samplingrate (Abtastrate) genannt. Die Abtastung muss mit mindestens der doppelten Frequenz, wie die höchstmöglich, auftretende erfolgen. Man nennt dies die Nyquist Rate.

2. Durch die Quanitisierung wird die digitale Repräsentation ermittelt. liegt das durch die Samples repräsentierte zeitdiskrete Signal vor, so müssen diese noch durch eine geeignete Zahl an Bits repräsentiert werden. Diese Diskretisierung kann mit der Farbtiefe eines aus Pixeln aufgebauten Bildes vergleichen werden. Wurde die Bitzahl zu niedrig gewählt, so kommt es zum sogenannten Quantisierungsrauschen.
3. Durch (optionale) Komprimierung kommen hier diverse verlustlose und mit Verlusten behaftete Verfahren zum Einsatz. Im Zusammenhang sei beispielsweise die μ-Law Kodierung erwähnt (vgl. S. 1ff [Yen93]). Bei dieser werden Samples mit einer Länge von 14 Bits auf 8 Bits reduziert. Aber auch komplexere Verfahren, die mit der Aufteilung des Audiosignals in Subbänder arbeiten, können zum Einsatz kommen (vgl. [39]).

Die Schritte 1 und 2 können in beliebiger Reihenfolge stattfinden. Typische Samplingraten sind 11.025kHz, 22.05kHz und 44.1kHz. Audio CDs weißen Samples mit einer Tiefe von 16 Bits je Kanal auf. Bei digitaler Telefonie ist eine Tiefe von 8 Bits pro Kanal üblich.

LSB-Hiding

Bei diesem Verfahren wird die zu versteckende Information in den niederwertigsten Bits der Samples versteckt. Die zu versteckende Information wird nach geheimer zeitlicher Abfolge in einen Audiodatenstrom eingebracht. Je nach gewünschter Sicherheitsstufe besteht auch die Möglichkeit, die zu versteckende Information durch Bitsequenzen darzustellen, die wiederum an geheimen Positionen in das Trägermaterial eingebracht werden. Hinsichtlich der Robustheit bedeutet dies eine Steigerung, quantitativ geht diese Verbesserung jedoch mit einer Reduktion der erreichbaren Datenrate einher.

Fragen an die Studierenden: Wie hoch ist die erreichbare, technische Datenrate? Wodurch wird die erreichbare Kapazität durch das HAS eingeschränkt? Und worin liegen die Vor- bzw. Nachteile des Verfahrens?

Phasenkodierung

Bei diesem Verfahren wird das bereits vorliegende Audiosignal in Segmente zerlegt (vgl. S. 325 [Ben96]). Die geheimen, zu versteckenden Daten spiegeln sich in der Phase des ersten Segments wider. Die Phasen der folgenden Segmente werden entsprechend dem veränderten Phasenverlaufes des ersten Segmentes angepasst. Dieses Verfahren ist bei kleinen Änderungen im Phasenverlauf durch die menschlichen kaum wahrnehmbar, wenn die Phasenrelationen zwischen den Frequenzanteilen zu sehr verändert werden, kommt es zu einer Phasenstreuung.

Spread Spectrum

Mehrere Spread Spectrum Verfahren lassen sich klassifizieren (vgl. [46]). Im Zusammenhang mit digitaler Steganographie wird ausschließlich auf das DSSS (Direct Sequence Spread Spectrum)

eingegangen (vgl. S. 326 [Ben96]). Bei diesem Verfahren dem Trägermaterial eine pseudozufällige Sequenz von Chips hinzugefügt. Diese weißt Rauschcharakter auf. Die eingebetteten Daten spiegeln sich dann in der Phase des modulierten Signals wider. DSSS setzt bi-phase shift keying, weil die Phase wechselt, wann immer der Wert des modulierten Signals wechselt.

Echo Hiding

Dieses Verfahren wird analytisch in (vgl. S. 4ff [Dan96]) erläutert. Bei Echo Hiding kann das eingebettete Signal anhand von drei Parametern beschrieben werden. In Abbildung 4.10 werden diese Verfahrensparameter graphisch dargestellt:

- ursprüngliche Amplitude (initial amplitude),
- Dämpfung (decay rate) und
- Versatz (offset).

Verringert sich der zeitliche Abstand zwischen Original und Echo, so überlappen sich die beiden Signale. Ab einem bestimmten Punkt kann das menschliche Ohr nicht mehr zwischen Original und Echo unterscheiden. Die Verschmelzung geschieht bei einem Abstand von ca. $1ms$ (vgl. S. 327ff [Ben96]). Der Kodierer setzt zwei verschiedene Verzögerungszeiten (Versatz) um binäre Einsen und Nullen zu kodieren. Alle Parameter werden so gewählt, dass das resultierende Signal durch die menschlichen Sinne nicht wahrgenommen werden kann.

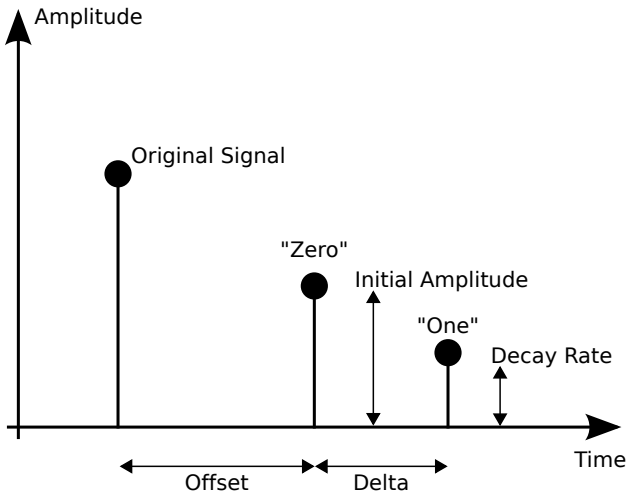

Abbildung 4.10: Parameter beim Echo Hiding [Ben96, vgl.]

4.5.5 Steganographische Angriffe auf versteckte Daten

Mit dem Verstecken von Daten geht eine Modifikation und u.U. auch Verschlechterung des Trägermaterials einher. Die Charakteristika dieser Veränderungen können oftmals als Signaturen für eingebettete Nachrichten gedeutet werden (vgl. S. 5 [Nei98]). Attacken auf steganographisches Material können mehrere Formen annehmen:

- Feststellung einer Einbettung,
- Extrahierung der eingebetteten Daten,
- Verhindern der Einbettung und
- Zerstören der eingebetteten Daten.

Während (vgl. S. [S. 01]) die Verfahren nach den Kategorien Beseitigungsattacken, Geometrieattacken, Kryptographische Attacken und Protokollattacken klassifiziert, teilt (vgl. S. 41 [Jah02]) die steganographichen Attacken in nur zwei Gruppen ein:

- Freundliche Attacken werden bewusst durch den Kunden durchgeführt. Zu ihnen zählen geometrische Transformationen, Ausschnittbildung, verlustbehaftete Datenkompression, Formatkonvertierungen, A/D- und D/A-Wandlungen.
- Feindliche Attacken zielen direkt darauf ab, Wasserzeichen zu zerstören. Zu ihnen zählen Tiefpassfilter, Addition von Rauschanteilen, Formatänderungen durch Weglassen von Zeilen, Spalten und Frames, Mehrfachmarkeriung mit verschiedenen Wasserzeichen.

Weitere feindliche Attacken lassen sich ausführen (vgl. S. 223ff [Fab98]):

- Bei "The Jitter Attack" wird ausgehend von einer gezielten Zerstörung von in den niederwertigen Bits versteckten Geheimbotschaften dem Medium "Jitter" in Form von Fluktuation hinzugefügt. Bezogen auf auditive Daten bedeutet dies ein bewusstes Auslassen und/oder Vervielfachen von Samples im Datenstrom. Bei visuellen Medien werden aus Pixelmatrizen Zeilen und/oder Spalten entfernt oder hinzugefügt. Weißt ein Algorithmus keine ausreichende Kapazität oder Synchronisierung auf, so wird auf diese Weise die Wasserzeicheninformation zerstört.
- Bei "StirMark" handelt es sich um ein geometrisches Verfahren. Es ist aus Überlegungen, einfache geometrische Verfahren zu kombinieren entstanden: Rotation, Resampling, Resizing, verlustbehaftete Komprimierung, etc. Die gemeinsame Anwendung dieser Möglichkeiten bringt die selben Fehler in das Material ein, wie jene, die beim Drucken mit einem hochwertigen Drucker mit anschließendem Scannen auftreten würden. Obwohl dieses Verfahren bei einfacher Anwendung durch die mennschlichen Sinne nahezu nicht-wahrnehmbar ist, konnten die meisten Copyright-Markierungssyteme umgangen werden (vgl. S. 226 [Fab98]).
- "The Mosaic Attack" wird zu den "Präsentations-Attacken" gezählt. Bei diesen Attacken besteht der Angriff in einer alternativen Darstellungsform. Bevor die Ursprungsinformation wiederhergestellt ist müssen ein oder mehrere Zwischenschritte durchgeführt werden. So ist trotz der Entfernung des in das Bild eingebrachten Wasserzeichens ist eine pixelgenaue Anzeige möglich. Das Bild wird vor dessen Nutzung in Teilbereiche zerschnitten, um anschließend vom Browser wieder zusammengefügt zu werden. Auf diese Weise wird das automatisierte Durchsuchen des World Wide Webs durch sogenannte "crawler" erschwert.
- Bei "Attack on Echo Hiding" wird analog zu den in 4.5.4 gegebenen Einbettungsschritten das Echo entfernt, in dem, basierend auf der Kenntnis der Parameter, die Faltungsformel umgekehrt wird. Da aber i. R. dem Angreifer die Echo-Parameter nicht bekannt sind, muss auf

ein Verfahren namens "Bilnd echo cancellation" zurückgegriffen werden (vgl. S. 229 [Fab98]). Dabei wird das Cepstrum des Signals analysiert und eine "brute force" Suche nach den passenden Parametern durchgefürt.

Weiters wird auf statistische Angriffe eingegangen (vgl. S. 8ff [And00]). Namentlich sei an dieser Stelle besonders der Chi-Quadrat-Test hervorzuheben: Der Test wird auf sogenannte POV (Pair-of-Values) angewandt. Ist die Verteilung der Elemente der POVs gleichverteilt, so kann mit einer hohen Wahrcheinlichkeit davon ausgegangen werden, dass Daten eingebettet wurden. Voraussetzung hierfür ist jedoch, dass die eingebetteten Daten ebenfalls einer zufälligen Verteilung unterliegen. Bei Text ist das i. R. der Fall.

4.6 Block 6: Trusted Computing

Dieses Kapitel beschäftigt sich mit Computersystemen, die sich durch eine vertrauenswürdige Programmausführung auszeichnen.

4.6.1 Definitionen, Terminologie

Trustworthiness Der mit "Vertrauenswürdigkeit" ins Deutsche übersetzte Begriff lässt sich mit "that something is worthy of being trusted" übersetzen (S. 3 [42]). Eine weitere Definition nach Peter G. Neumann lässt sich erwähnen (S. 9 [16]): "An object is trustworthy if and only if it is proven to operate as expected." Die Vertrauenswürdigkeit wird in diesem Fall also an der Vorhersehbarkeit des Verhaltens während der Ausführung aufgehängt.

Trust wird an der selben Stelle im Kontext des "trusted computings" definiert als (S. 3 [42]): "Trust merely implies that you trust something whether it is trustworthy or not, perhaps because you have no alternative, or because you are naiv or perhaps because you do not even realize that trustworthiness is necessary, or because of some other reason." Wieder liefert die von William A. Arbaugh erstellte Präsentation eine weitere Definition nach Peter G. Neumann: "An object is trusted if and only if it operates as expected."

Frage an die Studierenden: Woher ist der Name "Neumann" bekannt?

"John von Neumann" ist in der Informationstechnologie der Entwickler der "von Neumann"- Architektur. Sie steht nicht im unmittelbaren Zusammenhang mit der Thematik des Digital Rights Managements. Die Architektur bildet auch heute noch die Grundlage der meisten Computer, wie z. B. Workstations, Laptops, Supercomputer und Personal Computer. Die CPU (Central Processing Unit) besteht aus der Kontrolleinheit, sowie aus der arithmetischen und logischen Einheit. Sie interagiert mit dem Speicher und einem I/O-System (Input/Output) und führt Instruktionen aus,

die den Speicher verändern und Ein- bzw. Ausgabeoperationen zur Folge haben. Daten und Instruktionen werden bei der "von Neumann"-Architektur im selben Speicher abgelegt (vgl. S. 2-3 [EL98]).

Generell kann die Aussage getroffen werden, dass man von Trusted Computing spricht, wenn sich ein Computer verhält, wie erwartet (vgl. [16]). Befürworter der Technologie legen diese Aussage nun so aus, dass sich das System genau nach Benutzerwunsch verhält. Gegner der Technologie hingegen legen die Aussage in der Hinsicht aus, dass sich die Computersysteme entsprechend den Vorgaben der Hersteller verhalten.

(vgl. S. 39ff [Hoh06]) definiert die Ziele des Trusted Computings neben der integeren Ausführung eines Programms in der Bezeugung dieser integeren Ausführung. Um diese Ziele zu erreichen, werden zurzeit zusätzliche Bausteine verwendet, die auch Vertrauensanker genannt werden. Sie sind sowohl durch Software, als auch durch physikalische Eingriffe nicht änderbar. Eine Vertrauensbeziehung zwischen Anbieter und Nutzer muss dabei nicht vorliegen. Diese Beziehung wird durch zusätzliche Technik und in das Vertrauen der korrekten Funktionsweise dieser gesetzt. Dem referenzierten Dokument zu Folge bleibt jedoch zu bemerken, dass durch den ausschließlichen Einsatz von Trusted Computing Hardware nicht auch automatisch eine Erhöhung der Sicherheit und der Vertraulichkeit gegeben ist. Diese Aussage stützt sich auf dem Unentscheidbarkeitstheorem. Das Theorem wiederum besagt, dass es in der Informatik keine allgemeingültige Methode gibt, um unerwünschten Code aufzufinden.

Verschiedene Aspekte des Trusted Computings werden kritisiert (vgl. S. 1ff [Eri03]), (vgl. S. 1ff [Ros03]), (vgl. [21]), (vgl. S. [Chr05]), (vgl. S. 6ff [48]) und (vgl. S. 1ff [Arb02]):

- Die Produktbindung, bei der Produkte voneinander abhängig gemacht werden. Anwendungen und deren generierte Daten sind nicht mehr austauschbar, Lizenzen können wirklich an einzelnen Maschinen gebunden werden.
- Der Verlust der Kontrolle resultiert darin, dass Benutzer zusehends die Kontrolle über ihre Daten verlieren, da diese an bestimmte Hardware, beispielsweise einen "Security Chip", gebunden werden können. Diese Vorkehrungen werden durch die TPM Spezifikation im Migrationsbereich vorgeschrieben.
- Verlust der Anonymität durch die eindeutige Zuordnung zwischen PC und dessen Besitzer. Durch Anfragen, die von modifizierter Hard- und Software durchgeführt werden, können Rückschlüsse angestellt werden. Beispielsweise ist es möglich als Softwarehersteller auf diese Weise Einsichten in das Verhalten bei der Nutzung des Internets zu erlangen. Dieses Problem kann durch eine dritte "Stelle" umgangen werden: der Benutzer wird bei dieser Authentifiziert, und in weiterer Folge bestätigt diese dem Diensteanbieter, dass der Dienstanforderer der ist, für den er sich ausgibt, ohne dessen Identität preiszugeben.
- Praktische Anwendbarkeit, da zusätzliche Hard- und Software zusätzliche Fehlerquellen bieten. Außerdem können diese Teile oft ersetzt oder ... werden. Im schlimmsten Fall kann der Zugriff beispielsweise aufgrund von Verschlüsselung auf Dokumente verwehrt werden.

- Die Interoperabilität, denn technische Spezifikationen der TCG (Trusted Computing Group) müssen von allen Herstellern eingehalten werden. Missinterpretationen oder offen gelassene Teilspezifikationen können unterschiedlich ausgelegt werden und bei der Interpretation, sowie beim Austausch von Daten zu Problemen führen.

Mancherseits hingegen wird die Technologie des Trusted Computings befürwortet (vgl. S. 20ff [Pic05]), (vgl. S. 85ff [Fra05]): Größere Sicherheit im Internet: "Remote Attestation" ermöglicht die eindeutige Identifizierung von Personen im Internet

4.6.2 Architekturerweiterungen

Seth Schoen geht in seiner Publikation auf die Architekturerweiterungen beim Trusted Computing ein (vgl. S. 3ff [48]).

"Memory curtaining" bezieht sich demnach auf eine durch Hardware erzwungene Speicherisolierung, die verhindert, dass Programme Speicherbereiche anderer Programme modifizieren. Moderne Betriebssysteme unterstützen dieses Merkmal auf Basis entsprechend programmierter Treiber für den Speicherzugriff. Durch den hardwaremäßigen Schutz hat nicht einmal das Betriebssystem Zugriff auf die gesperrten Bereiche. "Secure I/O" handelt von sicheren Übertragungswegen für Ein- und Ausgabegeräte, die an Computersysteme angeschlossen sind. Dadurch kann der erfolgreiche Einsatz von "Keyloggern" oder "Screen-Grabbern", die die Aktivitäten des Benutzers ausspionieren, unterbunden werden. Unter "sealed storage" versteht man das sichere Speichern kryptografischer Informationen. Dazu zählt auch Schlüsselmaterial, das zur Entschlüsselung von einzelnen Datenbereichen auf Computersystemen herangezogen wird. Anderen Programmen als jenes, das die Veschlüsselung vorgenommen hat, wird der Zugriff auf diese veschlüsselten Bereich verwehrt. Die Information zum Ver- und Entschlüsseln wird dabei an die Software, mit der Dokumente erstellt werden, gebunden. "Remote attestation" wird als die innovativste Erungenschaft des Trusted Computings gepriesen. Unauthorisierte Änderungen an Software werden dabei entdeckt und in weiterer Folge verhindert. Diensteanbieter können so die Versorgung von kompromittierten Systemen mit Daten verweigern. Identitäten werden bei der "remote attestation" durch kryptographische Zertifikate unterschieden.

Die Systemarchitektur für ein vertrauenswürdiges System besteht (vgl. S. 7 [Han05b]) und (vgl. S. 42ff [Hoh06]) zu Folge im wesentlichen aus drei Elementen:

- Der CRTM (Core Root of Trust for Measurement) stellt den Grundpfeiler des Subsystems, welches durch die TGC (Core Root of Trust for Measurement) spezifiziert wurde, dar. Es bietet initiale Messmethoden zur Aufzeichnung der Plattformkonfiguration. Diese spielt bei der Attestierung des Systemzustandes eine entscheidende Rolle. Auf sie wird in Kapitel 4.6.4 eingegangen.
- Das TPM (Trusted Platform Module) stellt als zentrale Komponente von Computersystemen mit Unterstützung für Trusted Computing einen passiven Baustein dar, der nicht aktiv in die Vorgänge des Systems eingreifen oder diese blockieren kann. Die Art der Nutzung

dieser zusätzlichen Hardware obliegt in erster Linie der Software. Das Modul wird durch den sogenannten "LPC"-Bus (Low-Pin Count) realisiert. Die Interna dieses Bausteins sind fest programmiert und daher auch nicht nachträglich änderbar. Gegenwärtig wird er auf die Hauptplane von Computersystemen verlötet. Zukünftig wird das TPM in der Hauptplatine oder direkt im Prozessor untergebracht sein.

- Durch den TSS (Trusted Software Stack) erfolgt die softwareseitige Enbettung des TPMs in das Computersystem nach der TCP Spezifikation unter diesem Titel. Ziel dieses Teils ist es, die technische Sicht auf das TPM zu verbergen und den Anwendungen einfache Schnittstellen und Dienste anzubieten. Der Stack lässt sich in vier Schichten unterteilen, wobei die oberen Schichten unabhängig von der Realisierung des TPMs eine einheitliche Schnittstelle für die Funktionalität bieten soll.

4.6.3 Trusted Computing Group

Das von der im Jahr 1999 von den IT-Konzernen HP, IBM, Intel, Microsoft und Compaq gegründete TCPA (Trusted Computing Platform Alliance) definierte Ziel war der Zusammenschluss zur Verringerung von IT-Sicherheitsproblemen bei Computersytemen (vgl. S. 41ff [Hoh06]). Durch sie wurden die Spezifikationen 1.0 und 1.1 für hardwarebasierte Sicherheitserweiterungen für Personalcomputer veröffentlicht. 2003 wurde aufgrund der unflexiblen Satzung für Mitglieder der TCPA die Allianz. B. endet. Die Unternehmen AMD, HP, IBM, Intel und Microsoft gründeten als Nachfolger die TCG (Trusted Computing Group), die die Spezifikationen der TCP erweitert und ergänzt. Die Mitglieder der TCG lassen sich der referenzierten Publikation zu Folge in drei Gruppen einteilen:

1. fördernde Unternehmen (Protomoters): sind Mitglieder, die die Spezifikationen vorantreiben und volle Stimmrechte besitzen. Bekannte Vertreter dieser Gruppe sind die Unternehmen Sun, Sony, Microsoft, HP und Intel
2. mitgestaltende Unternehmen (Contributors): sind Mitglieder, die zur Spezifizierung beitragen und im Rahmen von Arbeitsgruppen Einfluss ausüben können. Entwurfsdokumente zukünftiger Spezifikationen können durch diese Teilnehmer eingesehen werden.
3. anwendende Unternehmen (Adopters): sind Mitglieder, die die Spezifikationen umsetzen. Sie haben im Rahmen ihrer Mitgliedschaft keine Möglichkeit zur Einflussnahme.

4.6.4 Trusted Platform Module

Das TPM ist ein passiver Baustein, der über den LPC-Bus mit dem restlichen Computersystem verbunden ist (vgl. S. 43ff [Hoh06]). Abbildung 4.11 zeigt dies in einer schematischen Ansicht. Weiters handelt es sich bei dieser Hardware um einen fest programmierten Baustein, dessen Funktionsweise nach der Herstellung nicht mehr modifiziert werden kann. Der Zugriff auf die Interna des Chips erfolgt über im Vorhinein definierte Schnittstellen.

Die Aufgaben des Trusted Platform Moduls lassen sich wie folgt zusammenfassen (vgl. S. 7-8 [Han05b]):

- Sicherer Speicher lässt sich in persistente und nichtpersistente Speicherbereiche unterteilen. Ein direkter Zugriff auf diese ist nicht möglich. Im nichtänderbaren Speicherbereich liegen Schlüssel und Zertifikate, die belegen, dass sich die Hardware des Computersystems bei der Herstellung in einem definierten, vertrauenswürdigen Zustand befanden. Als wichtigster Schlüssel sei an dieser Stelle der "Endorsement Schlüssel" genannt, welcher dem TPM eindeutig zugeordnet werden kann. Die Zertifikate, beispielsweise das "Plattform Zertifikat", bestätigen die Hersteller die ordnungsgemäße Herstellung von TC Komponenten, sowie die korrekte Zuordnung zwischen den TC Komponenten mit den Komponenten des Computersystems.
- Kryptografische Verfahren werden zum Nachweis der Integritätsprüfungen gegenüber Außenstehenden angewendet. Zum Einsatz kommen die klassischen kryptographischen Verfahren und werden im Modul integriert, um resistent gegenüber mutwillige Beeinflussung des Verfahrens selbst zu sein.
- Attestierung des Systemzustandes bedeutet das Nachaußentragen des Systemzustands in Form der PCRs (Platform Configuration Register). Mit Hilfe von Zertifikaten werden die PCRs digital siginiert, um die Echtheit der Inhalte dieser Register zu bestätigen.
- Ausstellung eines Attestation Identity Key, denn die TPM Identitäten bilden die Grundlage für den Attestierungsprozess. Die Beglaubigung für eni im TPM erzeugtes Schlüsselpaar stellt dabei das AIK (Attestation Identity Key) Zertifikat dar.
- Vertrauenswürdige Integritätsmessung erfolgt durch den CRTM

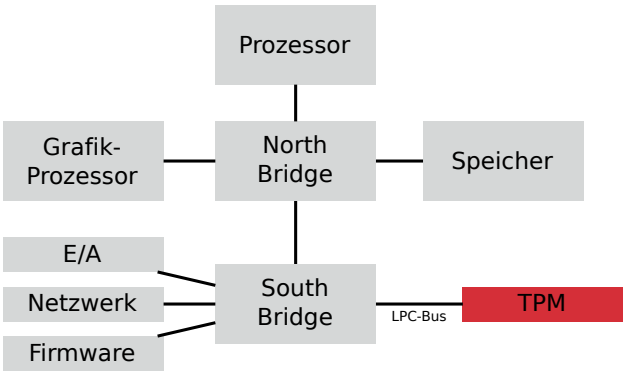

Abbildung 4.11: Einbindung des TPMs in ein PC-System [Hoh06, vgl. S. 43]

In Abbildung 4.12 werden die Komponenten in einem Trusted Platform Module gezeigt. Sie ergeben sich direkt aus den oben angeführten Aufgaben und werden an dieser Stelle aufgezählt (vgl. S. 44ff [Hoh06]):

- Zufallszahlengenerator für sichere Zufallszahlen als Quelle zur Schlüsselerzeugung,
- Schlüsselgenerator für asymmetrische Schlüsselpaare,
- asymmetrische Verschlüsselungseinheit zur Verschlüsselung und Signierung nach dem RSA-Algorithmus bei einer Schlüssellänge bis 2048 Bit,
- symmetrische Verschlüsselungseinheit, die jedoch nur modulintern verwendet wird,

- Hashberechnungseinheit nach dem SHA-1-Algorithmus und
- Authentifizierungseinheit zur Authentifizierung von Nachrichten von und zum TP Modul, basierend auf dem HMAC-Verfahren.

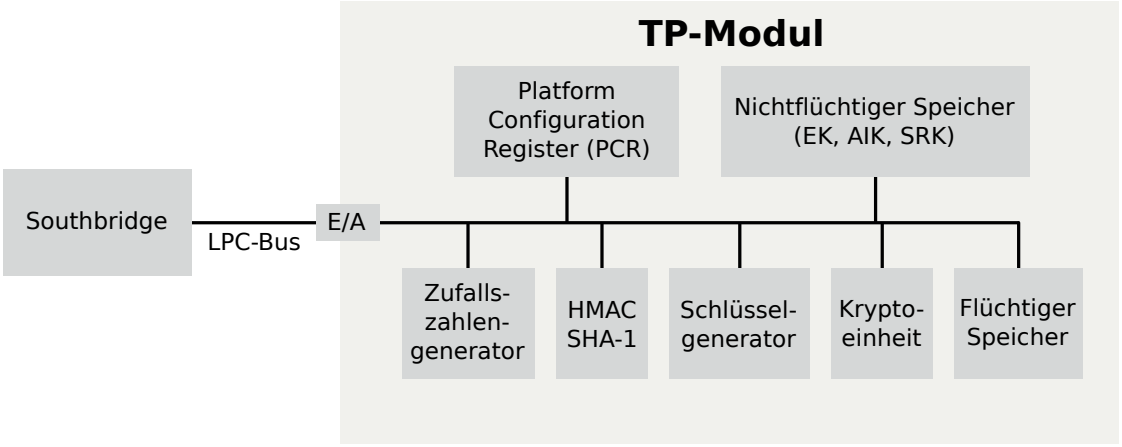

Abbildung 4.12: Komponenten des TPMs [Hoh06, vgl. S. 46]

4.6.5 Anwendungen für Trusted Computing

Für Trusted Computing ergeben sich mehrere Anwendungsfälle (vgl. S. 120 [Dol06]). Diese werden im Folgenden ausgeführt.

Sicheres Booten Dieser Vorgang lässt sich anhand der zuvor referenzierten Publikation in drei Teilbereiche untergliedern:

- Bei Trusted Boot überprüft das Sicherheitsmodul die relevanten Systemkomponenten lediglich; das startende System wird analysiert und gemessen, zusammengefasst kann diese Tätigkeit im Begriff des "Monitoring".
- Secure Boot erweitert den "Trusted Boot" um zusätzliche Aktionen, falls der gemessene Ist-Wert und der erwartete Referenzwert differieren. Beispielsweise kann das Starten des Betriebssystems unterbrochen oder eine Fehlermeldung auf der Konsole ausgegeben werden.
- Authenticated Boot erweitert wiederum den "Secure Boot" um mehrere Szenarien als bloßes "falsch" oder "richtig". Je nach vorliegenden Werten in den Plattformkonfigurationsregistern wird entschieden, wie weiter zu verfahren ist

Bislang gibt es nur wenig praxistaugliche Implementierungen, da die Konzepte nur äußerst schwierig umsetzbar sind.

Eng mit der Thematik verbunden ist das von Ferguson (vgl. S. 3 [Fer06]) untersuchte System zur Festplatten- und Partitionsverschlüsselung. Motivation zur Entwicklung war das Problem der "verlorengegangenen Laptops". In der Publikation ist von Raten in der Höhe von 1-2% pro Jahr die

Rede. Dem Sachwert der gestohlenen Hardware überwiegt meist der ideologische Wert der auf dem Gerät gespeicherten Dokumente.

Die Sicherheit des "BitLocker" Verfahrens liegt in der Verwendung des TPMs, vor allem der darin vorhandenen PCRs (Platform Configuration Register). Diese werden je nach gestarteter Software unterschiedlich initialisiert. Den Schlüssel zum Zugriff auf verschlüsselte Datenbereiche erhält man nur, indem die PCRs durch das Ausführen der zertifizierten Software entsprechend initialisiert wurden. Wird das System beispielsweise mit einer BootCD hochgefahren, so ist der Zugriff auf die verschlüsselten Datenbereiche verwehrt, da davon ausgegangen werden kann, dass das auf der CD enthaltene Betriebssystem vom am vorliegenden System installierten abweicht.

Verwendung als Schlüsselspeicher und Kryptomodul Der im Modul vorhandene Schlüsselspeicher kann auch herangezogen werden, um als Quelle für digitale Zertifikate dienen (vgl. [17]). Man spricht in diesem Zusammenhang von Cryptographic Service Providers (CSP), als welche die TPM-Chips fungieren.

4.6.6 Zugriff über den Software Stack der Trusted Computing Group

Der Zugriff auf die Funktionalität des TPMs erfolgt aus softwaretechnischer Sicht (vgl. [13]) zufolge mit Hilfe des TCG Software Stacks (TSS). Dies hat den Vorteil die technische Sicht auf das TPM zu verbergen und dem Anwender einfache Schnittstellen und Dienste zu bieten (vgl. S. 52ff [Hoh06]). Diese sind:

- TSP, der TSS Service Provider dessen Schnittstellen sind beispielsweise PKCS#11 und MSCAPI,
- TCS, die TSS Core Services, sie verwalten die Ressourcen beim Zugriff auf das TPM (z. B. simultane Zugriffe, Synchronisation längerer Befehlssequenzen),
- TDDL, die TPM Device Driver Library zur softwaremäßige Ansteuerung des TPMs über den TPM Device Driver, die darunterliegende Schicht; diese Schicht dient hauptsächlich zur Anpassung an die durch unterschiedliche Hersteller angebotene Realisierung,
- TDD, der TPM Device Driver bzw. die herstellerabhängige Ansteuerung des TPMs durch einen betriebssystemabhängigen Gerätetreiber.

Hinsichtlich der konkreten Implementierung kann der TDD (TPM Device Driver) im Kontext des Betriebssystems, die drei darüberliegenden Schichten (TDDL, TCS und TSP) können als Dienst abgebildet werden, die im Kontext eines Systemprozesses ablaufen.

Kapitel 5

Übungsteil der Lehrveranstaltung

Das Gruppenpuzzle bietet einen praxisorientierten Zugang zu den in der Lehrveranstaltung vorgestellten Inhalten. Diese Methodik des eigenständigen Wissenserwerbes wurde in Kapitel 3.2.4 beschrieben und hat den Vorteil, alle Beteiligten am Erfolg des Schlussergebnisses gleichermaßen teilhaben zu lassen.

Exemplarisches Beispiel für die Durchführung des Gruppenpuzzles liefert Martin Lehner in seinem Handbuch zur guten Lehre an Fachhochschulen ((vgl. S. 49 [Mar08]) und (vgl. S. 54 [Mar08])). Wie bereits in Kapitel 3.2.4 erwähnt, findet Vorab eine Aufteilung in Stammgruppen statt. Die Mitglieder dieser Stammgruppen werden zum Kompetenzerwerb in sogenannte Expertengruppen entsandt, um dort mit Mitgliedern aus den anderen Stammgruppen ein Spezialgebiet der Thematik, konkret dem Inhalt der Lehrveranstaltung, auszuarbeiten. Nach Durchführung der ersten Themenausarbeitung und der damit verbundenen Rückführung in die Stammgruppen zeichnet sich jedes Mitglied in diesen durch das Vorhandensein unterschiedlicher Kompetenzen im Kontext der Thematik der Lehrveranstaltung aus. Die in den Stammgruppen durchgeführten Tätigkeiten umfassen und erfordern alle durch die Expertengruppen abgedeckten Kompetenzen. Dadurch wird die Abhängigkeit des Erfolges des Schlussergebnisses von der Arbeit aller Gruppenmitgliedern begründet.

Die zuvor in Kapitel 4.1 getroffene Aufteilung des Softwareschutzes in technische, rechtliche und organisatorische Aspekte wird auf die Thematik des Digital Rights Managements (DRM) umgelegt und spiegelt sich in den zur Ausarbeitung angebotenen Themen in den Experten- und Stammgruppen wider. Grundsätzlich werden die Ausarbeitungen in Gruppen zu je vier Mitgliedern durchgeführt. Da zur Aufteilung nur drei Bereiche vorliegen und die Lehrveranstaltung in technischen Studiengängen durchgeführt wird (siehe dazu auch Kapitel 2 zur Unterrichtsplanung), entsenden die Stammgruppen zwei Mitglieder in Expertengruppen mit technischem Schwerpunkt und jeweils ein Mitglied in Expertengruppen mit organisatorischem bzw. rechtlichen Schwerpunkt.

Die Stammgruppen werden durch den Lehrbeauftragten der Lehrveranstaltung festgelegt. Dies soll die realen Bedingungen bei der Projektdurchführung widerspiegeln, da hier Projektteams oft willkürlich durch vorgesetzte Stellen zusammengestellt werden. Wer in die Expertengruppen

entsandt wird, wird individuell durch die Gruppen selbst bestimmt. In Absprache mit dem Lehrbeauftragten werden bei den Ausarbeitungen in den Expertengruppen auch von den Studierenden vorgeschlagene Themen zus Ausarbeitung akzeptiert, sofern diese sich mit den im Vorlesungsteil (siehe Kapitel 4) vorgestellten Lehrinhalten im Einklang befinden. Jede Gruppe kann sich für eines der angebotenen Themen entscheiden. Die vorgeschlagenen durch die Expertengruppen auszuarbeitenden Themen decken die drei zuvor erwähnten Aspekte ab:

- rechtlich, durch den Rahmen im österreichischen Urheberrecht,
- organisatorische Maßnahmen zum Schutz digitaler Inhalte und letztlich
- technisch, wobei sich diese wieder untergliedern lassen:
  - Diskrete Transformationen am Beispiel von Discrete Cosinus Transformation und Discrete Fourier Transformation,
  - Diskrete Transformationen am Beispiel der Discrete Wafelet Transformation,
  - Technischer Überblick aktueller DRM-Systeme,
  - Messung von Unterschieden in Grafiken,
  - Verfahrensanalyse zum Content Scrambling System und
  - Verfahrensanalyse zu Digital Video Broadcasting.

Nach den Ausarbeitungen in den Expertengruppen werden die Expertengruppenteilnehmer wieder in ihre Stammgruppen zurückgeholt. Als Ergebniss der in den Stammgruppen durchgeführten Arbeit wird je Gruppe wieder folgendes erwartet:

- eine Seminararbeit mit einem Umfang von ungefähr 15 Seiten; so verfasst, dass das Dokument durch die Zielgruppe verstanden wird und
- eine Präsentation der Ergebnisse mit einer Dauer von 10 Minuten; jedes Projektmitglied präsentiert seine Ausarbeitung. Das Konzept der Referate wird in 3.2.3 vorgestellt.

Die von den Stammgruppen ausgearbeiteten Themen sollen alle Aspekte des Digitale Rights Management (DRM) abhandeln. Leitfäden informieren Unternehmen oder öffentliche Einrichtungen, wie z. B. Schulen oder Bibliotheken über die zum Einsatz notwendigen Maßnahmen. Exemplarisch sollen hier der zeitliche und der finanzielle Aufwand abgeschätzt werden. Dazu ist es notwendig, im Vorfeld den Einsatzkontext (Unternehmensgröße, Medientypen) festzulegen. Dieser kann von den Gruppen frei gewählt werden, muss jedoch in der zu verfassenden Seminararbeit dokumentiert werden. Weiteres wird der Leser des Leitfadens über die Folgen durch den Einsatz der Technologie informiert.

Folgende Themen werden angeboten:

- Leitfaden zum Einsatz von DRM in Unternehmen,
- Leitfaden zum Einsatz von DRM in Schulen und Bibliotheken,
- Leitfaden zum Einsatz von “Trusted Computing” in Unternehmen und
- Leitfaden zum Einsatz von “Trusted Computing” in Schulen und Bibliotheken.

Die Ergebnisse der zweiten Ausarbeitung werden wieder in einer Seminararbeit festgehalten und in Form von Gruppenreferaten präsentiert.

Kapitel 6

Zusammenfassung und Ausblick

Im Folgenden werden die aus der konkreten Unterrichtsplanung erhobenen Erkenntnisse zusammengefasst, die in der Durchführung gewonnenen Erkenntnisse beschrieben und ein Ausblick auf mögliche Verbesserungen in der Durchführung der Lehrveranstaltung gegeben.

Im Übungsteil der Lehrveranstaltung wurde Augenmerkt auf die Gerechtigkeit bei der Arbeitsaufteilung bei den Gruppenarbeiten durch die Gruppenmitglieder gerichtet. Deswegen kommt es zum Einsatz des in Kapitel 3.2.4 vorgestellten Konzepts. Da sämtliche der nach der Ausarbeitung des Spezialthemas erworbenen Kompetenzen zur Ausarbeitung der Themen in den Stammgruppen unerlässlich sind, haben die sogenannten "Trittbrettfahrer" wenig Chancen, sich vor dem Beisteuern ihres Beitrages am Gesamtergebnis zu drücken. Dieser Umstand konnte auch in der durchgeführten Lehrveranstaltung beobachtet werden. Die Mitglieder der Stammgruppen werden erfahrungsgemäß am besten durch den Lehrbeauftragten ausgewählt. Dies hat den Vorteil, reale Projektumgebungen besser nachzubilden, denn auch hierbei ist die Gruppenbildung durch vorgesetzte Stellen möglich.

Die Technik des in Kapitel 3.2.1 vorgestellten Frontalvortrages zur Wissensvermittlung erwies sich im Vorlesungsteil der Lehrveranstaltung als äußerst effizient. Gemessen wurde der Erfolg mit Hilfe des in Kapitel 3.2.2 vorgestellten Konzepts der fragend-entwickelnden Methode. Zu Beginn der Lehrveranstaltung wurden die Lehrinhalte der vorangegangenen Lehreinheiten im Fach wiederholt. Diese Vorgangsweise spricht, und das kann als positiver Nebeneffekt gewertet werden, einmal mehr jene Studierende an, deren Wissenserwerb am effizientesten mit Hilfe auditiver Medien vonstattengeht. Beim Frontalvortrag wird der visuelle Lerntyp durch die Symbolisierung der Lehrinhalte durch Mindmaps. Die Eigenheiten dieser Methodik werden im Kapitel 3.2.5 abgehandelt.

Mathematische, sowie technische Verfahren wurden, soweit es der zeitliche Rahmen und die finanziellen Mittel des Studienganges zuliesen, in die Praxis umgesetzt. Konkret konnte dies mit dem Verstecken von geheimen Nachrichten in den niederwertigen Bits anderer Grafiken demonstriert werden. Das Beispiel wurde im Kapitel 4.5.3 vorgestellt und kommentiert, die Durchführung erfolgte in einem mit Computern und der entsprechenden Software ausgestatteten Lehrsaal. Die Rückmeldungen durch die Studierenden waren positiv, da grundlegende Konzepte der prozeduralen Programmierung aus den Grundlagensemestern wiederholt und vertieft werden konnten.

Die Erfahrung zeigt, dass seitens der Studierenden mit einer ablehendnen Haltung betreffend dem Einsatz des Digital Rights Managements zu rechnen ist. Trotz der einseitigen Tendenzen wurde bei der Planung der Lehrinhalte dieser Lehrveranstaltung großer Wert darauf gelegt, die Meinung der Studierenden möglichst nicht zu manipulieren. Ziel ist es deswegen, die Argumentation zur Untermauerung der jeweiligen Standpunkte zu unterstützen. Diskussionen werden auch weiterhin in das Unterrichtskonzept eingebaut sein, um in einem gemeinsamen Rahmen, der Lehrveranstaltung, die verschiedenen Blickwinkel kennenlernen zu können. Letztendlich ist, nach Meinung des Verfassers der vorliegenden Arbeit, die konstruktive Infragestellung der gelehrten Lehrinhalte durch die Studierenden ein wesentlicher, positiver Unterschied zwischen der an postsekundären Bildungseinrichtungen durchgeführten Lehre und jener, die an Bildungseinrichtungen mit niedrigerem Bildungsniveau angewandt wird.

Im Rahmen der Lehrveranstaltungsdurchführung werden die Teilnehmer auf die im Masterstudiengang angebotene Lehrveranstaltung der Steganographie vorbereitet. Während im Kontext des Digital Rights Management lediglich eine überblicksmäßige Darstellung präsentiert werden kann, erfolgt im späteren Unterrichtsangebot eine detaillierte Darstellung der einzelnen Verfahren. Dies setzt jedoch die Vermittlung nachrichtentechnischer Grundlagen voraus, deren Vermittlung bei der Planung der neuen Lehrveranstaltung berücksichtigt werden müssen.

Hinsichtlich des Lehrmaterials sind jährlich hohe Recherche-Investitionen nötig. Die gewählten Ansätze zur kommerzialisierung urheberrechtlich geschützter Inhalte von den im wirtschaftlichen Umfeld tätigen Unternehmen sind einem ständigen Wandel unterworfen. So bietet beispielsweise die Firma Apple in ihrem iTunes Store explizit Mediendaten ohne technischen Schutzmechanismen an. Die Verkaufsstatistiken zeigen, dass die Bereitschaft zur Bezahlung für die Mediennutzung vorhanden ist, selbst dann, wenn die Mediennutzer an der Vervielfältigung durch technische Maßnahmen nicht gehindert werden.

Die Aufteilung in Vorlesung und Übung erfordert einen höheren organisatorischen Aufwand, als dies bei einer integrierten Lehrveranstaltung der Falle wäre. Letztere zeichnet sich dadurch aus, dass im Rahmen der Lehrveranstaltung sowohl theoretische, als auch praktische Lehrinhalte vermittelt werden. Der Schritt zur Zusammenlegung wird oft aus Gründen der einfacheren Handhabung gewagt. Wie in Kapitel 2 dargelegt umfassen jeweils die Vorlesung und die Übung eine Semesterwochenstunde (SWS), was eine Zusammenlegung zu einer integrierten Lehrveranstaltung rechtfertigen würde. Davon abgesehen werden große Teile des Übungsteiles in Heimarbeit durch die Studierenden in Eigenregie durchgeführt.

Änderungen im Lehrplan müssen im Falle der Fachhochschulen jedoch durch eine Kommission genehmigt werden. Aufgrund dieser Notwendigkeit wirken sich die hier beschriebenen und mittlerweile getroffenen Änderungen erst auf den Lehrplan späterer Jahrgänge aus. Finden Verschiebungen von Lehrveranstaltungen zwischen den Semestern statt, kann die Auswirkung der Änderungen bis zu mehrere Jahre in Anspruch nehmen.

Wissenschaftliche Literatur

[A. 07] A. Nikolaidis and S. Tsekeridou and A. Tefas and V. Solachidis, V.; A survey on watermarking application scenarios and related attacks, Image Processing, 2001. Proceedings. 2001 International Conference on , Volume: 3 , 7-10 Oct. 2001, Page(s): 991 -994 vol.3, 2007.

[And00] Andreas Westfeld and Andreas Pfitzmann, Attacks on Steganographic Systems - Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools - and Some Lessons Learned,Ž01d Lecture Notes in Computer Science, Springer-Verlag, 2000, pp. 61–75.

[Arb02] Arbaugh„ Bill, Improving the TCPA Specification, Computer 35 (2002), no. 8, 77–79.

[Bal06] Balasubramanian et al., How Much the Eye Tells the Brain, Current Biology 16 (2006), 1428–1434.

[Bau00] F. Bauer, Entzifferte Geheimnisse: Methoden und Maxime der Kryptologie, 3. auflage ed., Springer-Verlag: Berlin, Heidelberg, New York, 2000.

[Ben96] Bender„ W. and Gruhl„ D. and Morimoto„ N. and Lu„ Aiguo, Techniques for data hiding, IBM Syst. J. 35 (1996), no. 3-4, 313–336.

[Bur04] Burg, J., Fundamentals of Digital Audio, http://imej.wfu.edu/articles/2004/1/01/download/Chapter4Primer.pdf, 2004, [Online; Stand 06. März 2009].

[Ceu] Ceusters, W. and Smith, B., Referent Tracking for Digital Rights Management, [Online; Stand 06. Februar 2009].

[Cha01] Chandramouli, R., Memon, N., Analysis of LSB based image steganography techniques.

[Che03] Cheun Ngen Chong and Ro Etalle and Pieter H Hartel, Comparing Logic-based and XML-based Rights Expression Languages, On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops. Springer-Verlag, LNCS, Springer-Verlag, 2003, pp. 779–792.

[Chr98] Christian Cachin, An information-theoretic model for steganography, Springer, 1998, pp. 306–318.

[Chr05] Chris J. Mitchell, Trusted Computing, The Institution of Engineering and Technology, 2005.

[Cum04] Cummins, J., Diskin, P., Lau, S., Parlett, R., Steganography and Digital Watermarking, http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf, 2004, [Online; Stand 14. Februar 2009].

[Cve04] Cvejic, N., Algorithms for Audio Watermarking and Steganography, 2004.

[Dan96] Daniel Gruhl and Anthony Lu, Echo hiding, 1996, pp. 295–315.

[Dit00] Dittmann, J., Digitale Wasserzeichen, Springer-Verlag Berlin Heidelberg, 2000.

[Dol06] Dolle, W., Nerb, M., Wegener, C., In Kinderschuhen, Linux Magazin 12 (2006), .

[EL98] Rudolf Eigenmann and David J. Lilja, Von neumann computers, 1998.

[Eri03] Erickson„ John S., Fair use, DRM, and trusted computing, Commun. ACM 46 (2003), no. 4, 34–39.

[Fab98] Fabien A.P. Petitcolas , Ross J. Anderson, and Markus G. Kuhn, Attacks on Copyright Marking Systems, Lecture Notes in Computer Science 1525 (1998), 218–238.

[Fer06] Ferguson, N., AES-CBC + Elephant diffuser : A Disk Encryption Algorithm for Windows Vista, 2006.

[Fis03] Fischer, M., Grollmann, P., Roy, B., Steffen, N., E-Learning in der Berufsbildungspraxis: Stand, Probleme, Perspektiven, ITB-Forschungsberichte 06 (2003), .

[Fra05] Fraenkl, G., Digital Rights Management in der Praxis, VDM Verlag Dr. Müller, 2005.

[Fri06] J. Fritz, So wirklich wie die Wirklichkeit, http://www.staff.uni-marburg.de/~feldbusc/page12/files/03FRITZ.PDF, 2006, [Online; Stand 01. Jänner 2009].

[Gas08] Gasser, A., DRM (Digital Rights Management) in der Praxis, Master's thesis, TU Vienna, 2008.

[Gau09] Hugo Gaudig, Didaktische Präludien, Teubner Verlag, 1909.

[Gau69] H. Gaudig, Die Schule der Selbsttätigkeit, Julius Klinkhardt, 1969.

[Han05a] Hanen, B., Wisan, M., JPEG Compression, http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/fall2005/benmatt/paper.pdf, 2005, [Online; Stand 05. März 2009].

[Han05b] Hans Brandl and Infineon Technologies Ag, Introduction Trusted Computing: The TCG Trusted Platform Module Specification, 2005.

[Har05] Harth, A., Decker, S., Optimized Index Structures for Querying RDF from the Web, http://sw.deri.org/2005/02/dexa/yars.pdf, November 2005.

[Hoh06] Adolf Hohl, Vertrauliche und nachvollziehbare Verarbeitung von Nutzerdaten in Informationsdiensten auf Basis von TCG, Februar 2006.

[Hub03] P. Hubwieser, Didaktik der Informatik: Grundlagen, Konzepte, Beispiele, Springer Verlag, 2003.

[Jah02] Jahnke, T., Die Bedeutung von digitalen Wasserzeichen in elektronischen Bildern, 2002.

[Jef99] Jeffrey A. Bloom and Ingemar J. Cox and Senior Member and Ton Kalker and Jean-paul M. G. Linnartz and Matthew L. Miller and C. Brendan S. Traw, Copy protection for DVD video, Proceedings of the IEEE, 1999, pp. 1267–1276.

[Jol06] Jolly T. Holden, Philip J.-L. Westfall, An Instructional Media Selection Guide for Distance Learning, http://www.usdla.org, February 2006.

[jSB02] Dr. jur. Stefan Bechtold, Vom Urheber zum Informationsrecht – Implikationen des Digital Rights Management, Verlag C.H. Beck München, 2002.

[Kah67] D. Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Macmillan: New York, 1967.

[Kar00] Karl Fürst and Thomas Schmidt, Abstract: Internet Electronic Data Interchange with XML and JAVA, 2000.

[Kar03] Karen Coyle, The Technology of Rights: Digital Rights Management, 2003.

[Kun04] Kunze, M., Konzeption und Realisierung eines fairen Software-Kopierschutzes basierend auf einer Client/Server-Architektur, http://www.4fo.de/download/diplomarbeit_kunze.pdf, 2004, [Online; Stand 01. Februar 2009].

[Lot01] Lothar Papula, Mathematik für Ingenieure und Naturwissenschaftler Band 2, 10. auflage ed., Vieweg, Oktober 2001.

[Mar08] Martin Lehner, Beispiel guter Lehre an Fachhochschulen, FO.FO.S, Wien, 2008.

[Mat06] Matias Madou and Ludo Van Put and Koen De Bosschere, Understanding Obfuscated Code, Program Comprehension, 2006. ICPC 2006. 14th IEEE International Conference, 2006, pp. 268–274.

[Nei98] Neil F. Johnson and Sushil Jajodia, Steganalysis: The investigation of hidden information, in Proceedings of the IEEE Information Technology Conference, 1998, pp. 113–116.

[Pan04] Pan, J., Huang, H., Jain, L., Intelligent Watermarking Techniques, World Scientific Publishing Co. Pte. Ltd., 2004.

[Pet99] Peter C. Fishburn and Andrew M. Odlyzko, Competitive pricing of information goods: Subscription pricing versus pay-per-use, Economic Theory 13 (1999), 447–470.

[Pet00] Peterßen, W., Handbuch Unterrichtsplanung, Oldenbourg, 2000.

[Pic05] Arnold Picot, Distribution und Schutz digitaler Medien durch Digital Rights Management , 1. auflage ed., Springer Verlag, 2005.

[Pil86] Piller, E., Weißenbrunner, A., Software - Schutz. Rechtliche, organisatorische und technische Maßnahmen, Springer-Verlag KG, 1986.

[Pop98] Popa, R., An Analysis of Steganographic Techniques, http://ad.informatik.uni-freiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf, 1998, [Online; Stand 08. März 2009].

[Pra08] Vaughan Pratt, Algebra, The Stanford Encyclopedia of Philosophy (Edward N. Zalta, ed.), Fall 2008.

[Pro03] Provos, N., Honeyman, P., Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy 3 (2003).

[Rac03] Rachna Dhamija, A framework for evaluating digital rights management proposals, In 1st International Mobile IPR Workshop, 2003.

[Ran02] Rankl, W., Effing, W., Handbuch der Chipkarten, Carl Hanser Verlag München Wien, 2002.

[Rei06] Kersten Reich, Konstruktivistische Didaktik, 3. auflage ed., Beltz Verlag, 2006.

[Rhe01] Rheinberg, F., Leistungsbeurteilung im Schulalltag: Wozu vergleicht man was womit?, www.psych.uni-potsdam.de/people/rheinberg/messverfahren/Leistbeurteilung.pdf, 2001, [Online; Stand 24. April 2009].

[Roe05] Roesler, A., Stiegler, B., Grundbegriffe der Medientheorie, UTB, 2005.

[Ros98] Ross J. Anderson and Fabien A. P. Petitcolas, On the limits of steganography, IEEE Journal of Selected Areas in Communications 16 (1998), 474–481.

[Ros03] Ross Anderson, Cryptography and competition policy: Issues with trusted computing, In Proc. Workshop on Economics and Info. Sec, ACM Press, 2003, pp. 1–11.

[S. 01] S. Voloshynovskiy and S. Pereira and T. Pun and J. J. Eggers and J. K. Su, Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks, IEEE Communications Magazine 39 (2001), 118–126.

[Sch94] S. Schmidt, Kognitive Autonomie und soziale Orientierung, Suhrkamp, 1994.

[Seu04] Seufert, C., Steganographie - Die Kunst der verborgenen Übermittlung von Informationen, http://docs.tx7.de/BA-Mannheim/studienarbeiten/2004-10-20_studienarbeit_christiane_seufert.pdf, 2004, [Online; Stand 08. Februar 2009].

[Sha07] Shangping Zhong and Xueqi Cheng and Tierui Chen, Data hiding in a kind of PDF texts for secret communication, International Journal of Network Security 4 (2007).

[STW04] Andreas U. Schmidt, Omid Tafreschi, and Ruben Wolf, Interoperability challenges for drm systems, Presented at: International Workshop for Technology, Economy, Social and Legal Aspects of Virtual Goods, 2004.

[Web02] S. Weber, Was heißt "Medien konstruieren Wirklichkeit?", http://www.mediamanual.at/mediamanual/themen/pdf/diverse/40_Weber.pdf, 2002, [Online; Stand 11. Jänner 2009].

[Yen93] Yen Pan, Digital Audio Compression, Digital Technical Journal 5 (1993).

[Zim08] Zimbardo, P., Gerrig, R., Psychologie, 18. auflage ed., Pearson Education, 2008.

Nicht-wissenschaftliche Literatur

[1] AKM - Staatlich genehmigte Gesellschaft der Autoren, Komponisten und Musikverleger: Was Wir Tun. http://www.akm.co.at/index.php?content=%2Fwirueberuns%2Fwaswirtun%2Findex.php. [Online; Stand 04. Oktober 2009].

[2] AKM - Staatlich genehmigte Gesellschaft der Autoren, Komponisten und Musikverleger: Wer Wir Sind. http://www.akm.co.at/wirueberuns/werwirsind/index.php. [Online; Stand 04. Oktober 2009].

[3] ashberg.de - B-Sprache/Bebe-Sprache - Ein Übersetzer in PHP. http://www.ashberg.de/bsprache/. [Online; Stand 04. Oktober 2009].

[4] bm:ukk - Glossar U-Z: Verwertungsgesellschaften. http://www.bmukk.gv.at/kunst/glossar_u_z.xml. [Online; Stand 04. Oktober 2009].

[5] Digital Restrictions Management. http://www.drm.info. [Online; Stand 29. September 2009].

[6] Extracting data embedded with JSteg. http://www.guillermito2.net/stegano/jsteg/index.html. [Online; Stand 04. Oktober 2009].

[7] Introduction to the study by BSA president and CEO Robert Holleyman. http://global.bsa.org/globalpiracy2008/index.html. [Online; Video zur Einführung in die Thematik durch den BSA Präsidenten und CEO Robert Holleyman; Übersetzt durch den Verfasser der vorliegenden Arbeit; Stand 19. Oktober 2009].

[8] JSteg. http://zooid.org/~paul/crypto/jsteg/. [Online; Stand 04. Oktober 2009].

[9] Moodle.org: open-source community-based tools for learning. http://www.moodle.org. [Online; Stand 04. Oktober 2009].

[10] ORF-GIS | GEBUEHREN - www.orf-gis.at. http://www.orf-gis.at/index.php?kategorie=gebuehren&thema=uebersicht. [Online; Stand 04. Oktober 2009].

[11] ORF-GIS | GEBUEHREN - www.orf-gis.at. http://www.orf-gis.at/files/48_GIS_Infomappe_Mrz08.pdf. [Online; Stand 04. Oktober 2009].

[12] RIS - Gesamte Rechtsvorschrift für Rundfunkgebührengesetz - Bundesrecht, Fassung vom 04.10.2009. http://www.ris2.bka.gv.at/GeltendeFassung.wxe?QueryID=Bundesnormen&Gesetzesnummer=10012892. [Online; Stand 04. Oktober 2009].

[13] TCG Software Stack (TSS) Specification Version 1.10. http://www.trustedcomputinggroup.org/files/resource_files/647B51B6-1D09-3519-AD0E37E883F62329/TSS_Version__1.1.pdf. [Online; Stand 04. Oktober 2009].

[14] The MathWorks - Product Listing - Products by Category. http://www.mathworks.com/products/product_listing/?BB=1. [Online; Stand 04. Oktober 2009].

[15] The MathWorks Deutschland - MATLAB 7.9 - Überblick und wichtige Funktionen. http://www.mathworks.de/products/matlab/description1.html. [Online; Stand 04. Oktober 2009].

[16] Trusted Computing. http://www.usenix.org/events/sec05/tech/arbaugh.pdf. [Online; Stand 04. Oktober 2009].

[17] Trusting The Trusted Platform Module - Review Tom's Hardware : How Hardware-Based Security Protects PCs. www.tomshardware.com/reviews/hardware-based-security-protects-pcs,1771-2.html. [Online; Stand 04. Oktober 2009].

[18] VG Wort - Im Portrait. http://www.vgwort.de/portrait_1.php. [Online; Stand 17. Oktober 2009].

[19] Studienpläne für die Bachelor- und Masterstudien der Studienrichtung Informatik an der Technischen Universität Wien. http://www.tuwien.ac.at/fileadmin/t/rechtsabt/downloads/informatik-studienplan-2009.pdf, October 2009.

[20] Business Software Alliance. Fifth Annual BSA and IDC Global Software Piracy Study. http://global.bsa.org/idcglobalstudy2007/studies/2007_global_piracy_study.pdf. [Online; Stand 04. Oktober 2009].

[21] Andersson, R. 'Trusted Computing' Frequently Asked Questions. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html, 2003. [Online; Stand 11. März 2009].

[22] Aronson, E. Jigsaw Classroom. http://www.jigsaw.org. [Online; Stand 04. Oktober 2009].

[23] James Atherton. Learning and Teaching: Constructivism in learning. http://www.learningandteaching.info/learning/constructivism.htm, 2005. [Online; Stand 04. Jänner 2009].

[24] Robert A. Beezer. A First Course in Linear Algebra. http://linear.ups.edu, September 2008.

[25] M. Boudourides. Constructivism and education: a shopper's guide. http://www.math.upatras.gr/~mboudour/articles/constr.html, 1998. [Online; Stand 04. Jänner 2009].

[26] Bromme, R., Rambow, R. Die Verbesserung der mündlichen Präsentation von Referaten: Ein Ausbildungsziel und zugleich ein Beitrag zur Qualität der Lehre. http://wwwpsy.uni-muenster.de/Psychologie.inst3/AEbromme/service/leitfaden/referate.html, 1993. [Online; Stand 14. Jänner 2009].

[27] Clark, R. Notes on the Resolution and Other Details of the Human Eye, December 2007.

[28] Cordts, D. Standards zur Modellierung von Metadaten für digitale Musik. http://is-frankfurt.de/veranstaltung/Groffmann_SS05/Thema%205_Cordts_dl.pdf, 2005. [Online; Stand 06. Februar 2009].

[29] Department Technik, Informatik und Naturwissenschaften. Gruppenpuzzle - Beschreibung, December 2004.

[30] Studenten des Hauptseminars "Multimediale Informationsverarbeitung". Digital Rights Management, Sommersemester 05. http://www.ldv.ei.tum.de/studium/vorlesungen/downloads/miv/ss2005/00_Tagungsband.pdf, 2005. [Online; Stand 01. September 2008].

[31] David Engster. MATLAB Tutorial. http://www.physik3.gwdg.de/~engster/matlab_tut.pdf, März 2004.

[32] Fachhochschule St. Pölten GmbH. Modulhandbuch - "IT Security". studiengangs-internes Dokument; Erlaubnis zum Zitieren nach Rücksprache durch den Studiengangsleiter erteilt, 2001.

[33] Felten, E. et al. Reading between the lines: Lessons from the sdmi challenge. http://www.usenix.org/publications/library/proceedings/sec01/craver.pdf, 2001. [Online; Stand 24. Mai 2009].

[34] K. Glorian. Frontalunterricht. http://www.freinet.uni-bremen.de/Gedanken/frontalunterricht.html, 2004. [Online; Stand 04. Jänner 2009].

[35] Gusenstätter, A. eLearning Glossar. http://www.foraus.de/download/elearn_tipps/glossar030801.pdf, 2009. [Online; Stand 13. April 2009].

[36] J. Hsiao. Constructivism Theory. http://www.edb.utexas.edu/csclstudent/Dhsiao/theories.html#construct. [Online; Stand 03. Jänner 2009].

[37] Iannella, R. Digital Rights Management (DRM) Architectures. http://www.dlib.org/dlib/june01/iannella/06iannella.html, 2001. [Online; Stand 04. Februar 2009].

[38] Immanuel Kant. "zitiert in Wilhelm Ostwalds Vierteljahresschrift Annalen der Naturphilosophie, erster Band, erstes Heft, o.O, 1901/1902, S. 52 (zitiert nach http://de.wikiquote.org/wiki/Immanuel_Kant)".

[39] Jeschke, M., Sporer, T. MP3-Grundlagen, Aufbau und Funktion. http://www.fh-jena.de/contrib/fb/et/personal/ansorg/mp3/mp3_2_res.htm, 2000. [Online; Stand 06. März 2009].

[40] Leonardo Chiariglione. Riding the media bits – opening content protection. http://www.chiariglione.org/ride/opening_content_protection/opening_content_protection.htm, 2003. [Online; Stand 24. Mai 2009].

[41] Martin Pöll. Matlab: Numerik, Visualisierung, Programmierung. http://unix-docu.uibk.ac.at/zid/software/unix/num/matlab.html, November 2008.

[42] Peter G. Neumann. Principled Assuredly Trustworthy Composable Architectures. http://www.csl.sri.com/neumann/chats4.pdf, 2004. [Online; Stand 11. Februar 2009].

[43] Petitcolas, F. The Image downgrading Problem. http://www.petitcolas.net/fabien/steganography/image_downgrading/index.html. [Online; Stand 29. September 2009].

[44] Pohl, W. Methodenblatt - Mindmapping. http://www.pohlw.de/lernen/methoden/methoden_09.pdf, 2006. [Online; Stand 30. Jänner 2009].

[45] Kersten Reich. Methodenpool. http://methodenpool.uni-koeln.de, 2008. [Online; Stand 10. Dezember 2008].

[46] Rudolph, D. Spread Spectrum Modulationen. http://www.diru-beze.de/funksysteme/skripte/DiFuSy/DiFuSy_SprSpec_WS0405.pdf, 2004. [Online; Stand 06. März 2009].

[47] M. Schlup. MATLAB Kompendium. https://home.zhaw.ch/~spma/Scripts/SiSy_GSA/MatlabKompendium.pdf, Februar 2007.

[48] Schoen, S. Trusted Computing: Promise and Risk. http://hdl.handle.net/2038/871, 2006. [Online; Stand 11. März 2009].

[49] Inc. The MathWorks. MATLAB. http://www.mathworks.com/access/helpdesk/help/techdoc/matlab.shtml, November 2008.

[50] Walker, B. Imaging Nuggets: Digital Audio III: Metadata. http://www.amigos.org/preservation/ImNuggDigAudioIIIMeta.html, 2005. [Online; Stand 15. März 2005].

[51] ZUM Wiki. Gruppenpuzzle. http://wiki.zum.de/Gruppenpuzzle, 2009. [Online; Stand 13. April 2009].

Anhang A

Source Code

Einführung in MATLAB

Listing A.1: Das in MATLAB integrierte Hilfesystem

```
>> help who
 WHO    List current variables.
    WHO lists the variables in the current workspace.

...
>>
```

Listing A.2: Variablendefinition in MATLAB

```
>> a = 1;
>> hello = 'Hello World!';
>> b = [ 1 2 3 ];
>> c = [ 1 2 3 ; 4 5 6 ];
>> whos
  Name        Size             Bytes  Class     Attributes

  a           1x1                  8  double
  b           1x3                 24  double
  c           2x3                 48  double
  hello       1x12                24  char

>>
```

Listing A.3: Multiplikation und Division von Matrizen in MATLAB

```
>> a = [ 2 2 2 ; 2 2 2 ]

a =

     2     2     2
     2     2     2
>> b = [ 2 2 2; 2 2 2 ]

b =

```

```
     2     2     2
     2     2     2

>> a * b
??? Error using ==> mtimes
Inner matrix dimensions must agree.

>> a .* b

ans =

     4     4     4
     4     4     4

>>
```

Listing A.4: Beispiel für Built-Ins in MATLAB

```
>> zeros(4)

ans =

     0     0     0     0
     0     0     0     0
     0     0     0     0
     0     0     0     0
```

Listing A.5: Beispiel für die Bit-Operatoren in MATLAB

```
>> sprintf('0x%02X', 15)
ans =
0x0F

>> sprintf('0x%02X', bitand(240,15))
ans =
0x00

>> sprintf('0x%02X', bitor(240,15))
ans =
0xFF

>> sprintf('0x%02X', bitshift(15,4))
ans =
0xF0

>> sprintf('0x%02X', bitcmp(15,8))
ans =
0xF0
```

Listing A.6: Beispiel für Bedingungen und Schleifen in MATLAB

```
>> a = 3;
>> if (a > 2 && a < 5),
```

```
sprintf('a is greater than 2 and smaller than 5.')
end

ans =

a is greater than 2 and smaller than 5.
```

Listing A.7: Beispiel für Bedingungen und Schleifen in MATLAB

```
>> for n = 1:3,
sprintf('Value of n: %d',n)
end

ans =

Value of n: 1


ans =

Value of n: 2


ans =

Value of n: 3
```

Listing A.8: Beispiel zur Implementierung von Funktionen in MATLAB (`funkt.m`)

```
function [ lOut ] = funkt( pIn )
%FUNKT Dies ist eine Beispielfunktion
%   Alle Funktionsparameter werden um 1 erhoeht und anschlieszend das
%   bitweise 8-Bit Komplement gebildet.

lOut = zeros(size(pIn));
lSize = size(pIn);
for lCnt = 1:lSize(2),
    lOut(lCnt) = bitcmp(pIn(lCnt) + 1,8);
end

end
```

Listing A.9: Beispiel zur Implementierung von Funktionen in MATLAB

```
>> a = [ 1 2 3 ];
>> funkt(a)

ans =

   253   252   251
```

Listing A.10: Beispiel zur Visualisierung von Daten in MATLAB

```
>> x = [0 1 2 3];
```

```
2 >> k = 2;
3 >> d = 0;
4 >> y = k * x + d
5
6 y =
7
8      0      2      4      6
9
10 >> plot(x,y)
```

Beispiel zu Steganographie in MATLAB

Das im Internet unter [43] gefundene Beispielscript zum Verstecken von digitalen Informationen in den niederwertigsten Bits von Bitmap-Bilddateien wurde für den Unterricht zum besseren Verständnis adaptiert.

Listing A.11 zeigt in möglichst kurzer Form und in Anlehnung an die in Abbildung 4.7 vorgestellte Vorgangsweise in der Steganographie. Nachdem die vorliegenden Bilder im Bitmap-Format in den ersten beiden Zeilen eingelesen wurden, wird in Zeile festgelegt, wieviele der niederwertigsten Bits zum Verstecken der geheimen Botschaft "Message" verwendet werden. Die Funktion "LSBHide" versteckt demnach die Nachricht "Message" im Trägermaterial "Cover" und liefert als Rückgabewert das Stegoobjekt "Stego". Die Funktion "LSBRecover" hingegen gibt zurück, wieviel von der versteckten Information bei der Einbettung verwendet wird bzw. wieviel davon nach der Übertragung wiederhergestellt werden kann. Im Folgenden werden diese beiden Funktionen erläutert. Sie stellen das zentrale Element des Algorithmuses zum Verstecken in den niederwertigsten Bits dar.

Listing A.12 listet das Programm zum Verstecken der geheimen Nachricht auf. Zeile 7 generiert die Bitmaske, damit die Bits an der Stelle, an der eingebettet wird, auf 0 (Null) gesetzt werden können. Dies passiert in den Zeilen 9 bis 17. Die drei verschachtelten "for"-Schleifen spiegeln die drei Ebenen, aus denen das Bild aufgebaut ist, wider:

- Höhe (Laufvariable "lY"),
- Breite (Laufvariable "lX") und
- Farbtiefe (Laufvariable "lZ").

Zeile 14 verknüpft die Bitstellen zur Einbettung mit logisch-Und mit Hilfe von "bitand". Die verschachtelten "for"-Schleifen in den Zeilen 22 bis 28 bereiten die zu versteckende Nachricht durch Verschieben der höherwertigen Bits an die niederwertigen Stellen durch "bitshift" vor. Dazu wird in Zeile 21 ein identgroße Matrix aus "uint8" Werten generiert. Die gleiche Vorgangsweise wird zur Vorbereitung des Stegoobjekts in Zeile 32 angewandt. Das Zusammenführen der vorbereiteten Nachricht, sowie des ursprünglichen Bildes, dem Trägermaterial, erfolgt in den Zeilen 33 bis 39 mit Hilfe von "bitor", der logischen Oder-Verknüpfung.

Das Wiederherstellen erfolgt analog zum Verstecken. Siehe dazu Listing A.13. Die niederwertigsten Bits, die die höherwertigen Bits der versteckten Nachricht darstellen, werden durch "bitshift" an die höherwertigen Positionen gebracht (Zeile 9 bis 15). In den Zeilen 20 bis 26 erfolgt ausschließlich eine Umwandlung der Datentypen. Diese ist bedingt und erforderlich durch Eigenheiten in der Abarbeitung durch MATLAB.

Zu Demonstrationszwecken sei im Listing A.14 noch das Originalprogramm angeführt. Es zeigt, dass sich durch die Schachtelung der Bitoperationen die Länge des erforderlichen Programmcodes stark reduzieren lässt. Zur Erklärung der grundlegenden Funktionalität wird dieser jedoch nicht herangezogen, da er von den Studierenden ein ausreichendes Verständnis des gesamten Algorithmuses oder der Programmiersprache voraussetzt.

Listing A.11: LSB Beispielapplikation (Modularisiert)

```
Cover = imread('01.bmp', 'bmp');
Message = imread('02.bmp', 'bmp');
n = 4; % Number of bits to replace 1 <= n <= 7

[Stego] = LSBHide(Cover, Message, n);
[Extracted] = LSBRecover(Stego,n);

imwrite(Stego,'stego.bmp','bmp')
imwrite(Extracted,'extracted.bmp','bmp')
```

Listing A.12: LSB Versteckalgorithmus

```
function [Stego] = LSBHide(Cover, Hidden, n)
%LSBHide
% [Stego] = LSBHide(Cover, Hidden, n)
% Hide Hidden in the n least significant bits of Cover

% zero out LSBs
CoverBlend = bitcmp(2^n - 1, 8);

lSize = size(Cover);
CoverPrepared = uint8(zeros(lSize));
for lZ = 1:lSize(3)
    for lY = 1:lSize(1)
        for lX = 1:lSize(2)
            CoverPrepared(lY,lX,lZ) = bitand(Cover(lY,lX,lZ),CoverBlend);
        end
    end
end

% move MSBs to LSBs of HiddenMessage
lSize = size(Cover);
HiddenPrepared = uint8(zeros(lSize));
for lZ = 1:lSize(3)
    for lY = 1:lSize(1)
        for lX = 1:lSize(2)
            HiddenPrepared(lY,lX,lZ) = bitshift(Hidden(lY,lX,lZ),n-8);
        end
    end
end

% create stego object
lSize = size(CoverPrepared);
Stego = uint8(zeros(lSize));
for lZ = 1:lSize(3)
```

```
    for lY = 1:lSize(1)
        for lX = 1:lSize(2)
            Stego(lY,lX,lZ) = uint8(bitor(CoverPrepared(lY,lX,lZ), HiddenPrepared(
                lY,lX,lZ)));
        end
    end
end
```

Listing A.13: LSB Wiederherstellalgorithmus

```
function [Extracted] = LSBRecover(Stego, n)
%LSBRecover
% [Extracted] = LSBRecover(Stego, n)
% Recover n least significant bits of Stego object into hidden message

% use LSBs of stego object as MSBs
lSize = size(Stego);
StegoPrepared = uint8(zeros(lSize));
for lZ = 1:lSize(3)
    for lY = 1:lSize(1)
        for lX = 1:lSize(2)
            StegoPrepared(lY,lX,lZ) = bitshift(Stego(lY,lX,lZ),8-n);
        end
    end
end

% extract data (only convert data types)
lSize = size(Stego);
Extracted = uint8(zeros(lSize));
for lZ = 1:lSize(3)
    for lY = 1:lSize(1)
        for lX = 1:lSize(2)
            Extracted(lY,lX,lZ) = uint8(StegoPrepared(lY,lX,lZ));
        end
    end
end
```

Listing A.14: LSB Beispielapplikation (Original)

```
Hare = imread('arctic_hare.bmp', 'bmp');
F15 = imread('F15.bmp', 'bmp');
n = 4; % Number of bits to replace 1 <= n <= 7

[Stego, Extracted] = LSBHide(Hare, F15, n);

figure, imshow(Stego)
figure, imshow(Extracted)

function [Stego, Extracted] = LSBHide(Cover, Hidden, n)
%LSBHide
% [Stego, Extracted] = LSBHide(Cover, Hidden, n)
% Hide Hidden in the n least significant bits of Cover

```

```
15 Stego = uint8(bitor(bitand(Cover, bitcmp(2^n - 1, 8)) ,
16            bitshift(Hidden, n - 8)));
17 Extracted = uint8(bitand(255, bitshift(Stego, 8 - n)));
```