Prof. Dr. Freimut Bodendorf
Dr. Susanne Robra-Bissantz
Bernd Weiser
Florian Lang

Internet und Urheberrecht

1 Einführung

Die Möglichkeit zur verlustfreien Vervielfältigung digitaler Inhalte zu verschwindend geringen Grenzkosten sowie deren Verbreitung über das Internet stellt die Urheber dieser Inhalte vor große Probleme hinsichtlich der Wahrung ihrer Interessen.

In der Softwareindustrie ist das Problem des illegalen Vertriebs von Raubkopien über das Internet seit längerem bekannt. Zum Aufflammen der Diskussion um den Urheberschutz kam es jedoch erst, nachdem Forscher des Erlanger Fraunhofer-Instituts durch Entwicklung des MP3-Standards den Austausch von Musikdaten über das Internet dramatisch erleichterten. Die allgemeine Beliebtheit des digitalisierbaren Guts „Musik“, die Einfachheit des Austauschs und nicht zuletzt die gezielt hochpreisige Marktstrategie der Musikindustrie haben dazu geführt, dass der Austausch kopierter Musik innerhalb kürzester Zeit zum Volkssport mit dem Charakter eines Kavaliersdelikts avancierte. Zuvor war das Beziehen illegaler Kopien aus dem Internet die Domäne einiger weniger Spezialisten, die über die technische Ausrüstung verfügten, die zum Download umfangreicher Computerspiele oder Business-Applikationen benötigt wurde. In größerem Umfang wurden Raubkopien von Software nur „offline“, also z.B. durch Kopieren von CDs produziert. Die Bemühungen der Industrie, dem durch Kopierschutzverfahren zu begegnen, konzentrierten sich daher auf die Verhinderung der Vervielfältigung des originalen Datenträgers (z.B. durch Einstreuen fehlerhafter Sektoren auf einer CD). Diese Situation hat sich gewandelt. Spätestens seitdem breitbandige Internet-Anschlüsse auch für Privatanwender erschwinglich sind, besteht aus Sicht der Contentindustrie (Labels, Verlage, Filmverleihe) dringender Bedarf nach neuen Technologien und Geschäftsmodellen, die den geistigen Eigentümern digitaler Dokumente zu ihrem Recht verhelfen sollen.

2 Juristische Grundlagen

2.1 Anwendbarkeit des deutschen Urheberrechts

In *persönlicher Hinsicht* schützt deutsches Urheberrecht nur deutsche Urheber und Nutzungsrechtsinhaber. Auch juristische Personen unterstehen deutschem Urheberrecht, sofern sie ihren Sitz in Deutschland haben. Entsprechende Anwendung auf Ausländer findet es nur bei EU-Bürgern aufgrund des Diskriminierungsverbots [Art. 6 Abs. 1 EGV] und in einigen, hier unbedeutenden Ausnahmefällen. Im Internet gelten keine urheberrechtlichen Besonderheiten oder Ausnahmen.

In *räumlicher Hinsicht* schützt deutsches Urheberrecht, einschließlich der vorgenannten internationalen Bestimmungen, nur gegen Verletzungen „im Inland“. Bei Verletzungen „im Ausland“ gilt der allgemeine Grundsatz, dass, soweit überhaupt ein deutsches Gericht zuständig ist, dieses das ausländische Recht anwenden muss [Art. 38 EGBGB]. Da im Internet verbrei-

tete Inhalte unabhängig von ihrem Speicherort global abrufbar sind, ist eine Abgrenzung hier nicht möglich. Daher wird allgemein angenommen, dass jede Verletzung, die per Internet auch in Deutschland erfolgen kann, im „Inland“ stattfindet – z.B. durch den von Deutschland aus getätigten Abruf raubkopierter Inhalte deutscher Urheber von einem US-Server [z.B. LG Berlin, Beschluss vom 14. März 1997, Az. 16.0.166/97].

Daher ergibt sich grundsätzlich:

- Wird das *Werk eines Deutschen in Deutschland* rechtswidrig kopiert, dann gilt deutsches Urheberrecht.
- Wird das *Werk eines Deutschen im Ausland* rechtswidrig kopiert, dann gilt grundsätzlich das ausländische Recht. Sind die Kopien aber über das Internet auch in Deutschland abrufbar, so gilt deutsches Urheberrecht, da es sich dann um eine „im Inland“ begangene Verletzung handelt.
- Wird das *Werk eines Ausländers in Deutschland* rechtswidrig kopiert, dann ist über den Grundsatz der Inländerbehandlung im Rahmen der internationalen Abkommen die Verfolgung entsprechend dem deutschen Urheberrecht möglich.
- Wird das *Werk eines Ausländers im Ausland* rechtswidrig kopiert, dann ist dies – egal, ob es auch über das Internet abrufbar ist – in Deutschland nicht von Belang.

2.2 Ausgewählte Problemfälle

2.2.1 Bildschirmanzeige von geschützten Inhalten

Die Bildschirmanzeige urheberrechtlich geschützter Inhalte mit Hilfe eines Browsers stellt vor dem Urheberrecht eine nicht-dauerhafte Vervielfältigung dar. Diese ist zulässig, soweit sie ausschließlich zum privaten oder „sonstigen eigenen Gebrauch“ geschieht [§ 53 UrhG]. Der sonstige eigene Gebrauch umfasst auch die eigene berufliche oder erwerbswirtschaftliche Verwendung, z.B. in einem Unternehmen, soweit diese Verwendung nicht den Rahmen des Unternehmens verlässt [BGH, Urteil v. 16. 1. 1997, Az. I ZR 9/95 - CB-Infobank I]. Unzulässig ist jedoch die öffentliche Wiedergabe eines „erschienenen“, d. h. bereits außerhalb des Internet in körperlicher Form veröffentlichten Werkes, wenn sie Erwerbszwecken des Veranstalters dient und die Teilnehmer ohne Entgelt für die Inhalte zugelassen werden [§ 52 UrhG]. Letzteres ist in der Regel in Internet-Cafés der Fall. Das Kriterium der „öffentlichen“ Vorführung kann durch die Café-Betreiber jedoch umgangen werden, indem sie ihr Angebot z.B. an eine Club-Mitgliedschaft binden.

2.2.2 Download von geschützten Inhalten

Downloads von Inhalten aus dem Internet stellen Vervielfältigungen dar. Auch diese sind zum ausschließlich privaten oder sonstigen eigenen Gebrauch inklusive der oben erwähnten

eingeschränkten beruflichen Nutzung zulässig. Downloads dürfen also auf dem eigenen PC gespeichert und verwendet werden.

Die *Verbreitung* der heruntergeladenen Inhalte durch den Nutzer, z.B. durch Einstellen in die eigenen Web-Seiten, ist ohne ausdrückliche Genehmigung des Urhebers oder des Nutzungsrechtsinhabers dagegen unzulässig [§ 17 UrhG]. Das Einstellen in eigene Web-Seiten stellt eine öffentliche Verbreitung dar, weil die Nutzer die Inhalte zumindest auf ihre Bildschirme holen und damit vervielfältigen.

Zulässig sind dagegen die Wiedergabe von heruntergeladenen Inhalten in eigenen Worten (Abstracts) und das wörtliche Zitieren kleinerer Teile der fremden Werke. Letzteres darf aber nur geschehen, wenn der Urheber und die Quelle angegeben werden [§ 63 UrhG].

So genannte gemeinfreie Werke und Daten können von jedermann beliebig genutzt werden (vervielfältigt, bearbeitet, veröffentlicht usw.). Sie fallen nicht unter das Urheberrecht, weil sie entweder aus sich heraus nicht schutzfähig sind oder weil der urheberrechtliche Schutz bereits abgelaufen ist. Dies geschieht spätestens 70 Jahre nach dem Tod des Urhebers.

2.2.3 Verweis auf geschützte Inhalte

Linking ist ein Grundprinzip des World Wide Web. Im Gegensatz zu einer immer wieder geäußerten Meinung handelt es sich bei Links aber nicht um Zitate im Sinne des UrhG, denn ein Zitat setzt schon begrifflich voraus, dass der fremde Inhalt im Rahmen des eigenen Inhalts präsentiert wird. Ein Link auf einen fremden Inhalt stellt aber nur einen Verweis dar, ohne den fremden Inhalt auf der eigenen Seite wiederzugeben. Er ist daher rechtlich wie ein bloßer Verweis oder eine Fußnote in wissenschaftlichen Werken einzuordnen. Eine urheberrechtliche Relevanz besteht nicht.

Etwas anderes gilt aber, wenn der Link zu einem fremden Inhalt führt, der nach dem Anklicken in einem Rahmen (Frame) des eigenen Angebots dargestellt wird. Soweit dann nicht mehr erkennbar ist, dass es sich um einen fremden Inhalt handelt, liegt ein Verstoß gegen § 13 UrhG vor, weil die fremde Urheberschaft geleugnet wird.

Uneinigkeit herrscht allerdings, ob diese Einschätzung auch dann gilt, wenn am Anfang der im eigenen Frame dargestellten fremden Seite der Urheber durch ein Logo oder den Seitentitel eindeutig bezeichnet ist. Eine Verletzung von Urheberrechten liegt jedenfalls dann vor, wenn das nicht der Fall ist oder nicht auf den Seitenanfang verwiesen wird.

Etwas anders gelagert ist der Fall, wenn fremden Webseiten Linksammlungen entnommen werden. Hier stellt sich die Frage, ob Linksammlungen überhaupt dem Schutz des Urheberrechts unterliegen. Der einzelne Link ist nicht urheberrechtlich geschützt, da er lediglich die Wiedergabe einer allgemein verfügbaren Adresse darstellt, die jeder andere auch selbst erstellen und in seine Web-Seiten einbinden könnte. Die Linksammlung als Ganzes genießt

aber, einen entsprechenden Umfang vorausgesetzt, den Schutz als Datenbank [§ 4 UrhG - Sammelwerke und Datenbankwerke].

2.2.4 Austausch geschützter Inhalte

Die Rechtmäßigkeit des Austauschs geschützter Inhalte im Internet hängt in einigen Aspekten von der Rechtmäßigkeit von Kopien des geschützten Inhalts ab.

Vorreiter bei der Rechtsprechung ist der Audiobereich aufgrund des aktuell diskutierten Austauschs von Musikstücken im Audioformat MP3.

Kopien geschützter Inhalte

Hinsichtlich der Rechtmäßigkeit der Erstellung von MP3-Dateien aus Musikstücken und deren Kopie gibt es keine Besonderheiten gegenüber der traditionellen Vervielfältigung und Weitergabe.

Rechtmäßig ist die Vervielfältigung von Musikstücken – und damit auch die Erstellung und Weitergabe von MP3-Dateien – aus eigenen, rechtmäßig erworbenen Tonträgern zum eigenen Gebrauch aufgrund von § 53 UrhG. Laut ständiger Rechtsprechung dürfen z.B. von einer erworbenen CD „einzelne“ (Richtwert: bis zu 7) Kopien selbst oder durch Dritte erstellt werden. Verboten ist das Erstellen von mehr als „einzelnen“ Kopien oder deren kommerzielle Verwendung.

Ebenfalls rechtmäßig erstellt und vervielfältigt sind Kopien von Musikstücken, wenn folgende Personen/Rechtsträger zugestimmt haben:

- die Urheber des Musikstücks, also in der Regel der Komponist und der Textdichter [§§ 7, 15 UrhG],
- die ausübenden Künstler, die die Musik spielen und/oder singen [§§ 73, 75 UrhG],
- der Hersteller des Tonträgers, der als Original zur Erstellung der MP3-Dateien dient [§ 85 UrhG].

Gegebenenfalls müssen zustimmen:

- der Rechtsträger, auf den die obigen Personen (Urheber oder ausübende Künstler) ihre Rechte übertragen haben, also insbesondere Musikverlage,
- das Sendeunternehmen, wenn eine Ausstrahlung in Rundfunk oder Fernsehen als Original zur Herstellung einer MP3-Datei dient [§ 85 UrhG].

Fehlt es auch nur an einer einzigen erforderlichen Zustimmung, so ist jede Vervielfältigung und Verbreitung rechtswidrig.

Angebot geschützter Inhalte im WWW

Schon das Angebot von rechtswidrig erstellten MP3-Dateien zum Download ohne Zustimmung der Rechteinhaber ist ohne Zweifel rechtswidrig. Das gilt bei einem Angebot im Internet bereits auf Grund des Kopierens der Datei auf die Festplatte des Web-Servers, da hier nicht mehr von einer Vervielfältigung für private Zwecke auszugehen ist.

Download

Wer sich rechtswidrig angebotene MP3-Dateien aus dem Internet herunterlädt, der verhält sich ebenfalls rechtswidrig. Entgegen einer verbreiteten Ansicht[1] ergibt sich das aus der Überlegung, dass man an rechtswidrig erstellten Kopien keine Rechte erwerben kann. Diese jedoch wären notwendig, um ein rechtmäßiges Abbild der MP3-Dateien auf dem eigenen Rechner zu erstellen. Dies basiert auf folgenden Grundgedanken des deutschen Urheberrechts:

- Wer keine Rechte hat, wie z.B. ein Raubkopierer, kann auch keine Rechte auf Dritte übertragen.
- Es gibt im Urheberrecht keinen gutgläubigen Erwerb von Rechten.

Linking

Das Setzen von Links zu Angeboten, die rechtswidrig erstellte MP3-Dateien enthalten, kann keine urheberrechtlichen Konsequenzen haben, es kommen aber möglicherweise strafrechtliche Tatbestände wie Beihilfe oder sogar Mittäterschaft in Betracht.

Weitergabe an Dritte

Die Weitergabe von raubkopierten MP3-Dateien ist rechtswidrig, denn gem. § 96 UrhG dürfen rechtswidrig erstellte MP3-Dateien weder verbreitet noch zur öffentlichen Wiedergabe benutzt werden. Entsprechendes gilt, wenn es sich um Aufzeichnungen von Funksendungen handelt.

2.3 Übergang von Urheberrechten

Wer Inhalte erstellt, die als Werk im Sinne des UrhG anzusehen sind, ist deren Urheber. Es ist unerheblich, ob die Erstellung z.B. im Auftrag des Arbeitgebers oder eines Dritten erfolgt. Der Auftraggeber kann Urheberrechte nur durch eine explizite Übertragung erwerben. Dies geht so weit, dass eine mit der Produktion von Inhalten beauftragte Agentur die Rechte an diesen Inhalten nur ausdrücklich auf den Auftraggeber übertragen kann, und dies auch nur, sofern sie ihr zunächst selbst von den eigenen Mitarbeitern übertragen worden sind. Ein so genannter gutgläubiger Erwerb durch den Auftraggeber ist im deutschen Urheberrecht nicht

[1] Nachw. bei Spindler, Juristen-Zeitung 2002, 60, 61 f.

vorgesehen. Bei jeglicher Produktion von Inhalten durch Dritte oder Angestellte sind daher die urheberrechtlichen Bedingungen vertraglich festzulegen.

3 Digital Rights Management

Aufgabe des Digital Rights Management (DRM) ist es, die Wahrung von Urheberinteressen auch entgegen vorsätzlicher Bemühungen von Raubkopierern sicher zu stellen. Dies wird durch die folgenden drei Hauptfunktionen des DRM erreicht:

- **Eigentumsnachweis:** Der Eigentumsnachweis muss digitale Dokumente einem Rechteinhaber eindeutig zuordnen können und zudem resistent sein gegen manipulative Eingriffe.
- **Nutzungsbeschränkung:** Im Rahmen der Nutzungsbeschränkung werden verschiedenste Ansätze verfolgt, um digitale Medienprodukte hinsichtlich ihrer Nutzungshäufigkeit und -dauer, sowie der zur Nutzung berechtigten Personen einzuschränken. So dienen z.B. Verschlüsselungstechniken dazu, die Nutzung (Lesen, Abspielen) digitaler Dokumente auf einen berechtigten Personenkreis zu beschränken. Ein besonders kritischer Fall der Nutzung ist die Vervielfältigung, die durch Techniken des Kopierschutzes beschränkt ist.
- **Kopierschutz:** Zu den Kopierschutztechniken zählen nicht nur Verfahren, die das lokale Abspeichern geschützter Dokumente bzw. die Vervielfältigung bereits auf der Festplatte vorhandener Dateien verhindern sollen, sondern auch Methoden, die es ermöglichen, solche Vorgänge später nachvollziehbar zu machen. Einem Dokument ist dann z.B. stets der Zeitpunkt des Kopierens sowie die Identität der hierzu eventuell nicht autorisierten Person zu entnehmen.

Ein Digital Rights Management System (DRMS), das diese Funktionen zuverlässig erfüllt, kann zum Online-Vertrieb digitalisierbarer Güter wie Texte, Bilder, Video- und Audiomaterial, aber auch beliebiger Property-Rights, die z.B. zum Bezug einer Dienstleistung berechtigen, dienen. Erlösmodelle wie Pay-Per-View, automatisierte Content Syndication[2], kostenpflichtige Newsletter, Music-On-Demand usw. sind essenziell von zuverlässigen DRMS abhängig, die die Umsätze von Rechteinhabern, Content Syndikatoren und Online-Dienstleistern sichern.

---

[2] Kostenpflichtiger Austausch von Inhalten zwischen den Webangeboten unterschiedlicher Anbieter, z.B. das Mieten tagesaktueller Wirtschaftsnews bei Content Providern wie der Deutschen Presseagentur (dpa), die auf der eigenen Website eingestellt werden.

3.1 Basistechnologien

Im Folgenden werden die Technologien erläutert, auf denen DRMS aufbauen („Enabling Technologies“ der DRMS). Der Schlüssel zu sicherem DRM ist es, einem zu schützenden Dokument bestimmte Metainformationen eindeutig zuordnen zu können. Solche Metainformationen (Informationen über Informationen) betreffen z.B. die Identität des Urhebers oder sonstiger Rechteinhaber, die Kopier- und Nutzungsrechte bestimmter Nutzergruppen oder Personen usw. Ein DRMS gewährleistet, dass jegliche Nutzung geschützter digitaler Dokumente stets konform ist mit den in diesen Metainformationen hinterlegten Bedingungen.

3.1.1 Metatags

Im einfachsten Fall werden in die zu schützenden Dokumente neben den eigentlichen Informationen Metatags eingefügt, also Platzhalter für Urheberinformationen. Dieses Vorgehen wird bereits von den verschiedensten Dokumententypen unterstützt. Viele Publishing-Applikationen erlauben dem Anwender, produzierte Inhalte mit urheberrechtlichen Metainformationen wie dem Namen des Autors etc. auszustatten, die jedoch oft leicht manipulierbar sind. Um Webinhalte zu schützen, werden Metatags wie `<author_name>` und `<doc_id>` etc. in das HTML-Dokument eingefügt.

Problematisch ist hierbei jedoch die Durchsetzung einer Konvention, welche Metatags mindestens vorhanden sein müssen, welche Bezeichnungen für die Metatags zu wählen sind und welche Art von Information ein DRMS in einem Metatag bestimmter Bezeichnung erwarten kann. Daher erscheint der Einsatz der Extensible Markup Language (XML) naheliegend[3]. Während in HTML eine bestimmte Tagmenge als Standard definiert ist (z.B.
 als Zeilenvorschub) kann die Struktur eines XML-Dokuments einschließlich aller Tagbezeichnungen von Grund auf selbst definiert werden. Diese Definitionen sind in der Document Type Definition (DTD) hinterlegt, die von XML-Dokumenten referenziert wird, die sich diesem Dokumenttyp zuordnen. Um eine einheitliche Basis für ein Digital Rights Management zu schaffen, z.B. zur Rechteverwaltung für Presseartikel, ist lediglich eine verbindliche DTD zu definieren. In dieser ist z.B. hinterlegt, dass ein gültiger[4] Presseartikel neben den Tags für z.B. Überschrift, Datum und Fließtext auch Metatags zur Identifikation der Urheber, den Nutzungsrechten der

---

[3] Vgl. zu diesen Standards die Vorlesung Daten- und Wissensmanagement, vertiefende Informationen beim World Wide Web Consortium unter http://www.w3c.org (Spezifikationen) und unter http://www.xml.org (Anwendungen).

[4] Engl. "valid“. Bei XML wird unterschieden zwischen Gültigkeit und Wohlgeformtheit. Gültig ist ein Dokument, wenn es auf eine DTD ausgerichtet wurde und die Vorgaben der DTD einhält. Ein Dokument, das nicht auf eine DTD ausgerichtet wurde, kann noch den Status der Wohlgeformtheit erreichen, wenn es eine XML-konforme Syntax aufweist.

Empfänger usw. mit den in der DTD für Presseartikel vorgeschriebenen Bezeichnungen der Tags zu enthalten hat. Ungültige XML-Dokumente werden von den DRM-Applikationen nicht akzeptiert. Damit ein solcher Mechanismus greifen kann, ist es jedoch notwendig, den Zugriff auf solche XML-Dokumente geeignet zu beschränken. Denn sobald sie mit einer Applikation abgerufen werden können, die den DRM-Mechanismus nicht unterstützt (z.B. ein XML-fähiger Browser ohne DRM-Plugin) läuft die angestrebte kontrollierte Rechteverwaltung ins Leere. Der XML-basierte Metatagging-Standard XrML (Extensible Rights Markup Language) sieht daher neben einer geeigneten DTD noch eine Verschlüsselungstechnik vor.

XML hat sich beim interorganisationalen Dokumenten- und Datenaustausch bereits weitgehend etabliert, da sich über die Definition anwendungsspezifischer DTD die Kommunikation in heterogenen IV-Landschaften mit einfachsten Mitteln standardisieren lässt. Eine Vielzahl von B2B-Anwendungsumgebungen greift auf XML zurück, da beliebige Dokumentenarten flexibel definiert können (z.B. XML für EDI). Auch im DRM spielt XML diese Stärke aus. Ein XML-basiertes DRMS ist in der Lage, beliebige Dokumententypen zu verwalten.

Ein Nachteil dieses Ansatzes besteht darin, dass es nicht möglich ist, die *innere* Struktur der Metainformationen vorzuschreiben, d.h. eine Zahl oder ein einziges Zeichen als Inhalt des in der DTD vorgesehenen Tags `<author_name>` würde vom DRMS als gültig interpretiert werden, sofern die DRM-Applikation nicht zusätzliche, nicht aus der DTD abgeleitete Gültigkeitstests durchführt. Da dieses Problem in vielen Anwendungsbereichen eine Rolle spielt, sollen in Zukunft „XML-Schemas“ die DTD ablösen. Sobald die entsprechende Spezifikation vom World Wide Web Consortium verabschiedet wird, können Schemas eingesetzt werden, um interne Datenstrukturen der Tags ebenfalls mit Gültigkeitsregeln zu versehen. So können z.B. gültige Inhalte des Tags `<author_name>` als aus mindestens zwei nicht numerischen Worten bestehend definiert werden.

Alle auf Metatags basierenden Ansätze kranken jedoch an einem grundlegenden Nachteil: Die zu schützende Information selbst und die Metainformation, die die Aussagen über den Schutzstatus der Information trifft, liegen im Dokument getrennt vor. Mit krimineller Energie kann es also unter Umgehung der Verschlüsselung möglich sein, in das Dokument einzugreifen und Metainformationen zu manipulieren, ohne die geschützten Informationen dabei zu zerstören. Auch können die geschützten Inhalte ausgeschnitten und beliebig weiterverwendet werden, wobei jegliche Urheberinformation verloren geht. Im Rahmen des DRM wurden daher Ansätze entwickelt, die auf die direkte, untrennbare Einbettung von Metadaten in die zu schützenden Daten abzielen (vgl. Abschnitt 3.1.2 „Digitales Wasserzeichen“) oder diese anhand bestimmter Muster identifizieren und ihnen an dritter Stelle hinterlegte Metainformationen zuordnen (vgl. Abschnitte 3.1.3 „Digitaler Fingerabdruck“ und 3.1.4 „Akustischer Fingerabdruck“).

3.1.2 Digitales Wasserzeichen

Mit steganografischen[5] Verfahren lassen sich digitale Wasserzeichen in Dateien einbetten, die Metainformationen enthalten. Diese Vermerke sind fest mit den eigentlich informationstragenden Daten (Video, Audio, Bitmap, ...) verwoben. Dies ist die Voraussetzung für die Robustheit der Wasserzeichen gegen Versuche, sie zu entfernen oder zu manipulieren. Die Entfernung digitaler Wasserzeichen aus einem elektronischen Dokument ist zwar dennoch oft möglich, jedoch aufgrund der engen Verknüpfung von Information und Metainformation stets mit Datenverlusten verbunden, im Falle von digitaler Musik z.B. mit einer merklichen Verschlechterung der Klangqualität. Die Diskussion um den Urheberrechtsschutz an digitaler Musik verlieh dem Thema Wasserzeichen in der jüngeren Vergangenheit neue Brisanz. 1999 wurde durch Branchenvertreter die Secure Digital Music Initiative gegründet, dem auch das Erlanger Fraunhofer Institut angehört, das den MP3-Standard entwickelte. Auch die Technologie zur Einbettung von Wasserzeichen in einen MP3-Audiostream soll nun in Mittelfranken perfektioniert werden.

Zur Digitalisierung von Musik in CD-Qualität wird gewöhnlich mit einer Frequenz von 44,1 kHz abgetastet, d.h. es wird 44.100 mal pro Sekunde ein Ton-Intensitätswert (i.d.R. zwischen 0 und 65.535=2^16-1) gemessen und gespeichert. Um nun eine solche Datei mit einem Wasserzeichen zu versehen, können z.B. zwei Bit jedes 150. Abtastwertes für die Codierung von Copyright-Informationen verwendet werden. Eine Verschlechterung der Musikqualität ist hierbei unvermeidlich, wenn auch meist nicht durch den Benutzer erkennbar. Im Fall digitalisierter Musik ist eine solch geringfügige Manipulation des originalen Datenstroms nicht durch das menschliche Ohr wahrnehmbar. Das Abzweigen von 2 aus 16 Bit zur Codierung des Wasserzeichens bedeutet eine Verfälschung des Intensitätswerts um maximal 2^2/2^16=0,006%. Da dies zudem nur (z.B.) bei jedem 150. Samplewert geschieht, ist die Klangverschlechterung minimal. Ähnliches gilt für Videosignale.

Die Grundfunktion digitaler Wasserzeichen ist die Identifikation des Trägers der Urheberrechte des signierten Dokuments (Eigentumsnachweis). Die Urheberinformationen werden bei der Vervielfältigung des Originaldokuments mitkopiert. Als Kopierschutz können digitale Wasserzeichen nur dann auf direktem Weg dienen, wenn die zum Kopieren verwendete Hard- oder Software integraler Bestandteil eines DRMS und daher mit entsprechenden Abfragen ausgerüstet ist (ähnlich den in Abschnitt 3.1.1 behandelten Metatags). Entsprechend einfach kann ein solcher „Schutz“ umgangen werden. Dieses Problem zeigt sich schon des

---

[5] Steganografie („Verdecktes Schreiben“): Kommunikation auf eine Art und Weise, welche die Existenz einer Kommunikation verbirgt

längeren beim Kopieren von Orginial-CDs, da CD-Brenner für PCs ebenso wie die meisten Brennprogramme das auf handelsüblichen CDs enthaltene Kopierschutz-Bit ignorieren. Lediglich manche CD-Recorder für den HiFi-Heimbereich weigern sich, solche Tonträger als Quelle für Kopien zu akzeptieren. Angesichts vieler einschlägiger Angebote zur „Umrüstung“ solcher CD-Recorder scheint jedoch auch dies keinen Schutz zu bieten.

Die verschiedenen Ansätze für digitale Wasserzeichen unterscheiden sich stark hinsichtlich der Robustheit des Wasserzeichens. Das Wasserzeichen darf weder gelöscht noch das Auslesen unmöglich gemacht werden können. Bei der Entwicklung von Wasserzeichen-Verfahren muss eine ganze Anzahl von Eingriffen in das Material berücksichtigt werden, die auch zu Änderungen im eingebrachten Wasserzeichen führen. Diese Veränderungen können in freundliche und feindliche Attacken unterteilt werden. Freundliche Attacken bezeichnen Bildveränderungen, die ein Kunde am Bildmaterial vornimmt, ohne bewusst das Wasserzeichen verändern oder löschen zu wollen. Darunter würden z.B. Skalierungen und Kompressionsverfahren fallen. Natürlich können freundliche Attacken auch von einem Piraten benutzt werden, um ein Wasserzeichen zu löschen. Feindliche Attacken sind Bildänderungen, die das Bildmaterial zwar kaum verändern, aber größtmöglichen Schaden am Wasserzeichen verursachen, z.B. mittels Aufaddieren eines schwachen Rauschens.

Ein gegenwärtig verfolgter Ansatz des Urheberschutzes durch Wasserzeichen macht sich den Unterschied zwischen robusten und instabilen Wasserzeichen zu Nutze. Die zu schützenden Dokumente werden hierbei sowohl mit einem robusten als auch einem instabilen Wasserzeichen ausgestattet, das bereits bei geringsten Manipulationen verloren geht. Abspielgeräte (z.B. DVD-Player) können nun so programmiert werden, dass sie nur noch solche Dateien akzeptieren, die entweder kein Wasserzeichen (ungeschützte Datei) oder beide Wasserzeichen tragen (Originaldatei). Bei Vorliegen des robusten Wasserzeichens allein wird die Wiedergabe verweigert.

Digitale Wasserzeichen eignen sich sowohl zum Schutz von statischen Contents ohne Zeitkomponente (Bilder, Grafiken, ...) als auch von Streaming Content wie Audio und Video. Zum Schutz von Bilddokumenten existieren Plugins für gängige Grafikapplikationen (z.B. Digimarc für Adobe Photoshop), die das Verweben von Grafiken mit Copyright-Informationen einfach und sicher ermöglichen.

Aus naheliegenden Gründen ist die beschriebene Wasserzeichentechnologie nicht geeignet zur Signatur von Informationen, die kein Rauschen (leichte Veränderungen der Informationen, wie sie z.B. bei der analogen Übertragung entstehen können) zulassen. Bei ausführbaren Programmen, Fließtexten, Quellcodes oder ähnlich sensiblen Daten können Eingriffe in nur wenige Bit zu empfindlichen Datenverlusten führen. Zwar können solche Dateien ebenfalls mit Metainformationen ausgestattet werden, jedoch nur außerhalb der eigentlich infor-

mationstragenden Bereiche, also mit entsprechend geringem Schutz gegen manipulative Eingriffe (vgl. Abschnitt 3.1.1 „Metatags“).

3.1.3 Digitaler Fingerabdruck

Die Technologie der digitalen Fingerabdrücke versucht die Schwächen der Metatags und der digitalen Wasserzeichen zu umgehen, indem die Informationen über Urheber- und Nutzungsrechte aus dem Dokument heraus an eine dritte, vertrauenswürdige Stelle verlagert werden. Meist dient hierzu ein DRM-Server des Anbieters der kostenpflichtigen Dienste oder Inhalte. Die Dokumente werden anhand eines charakteristischen Werts identifiziert, der für jedes Dokument eindeutig ist. Nachdem das Dokument identifiziert wurde, können ihm die zentral hinterlegten Metainformationen zugeordnet werden. Der Identifikationswert ist nicht gesondert im Dokument abgelegt, sondern ist eine Funktion des Dateiinhalts (Hashwert). Da sich also keinerlei Metainformationen im zu schützenden Dokument befinden, können diese auch nicht manipuliert werden.

Der digitale Fingerabdruck kann in proprietären Systemen wie z.B. einer Musiktauschbörse dienen, um geschützte Werke aus dem Angebot herauszufiltern oder den Download nur unter besonderen Konditionen (Zahlung eines Entgelts) zu ermöglichen. Der Hashwert-Ansatz kann jedoch auch dazu dienen, um Urheberrechtsinteressen in offenen Netzen zu schützen. So können z.B. automatische Agenten (in diesem Fall Spider genannt) das Internet ständig nach Dokumenten absuchen, die den Fingerabdruck einer urheberrechtlich geschützten Datei tragen. Handelt es sich um rechtswidrige Angebote, können die Betreiber der entsprechenden Internet-Angebote zum Entfernen der Dateien aufgefordert oder ggf. strafverfolgt werden.

Der Ansatz ist jedoch nicht unproblematisch, da kleinste Änderungen im zu schützenden Dokument, die Nutzer problemlos vornehmen können, zu einem anderen Hashwert führen und die Identifikation verhindern. Dokumente mit bislang unbekannten Hashwerten müssen also vom DRMS vollständig indexiert werden, ebenso die Hashwerte von frei verbreitbaren Werken, da diese von den nicht indexierten geschützten Dokumenten unterscheidbar sein müssen.

Die Sensibilität von Hashfunktionen gegenüber kleinsten Änderungen im Datenmaterial ist deren wichtigste Eigenschaft, da erst sie eine eindeutige Identifikation erlaubt. Doch ist diese Sensibilität gleichzeitig auch ihre größte Schwäche, sofern das gewählte Geschäftsmodell das Vorhandensein mehrerer Versionen desselben Dokuments technisch zulässt. Am Beispiel digitaler Musik führt das Erzeugen von MP3-Daten vom selben Original auf identischer

Hard- und Software in aller Regel zu Dateien mit unterschiedlichen Hashwerten[6]. Das DRMS kann also auf neu ins System eingespeiste Dateien erst verzögert reagieren, nämlich nach erfolgter Indexierung. Ein Lösungsansatz kann hier sein, dass das DRMS den Austausch von Dokumenten mit nicht indexiertem Hashwert präventiv verhindert. Dies geht jedoch stark zu Lasten der Benutzerfreundlichkeit des Systems. Um den Schwächen des digitalen Fingerabdrucks im Bereich digitaler Musik zu begegnen, wurde der Ansatz des akustischen Fingerabdrucks entwickelt (vgl. Abschnitt 3.1.4).

3.1.4 Akustischer Fingerabdruck

Die Angreifbarkeit von Metatags und Wasserzeichen zu umgehen und gleichzeitig anwendungsfreundlicher zu sein als der digitale Fingerabdruck ist das erklärte Ziel der Verfechter des akustischen Fingerabdrucks. Der Begriff „akustisch“ wird verwendet, da die Technik zwar prinzipiell auch auf Videodaten und Grafiken übertragbar ist, bisher jedoch vor allem im Audiobereich Anwendung findet.

Während der digitale Fingerabdruck Audiodateien anhand ihres individuellen Bitstreams identifiziert, erfolgt dies beim akustischen Fingerabdruck anhand des „Klangs“ der Musik. So wird gewährleistet, dass ein Musikstück auch dann noch erkannt wird, wenn es mit unterschiedlichsten Bitraten digitalisiert wurde, von unterschiedlichen Originalen gewonnen wurde, oder bei der Digitalisierung unterschiedliche Hard- und Software zum Einsatz kam. Entsprechende Lösungen wurden bereits zur Marktreife entwickelt (Anbieter sind z.B. die Firmen Audible Magic und Cantametrix). Diese setzen bei der digitalen Signalverarbeitung (DSP) psycho-akustische Erkenntnisse ein, um den urheberrechtlich geschützten Titeln anhand des charakteristischen Höreindrucks die korrekten Metainformationen zuordnen zu können.

Die Sensibilität dieser Technik gegenüber Unterschieden des Tonmaterials wird durch den verwendeten Algorithmus beeinflusst. Die von Cantametrix entwickelte Technik ist nach Angaben des Herstellers tolerant genug, um unterschiedlich gewonnene digitale Abbilder der selben Musik als identisch zu identifizieren, jedoch sensibel genug, um z.B. eine Live-Darbietung von einer Parodie desselben Stücks zu unterscheiden.

---

[6] Der Grund hierfür ist, dass Audio-CDs grundsätzlich mit mehr oder weniger großen Lesefehlern ausgelesen werden, ob vom HiFi CD-Spieler oder PC CD-Laufwerk. Die bei Daten-CDs für die Fehlerkorrektur vorgesehenen Teilbereiche der einzelnen Sektoren werden bei Audio-CDs für Musikdaten verwendet.

3.1.5 Verschlüsselung

Gerade bei DRMS, die sich des Metatagging-Ansatzes bedienen, ist es notwendig, die geschützten Dokumente durch Verschlüsselung gegen Eingriffe in die im Dokument gesondert abgelegten Metainformationen zu schützen[7]. Hierzu kann auf erprobte Verschlüsselungsalgorithmen zurück gegriffen werden. Da DRM zunehmend für den Online-Vertrieb multimedialer Inhalte eine Rolle spielt, wird hier kurz auf die wesentlichen Ansätze zur Verschlüsselung von Streaming Content (Audio, Video) eingegangen.

Es kommen hier zwei Verfahren zum Einsatz: das Secure-Envelope- und das Scrambling-Verfahren. Diese unterscheiden sich dahingehend, ob der Verschlüsselungsalgorithmus bereits in den „Codec“ integriert ist oder nicht. Jedes Dateiformat zum Transport multimedialer Inhalte definiert sich durch einen so genannten Codec. Dies ist der Algorithmus der bei der Aufbereitung des Orginialinhalts zu einer kompakten Datei verwendet wird. Die meisten Codecs (z.B. AVI, MPEG, DivX, MP3,...) bedienen sich integrierter Kompressionsverfahren, um die benötigte Speicherkapazität und Bandbreite zu reduzieren. Hierbei werden meist Qualitätskompromisse notwendig. Anwenderbedürfnisse und Entwicklerziele entscheiden über die Art des Kompromisses (z.B. beim GIF-Codec: Bildschärfe vor Farbtiefe). Zur Wiedergabe der produzierten Dateien wird ebenfalls der entsprechende Codec benötigt, der die erhaltenen Daten korrekt interpretiert, entpackt und unkomprimiert darstellt.

Um Inhalte zu verschlüsseln, muss der Codec mit einem Chiffrieralgorithmus kombiniert werden. Erfolgt die Ver-/Entschlüsselung und das Codec-Verfahren getrennt, so spricht man vom Secure Envelope-Verfahren, da die bereits komprimierten Informationen in einem zweiten Schritt in einen „sicheren Umschlag“ gesteckt werden. Die hier eingesetzten Verschlüsselungsverfahren sind zwischen den Codecs übertragbar, d.h. es können beliebige Dateiformate verschlüsselt werden. Da jedoch das Komprimieren und Dekomprimieren multimedialer Daten ebenso wie die Ver-/Entschlüsselung auch für moderne Prozessoren noch eine große Herausforderung darstellt, werden aus Effizienzgründen oft Codec und Chiffrier-Algorithmus direkt kombiniert, so dass Ver-/Entschlüsselung und Codec-Verfahren zusammen (einstufig) erfolgen (Scrambling-Verfahren).

---

[7] Die XML Encryption Working Group des W3C unternimmt daher Bemühungen einen Verschlüsselungsstandard für den Austausch von XML-Dokumenten zu spezifizieren [http://www.w3.org/Encryption/2001].

3.2 Beispiel eines Digital Rights Management Systems

Digital Rights Management Systeme (DRMS) stellen die vollständige informationstechnische Infrastruktur bereit, die notwendig ist um Rechte, die sich auf digitale Informationen und Dienstleistungen beziehen, zu verwalten und zu schützen. Autoren, Verlage und andere Informationsdienstleister werden in die Lage versetzt, ihre Werke und Dienste mit Nutzungsrechten und -regeln auszustatten, deren Einhaltung durch das DRMS gewährleistet wird. Diese Rechte und Regeln bilden Informationen ab über bestimmte Besitzrechte, Nutzungsrechte und Erwerbsmodalitäten, aber auch Garantien oder sonstige für den elektronischen Vertrieb relevante Informationen. Durch die Standardisierung der Ausstattung digitaler Dokumente mit solchen Rechten und Regeln mittels zuverlässiger Methoden wird die Basis geschaffen für einen lebensfähigen elektronischen Handel mit digitalisierten Informationen. Am Beispiel des Windows Media Rights Manager soll hier ein solches DRMS illustriert werden.

Das DRMS „Windows Media Rights Manager“ wurde für den Vertrieb von WMA- bzw. WMV-codierten Audio- und Videodaten entworfen. Es wird von den gängigsten Medienwiedergabeprogrammen unterstützt (MusicMatch, Sonique, WinAMP, Windows Media Player etc.). Es bietet die Möglichkeit zur flexiblen Definition von Nutzungsregeln und -beschränkungen, so dass verschiedenste Geschäftsmodelle realisiert werden können. So kann z.B. der Zeitraum definiert werden, in dem erworbene Inhalte abgespielt werden dürfen, um Online-Videotheken oder Testangebote realisieren zu können. Auch kann die Nutzung bzgl. Häufigkeit oder Dauer des Abspielens beschränkt werden. Ebenfalls möglich ist die so genannte „Super Distribution“, d.h. bezogene Inhalte dürfen kopiert und weitergegeben werden, da die Empfänger eine persönliche Lizenz erwerben müssen, um die Inhalte betrachten zu können. Die Nichtübertragbarkeit von Lizenzen wird gewährleistet, indem sich unterschiedliche Installationen der Abspielsoftware bei der Clearing-Stelle (siehe unten) individuell identifizieren.

Ablauf des Lizenzierungsprozesses mit dem Windows Media Rights Manager:

1. Verpacken der Inhalte

Eine im WMA oder WMV-Format vorliegende Originaldatei wird vom Anbieter (dem Inhaber der Urheberrechte) verschlüsselt (Secure Envelope) und mit einigen wenigen Metainformationen versehen wie einer eindeutigen Kennung und der Webadresse, bei der die Abspiellizenz erworben werden kann.

2. Einrichten einer Clearing-Stelle

Der Anbieter hinterlegt die seinem Geschäftsmodell entsprechenden Nutzungsregeln zusammen mit dem Schlüssel in einer Lizenz, die über eine Clearing-Stelle abgerufen werden kann. Durch die Trennung der Nutzungsregeln von den Inhalten können die Anbieter auch

dann noch das Lizenzierungsmodell anpassen, wenn sich die betreffenden Dateien bereits verbreitet haben.

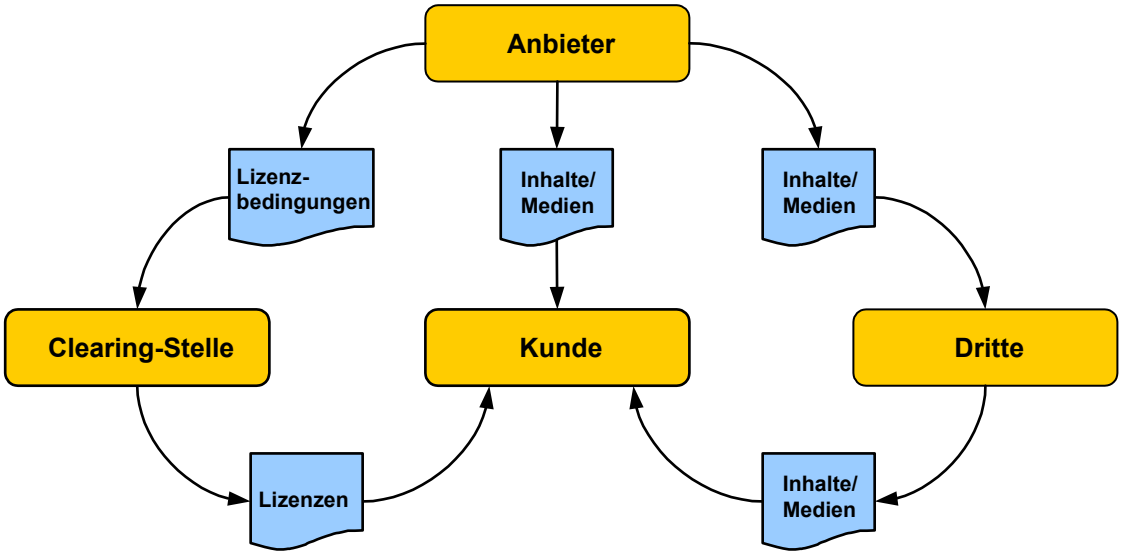

Abbildung 3-1: Windows Media Rights Management System

3. Veröffentlichen der Inhalte

Die geschützten Dateien können nun vom Anbieter selbst oder durch Dritte vertrieben werden, indem sie zum Download bereitgestellt, per E-Mail versandt oder auf CD gepresst werden. Die erwähnte Super Distribution ist ebenfalls möglich.

4. Erwerb einer Lizenz

Öffnet ein Kunde ein komplett heruntergeladenes Dokument oder ruft einen Stream ab, so wird er auf die Webadresse der Clearing-Stelle verwiesen, die im Dokument vermerkt ist. Dort kann mit unterschiedlichen Bezahlverfahren eine Lizenz erworben werden. Dieser Mechanismus kann auch für frei verfügbare Werke genutzt werden, deren Anbieter ein Interesse hat, Nutzungsgewohnheiten auszuspähen. Dem Benutzer bleibt der Erwerb einer solchen „Gratislizenz“ verborgen.

5. Abspielen der Inhalte

Mit Hilfe des mit der Lizenz erworbenen Schlüssels kann der Nutzer die erhaltenen Dokumente im Rahmen der lizenzierten Nutzungsrechte betrachten. Ist eine zeitliche Nutzungsbeschränkung oder ein Abspiellimit (Dauer, Häufigkeit) vereinbart, so wird die Datei mit Eintritt dieser Bedingungen unbrauchbar bis eine weitere Lizenz erworben wird.

Auf individuell zu erwerbenden und inhaltsspezifischen Lizenzen beruhende DRMS schützen Urheberinteressen mit großer Zuverlässigkeit. Dennoch stehen diese Ansätze allgemein in der Kritik, da persönliche Daten wie individuelle Interessen an Diensten und Inhalten ein-

schließlich aller Nutzungsgewohnheiten vollständig Preis gegeben werden. Viele DRMS überwachen jede einzelne Handlung des Lesens, Anhörens und Betrachtens im Internet durch individuelle Nutzer, wobei hochsensible Informationen über die Betroffenen gesammelt werden. Zwar haben Rechteinhaber einen Anspruch auf Wahrung dieser Rechte, doch ebenso haben Nutzer das Recht auf Datenschutz und Informationsfreiheit, wie von offiziellen Datenschutz-Gremien der EU, des Bundes und der Länder übereinstimmend festgestellt wird. Insbesondere der stumme Lizenzerwerb gefährdet das Telekommunikationsgeheimnis, da dem Nutzer die Protokollierung seiner Nutzungsgewohnheiten verborgen bleibt. Nachweislich ist diese weitgehende Nutzertransparenz nicht notwendig, doch sind die gewonnenen Daten für Anbieter von höchstem Wert, da sowohl das Verhalten als auch das demografische Profil der Nutzer für die Marketing-Aktivitäten der Anbieter eine exzellente Datenbasis darstellen.

4 Quellen

ASPSecure, http://www.aspsecure.com

Audible Magic, http://www.audiblemagic.com

Cantametrix, http://www.cantametrix.com

Committee on Intellectual Property Rights in the Emerging Information Infrastructure: The Digital Dilemma – Intellectual Property in the Information Age, Washington D.C. 2000, http://www.nap.edu/html/digital_dilemma/

Digimarc, http://www.digimarc.com

Digital Rights Management 2001, http://www.thirdwave.de

Digital World Services – The Bertelsmann Digital Rights Management Company, http://www.dwsco.com

Fraunhofer Institut für Integrierte Schaltungen, http://www.iis.fhg.de

GMD Forschungszentrum Informationstechnik, http://www.darmstadt.gmd.de

Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation: Gemeinsamer Standpunkt zu Datenschutz und Urheberrechtsmanagent, http://www.lda.brandenburg.de/ internat/iwgdpt/27_04.htm

InterTrust Technologies, http://www.intertrust.com

Nethics e.V., http://www.nethics.net

Secure Digital Music Initiative, http://www.sdmi.org

Strömer Rechtsanwälte, Online- und Multimediarecht, http://www.netlaw.de

Dr. Jürgen Weinknecht (RA), http://www.weinknecht.de

Windows Media Rights Manager, http://www.microsoft.com/windows/windowsmedia/en/wm7/drm.asp

World Wide Web Consortium, http://www.w3c.org

XML/EDI Group, http://www.xmledi-group.org

XML Industry Portal, http://www.xml.org

XrML (Extensible Rights Markup Language), http://www.xrml.org