Zeitschrift für Urheber- und Medienrecht ZUM 10/2000

Multimediale Inhalte und technischer Urheberrechtsschutz im Internet

Von Dr.-Ing. Hannes Federrath

International Computer Science Institute, Berkeley, Kalifornien

E-Mail: **hannes@icsi.berkeley.edu**

Dieses Papier entstand zum Vortrag "Neueste technische Entwicklungen und Nutzungen im Internet – MP3, Streaming, Webcasting on demand-Service u.a." beim XIV. Symposion zum Film- und Medienrecht am 30. Juni 2000 in München zum Thema Lizenzrecht und Internet. Es wurde von einem Techniker mit dem Ziel geschrieben, technische Zusammenhänge für einen Nichttechniker verständlich zu machen. Die Vortragsfolien können **hier** (435.387 KB) abgerufen werden. Ein herzlicher Dank für wertvolle Hinweise und Diskussionen während der Vorbereitung des Vortrags und beim Schreiben des Papiers geht an Stefan Bechtold und Thomas Hecht.

Zusammenfassung

Der Kampf gegen die illegale Bereitstellung und Nutzung urheberrechtlich geschützter Daten im Internet mit Hilfe technischer Mittel scheint angesichts der phantasievollen Umgehungsmöglichkeiten von Sperren aussichtslos. Die Markierung geschützter Inhalte mit Hilfe digitaler Wasserzeichen und digitaler Fingerabdrücke ermöglicht wenigstens die Verfolgung individuell markierter Kopien und besitzt damit für den Piraten abschreckende Wirkung. Eine Verbreitung von digitalen 1:1 Kopien könnte mit Hilfe hardwaregestützter kryptographischer Verfahren verhindert werden. Allerdings sind solche Technologien sehr teuer und helfen in der Praxis sehr wahrscheinlich auch nur eine begrenzte Zeit. Versuche, das Internet dermaßen zu verändern, daß die Benutzer bei allen Handlungen (egal, ob legal oder illegal) verfolgbar sind, scheitern technisch an der Verfügbarkeit und Nutzbarkeit von Anonymisierungsdiensten und dürften zudem in Konflikt stehen mit datenschutzrechtlichen Bestimmungen.

1 Einführung

Für Menschen, die ihren Lebensunterhalt über Lizenzgebühren bestreiten, dürften die Digitalisierung und das Internet ein Segen und ein Fluch zugleich sein. Die Distributionsmöglichkeiten sind global und billig; die Digitalisierung ermöglicht den verlustfreien Transport zum Konsumenten, aber auch die sehr einfache Herstellung und illegale Verbreitung exakt gleicher Kopien ohne Qualitätsverlust. Deshalb stellt sich die Frage, ob und wie Piraten daran gehindert werden können, illegale Kopien zu verbreiten. In diesem Papier werden die *technischen* Zusammenhänge und Möglichkeiten hierfür untersucht und bewertet.

Für eine Bewertung in Frage kommende Kriterien, teilweise nichttechnischer Natur, sind die *Angemessenkeit* (speziell die Kosten und die Akzeptanz beim Konsumenten) und die *Stärke* (speziell gegen welche Stärke eines Angreifers/Piraten ein Schutzsystem noch hilft). Ein weiteres Kriterium ist die *Überwachbarkeit der Konsumenten*.

2 Distribution von multimedialen Inhalten

Man kann Verteilung von multimedialen Inhalten unterscheiden nach Offline-Verteilung, z.B. über Compact Disc oder andere Datenträger und Online-Verteilung, z.B. per Rundfunk, über spezielle Verteilkabel, Telefon oder über das Internet.

Online verteilte Inhalte können synchron und asynchron konsumiert werden. Synchron/asynchron bezieht sich auf den zeitlichen Zusammenhang zwischen Datenübertragung und Konsumierung (Tabelle 1). *Asynchron*: Inhalte, die auf einem Datenträger verteilt werden, können zu jeder beliebigen Zeit und auch mehrmals konsumiert werden. Synchron: Inhalte, die synchron übertragen werden (z.B. Rundfunk, Fernsehen, aber auch Streaming-Daten im Internet), müssen vom Konsumenten erst gespeichert werden, damit sie asynchron oder wiederholt konsumiert werden können.

Die Tatsache, daß eine Abspielsoftware (z.B. Windows Media Player oder Real Player) das Abspeichern nicht im Funktionsumfang anbietet, bedeutet keinesfalls, daß ein Pirat nicht in der Lage wäre, ein Programm zu schreiben, mit dem das Abspeichern möglich ist.

Tabelle 1. Verteilungsformen Multimediadaten

	Online	Offline
Synchron	Rundfunk, Fernsehen	–
Asynchron	z.B. Abruf von Webseiten im Internet	z.B. Distribution über Datenträger (CD, DVD)

Neben Offline/Online kann man auch nach der Eignung des Mediums zur Interaktivität unterscheiden.

2.1 Klassische Distribution von Inhalten

Gemäß der Tabelle 1 sollen Dienste, die synchron und Online oder asynchron und Offline verteilt werden, als klassische Distributionsformen bezeichnet werden. Die Verteilung von multimedialen Inhalten über das Internet wird im Abschnitt 2.2 behandelt.

Eines der wesentlichen Merkmale der klassischen Distribution ist die Verteilung exakt gleicher Kopien an alle Konsumenten. Dies hat zur Folge, daß einer illegalen Kopie nicht anzusehen ist, wer die Kopie aus dem Original angefertigt hat und welchen Verteilweg sie genommen hat.

Ein Schutz vor Verbreitung digitaler 1:1-Kopien wurde in der Praxis bisher lediglich dadurch erreicht, daß das Herstellen solcher Kopien zu aufwendig oder zu teuer war. Die technische Entwicklung ermöglicht heute jedoch das preiswerte Anfertigen von Kopien. Beispiel CD-R: Noch vor ein paar Jahren war das Anfertigen einer digitalen 1:1-Kopie einer Musik-CD teurer als der Kauf der Original-CD.

Eine Möglichkeit zum Schutz vor illegalen Kopien besteht darin, die Daten auf dem Datenträger zu verschlüsseln und in einer separaten, ausforschungssicheren Hardware zu entschlüsseln (z.B. eine Chipkarte, die jedem Datenträger beiliegt, ähnlich einem Dongle, mit dem teure Software gegen Raupkopieren geschützt wird). Das Abspielgerät besitzt dann einen Schacht für den Datenträger und einen für die Chipkarte. Eine digitale Kopie der verschlüsselten CD wäre damit ohne die zugehörige Chipkarte wertlos. Allerdings dürfen die entschlüsselten Daten im Abspielgerät nicht unberechtigt abgegriffen werden können, um aus ihnen eine unverschlüsselte digitale 1:1-Kopie herstellen zu können, was aber mit einem PC leicht möglich sein wird. Deshalb ist ein solches Verfahren in der Praxis untauglich und zudem teuer, weshalb es praktisch nicht angewendet wird.

Eine abgeschwächte Variante der vorgenannten Möglichkeit ist heute beispielsweise in DVD-Spielern (Digital Versatile Disk) bzgl. des sogenannten Content Scrambling Systems (CSS) und des "Ländercodes" realisiert. In die Player-Hardware ist ein Schutzmechanismus integriert, der das Entschlüsseln verschlüsselter DVDs ermöglicht und das Ändern des Ländercodes auf eine maximale Anzahl begrenzt. Dieses Schutzsystem wurde allerdings bereits geknackt und die entsprechenden Codes kursieren im Internet.

Eine andere Möglichkeit wäre es, jedem Datenträger einen maschinenlesbaren, aber schwer kopierbaren Code mitzugeben, der z.B. in einem Hologramm enthalten ist. Da ein Hologramm schwer kopierbar ist, ist eine 1:1-Kopie der verschlüsselten Daten ohne den Code wertlos. Allerdings kann man davon ausgehen, daß bereits nach kurzer Zeit ebenfalls die Codes im Internet kursieren würden, womit ein solches Verfahren auch nur gegen Gelegenheitstäter hilft.

Synchrone Distributionsformen (Rundfunk, Fernsehen) sind von der leichten Kopierbarkeit im gleichen Maße betroffen, da es einfach möglich ist, die Inhalte digital aufzuzeichnen und ebenfalls asynchron (d.h. zeitversetzt) weiterzuverbreiten.

Die illegale synchrone Re-Distribution von Rundfunk und Fernsehen, d.h. das unberechtigte "Ausstrahlen" z.B. im Internet dürfte derzeit in den meisten Fällen noch am

Mangel an technischer Ausstattung scheitern. Allerdings werden die Rechner und Internetverbindungen immer schneller. Software, mit der Jedermann seine eigene Internet-Radiostation betreiben kann, ist bereits am Markt. Beispiel Shoutcast: "SHOUTcast is Nullsoft's Winamp-based distributed streaming audio system. Now you can listen to live streaming audio, and even broadcast your own SHOUTcast station from the comfort of your regular Internet connection." (**http://www.shoutcast.com/**)

Solche Programme sind sowohl für live- als auch für on-demand MP3 Internet Broadcast geeignet. Natürlich könnten diese Stationen auch mit fremden Inhalten gespeist werden.

2.2 Distribution von Inhalten im Internet

Bei der Distribution von Inhalten im Internet werden *heute* an alle Konsumenten ebenfalls exakt gleiche Kopien übermittelt. Insofern gelten alle Aussagen hierzu aus dem vorangegangenen Abschnitt.

Das Herstellen und die Re-Distribution von legalen wie illegalen Kopien kann heute über Dienste stattfinden, die teilweise darauf spezialisiert sind, bestimmte Medienformen möglichst unkontrollierbar zu verbreiten. Zur Verbreitung können verwendet werden:

1. Private Webpages, News-Groups, E-Mail verwendet werden, auch wenn diese Dienste nicht spezialisiert sind auf bestimmte Medienformen;
2. Scour, ein "shared directory", das mit komfortablen Suchfunktionen ausgestattet ist und spezialisiert, aber nicht beschränkt ist auf Bilder, Videos und Musikstücke; **http://www.scour.com/**;
3. Napster, eine kostenlose Vermittlungsdatenbank für MP3-Dateien; die Datei wird anschließend direkt zwischen dem Anbieter und Interessenten übermittelt, ohne durch den Napster-Server zu laufen; **http://www.napster.com/**;
4. Gnutella, ein dezentralisiertes System zum Bereitstellen von beliebigen Inhalten, bei dem sowohl die Vermittlungsdatenbank als auch die Daten dezentralisiert sind; **http://gnutella.wego.com/**.

Eine Verfolgung illegaler Inhalte ist bei den genannten Systemen theoretisch möglich, da auf der Netzwerkebene des Internet Adressierungsinformationen verwendet werden können, um den Anbieter bzw. Konsumenten zu verfolgen. Dies machen sich z.B. der Media Enforcer (**http://mediaenforcer.tripod.com/enforcer/**) und Zeropaid (**http://www.zeropaid.com/busted**) zunutze, um die IP-Adressen von Tauschhändlern herauszubekommen. Zeropaid betreibt beispielsweise einen Gnutella-Server, der die Interessenten von Kinderpornographie mit eindeutigen Dateinamen locken soll. Hinter den Dateien verbergen sich allerdings nicht die erwarteten Inhalte, jedoch erfährt Zeropaid die IP-Adresse des an dem Material Interessierten, um ihm anschließend möglichst das Handwerk zu legen.

Zukünftig könnten völlig legal angebotene Anonymisierer allerdings jegliche Verfolgung verhindern. Freenet (**http://freenet.sourceforge.net/**) ist beispielsweise ein dezentralisiertes System, bei dem sich Inhalte, sofern sie von anderen Nutzern tatsächlich abgerufen werden, nicht einfach löschen lassen, da sie sich durch eine spezielle Caching-Technik im "Freenet" ausbreiten. Der Dienst wurde entwickelt, um *free speech* im Internet zu realisieren, d.h. unter anderem die Möglichkeit, unzensiert und anonym im Internet zu publizieren. Freedom (**http://www.freedom.net/)**, ist ein kommerzielles System, das zur Verschleierung von Absender- und Empfängerinformationen (inkl. IP-Adressen) angeboten wird. Eigene Forschungsarbeiten belegen ebenfalls, daß die Anonymisierung von Internetzugriffen zwar aufwendig, aber technisch möglich ist. Zum unbeobachtbaren Surfen im Web ist das System Web Mixe verfügbar (**http://www.inf.tu-dresden.de/~hf2/anon/)**.

Bezüglich des technischen Schutzes des Urheberrechtes sind Forderungen nach einem Verbot von privater, anonymer und unbeobachtbarer Kommunikation lediglich das Resultat unzureichender Schutzmechanismen im Vorfeld. Anstelle die Wirkung zu bekämpfen, sollte besser bei den technischen Ursachen begonnen werden, d.h. das leichte und unkontrollierte bzw. illegale Kopieren und Verbreiten von Inhalten muß erschwert werden.

Sollen urheberrechtlich geschützte Inhalte vor illegaler Verbreitung geschützt werden, empfiehlt es sich, *zukünftig neue Techniken* anzuwenden:

1. **Watermarking:** Damit urheberrechtlich geschützte digitale Mediendaten als solche erkennbar sind und nach Manipulationen erkennbar bleiben, müssen sie mit digitalen Wasserzeichen versehen werden.
2. **Encryption:** Um individualisierte und kostenpflichtige Dienste vor unberechtigter Nutzung zu schützen, müssen die übertragenen Inhalte verschlüsselt sein.
3. **Traitor Tracing:** Für den Schutz der Urheberrechte an multimedialen Inhalten wird man zunehmend dazu übergehen, individualisierte Kopien zu verteilen, um eine Rückverfolgung des illegalen Distributionsweges zu ermöglichen.

Auf die genannten Techniken wird im Abschnitt 4 ausführlicher eingegangen. Encryption dürfte die mit Abstand ausgereifteste Technik sein, die auch sofort zur Verfügung steht, während Traitor Tracing und Watermarking teilweise noch im Entwicklungs- und Einführungsprozeß sind.

2.3 Thema Angreifermodell

Für alle Techniken gilt, daß sie gegen einen Angreifer schützen sollen, der mit Intelligenz versucht, das System zu knacken. Die Stärke eines Angreifers wird im Angreifermodell festgelegt, das bestimmt, gegen welche Angreifer das System schützen soll.

Neben allerlei technischen Details gilt: Man sollte einem Angreifer nie zuwenig zutrauen. Beispiel "security by obscurity": Es ist durch Beispiele belegt, daß das Geheim- und Zurückhalten von Informationen über ein Sicherungssystem nicht zwangsläufig zum einem Sicherheitsgewinn führt, sondern umgekehrt zu einem Sicherheitsverlust führen kann, weil beim Design wichtige Angriffe übersehen wurden. Das beste Gegenmittel ist Offenheit.

Die Kosten, die ein Angreifer zum Knacken eines Systems aufwenden wird, müssen selbstverständlich in einem gesunden Verhältnis zu den Kosten des Schutzes stehen. Insofern mag ein Schutzmechanismus, der gegen einen "Gelegenheitstäter" etwas hilft, aber nichts gegen einen professionellen Knacker, durchaus sinnvoll sein, wenn die Verluste hauptsächlich durch den Gelegenheitstäter auftreten. Die globale Verfügbarkeit von Informationen und automatisierten Tools im Internet läßt aber zunehmend die Grenzen zwischen Amateur und Profi verschwimmen, weshalb in der Praxis von einem starken Angreifer ausgegangen werden sollte.

3 Übertragungsprotokolle im Internet

Bevor im Abschnitt 4 näher auf den Schutz von Daten eingegangen wird, sollen einige Grundbegriffe der Übertragungsprotokolle im Internet eingeführt werden, da deren Verständnis die Voraussetzung für die Beurteilung der praktischen Anwendbarkeit der Mechanismen in Abschnitt 4 ist.

Nutzerdaten werden im Internet mit Hilfe von zwei Übertragungsprotokollen transportiert, dem Transmission Control Protocol (TCP) und dem User Datagram Protocol (UDP), siehe Tabelle 2.

Tabelle 2. Übertragungsprotokolle im Internet

	TCP	UDP
Punkt-zu-Punkt	Etabliert, Beispiel: HTTP (WWW)	Etabliert, aber teilweise keine Quality-of-Service-Zusicherungen, Beispiel: Real Player
Multicast/Broadcast	–	In Entwicklung und Erprobung

3.1 Transmission Control Protocol (TCP)

Das Transmission Control Protokol (TCP) wird bei Punkt-zu-Punkt-Verbindungen zwischen zwei Endpunkten, z.B. einem Browser und einem Webserver eingesetzt. Bei TCP wird darauf geachtet, daß alle vom einen Endpunkt gesendeten Bits auch tatsächlich beim anderen Endpunkt ankommen und auch deren Reihenfolge nicht durcheinander kommt. Falls Daten beim Transport verloren gehen, werden sie erneut gesendet (*Retransmission*). Dieses Transportprotokoll wird z.B. beim Transport von Webseiten, E-Mails, Dateien etc. angewendet, da man sicher gehen möchte, daß die Daten auch wirklich beim Empfänger ankommen.

Sollen mit Hilfe von TCP-Verbindungen viele Nutzer mit dem gleichen Inhalt von einem Server versorgt werden, muß jeder Nutzer eine eigene Verbindung zum Server aufbauen (Abbildung 1). Der Bandbreitebedarf wächst dadurch linear mit der Teilnehmerzahl, da der Server jeweils eine Verbindung pro Client und Request unterhält. Selbst wenn mehrmals die gleichen Inhalte vermittelt werden sollen, erfolgt keine Konzentration, um Bandbreite zu sparen. Daß ein solches Vorgehen nicht besonders effektiv ist, liegt auf der Hand, allerdings ist TCP auch nicht unbedingt für solche Verkehrsformen wie Broadcasting gedacht gewesen.

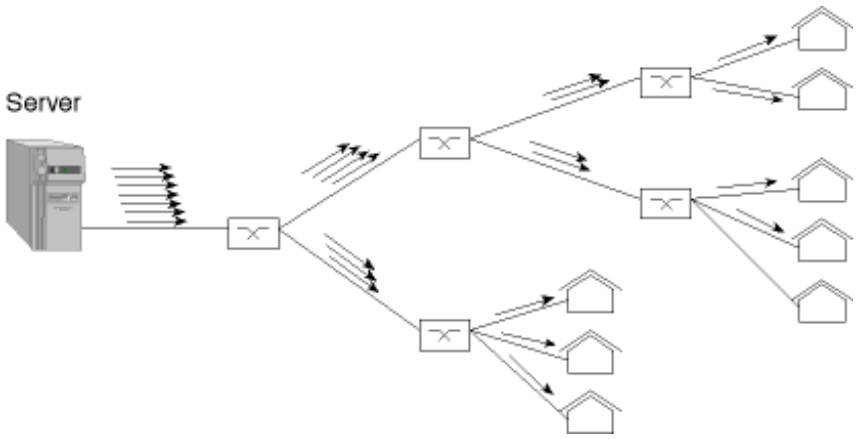

Abbildung 1. Punkt-zu-Punkt-Verbindungen

Deshalb wird mit Hilfe einer Replikation des Datenbestandes (die Server R1 und R2, siehe Abbildung 2, werden mit Kopien der Inhalte des Servers versorgt) und sogenannter Caching-Technologien versucht, einen Lastausgleich und bessere Antwortzeiten zu erreichen. Einen solchen Service bietet z.B. die Firma Akamai (**http://www.akamai.com/**) an.

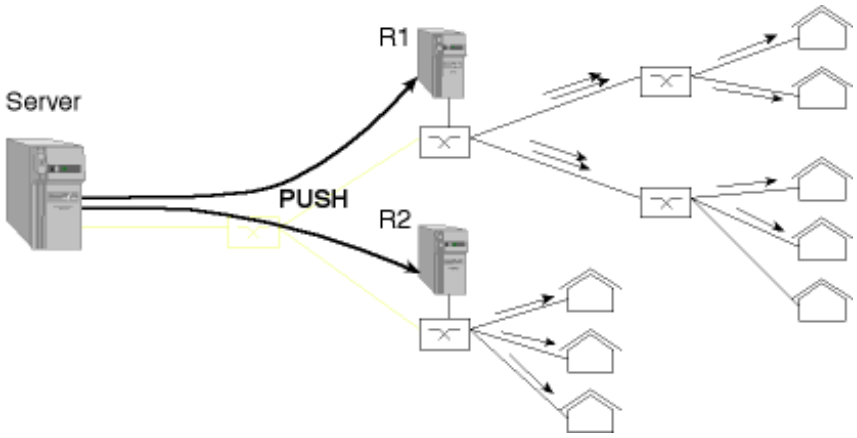

Abbildung 2. Replikation des Datenbestandes

Die Replikation löst allerdings nicht das Grundproblem der Mehrfachverteilung von Informationen, sondern reduziert es nur, da es trotzdem vorkommen wird, daß mehrere Nutzer gleichzeitig den gleichen Inhalt von einem Server abrufen.

3.2 User Datagram Protocol (UDP)

Beim User Datagram Protocol (UDP) sendet der Sender Datenpakete aus, die in Abhängigkeit von der Auslastung des Netzes den Empfänger rechtzeitig, zu spät (*delayed*) oder auch gar nicht (*dropped*) erreichen. UDP wird hauptsächlich für Datenströme verwendet, bei denen eine Retransmission nicht möglich ist. Beispielsweise bei Audio- und Videoströmen, die synchron gesendet und konsumiert werden, ist es nicht sinnvoll, verlorengegangene Datenpakete erneut zu senden, da der fehlende "Abschnitt" des Datenstroms zeitlich hinter dem aktuell gesendeten liegt. UDP-Pakete werden beispielsweise vom Real Player (**http://www.real.com/**) verarbeitet. Der Verlust von Datenpaketen macht sich je nach Kodierung der Medienströme durch Qualitätsverschlechterung oder Aussetzer bemerkbar.

Neben der Punkt-zu-Punkt-Übertragung von UDP-Paketen lassen sich auch Punkt-zu-Mehrpunkt-Übertragungen (Multicast, Broadcast) realisieren. Diese Klasse von UDP-Verkehr wird zukünftig den Bereich des Webcasting abdecken (siehe Abbildung 3). Dabei verbindet sich ein Benutzer z.B. mit einen Videodatenstrom über eine sogenannte Multicast-Adresse (*join*). Dies wird durch das sogenannte Internet Group Management Protocol (IGMP) realisiert.

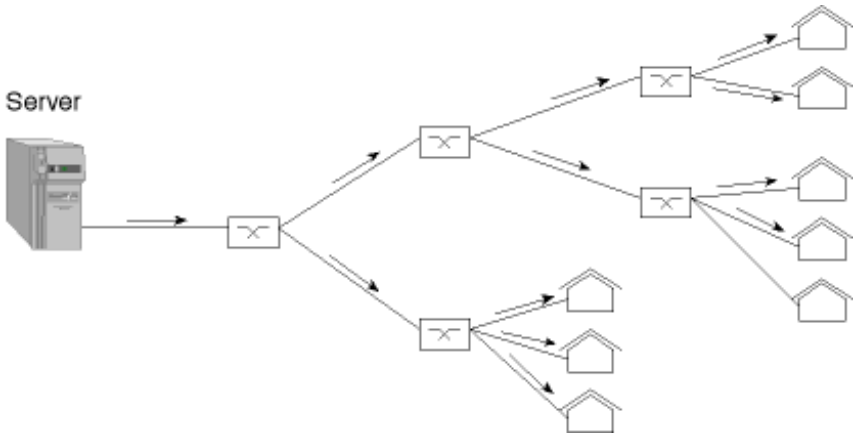

Abbildung 3. Multicast von Streamingdaten

Derzeit wird massiv an der Zusicherung sogenannter Quality-of-Service-Merkmale (QoS) gearbeitet, um die auftretenden Verzögerungen und Datenverluste derart vorhersagen bzw. vermeiden zu können, daß dem Endbenutzer eine gleichbleibend hohe Qualität der Übertragung zugesichert werden kann. Die bisher entwickelten Protokolle, die alle Sonderformen von UDP sind, tragen Namen wie Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP) und Real-Time Streaming Protocol (RTSP). Im Zusammenhang mit QoS spielt das Resource Reservation Protocol (RSVP) noch eine Rolle. In der gegenwärtigen Distributionspraxis im Internet spielen die genannten Protokolle noch keine große Rolle, was sich aber mit steigenden Übertragungskapazitäten ändern wird. An technischer Einführungsliteratur in die Multicastprotokolle kann z.B. *D. Kosiur, IP Multicasting, Wiley, 1998* empfohlen werden.

4 Techniken zum Schutz

Im folgenden sollen die Techniken Watermarking, Encryption (Verschlüsselung) und Traitor Tracing für den Schutz von Urheberrechten vorgestellt werden.

4.1 Watermarking

Beim Watermarking werden in digitale Mediendaten z.B. Informationen über den Urheber der Daten eingebettet. Die mit dem Original festverbundene, eingebettete Information wird als Watermark bezeichnet (Abbildung 4). Dieser Einbettungsprozeß muß so *robust* erfolgen, daß es unmöglich ist, das Watermark unberechtigt zu entfernen, wenn der Angreifer versucht, das Objekt zu manipulieren. Dabei sind viele verschiedene Manipulationen denkbar: Analog-Digital-Wandlung, Digital-Analog-Wandlung, Ausdrucken und erneutes Einscannen, Verändern von Größe, Auflösung, Farbtiefe, Kompression, Verzerrung, Ausschneiden von Bildteilen. Weiterhin dürfen die Mediendaten natürlich nicht durch das Watermark beeinträchtigt werden.

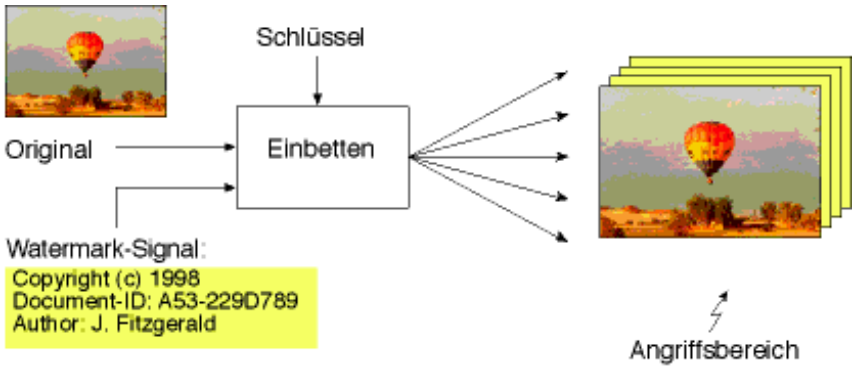

Abbildung 4. Watermarking

Ein praktisches Anwendungsbeispiel für watermarkierte Ton- und Videodaten ist das automatisierte Erstellen von Distributionsprotokollen beim Webcasting. Ein Scanner, der z.B. von einer Verwertungsgesellschaft betrieben wird, analysiert die gesendeten Daten z.B. eines Webradios nach eingebetteten Watermarks, um anschließend die Rechte des Künstlers wahrnehmen zu können, Hitlisten zu erstellen etc.

Was die Sicherheit von Watermarking gegenüber Angreifern betrifft, die ernsthaft versuchen, Watermarks zu entfernen, sind Theorie und Praxis noch erheblich voneinander entfernt. So manipuliert das Programm StirMark (Kuhn, Petitcolas, **http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/**, 1997) ein digitales Bild derart, daß der Bildinhalt weitgehend unverfälscht bleibt, aber das Watermark hinterher nicht mehr erkannt wird. Solche Resultate zeigen, daß noch Einiges an Forschungs- und Entwicklungsarbeit geleistet werden muß, bevor Watermarkingtechnologien ernsthaft gegen intelligente Angriffe sicher sind.

4.2 Encryption

Heutzutage existieren derart ausgereifte Verschlüsselungsverfahren, daß bei richtiger Anwendung das Knacken der Codes praktisch unmöglich ist. Für individualisierte und insbesondere kostenpflichtige Dienste sollten also, wann immer möglich, die Mediendaten verschlüsselt werden, um sie vor unberechtigtem Zugriff auf den Übertragungswegen zu schützen.

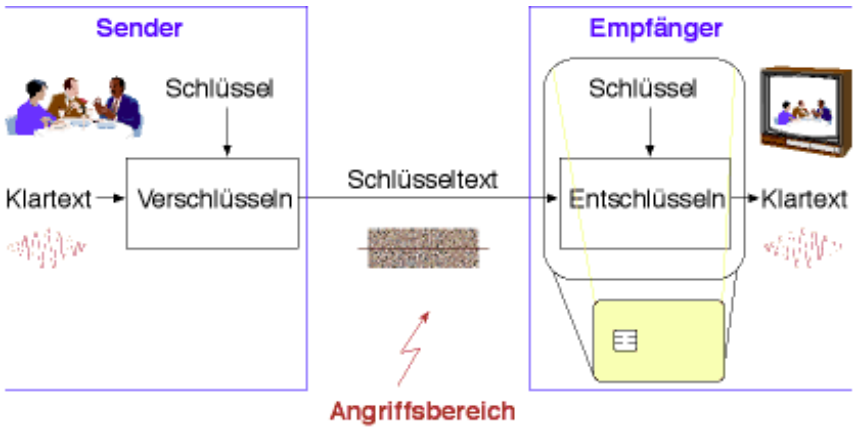

Abbildung 5. Verschlüsselung auf Übertragungswegen

Die individuelle Verschlüsselung (d.h. jeder Kunde besitzt einen eigenen Schlüssel) hat allerdings den Nachteil, daß jeder Kunde einen eigenen Medienstrom erhalten müßte, was wiederum mit einer enormen Verschwendung an Übertragungskapazität verbunden wäre (vgl. auch Abbildung 1), zumindest wenn alle Kunden zeitgleich mit den gleichen Mediendaten versorgt werden sollen.

In der Praxis wird deshalb meist ein einziger verschlüsselter Medienstrom übertragen. Alle Kunden erhalten den gleichen Schlüssel, der sich z.B. in einer Chipkarte oder in einer "Set-Top-Box" befindet und der das Gerät nie verläßt. Andernfalls wäre die illegale Verbreitung des Schlüssels möglich. Mit diesem Schlüssel ist es dann möglich, einen temporär gültigen Sitzungsschlüssel zu entschlüsseln, mit dem der eigentliche Medienstrom verschlüsselt wurde. Solche Verschlüsselungstechniken werden heute noch nicht überall angewendet. Die Verwendung eines einzigen Schlüssels hat den gravierenden Nachteil, daß viele Stellen (z.B. alle Hersteller von Player-Hardware) den Schlüssel erfahren müssen, um ihn in das Endgerät zu integrieren. Sobald eine Stelle "undicht" wird, ist das gesamte Sicherheitssystem gefährdet. Dies ist beispielsweise beim Content

Scrambling System der DVD geschehen.

Das "Scrambling" von Pay-TV-Kanälen basiert meist auf deutlich schwächeren Schutzmechanismen und kann nicht unbedingt als "Verschlüsselung" bezeichnet werden. Häufig werden die Daten nur "verschleiert" und halten ernsthaften Angriffen nicht stand.

4.3 Traitor Tracing

Die Sicherheit eines Verschlüsselungsverfahrens mit gleichem Schlüssel für alle Teilnehmer (siehe vorangegangener Abschnitt) hängt entscheidend vom *physischen Schutz* des Schlüssels ab. Physischer Schutz gelingt jedoch bestenfalls für eine beschränkte Zeit, da immer wieder einmal neue Methoden zum unberechtigten "Auslesen" von geheimen Informationen z.B. aus Chipkarten gefunden werden. Besser wäre es also, wenn jeder Kunde einen eigenen individuellen Schlüssel zur Entschlüsselung des Medienstroms bekäme. Ein Verschlüsselungsverfahren, mit dem es möglich ist, einen einzigen verschlüsselten Medienstrom an alle Empfänger zu senden, der dann mit mehreren individuellen Schlüsseln entschlüsselt wird, wird als Gruppenverschlüsselung (auch: *Broadcast Encryption*) bezeichnet (Abbildung 6).

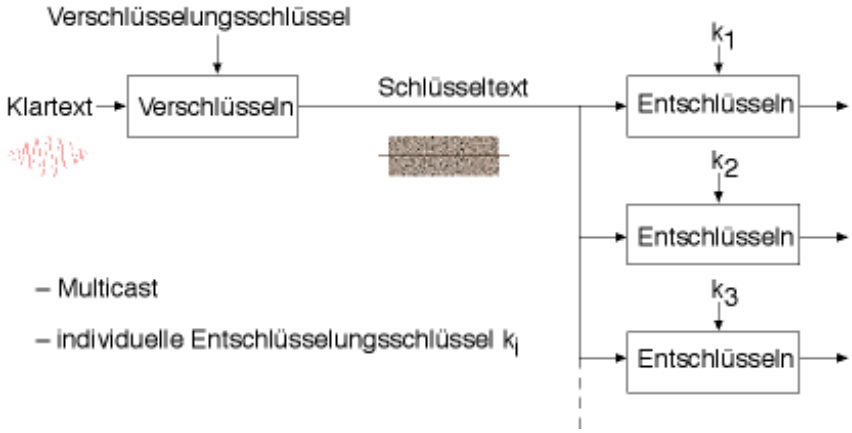

Abbildung 6. Gruppenverschlüsselung

Taucht ein Entschlüsselungsschlüssel illegal im Internet auf, kann der legale Besitzer ermittelt und ggf. verantwortlich gemacht werden für die unberechtigte Veröffentlichung des Schlüssels. Dieser Prozeß der Rückverfolgung (*Traitor Tracing*) gelingt jedoch nur, wenn

1. gespeichert wurde, welcher Kunde welchen Schlüssel erhalten hat, und
2. es einem besonders böswilligen Kunden, der sich gleich mehrere Schlüssel legal kauft, nicht gelingt, einen neuen gültigen Schlüssel aus den legal erworbenen zu berechnen (sog. *Collution Attack*) und diesen illegal zu verbreiten.

Gruppenverschlüsselung hilft natürlich nichts gegen Piraten, die einen legal empfangenen Medienstrom entschlüsseln und erneut (illegal und unverschlüsselt) in das Internet einspeisen. Wollte man dies erkennen, müßte zusätzlich ein individuelles Watermark in den Medienstrom eingebracht werden, das den Kunden identifiziert.

5 Zusammenfassung

Die Paradigmen der Datenbereitstellung im Internet ändern sich derzeit massiv. Von der Bereitstellung der Daten an *einer* Stelle im Internet wird mehr und mehr dazu übergegangen, die Daten zu replizieren und zu verteilen. Die bekannten Adressierungsmechanismen (URL, Unified Ressource Allocator, "http://...") werden zunehmend ersetzt durch Schlüsselwörter, die keine explizite Information über den Speicherort enthalten. "Das Netz" sucht sich gewissermaßen die gewünschten Informationen selber, sofern die gewünschte Information eindeutig angegeben wurde, ansonsten (je nach Implementierung) werden Suchmaschinen angefragt und dem Nutzer eine Auswahl angezeigt, oder er bekommt (wie heute) eine Fehlermeldung. Beispiele für diese neue Strategie der Datenbereitstellung sind Napster (**http://www.napster.com)**, Gnutella (**http://gnutella.wego.com/)** und Freenet (**http://freenet.sourceforge.net)**.

Weiterhin existieren inzwischen mehrere auch praktisch nutzbare Dienste, mit denen sowohl das Abrufen als auch das Anbieten von Information im World Wide Web *unbeobachtbar* erfolgen kann. Hier werden wie bisher die Daten an einem festgelegten Speicherort gehalten. Jedoch werden die Zugriffe mit Hilfe spezieller Verschlüsselungsmechanismen verschleiert. Auch das Anbieten von Daten kann mit diesen Systemen erfolgen, wobei niemand außer dem Anbieter der Daten Kenntnis darüber erlangt, an welchem Ort, d.h. an welcher Web-Adresse die Daten gespeichert sind. Beispiele für solche Dienste sind Anonymizer (**http://www.anonymizer.com/**) und Freedom (**http://www.freedom.net/**).

Internet wird die klassischen Broadcast-Medien nicht ablösen, aber ergänzen und ggf. für bestimmte Kommunikationsformen in den Hintergrund drängen, insbesondere dort, wo Interaktivität, on-demand Services oder gezielte Informationen (z.B. Nachrichten) vom Konsumenten gewünscht sind. Wann immer möglich, sollte dann die Distribution mit den in diesem Papier angerissenen Schutzmechanismen gekoppelt werden.

* * *