Rechte und Lizenzen II
Schwerpunkt: Bildrechte
Fachtagung des AsKI e.V. im Museum für Kommunikation, Frankfurt am Main am 26. März 2004

Digitale Wasserzeichen: Verteidigung von Authentizität und Urheberrecht in der Multimedia-Kommunikation

Vortrag von Prof. Dr.-Ing. Johannes Huber, *Universität Erlangen*

Johannes Huber, Robert Bäuml, Roman Tzschoppe
Lehrstuhl für Informationsübertragung
Friedrich-Alexander-Universität Erlangen-Nürnberg

1. Multimedia-Kommunikation

Die Multimedia-Kommunikation beruht auf der einheitlichen Repräsentation von Information jeglicher Art mittels Daten, ohne Beschränkung der Allgemeinheit durch Binärsymbole, sog. Bit. Grundlage hierfür ist die Digitalisierung analoger informationstragender Signale mittels Abtastung und Quantisierung. Als Beispiele seien hierzu die Digitalisierung von Audiosignalen im Format der Compact-Disc (CD, Entnahme von 44100 Abtastwerten pro Sekunde, Quantisierung der einzelnen Abtastwerte in 65536 = 2^{16} Stufen, d.h. Repräsentation der Quantisierungsintervalle durch 16 Bit: Datenstrom: 44100 x 16 x (2 Stereokanäle) = 1411200 Bit/Sekunde) und die digitale Photographie (z.B. 4 Millionen Bildpunkte (Pixel), Quantisierung der Helligkeit von drei Grundfarben (Rot, Grün, Blau) in je 4096 = 2^{12} Stufen: Datenmenge: 4000000 x 3 x 12 = 144 MBit/Bild) genannt. Darauf aufbauend wird mittels **Quellencodierung** eine kompakte digitale Repräsentation des Medieninhalts erreicht, indem nur die Daten gespeichert bzw. übertragen werden, die zur umkehrbar eindeutigen Wiederherstellung des Signals unbedingt erforderlich sind (Redundanzreduktion), und indem gegebenenfalls Inhalte entfernt werden, die von potentiellen Konsumenten nicht wahrgenommen werden (Irrelevanzreduktion). Auf diese Weise wird erreicht, dass auch umfangreichere Dokumente und Signale durch Informationsverarbeitungsanlagen zu handhaben, auf gängigen Medien zu speichern und über Kommunikationsnetze zu übertragen sind. Allerdings wirken sich Bitfehler bei hoch komprimierter Informationsrepräsentation extrem störend im rekonstruierten Signal aus. Deshalb werden meist in einer sog. **Kanalcodierung** Kontrollsymbole, also künstliche Redundanz, in den Datenstrom eingefügt, die in begrenztem Umfang eine Korrektur von

Bitfehlern erlauben. Auf diese Weise ist es prinzipiell möglich, auch über nur beschränkt zuverlässige Datenkanäle (Speichermedien, Übertragungseinrichtungen usw.) Information absolut störungsfrei zu übertragen.
Die prinzipiellen Möglichkeiten und Grenzen der digitalen Informationsrepräsentation, Datenkompression und –sicherung, sowie der Kryptologie wurden inzwischen durch die **Informationstheorie,** einem umfassenden und besonders ästhetischen mathematischen Theoriegebäude, das 1948 durch C.E. Shannon (1916 – 2001) begründet wurde, weitestgehend geklärt.

2. Motivation für die Anwendung digitaler Wasserzeichen

Infolge der Vereinheitlichung der Informationsrepräsentation in der Multimedia-Kommunikation und der Anwendung von Methoden der Informationstheorie ergeben sich völlig neue Anforderungen an den Urheberrechtsschutz und den Nachweis der Authentizität von Dokumenten. Während analoge Medien aufwändige Vertriebsstrukturen (Buch- und Zeitschriftenhandel, Schallplattenladen, Videothek usw.) erforderten, die ihrerseits den Einbau vielfältiger Schutzmechanismen erlaubten, können digitale Dokumente über Datennetze (meist das Internet) beliebig und weitgehend unkontrollierbar verbreitet werden. Der Qualitätsverlust von einer Kopie zur nächsten bot bei analogen Medien einen inhärenten Kopierschutz (z. B. Audio- und Video-Kassette, optische Fotokopie usw.), wohingegen digitale Dokumente in beliebig vielen Generationen absolut identisch kopierbar sind, ja beim Kopiervorgang durch Signaldetektion und Fehlerkorrektur sogar eine Auffrischung (Regeneration) des Datensignals erfolgt. Weiterhin war eine Manipulation analoger Medieninhalte meist aufwändig, kostspielig und zudem oft schlecht zu verschleiern; für Multimedia-Daten stehen dagegen nun höchst leistungsfähige Software-Pakete für Personal-Computer zur Manipulation von Texten, Bildern sowie von Audio- und Videosignalen zur Verfügung, so dass bei Dokumenten, die nicht mittels Verfahren der Kryptographie ge-

schützt sind, ein Vertrauen in die Authentizität des Materials derzeit in keiner Weise begründet ist. Beliebige Manipulationen sowie die widerrechtliche und ungehemmte exponentielle Verbreitung von digitalisierten Medieninhalten sind prinzipiell nur mittels hochentwickelter Sicherungsmaßnahmen zu vermeiden oder zu begrenzen.

3. Digitale Wasserzeichen

Als ***digitale Wasserzeichen*** bezeichnet man möglichst unmerkliche digitale Hintergrundinformation in Dokumenten auf der Ebene der für den Menschen nutzbaren Repräsentation, also in Bildern, Ton- oder Videosignalen, lesbaren Texten usw. Das Original bildet zusammen mit dem eingebettetem Wasserzeichen das geschützte Dokument, das den bei der Multimedia-Kommunikation üblichen Verarbeitungsschritten unterworfen werden kann (Datenkompression, Übertragung, Vervielfältigung usw.). Dabei besteht prinzipiell ein wechselseitiger Austausch zwischen den folgenden Parametern:

- Informationsmenge des eingebetteten Wasserzeichens
- Robustheit gegen Angriffe auf das Wasserzeichen
- Verzerrung des Originalsignals (Trägersignals) durch die Wasserzeicheneinbettung, die sog. Einbettungsverzerrung

Üblicherweise wird die Wasserzeicheninformation zunächst kryptographisch verschlüsselt. Die auf diese Weise erzeugte Datensequenz steuert geringfügige Veränderungen des Originalsignals (auch als Trägersignal bezeichnet) zur Markierung mit dem Wasserzeichen, siehe Bild 1. Digitale Wasserzeichen allein bieten keinerlei Schutz gegen unerlaubtes Verbreiten, Diebstahl oder Manipulation; vielmehr sind flankierend Rahmenbedingungen zu schaffen, durch welche die eigentliche Rechtsverteidigung erfolgt. In diesem Sinne besteht eine gewisse Analogie zu üblichen Wasserzeichen in Papierdokumenten, z.B. bei Geldscheinen: Erst wenn eine autorisierte Stelle darüber wacht, dass Rechtsverletzungen auch verfolgt werden, kann

durch die Einbringung des Wasserzeichens eine gewisse Schutzfunktion erzielt werden. Das Wasserzeichen dient dabei in erster Linie dazu, den Umstand einer Rechtsverletzung deutlich und nachweisbar werden zu lassen. Als Unterschied zu üblichen Wasserzeichen in Papierdokumenten ist anzumerken, dass es hier für einen potentiellen Rechtsbrecher zunächst kaum erkennbar sein mag, dass ein digitales Wasserzeichen in ein Dokument eingebettet ist. Damit kann in gewissen Grenzen vermieden werden, dass kriminelle Energie zum Angriff gegen das Sicherungsmerkmal „digitales Wasserzeichen" überhaupt freigesetzt wird. In vielen Anwendungsfällen mag aber auch der Hinweis auf die Sicherung des Dokuments durch ein Wasserzeichen der Abschreckung dienen.

Digitale Wasserzeichen sollen vorwiegend bei der Erleichterung von Wiedergabe- und Kopierkontrolle, zum Eigentumsnachweis, Urheberrechtsschutz usw. Anwendung finden. Durch den Nachweis eines nur mit seinem eigenen geheimen Schlüssel lesbar zu machenden Wasserzeichens im Dokument kann sich zumindest der Einbetter eines Wasserzeichens zweifelsfrei identifizieren. Für die Sicherung der Identität von Rechtsinhaber und Einbetter ist jedoch wiederum die Existenz einer unabhängigen, vertrauenswürdigen Organisation unabdingbar. Die Verbreitung von unberechtigt hergestellten Kopien kann erschwert werden, indem jede legal vertriebene Kopie mit einem individuellen Wasserzeichen, das z.B. eine Seriennummer enthält, versehen wird. Die Quelle der unrechtmäßigen Weiterverbreitung ist auf diese Weise ausfindig zu machen und damit ein Rechtsbrecher bezüglich Schadensersatz zu belangen.

Werden sogenannte ***zerbrechliche Wasserzeichen*** eingesetzt, so lassen sich Bereiche in Dokumenten (Bilder, Texte, Tondokumente) lokalisieren, in denen unberechtigt Manipulationen vorgenommen wurden. In solchen Bereichen wird durch die Manipulationen das Wasserzeichen zerstört. Durch die Anwendung geeigneter kryptographischer Verfahren kann dabei sehr sicher verhindert werden, dass der Manipu-

lator in der Lage ist, das Wasserzeichen originalgetreu zu ersetzen. Da aber ein nicht mehr zu detektierendes Wasserzeichen weit weniger Beweiskraft besitzt als dessen Nachweis, sind dieser Form der Sicherung der Authentizität von Dokumenten enge Grenzen gesetzt.

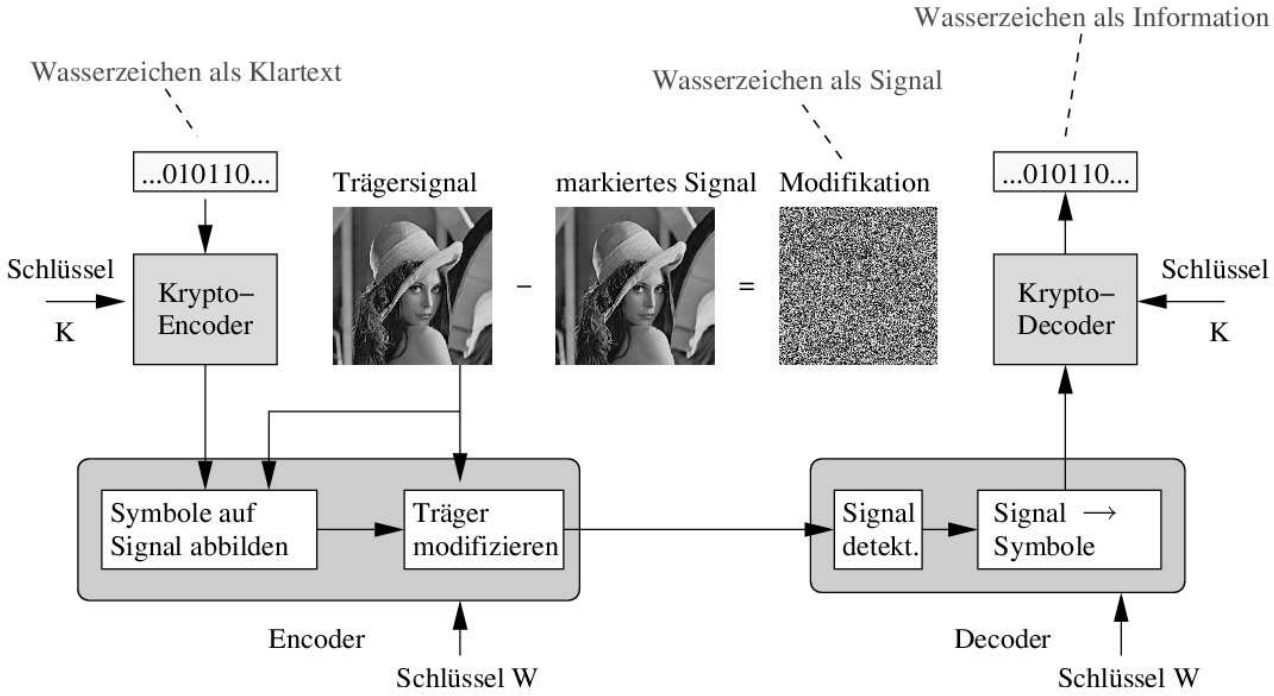

Bild 1: Prinzipielle Methode der Einbettung digitaler Wasserzeichen

Daneben lässt sich die Technik der digitalen Wasserzeichen natürlich auch einsetzen, um Information versteckt in anderen Signalen, also im Verborgenen, zu übertragen (Steganographie) oder auch nur für den eleganten unsichtbaren Transport von (z.B. erläuternder) Nebeninformation im Multimedia-Dokument (Meta-Information).

Der wirksame Einsatz digitaler Wasserzeichen benötigt deren Verknüpfung mit kryptologischen Methoden, oftmals in mehreren Stufen, so bei der Einbettung, um statis-

tische Analyse zur Auffindung des Wasserzeichens wirkungslos werden zu lassen und für die Wasserzeicheninformation selbst, um die Authentizität des berechtigten Einbetters nachzuweisen bzw. unberechtigte Einbetter zweifelsfrei entlarven zu können. Die Hinterlegung von geheimen Schlüsseln berechtigter Einbetter bei einer unabhängigen, anerkannten und vertrauenswürdigen Agentur sei hierfür als Möglichkeit genannt. Alle gängigen symmetrischen Verfahren der Kryptologie können Anwendung finden. Zudem ist die Wasserzeicheninformation grundsätzlich durch hochwirksame, niederratige Kanalcodes gegen Interferenz durch das Trägersignal, Signalverzerrungen infolge Kopier- und Kompressionsvorgängen bei der Verarbeitung des digitalen Dokumentes und insbesondere gegen Angriffe auf das Wasserzeichen zu sichern.

4. Technische Verfahren der Wasserzeicheneinbettung

Heute werden vorrangig so genannte „blinde“ digitale Wasserzeichenverfahren diskutiert, bei denen zur Wasserzeichendetektion (Nachweis des Vorhandenseins des Wasserzeichens) und/oder zur Wasserzeichendecodierung (Auslesen der Wasserzeicheninformation) kein wasserzeichenfreies Referenzexemplar des Trägersignals benötigt wird. Als blinde Wasserzeichenverfahren gelangen vorrangig sog. „Spread-Spectrum-Verfahren“ und Verfahren, die auf sog. „Costa-Codes“ beruhen, zur Anwendung.

4.1. Spread-Spectrum-Verfahren

Die Spread-Spectrum-Verfahren sind der digitalen Funkübertragung mit Bandspreizung entlehnt. Diese Verfahren dienten ursprünglich in vorwiegend militärischen Anwendungen dazu, durch die Verteilung des Sendersignals auf eine extrem große Spektralbandbreite die spektrale Leitungsdichte soweit zu verringern, dass ein Signalnachweis neben thermischem Rauschen kaum mehr gelingt. Der Übertragung

dieser Methode auf digitale Wasserzeichen entspricht eine additive Einbettung eines sehr schwachen Wasserzeichensignals, das dabei auf sehr viele Werte des Trägersignals verteilt wird. Dies wird durch die Repräsentation der einzelnen Binärsymbole der Wasserzeicheninformation mittels langer Folgen pseudozufälliger Signalwerte mit geringer Amplitude erreicht. Empfangsseitig, also zur Wasserzeichendetektion oder -decodierung, erfolgt eine Korrelation des Signals mit diesen Folgen (elementweise Multiplikation und anschließende Summation),wodurch einerseits eine große Verstärkung des Wasserzeichensignals und andererseits eine hochwirksame Unterdrückung des Trägersignals erreicht wird. Hierzu ist neben der Kenntnis der pseudozufälligen Signalfolgen auch deren genaue Lokalisation (Synchronisation) in der Folge von Abtastwerten aus dem Trägersignals erforderlich. Da hierbei aber üblicherweise viele Tausende Abtastwerte aus dem Trägersignal zur Einbettung nur eines Bits des digitalen Wasserzeichens erforderlich sind, eignen sich Spread-Spectrum-Verfahren nur bei sehr geringen Wasserzeicheninformationsmengen.

4.2. Costa-Codes

In einer grundlegenden informationstheoretischen Arbeit hat Costa im Jahr 1983 gezeigt, dass bei sendeseitiger Kenntnis des Trägersignals die Übertragung eines Signals mittels Einbettung in dieses Trägersignal prinzipiell genauso effizient erfolgen kann wie bei direkter Signalübertragung. Dieser Vorgang wird in der Fachwelt als „Schreiben auf verschmutztes Papier“ („writing on dirty paper“) umschrieben: Auf verschmutztes Papier lässt sich prinzipiell genau so viel Information schreiben wie auf weißes Papier, wobei nur dem Schreiber, nicht jedoch dem Leser zuvor die spezielle Form der Verschmutzung des Papiers bekannt sein muss. In unserem Fall bildet das Trägersignal, also das Multimedia-Dokument, das verschmutzte Papier, in das ein digitales Wasserzeichen eingeschrieben wird. Die Wasserzeicheneinbettung erfolgt hier nicht additiv, sondern durch eine von der Wasserzeicheninformation ge-

steuerte geringfügige Manipulation des Trägersignals. Mittels informationstheoretischer Methoden kann auf sehr allgemeine Weise nachgewiesen werden, dass solche Costa-Codes sowohl hinsichtlich des Austausches von eingebetteter Wasserzeicheninformationsmenge gegen Einbettungsverzerrung als auch hinsichtlich der Resistenz der Wasserzeicheninformation gegenüber additiven Rauschstörungen, z.B. bei Angriffen gegen das Wasserzeichen, optimale Eigenschaften besitzen. Da jedoch optimale Costa-Codes hoch komplexe Verfahren in vieldimensionalen Signalräumen darstellen, besitzen sog. skalare Costa-Verfahren (Scalar Costa-Scheme: SCS-Watermarking), die nur wenig suboptimal, aber relativ einfach zu implementieren sind, eine große Bedeutung für die Praxis. Costa-Verfahren eignen sich insbesondere bei großen Wasserzeicheninformationsmengen, z.B. ab 0,001 bis über 1 Bit pro Abtastwert aus dem Trägersignal.

5. Angriffe auf digitale Wasserzeichen

Weiß ein potentieller Rechtsbrecher um die Sicherung eines Multimedia-Dokuments durch ein digitales Wasserzeichen, so wird er Anstrengungen unternehmen, das Dokument so zu verändern, dass es dem Einbetter nicht mehr gelingt, durch Wasserzeichendetektion seine Rechte nachweisen zu können. Von einem robusten Wasserzeichen wird deshalb gefordert, dass dessen Verschleierung eine solch starke Verzerrung des Dokumentes verursacht, dass das angegriffene Dokument dadurch für den Angreifer zugleich nutzlos wird. Spread-Spectrum und insbesondere auf Costa-Codes beruhende Verfahren können mittels niederratiger Kanalcodierungsverfahren, also bei geringen Wasserzeicheninformationsmengen, durchaus so gestaltet werden, dass bezüglich Angriffen durch *additive Störsignale* diese Forderung weitgehend sicher zu erfüllen ist. Große Schwierigkeiten stellen jedoch nach wie vor so genannte Desynchronisationsangriffe dar, bei denen durch leichte, dem Nutzer des Dokumentes kaum auffallende oder störend wirkende Deplatzierungen (zeitliche oder örtliche

Verschiebungen) von Signalwerten ein Aufsynchronisieren für den Algorithmus der Wasserzeichendetektion bzw. -decodierung so weit erschwert wird, dass der eindeutige Nachweis der Existenz eines Wasserzeichens nicht mehr gelingt. Dieses Problem ist insbesondere bei Dokumenten ohne Ordnung vermittelnder Strukturen gegeben, wie z. B. bei Bilddokumenten die keinerlei geradlinige Elemente enthalten oder Tondokumente ohne harmonische Klänge.
Die Entfernung von Wasserzeichen kann wirkungsvoll durch die Verhinderung der Wasserzeichendetektion durch Unbefugte mittels kryptologischer Verfahren sowie die Anwendung nichtlinearer, d. h. trägersignalabhängiger Einbettungsverfahren (z. B. SCS- Watermarking) vermieden werden.

6. Schlussbemerkung

Digitale Wasserzeichen bieten vielfältige Möglichkeiten, um im Zusammenwirken mit traditionellen Maßnahmen Urheberrechte und Authentizität bei digitalen Multimedia-Dokumenten wirksam zu verteidigen. Obwohl in den letzten Jahren viele neue leistungsfähige Lösungen zu technischen Fragestellungen gefunden wurden, fehlen für den hochwirksamen Einsatz jedoch insbesondere flankierende organisatorische Strukturen, sowie rechtliche Grundlagen auf internationaler Ebene. Der immerwährende Wettlauf zwischen Verbesserungen von Sicherungsverfahren und raffinierter werdenden Angriffstechniken findet natürlich in diesem Bereich in ganz gleicher Weise statt, wie bei allen Anstrengungen zum Schutz vor kriminellen Handlungen.