Steinebach, Dittmann, Neubauer; Anforderungen an digitale Transaktionswasserzeichen für den Einsatz im e-Commerce, Von e-Learning bis e-Payment - Das Internet als sicherer Marktplatz, Klaus P. Jantke, Wolfgang S. Wittig, Jörg Herrmann (Hrsg.), Tagungsband LIT '02, 26./27. September 2002, Leipzig, Akademische Verlagsgesellschaft Aka GmbH, Berlin, S. 209 - 217, ISBN 3-89838-033-5, 2002

Anforderungen an digitale Transaktionwasserzeichen für den Einsatz im E-Commerce

Steinebach[1], Dittmann[2], Neubauer[3]

[1] Fraunhofer Institute IPSI, Dolivostr.15, 64293 Darmstadt, Germany
martin.steinebach@ipsi.fraunhofer.de

[2] Platanista GmbH, Pankratiusstraße 7,64289 Darmstadt, Germany, dittmann@platanista.de

[3] Fraunhofer Institute IIS-A, Am Wolfsmantel 33, 91058 Erlangen, Germany
neu@iis.fhg.de

Kurzfassung

Digitale Wasserzeichen sind heute ein wichtiger Bestandteil von Systemen zum Copyrightschutz digitaler Daten. Es hat sich gezeigt, dass eine besondere Form digitaler Wasserzeichen in sogenannten Data-on-demand Systemen, also Systemen, die dem Benutzer gezielt die Information zur Verfügung stellen, die er angefordert hat (Video-on-demand, Audio-on-demand Services) eingesetzt werden kann. Diese Dienste stellen die angeforderten Daten meistens in komprimierter Form zur Verfügung. Sollen personalisierte Wasserzeichen (in diesem Zusammenhang Transaktionswasserzeichen genannt) in die komprimierten Daten eingebracht werden, benötigt man Verfahren, die Wasserzeichen in kodierte Daten einbringen können, ohne die Daten vollständig zu dekodieren. Im Beitrag werden Grundlagen zu digitalen Wasserzeichen und Anforderungen sowie Anwendungen für Transaktionswasserzeichen im E-Commerce behandelt.

1 Motivation

Mit der weiten Verbreitung des Internets, auch und vor allem in privaten Haushalten, wird digital repräsentierte Information für jedermann leicht zugänglich. Dies bietet neben den enormen Möglichkeiten der Informationsverbreitung auch hohe Risiken, speziell im Bereich des Urheberrechtsschutzes multimedialer Daten. Aus diesem Grund sind sogenannte digitale Wasserzeichen, d.h. nicht-wahrnehmbare Zusatzinformation, heute ein wichtiger Bestandteil von Systemen zum Copyrightschutz digitaler Daten.

Die Entwicklung von Verfahren zum Einbetten und Extrahieren digitaler Wasserzeichen in Multimediadaten gewinnt daher mit der zunehmenden Verbreitung des Internets immer mehr an Bedeutung. Eine wichtige Bedingung für die Akzeptanz von Wasserzeichen ist, dass die Qualität der Multimediadaten nach dem Wasserzeicheneinbettungsprozess sichergestellt sein muss. Ohne diese grundlegende Eigenschaft können Wasserzeichen nicht in Betracht gezogen werden, wenn es sich bei den markierten digitalen Medien um die zu verkaufende Ware im E-Commerce handelt. Die Ware würde durch nicht-transparente Wasserzeichen in ihrem Wert gemindert werden. Dies hat zur Folge, dass entweder die Verkäufer von vornherein die Verfahren nicht anwenden, um keinen Wettbewerbsnachteil zu erhalten, oder aber, die Ware wird zwar geschützt, aber vom Kunden nicht angenommen.

1.1 Anwendungsgebiete

Wir betrachten hier ausschließlich Szenarien, in dem eine Verbindung zwischen Anbieter und Kunde besteht. Der Kunde erwirbt online digitale Medien für unterschiedliche Verwendungszwecke. Die Vorgabe der bestehenden Verbindung zwischen Kunde und Anbieter ist wichtig, da Transaktionswasserzeichen während der Transaktion eingebettet werden. Daher können Informationen, die erst während der Transaktion bekannt sind als Wasserzeichen eingebettet werden. Fakten wie die Identität des Kunden oder das Verkaufsdatum sind vorher nicht bekannt.

Dabei sind verschiedene Varianten vorzufinden:

Video/Audio on Demand
Hier stellt ein Anbieter Medienströme wie z.B. Filme oder Musikstücke zur Verfügung. Der Kunde kann diese gegen eine Gebühr ähnlich wie beim Pay-TV empfangen. Die Übertragung wird in Echtzeit durchgeführt, es sind also Streaming-fähige Medienformate notwendig

Online-Kauf
Im Gegensatz zu den On-Demand Systemen werden hier digitale Güter vom Kunden zuerst heruntergeladen und danach verwendet. Auch hier kann es sich um Filme und Musikstücke handeln. Aber auch z.B. Cliparts oder Hintergrundbilder für den Computer sind denkbar.

Internet-Nachrichten
Die beiden bisher genannten Beispiele orientieren sich am Verkauf von Waren, nur das diese digital vorliegen. Digitale Medien können aber auch als Informationsquelle dienen. Hier liegt der Wert weniger in der Qualität als vielmehr in der Aktualität und dem Wahrheitsgehalt.

1.2 Sicherheit der Mediendaten

Alle oben beschriebenen Szenarien basieren auf Systemen, die dem Benutzer gezielt die Information zur Verfügung stellen, die er angefordert hat. Dabei werden die angeforderten Daten üblicherweise auf einem Datenserver des Anbieters in einer komprimierten Darstellung vorrätig gehalten. Aufgrund der begrenzten Datenübertragungsgeschwindigkeiten zum Endbenutzer werden die Daten ebenso meist in einer komprimierten Darstellung zum Benutzer übertragen, was folgende Vorteile mit sich bringt:

- die Übertragungszeiten sind wesentlich geringer
- der Serviceprovider spart erheblich Speicherplatz
- der Serviceprovider spart Rechenzeit, da während der Auslieferung keine Komprimierung der Daten vorgenommen muss

Die komprimierte Form der Daten ermöglicht jedoch auch einfaches (u.U. illegales) Kopieren der verteilten multimedialen Daten. Daher ist es sinnvoll, bereits während der Auslieferung der komprimierten Daten benutzerspezifische Wasserzeichen, in diesem Zusammenhang Transaktionswasserzeichen genannt, in die Daten einzubringen. Dazu benötigt man Verfahren, die Wasserzeichen in kodierte Daten einbringen können, ohne die Daten voll-ständig zu dekodieren.

Herkömmliche Sicherheit im Internet für Daten basiert meist auf Verschlüsselung. Im Fall von digitalen Medien muss berücksichtigt werden, das die Daten zum Konsumieren beim Endkunden immer vollständig entschlüsselt werden müssen. Oft werden die Daten danach in analoge Informationen umgewandelt und können spätestens dann völlig ungeschützt kopiert werden.

Wir sehen den Einsatz digitaler Wasserzeichen allerdings nicht als Alternative, sondern als Ergänzung zur Kryptographie: Die Übertragung wird durch Kryptographie geschützt. Die Daten selbst lassen sich durch den Einsatz digitaler Wasserzeichen mit einem Urheberschafts-, Kundenidentitäts- und / oder Integritätsnachweis versehen.

2 Grundlagen digitaler Wasserzeichen

Generell verstehen wir unter einem digitalen Wasserzeichen ein transparentes, nicht wahrnehmbares Signal, welches in das Datenmaterial (z.B. Bild, Video, Audiosignal, 3D-Modelle) mit einem Einbettungsalgorithmus unter Verwendung eines geheimen Schlüssels eingebracht wird. Analog dazu kann es mit einem Abfrageprozess und dem geheimen Schlüssel wieder ausgelesen werden.

Man kann digitale Wasserzeichen zur Kennzeichnung von Urheberrechten, von kundenspezifischen Kopien, zur Verfolgung von illegalen Kopien, zum Aufdecken von Manipulationen und zum Einbringen von Beschreibungselementen in das Datenformat benutzen. Genauere Betrachtungen werden hierzu in [1], [2] und [4] angestellt.

Digitale Wasserzeichen sind eine relativ junge Technologie. Daher existieren noch keine großflächig eingesetzten Verfahren für einzelne Medientypen. Aufgrund der Orientierung an der menschlichen Wahrnehmung von Auge und Ohr sind bisher keine medientyp-übergreifenden Verfahren bekannt. Für jeden neuen Datentyp, für den Wasserzeichen entwickelt werden sollen, muss neu untersucht werden, wie das das Wasserzeichen bildende (Rausch-)Signal erzeugt werden muss. Bei Bilddaten sind das Farbungenauigkeiten in den Pixeln, bei Audiosignalen sind es häufig rauschförmige

Signale. Schwierig ist es, Daten wie Text oder MIDI mit Wasserzeichen zu versehen, hier sind die Möglichkeiten das Signal unbemerkt zu modifizieren wesentlich eingeschränkt. Es müssen daher neue Wege gefunden werde, Freiheitsgrade zu identifizieren und zum Einbetten der Informationen heranzuziehen. Im Falle von Text kann es sich um Leerzeichen handeln, die zusätzlich im Text auftauchen, oder auch bestimmte Floskeln.

Heute existierende Verfahren sind anwendungsspezifisch und haben sehr uneinheitliche Verfahrensparameter und teilweise sehr geringe Sicherheitsniveaus. Es fehlen einheitliche Definitionen von Qualitätsparametern, um die Verfahren vergleichbar zu machen und den Anwendern eine Verfahrenstransparenz zu geben. Abhängig von den Anforderungen der verschiedenen Anwendungen können Aspekte von Wasserzeichen eventuell als weniger relevant angesehen werden als andere. Genauso können für manche Anwendungen gewisse Parameter Grundvoraussetzung sein. Oft kann das Bewerten von Parametern auch erst bei direkter Kenntnis der Situation erfolgen, da verschiedene Parameter sich gegenseitig beeinflussen. So kann ein Wasserzeichen zum Urheberrechtsnachweis im Allgemeinen nicht gleichzeitig für Robustheit und Transparenz optimiert werden. Hier muss eine Entscheidung getroffen werden, welcher Parameter im Einzelfall wichtiger ist.

Die wichtigsten Eigenschaften eines Wasserzeichenverfahrens sind Robustheit, Transparenz, Sicherheit, Komplexität, Kapazität, Verifikation, Invertierbarkeit.

- Robustheit: Robustheit bezeichnet die Widerstandsfähigkeit der in ein Datenmaterial eingebrachten Wasserzeicheninformation gegenüber zufälligen Veränderungen des Datenmaterials oder Medienverarbeitungen.
- Transparenz: Die eingebrachte Information ist nicht wahrnehmbar und somit transparent, wenn ein durchschnittliches Seh- bzw. Hörvermögen nicht zwischen markiertem Datenmaterial und Original unterscheiden kann.
- Sicherheit: Diese Eigenschaft beschreibt im Gegensatz zur Robustheit die Sicherheit gegen gezielte (nicht-blinde) Angriffe auf das Wasserzeichen selbst.
- Komplexität: Beschreibt den Aufwand, der erbracht werden muss, die Wasserzeicheninformation einzubringen und wieder auszulesen.
- Extraktionsmodus: Bestimmt ob zum Auslesen der Markierung das Originalsignal benötigt wird.
- Kapazität: Dieser Parameter misst, wie viel Information in das Original eingebracht werden kann.
- Geheime/öffentliche Verifikation: Dieser Parameter sagt aus, ob nur der Urheber oder eine dedizierte Personengruppe das Wasserzeichen aufdecken können (geheim) oder ob die Verifikation öffentlich erfolgen kann bzw. soll.
- Invertierbarkeit: Beschreibt die Möglichkeit das Wasserzeichen im Abfrageprozess aus dem Datenmaterial zu entfernen und das Original wieder zu rekonstruieren.

Digitale Wasserzeichen sind passive Schutzmechanismen, d.h. sie verändern die Signaldarstellung des Originalsignals nicht. Häufig sind sie sogar völlig transparent. Durch sie kann daher kein aktiver Schutz erfolgen, der eventuellen Missbrauch von Medien verhindert. Wird dies notwendig, müssen digitale Wasserzeichen durch eine aktive Umgebung ergänzt werden, die anhand der Wasserzeichen entscheiden und reagieren kann. In einer solchen Umgebung sind weitere Schutzmechanismen notwendig.

Eine grobe Unterteilung der Verfahren lässt sich in nicht-wahrnehmbare robuste Wasserzeichen zur Authentizitätsprüfung und in nicht-wahrnehmbare zerbrechliche Verfahren zum Integritäts-Nachweis vornehmen.

2.1 Verfahren zur Authentifizierung

Verfahren zur Authentizitätsprüfung auf Basis nicht-wahrnehmbarer robuster Wasserzeichen sind bisher am weitesten entwickelt. Es gibt es in Forschung und Industrie eine Vielfalt von Lösungen. Die existierenden Verfahren zeigen, dass es möglich ist, Informationen in Form von spezifischen Mustern oder direkt als Text in das Datenmaterial einzubringen.

Verschiedene Typen von Wasserzeichen sind bekannt:

- Ein Copyrightwasserzeichen enthält Hinweise bezüglich des Copyrightinhabers. Dazu sind 1-Bit oder N-Bit Wasserzeichen einsetzbar.

Ein 1-Bit Wasserzeichen stellt eine Art Stempel des Inhabers dar, der nachgewiesen werden kann. Ein N-Bit Wasserzeichen kann zusätzliche Informationen enthalten und / oder den Namen des Copyrightinhabers im Klartext enthalten.

- Ein Fingersprintwasserzeichen enthält Daten, anhand derer auf den Käufer geschlossen werden kann. Statt dem Namen des Urhebers wird z.B. die Kundennummer eingebettet. Tauchen später Kopien auf, enthalten diese einen Hinweis, mit dem auf den Ausgangspunkt der illegalen Kopien geschlossen werden kann. Eine detaillierte Beschreibung eines Ansatzes findet sich in [7].

Die Wasserzeichen sollten jeweils gegen die am häufigsten auftretenden Operationen wie Formatkonvertierung, verlustbehaftete Kompression und einfache lineare Transformationen robust sein. Probleme bereiten oft kombinierte lineare Transformationen und nicht-lineare Verarbeitungsoperatoren.

Die drei wichtigsten Parameter für Verfahren zur Schutz der Authentizität sind [1]:

- Sichtbarkeit/ verursachter Qualitätsverlust durch das Wasserzeichen
- Einzubringende Datenrate/ Informationsgehalt des Wasserzeichens
- Robustheit des Wasserzeichens

2.2 Verfahren zum Integritätsschutz

Der Integritätsschutz stellt eine neue Gruppe von Anforderungen an digitale Wasserzeichen. Während üblicherweise Informationen möglichst robust in ein Medium eingebettet und dabei nach einer Ausschnittsbildung ausgelesen werden sollen, ist hier die Verwendung anders: Es muss eine enge Verbindung zwischen Position des Wasserzeichens und eingebetteter Information hergestellt werden. Das führt zu erhöhten Anforderung an die Synchronisierung und die Zuverlässigkeit der Einbettung.

Bei Verfahren zur Anwenderauthentifizierung ist das Nicht-Markieren von für das Einbetten ungeeigneten Daten durchaus zulässig. Im Integritätsschutz muss gleichmäßig jede Position geschützt werden, um einen zuverlässigen Schutz zu erhalten und keine falschen Aussagen zu treffen. Dafür ist die Anforderung Robustheit niedriger, da hier zum einen nicht von Angriffen gegen die Robustheit ausgegangen werden muss, zum anderen ab einer gewissen Störung des Materials ein Verneinen der Integrität durch Nicht-Auffinden der Wasserzeichen durchaus erwünscht ist.

Daher sind hier folgende Eigenschaften am wichtigsten:

- Hohe Datenrate zum Einbetten der Inhaltsinformationen
- Sicherheit der Informationen gegen Manipulationen
- Invarianz der Inhaltsbeschreibung bzgl. des Einbettungsprozesses

2.3 Forschungsbedarf

Insgesamt weisen neuere Verfahren wesentlich verbesserte Eigenschaften hinsichtlich Robustheit und Sichtbarkeit auf. Um jedoch die Vergleichbarkeit der Verfahren zu ermöglichen fehlen klare Robustheits-Kriterien und Klassifikationsmerkmale.

Ein einheitlicher Robustheitstest kann z.B. mit der StirMark Testsuite [5] für Einzelbilder und Audiodaten durchgeführt werden. Dabei wird z.B. im Bildbereich eine Kombination von geometrischen Transformationen und Kompression durchgeführt. Frühere Wasserzeichenverfahren sind sehr anfällig auf solche Angriffe und es lassen sich die Wasserzeicheninformation nicht mehr korrekt auslesen. Problematisch erweist sich auch die Mosaikattacke. Bei ihr wird die Eigenschaft vieler Wasserzeichenverfahren ausgenutzt, dass die Wasserzeicheninformation zwar redundant verstreut über das Datenmaterial eingebracht wird, jedoch bei Bildausschnitten die Synchronisation beim Wiederfinden der Informationen im Teilausschnitt des Bildes verloren geht.

Neben StirMark existieren weitere Testverfahren anderer Forschergruppen. Diese behandeln Einzelbilder und Videos. Sowohl Certimark als auch Checkmark sind hier bekannt, sowie die Robustheitsspezifikation der „Secure Digital Music Initiative“ (SDMI).

Unabhängige Verfahren zur automatisierten Qualitätsprüfung der Medien nach dem Einbetten des Wasserzeichens sind ebenfalls bisher kaum betrachtet worden. In [O] zeigen wir hier einen Ansatz für Videodaten.

Weiterhin haben verschiedene Verfahren Probleme mit der einzubringenden Datenrate bei gleichzeitiger Robustheits- und Qualitätsgarantie. So wird es häufig schwierig, alle Copyright- oder Kundeninformationen in ein Bild zu integrieren. Im Audio- und Videobereich sind aufgrund der höheren Datenmenge des Trägersignals hier weniger Probleme zu beobachten.

Neben diesen Parametern müssen noch weitere Kriterien zur Beurteilung der Anwendbarkeit von digitalen Wasserzeichentechnologien berücksichtigt werden, die bisher meist vernachlässigt worden sind, wie Fälschungssicherheit oder Probleme bei der Mehrfachmarkierung.

Ein weiteres Problem: Digitale Wasserzeichenverfahren verhindern nicht die Mehrfachmarkierung eines Bildes oder von Tonmaterial. Die Verfahren sind sogar darauf entwickelt, mehrere Wasserzeichen aufzunehmen, um zum Beispiel Urheber, Produzent, Publisher usw. aufzunehmen. Problematisch erweist sich diese Eigenschaft bei der Urheberprüfung, wenn ein Angreifer das bereits markierte Datenmaterial mit seiner Urheberinformation versehen hat. Es gibt keinen Hinweis darauf, wer das Datenmaterial nun als erster markiert hat. Beide können die Wasserzeichen Information extrahieren. Selbst bei Vorlage des Originals ergeben sich Probleme, die als Invertierbarkeitsproblematik bezeichnet wird. Ein Angreifer findet im Netz ein bereits mit Wasserzeicheninformationen versehenes Bild und versucht ebenfalls seine Wasserzeicheninformation einzubringen, ohne das gefundene Bild zu verändern. Aus diesen Gründen müssen sogenannte Wasserzeicheninfrastrukturen entstehen, die einerseits dem Urheber eine eindeutige Kennzeichnung geben und andererseits einen Zeitstempel für das entsprechende Datenmaterial, damit im Zweifelsfall eindeutig auf den Urheber geschlossen werden kann, der zuerst das Wasserzeichen aufgebracht hat.

3 Wasserzeichen in den Anwendungsgebieten

Nachdem wir in Kapitel 2 die unterschiedlichen Typen digitaler Wasserzeichen erörtert haben, soll nun ihre Verwendung in den eingangs beschriebenen Szenarien aufgezeigt werden.

Abbildung 1 zeigt den generellen Lösungsansatz im Transaktionsszenario: Ein Kunde (1) meldet sich bei einem Server (2) an, um Mediendaten zu erhalten (3). Diese werden mittels eines Wasserzeicheneinbetters mit einem Wasserzeichen, beispielsweise der Identität des Kunden, versehen (4) und an den Kunden übertragen (5). Gibt der Kunde die Mediendaten z.B. illegal ins Internet weiter (6), so kann in dem im Internet gefundenen Material durch einen Wasserzeichendetektor der Ursprung der Daten festgestellt werden (7). Alternativ kann der Kunde selbst das Wasserzeichen auslesen (8).

3.1 Media On Demand

Der Bereich Media-On-Demand ist einer der klassischen Einsatzgebiete für Transaktionswasserzeichen. Es ergeben sich folgende spezielle Forderungen an die Einbettungsverfahren:

- Streaming-Fähigkeit: Diese Forderung erlaubt es dem Transaktionsserver Wasserzeichen in einer Blockverarbeitung vorzunehmen und somit bereits während der Lieferung Wasserzeichen einzubetten.
- Echtzeit-Fähigkeit: Sollte für praktische Anwendungen weit übererfüllt sein, um dem Transaktionsserver die parallele Verarbeitung mehrer Anfragen zu erlauben.
- Empfänger muss bekannt sein: Es ist kein Broadcast- oder Multicast-Betrieb möglich zumindest, wenn später die Empfänger unterscheidbar sein sollen.
- Wasserzeicheneinbettung in komprimierte Inhalte: Dies auch als Bitstrom-Wasserzeichen bekannte Verfahrensprinzip erlaubt es in bereits komprimierte Daten nachträglich Wasserzeichen einzubetten. Dies ist eine Schlüsselkomponente aller Transaktionswasserzeichensysteme [10].

Weitere Forderungen ergeben sich aus dem nachfolgenden Szenario „Online-Shop“.

3.2 Online-Shop

In dem Szenario Online-Shop werden digitale Wasserzeichen eingesetzt, um den Copyrightanspruch des rechtmäßigen Inhabers auch nach der Übertragung in das System des Anwenders zu gewährleisten. Das Wasserzeichen wird dazu (meist transparent) in die verkaufte digitale Ware eingebettet.

Wichtig ist hier die Einschränkung auf digitale Waren: Über Online-Shops können im Allgemeinen beliebige Waren verkauft werden, also auch z.B. Bücher, Nahrungsmittel oder sogar Fahrzeuge. Mit digitalen Wasserzeichen lässt sich aber nur arbeiten, wenn die verkauften Waren eine Änderung auf digitaler Ebene erlauben. Dazu müssen sie entweder von digitaler Natur sein, wie z.B. MIDI-Daten oder aber digitalisiert vorliegen, z.B. als mp3-Datei. Wird im Folgenden von Waren gesprochen, sind daher immer digitale Waren gemeint.

Die eingebetteten digitalen Wasserzeichen sollten in beiden Fällen erst beim Übertragen der digitalen Waren an den Kunden eingebracht werden. Im Falle der Fingerprintwasserzeichen ist dies selbstverständlich: Die Identität des Käufers kann erst während der Transaktion festgestellt werden. Aber auch bei den Copyrightwasserzeichen macht es Sinn, erst beim Übertragen der Daten das Wasserzeichen einzubetten. Software zum Einbetten von Wasserzeichen kann verbessert werden, bei einem Update müsste der gesamte Bestand neu markiert werden, wenn der bestmögliche Schutz gewährleistet werden soll. Dies würde weiterhin ein doppeltes Datenvolumen bedeuten: Sowohl markierte als auch nicht markierte Daten müssten für das eCommerce-System verfügbar sein.

3.3 Internet-Nachrichten

Eine Nachrichtenagentur vertreibt über das Internet Tondokumente, die einzelne Nachrichtensender kaufen und verwenden. Diese Dokumente sind von der Agentur mit inhaltsfragilen Wasserzeichen versehen worden. Sendet nun z.B. ein Radiosender das Tondokument, so wird gleichzeitig auch das Wasserzeichen mitübertragen. Ein skeptischer Hörer, der an der Unversehrtheit der Dokumente zweifelt, könnte dann bei einer neutralen Instanz prüfen lassen, ob die eingebetteten Daten mit dem Inhalt übereinstimmen.
Die dritte Instanz sollte nicht die Agentur oder der Sender sein, sondern eine Partei, die in der Lage ist, die Wasserzeichen zu lesen und zu prüfen, sonst aber unabhängig von den anderen Beteiligten ist. Kann nur diese Partei anhand eines Schlüssels die Daten auslesen, so muss immer der komplette Beitrag zur Prüfung gesendet werden. Alternativ könnte man den Schlüssel zum Auslesen öffentlich machen, aber die eingebetteten Informationen mittels eines Public Key Verfahrens verschlüsseln. Hier könnte nur die Agentur Informationen einbetten, die wieder ausgelesen werden können. Der Kunde wäre im Besitz des Detektors für das Wasserzeichen und des öffentlichen Schlüssels der Agentur. Problematisch hierbei ist, dass ein Angreifer dadurch in der Lage wäre, mit Angriffen zu experimentieren und zu prüfen, wann die Inhaltsmerkmale verändert werden.

4 Allgemeine Betrachtung der Qualitätskriterien

Nachdem wir im vorherigen Kapitel die Einsatzszenarien von Transaktionswasserzeichen

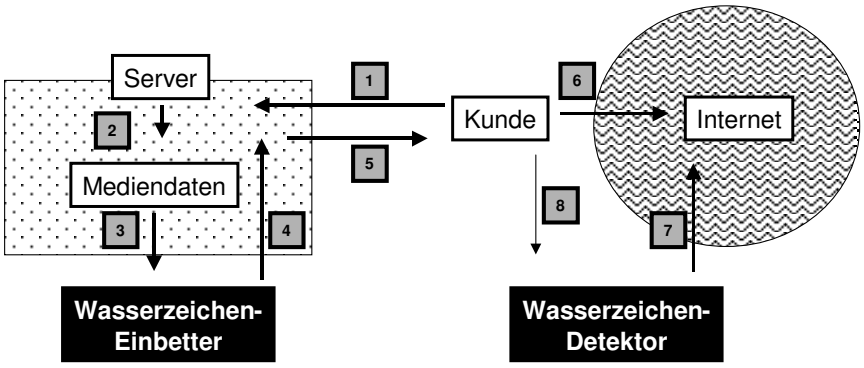

Abbildung 1: Das Transaktionsszenario

betrachtet haben, diskutieren wir hier die allgemeinen Anforderungen an die Algorithmen und Konzepte. Von besonderer Bedeutung sind hier diejenigen Eigenschaften, die für alle Szenarien gemeinsam relevant sind.
In Tabelle 1 unterscheiden wir zwischen wünschenswerten (W) und notwendigen Eigenschaften (N).

Tabelle 1: Szenarienabhängige Klassifizierung der Anforderungen an die Wasserzeichen

	Szenario		
Eigenschaft	**1**	**2**	**3**
Echtzeit-Einbettung	N	N	W
Hohe Transparenz	N	N	W
Starke Robustheit	W	W	W
Hohe Sicherheit	W	W	N
Hohe Datenrate	N	N	N

Die Szenarien 1 und 2, Media on Demand und Online-Verkauf, erfordern eine Echtzeit-Einbettung der Wasserzeichen, da hier u.a. Kundeinformationen eingebettet werden sollen. Durch die dazu notwendigen Fingerprinting-Verfahren ist ebenfalls eine hohe Datenrate erforderlich. Die hohe Transparenz ist notwendig, da eine hohe Qualität der Medien vom Kunden erwünscht ist. Robustheit und Sicherheit sind hier wünschenswert und wichtig, aber nicht grundlegend notwendig zum Einsatz der Verfahren.
Im Nachrichten-Szenario sind vor die allem Sicherheit und hohe Datenrate ausschlaggebend. Letzteres begingt sich durch die verhältnismäßig große Datenmenge, die eingebettet werden muss. Sicherheit ist notwendig, da sonst das Konzept des Integritätsschutzes nicht sinnvoll umgesetzt werden kann. Die übrigen Eigenschaften sind hier nur als wünschenswert einzustufen. Die Nachrichten können markiert werden, bevor der Kunde auf sie zugreift, Qualitätsansprüche sind niedriger als bei beispielsweise Musik und eine hohe Robustheit ist aufgrund des Konzepts der Erkennung von Veränderungen nicht ausschlaggebend.

Im folgenden diskutieren wir die Eigenschaften im Detail:

Hohe Sicherheit
Im Bereich Sicherheit spielen in den Szenarien für die Kundenidentifizierung vor allem Koalitionsangriffe eine wichtige Rolle. Da jedem Kunden ein individuelles Wasserzeichen generiert wird, entstehen aus dem Original unterschiedliche Wasserzeichen-markierte Kopien, die, wenn mindestens zwei Kundenkopien verglichen werden, Unterschiede durch die Wasserzeichen aufweisen. Beispielsweise werden bei einer Vielzahl von Verfahren durch die Bildung von Differenzen aus zwei Kundenkopien Wasserzeicheninformationen sichtbar und können direkt angegriffen und zerstört bzw. verändert werden. Bisher wird dieser Angriff leider in den meisten Verfahren nicht betrachtet. Den beschrieben Angriff nennt man Koalitionsangriff oder auf Fingerprint-Angriff. Details zu Angriffen sind unter [1] zu finden.

Hohe Datenrate
Will man den Koalitionsangriff umgehen, müssen spezielle Kundenidentifizierungsvektoren generiert werden, die als Wasserzeichen einbettet werden. Diese Vektore, die eindeutig einen Kunden identifizieren, halten zwar niemanden davon ab, einen Koalitionsnangriff über Differenzbildung durchzuführen, erlauben aber, aus der Menge der Kunden die beteiligten Angreifer zu detektieren. Um aber eine erfolgreiche Detektion garantieren zu können, werden diese Kundenspezifischen Vektoren allerdings sehr lang, wodurch viele Transkationswasserzeichenverfahren Probleme mit der einzubettenden Datenrate bekommen. Der lange Bitvektor für das Fingerprinting ist sozusagen zu gross und kann oftmals nicht vollständig eingebettet werden. Details zu Verfahren, die Koalitionsangriffe erkennen, sind unter [1] zu finden.

Hohe Robustheit
Robustheit bezeichnet die Eigenschaft von Wasserzeichen gegen absichtliche oder unabsichtliche Signalmodifikationen resistent zu sein. Sie ist eine wesentliche Eigenschaft von Transaktionswasserzeichen, deren Aufgabe es ja ist, eine sichere Verbindung zur Transaktion und damit zum Kunden herzustellen. Üblicherweise werden für verschiedene Medientypen

(Audio/Video) spezielle Angriffe zur Evaluierung herangezogen. Im Allgemeinen sind Robustheit gegenüber Filterung, Kodierung, Equalization und Resampling Stand der Technik. Für Videosignale stellt Digital-Analog-Umsetzung auch heute noch ein Problem dar, das im Audiobereich hingegen von einigen Verfahren schon gut gelöst wird.

Hohe Transparenz
Ebenso wichtig ist die Transparenz, d.h. die Nichtwahrnehmbarkeit der Wasserzeichen. Diese Forderung ergibt sich aus der Benutzerakzeptanz, die bei wasserzeichen-bedingter Qualitätsminderung entsprechend absinkt.
Ein Problem der Transparenzforderung ist der hohe Aufwand zum Nachweis. Im Audiobereich wird die Qualität mit Hilfe von Hörtests bestimmt, da die automatische algorithmusbasierte Ermittlung auch heute noch sehr unzuverlässig ist. Gleiches gilt auch für Videowasserzeichen. Ein besonderes Augenmerk ist auch auf die Auswahl des Testmaterials zu legen. Es hat sich herausgestellt, dass zur Aufdeckung kleiner Differenzen spezielles kritisches Material herangezogen werden muss, da mit durchschnittlichem Material für hochwertige Algorithmen die Unterschiede von den Testpersonen bereits nicht mehr detektiert werden können [8].

Echtzeit-Einbettung
Ein weiterer in der Praxis sehr relevanter Parameter ist die Komplexität der Wasserzeichen-Verfahren. Hier muss zwischen Einbetter- und Extraktorkomplexität unterschieden werden. Für Transaktionswasserzeichen ist vor allem eine niedrige Einbetterkomplexität zu fordern, da die Einbettung während des Liefervorganges auf dem Content/Delivery-Server durchzuführen ist. Die Extraktion hingegen muss nicht zwingend besondere Komplexitätsanforderungen erfüllen. Hier ist eine Entscheidung nur im Einzelfall möglich, da z.B. im Falle gerichtlicher Betrachtung fast beliebig viel Zeit für die Extraktion zur Verfügung steht. Andererseits sollten automatische Suchprogramme (Webcrawler) relativ schnell eine Entscheidung über ein evtl. vorhandenes Wasserzeichen fällen können.

4.1 Weitere notwendige Funktionen

Digitale Wasserzeichen alleine können keine umfassende Sicherheit bieten. Erst gemeinsam mit anderen Mechanismen wie beispielsweise Verschlüsselung entstehen sichere Anwendungsumgebungen. Einige dieser Mechanismen zählen wir hier kurz auf.

Kryptographie
Asymmetrische Verfahren können für eine vertrauliche Übertragung von Kundenanforderungen eingesetzt werden und können bei bei der Authentifizierung (s.u.) helfen. Session-Key-Protokolle dienen der vertraulichen Übertragung von Mediendaten.

Zeitstempeldienste
Sie ermöglichen in Kombination mit Inhaltsauszügen eine zuverlässige Verknüpfung von Trägerdatei, Wasserzeichen und Markierungszeitpunkt.

Authentifizierung
Da wir von Kunden ausgehen, die sich gegenüber Anbietern von zahlungspflichtigen Diensten eindeutig zu erkennen geben, sind Authentifizierungsmechanismen notwendig.

Wiederauffinden
Ein großes Problem stellt das Wiederauffinden von markiertem Material dar. Dem Inhaber von Urheberrechten hilft es wenig, die Gewissheit zu haben, seine Rechte nachweisen zu können. Er muss Material, das einen Rechtsbruch darstellt, zuvor auffinden.
Eine umfassende Lösung für Mediensicherheit durch digitale Wasserzeichen muss daher auch ein Konzept enthalten, wie markiertes Material gefunden werden kann. Dabei wird auch das Schlüsselmanagement eine Rolle spielen. Konzepte, die derzeit von uns verfolgt werden, sind die automatisierte Suche über Suchmaschinen im Internet und das erstellen von Search-Clients in Peer-to-Peer Netzen.
Im Bildbereich bietet die Firma Digimarc bereits einen Service an, mit dem mit ihrem Wasserzeichen versehenes Material im Internet aufgefunden wird. Dem Kunden werden dann die Informationen über die Funde weitergereicht.

Zusammenfassung

Im Beitrag haben wir für 3 ausgewählte E-Commerce-Szenarien gezeigt, wie digitale Transaktionswasserzeichen eingesetzt werden können. Aufbauend auf diesen Szenarien haben

wir gezeigt, welche Verfahrensparameter generell von Wichtigkeit bei der Auswahl von Verfahren sind und erarbeitet, welche konkreten Ausprägungen die Parameter haben sollten. Die erarbeitete Grundlage bietet für Anwender eine Orientierungshilfe für die Auswahl und den praktischen Einsatz konkreter Transaktions-wasserzeichen.

Literatur

[1] Dittmann, Jana: *„Digitale Wasserzeichen“,* Springer Verlag, ISBN 3 - 540 - 66661 - 3, 2000

[2] Dappa, Artur; Dittmann, Jana; Steinebach, Martin; Vielhauer, Claus (2001). „*Wasserzeichen und kryptographische Verfahren für Online-Dienste“* In: Elektronische Geschäftsprozesse - Grundlagen, Sicherheitsaspekte, Realisierungen, Anwendungen, Horster P. (Ed.), IT Verlag für Informationstechnik GmbH, Höhenkirchen, pp. 11 - 21, ISBN, 3-936052-00-X, 2001.

[3] Jana Dittmann, Stephan Klink, Andreas Lang, Martin Steinebach, *„Wasserzeichenunterstützende Firewalls*", Enterprise Security: Grundlagen, Strategien, Anwendungen, Realisierungen, Patrick Horster (Hrsg.), it Verlag für Informationstechnik GmbH, Höhenkirchen, pp. 246 - 257, ISBN 3-936052-03-4,2002.

[4] I. Cox, M. Miller, J. Bloom, *“Digital Watermarking”*, 2002 Academic Press, San Diego, USA, ISBN 1-55860-714-5

[5] Petitcolas, F. A. P.; Steinebach, Martin; Raynal, F.; Dittmann, Jana; Fontaine, C.; Fates, N. (2001), *“Public automated web-based evaluation service for watermarking schemes: StirMark Benchmark”* In: Security and Watermarking of Multimedia Contents III, Ping Wah Wong, Edward J. Delp III, Editors, Proceedings of SPIE Vol. 4314, Bellingham WA, USA, pp. 575 - 584, ISBN 0-8194-3992-4, 2001.

[6] Dittmann, Jana; Mukherjee, Anir-ban; Steinebach, Martin (2001). *„A computer aided visual model for ensuring video watermarking transparency”*. In: Security and Watermarking of Multimedia Contents III, Ping Wah Wong, Edward J. Delp III, Editors, Proceedings of SPIE Vol. 4314, Bellingham WA, USA; pp. 45 - 54, ISBN 0-8194-3992-4, 2001

[7] Dittmann, Jana; Hauer, Enrico; Vielhauer, Claus; Schwenk, Jörg; Saar, Eva (2001). *„Customer Identification for MPEG Video based on Digital Finger-prints”,* In: Proceedings of Advances in Multimedia Information Processing - PCM 2001, The Second IEEE Pacific Rim Conference on Multimedia, Beijing, China, Springer Verlag, Berlin, pp. 383 - 390, ISBN 3-540-42680-9, 2001.

[8] Christian Neubauer and Jürgen Herre, *“Digital watermarking and its influence on audio quality”*, In 105th AES Convention, San Francisco, Sep. 1998. Audio Engineering Society. preprint 4823.

[9] Christian Neubauer and Jürgen Herre, *Advanced audio watermarking and its applications*, In 109th AES Convention, Los Angeles, Sep. 2000, Audio Engineering Society, preprint 5176.

[10] Christian Neubauer, Ralph Kulessa, and Jürgen Herre, “*A compatible family of bitstream watermarking schemes*,” In 110th AES Convention, Amsterdam, May 2001. Audio Engineering Society. preprint 5346.