

Wasserzeichen in digitalen Audiodaten

- Eine Einführung -

von Till Wiebke
(www.tillwiebke.de)

Abstract

Dieses Dokument bietet einen Einblick in die Technik der digitalen Wasserzeichen und ihre Anwendung innerhalb digitaler Audiodaten. Im ersten Teil wird der historische Hintergrund von (digitalen) Wasserzeichen beschrieben, wichtige Begriffe des Themengebiets „digitale Wasserzeichen“ erläutert sowie Anwendungsgebiete aufgezeigt. Im zweiten Teil werden drei Wasserzeichenverfahren (LSB, Echo und MPEG2-Scalefactor) vorgestellt.

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlagen	2
2.1	Historischer Hintergrund	2
2.2	Definitionen	4
2.3	Anwendungsgebiete	5
3	Verfahren	9
3.1	Allgemeines	9
3.2	Least-Significant-Bit-Wasserzeichen	9
3.3	Echo-Wasserzeichen	9
3.4	MPEG2-Scale-Factor-Wasserzeichen	11
4	Zusammenfassung und Ausblick	14
	Abbildungsverzeichnis	15
	Literaturverzeichnis	16

1 Einleitung

Durch die Vorstellung des MP3-Kompressionsverfahren für digitale Audiodaten durch das Fraunhofer Institut Mitte der 1990er Jahre wurde ein Wandel im Umgang mit Audiodaten eingeleitet. Mittlerweile sind digitale Audiodaten überall im täglichen Leben anzutreffen. Bei Radiosendern kommt die Musik oft von einem zentralen Medienserver, als Handyklingelton wird der aktuelle Lieblingssong als MP3 verwendet und der Anruferbeantworter speichert die eingehenden Nachrichten mit Hilfe von Flashspeichern.

Doch der Einsatz von digitalen Audiodaten ist nicht unproblematisch. Eine Kopie ist nicht vom Original zu unterscheiden, die Urheberschaft und Besitzverhältnisse lassen sich nicht schlüssig beweisen und mit Hilfe von Bearbeitungsprogrammen ist es relativ einfach, Audiodaten unerkennbar zu verändern. Jedoch spielt die Authentizität von Audiodaten zum Beispiel bei Gerichtsverhandlungen eine entscheidende Rolle. So ließe sich die Aufnahme eines Telefonats verändern, so dass die Bestellung eines teuren Produkts und nicht von unverbindlichem Infomaterial „bewiesen“ wird.

Diesen Problemen kann man schlecht mit Signaturen (auf Basis asymmetrischer Verschlüsselungsverfahren) begegnen, da sich Signaturen leicht austauschen oder entfernen lassen. Eine Verschlüsselung der Daten bietet auch keinen Schutz, da sie zum Abspielen entschlüsselt werden müssen und so wieder abgegriffen werden können.

Eine Lösung sind digitale Wasserzeichen, die auf den Prinzipien der Steganographie basieren. Mit ihnen kann man Urheber- und Kundendaten oder Unversehrtheitsmerkmale mit den Audiodaten so verbinden, dass eine Entfernung entweder die Daten zerstören oder ihre Qualität mindern würde.

Ziel dieser Seminararbeit ist es, einen Einblick in den Bereich der digitalen Wasserzeichen und ihre Anwendung auf Audiodaten zu geben. Dazu wird im ersten Teil der historische Hintergrund von (digitalen) Wasserzeichen betrachtet und allgemeine Definitionen sowie Anwendungsgebiete erläutert.

Im zweiten Teil werden zwei grundsätzliche Verfahren (LSB- und Echo-Wasserzeichen) sowie ein konkreteres Verfahren (MPEG2-Scalefactor-Wasserzeichen) vorgestellt.

2 Grundlagen

2.1 Historischer Hintergrund

Digitale Wasserzeichen sind die digitalen Nachfolger der historischen Papierwasserzeichen, die seit Jahrhunderten angewendet werden. Die ersten bekannten Wasserzeichen werden auf das Jahr 1282 datiert und italienischen Papiermühlen zugeordnet. Sie bestanden aus Mustern, die mit Hilfe von dünnen Drähten in die Papiermasse eingebracht wurden. [1]

Ihre breite Verwendung begann im achtzehnten Jahrhundert in Amerika und Europa, wo sie als Markenzeichen der Papiermühlen, zur Identifizierung der ursprünglichen Papierbögen oder zum Schutz vor Fälschern von Geld und Dokumenten verwendet wurden. Doch bereits 1779 war der Schutz gebrochen. Die damalige Zeitung „Gentleman’s Magazine“ berichtet in ihrer 49. Ausgabe von John Mathison, der es geschafft hatte, die Wasserzeichen von Banknoten zu fälschen, wofür er exekutiert wurde [2].

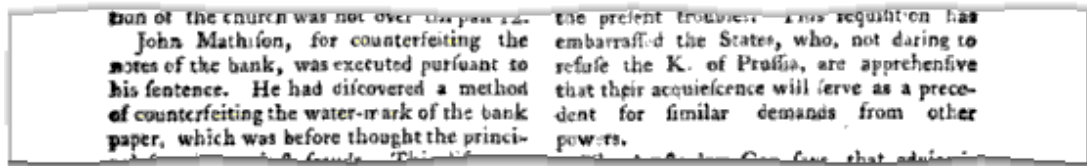


Abbildung 2.1: Ausschnitt aus Gentleman’s Magazine, Volume 49, von 1779 [2].

Dieser Vorfall führte dazu, dass die damalige Technik weiterentwickelt wurde, und die Wasserzeichen bis heute mit Hilfe von reliefierten Oberflächen eingebracht werden, wodurch die heute üblichen Graustufenzeichen möglich sind.

Bereits Mitte des 20. Jahrhunderts beschäftigte sich Emil Hembrooke für die „Muzak Corporation“ mit Techniken zur Markierung von Audiodaten. In seinem 1954 eingereichten und 1961 gewährten Patent beschreibt er eine Technik, mit der codierte Nachrichten in Audiosignale eingebettet werden können. Zur Einbettung wird in der Patentschrift ein schmalbandiger Filter erwähnt, um den Pegel in einem bestimmten Frequenzbereich

zu unterdrücken. Dadurch lassen sich zum Beispiel die Zeichen des Morsecodes oder Nullen und Einsen codieren. Als Vorteil der Erfindung wird bereits die Identifizierung von unerlaubten Vervielfältigungen und die dadurch entstehende Möglichkeit, Piraterie einzudämmen, sowie die prinzipielle Ähnlichkeit des Verfahrens zu Papierwasserzeichen erwähnt.

Wann genau die Entwicklung digitaler Wasserzeichen begann, lässt sich nicht eindeutig klären. Seit Beginn der 1990er Jahre wird der Begriff „digitales Wasserzeichen“ jedoch zunehmend häufiger diskutiert [1]. 1996 wurde der erste „Information Hiding Workshop“ abgehalten, bei dem digitale Wasserzeichen eine entscheidende Rolle spielten. Ende der 1990er Jahre wuchs nicht nur die Anzahl der Firmen und Zusammenschlüsse mit dem Ziel, Techniken für digitale Wasserzeichen zu entwickeln und kommerziell zu verwerten, sondern auch die Anzahl an Publikationen zum Thema stieg rasant an, wie Abbildung 2.2 zeigt.

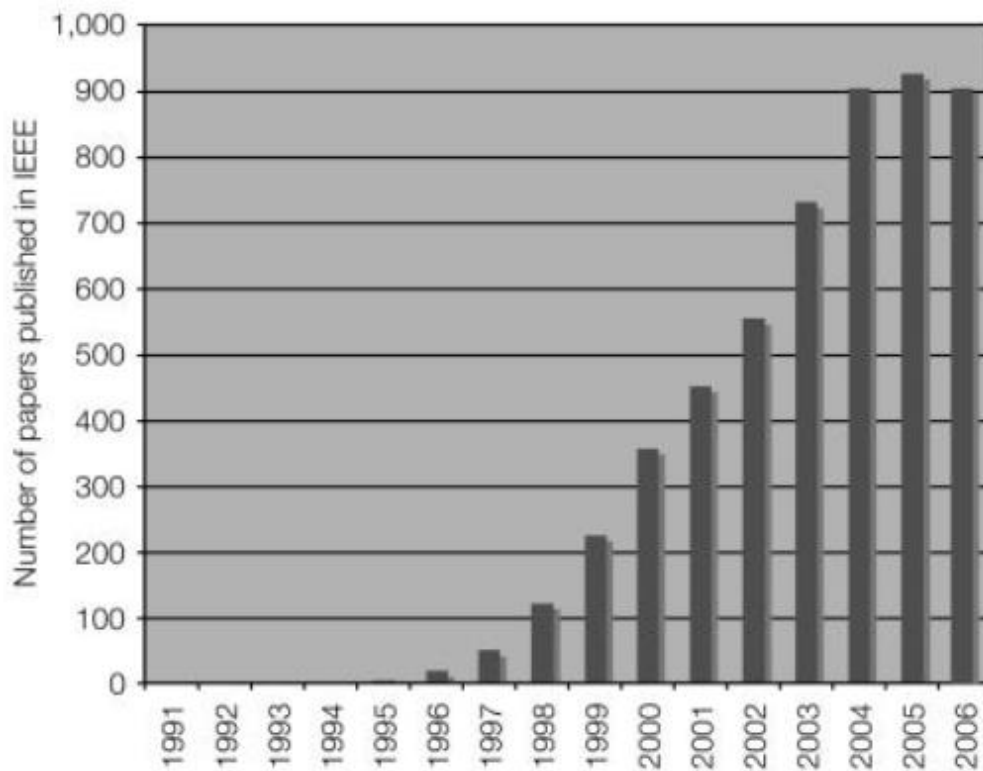


Abbildung 2.2: Anzahl der Veröffentlichungen des IEEE zum Thema digitale Wasserzeichen und Steganographie [4].

2.2 Definitionen

Um Wasserzeichen und ihre Einbettungsverfahren beschreiben und vergleichen zu können, müssen die Definitionen der folgenden Begriffe vorgenommen werden:

Fragilität und Robustheit Die Fragilität und Robustheit sind Maße für die Widerstandsfähigkeit eines Wasserzeichens gegenüber bestimmten Manipulationen des Trägermaterials. Oft werden sie in Zusammenhang mit einer bestimmten Manipulation gesetzt, da ein Verfahren für Audiodaten zum Beispiel robust gegen Lautstärkeveränderungen, jedoch fragil gegen Stauchungen und Streckungen des Materials sein kann.

Man spricht auch teilweise nur von der Fragilität bzw. der Robustheit, wobei man dann die Widerstandsfähigkeit gegen alle übliche Manipulationen, die das Trägermaterial nicht zerstören, meint.

Blinde Verfahren Bei einem blinden Wasserzeichenverfahren ist zur Detektion des Wasserzeichens innerhalb des markierten Materials das Original nicht notwendig. Im Gegenteil dazu wird für die Kontrolle eines nicht-blinden Verfahrens das nicht markierte Original benötigt.

Problematisch bei nicht-blinden Verfahren ist, dass das ungeschützte Original benötigt wird. Dieses könnte bei der Überprüfung des geschützten Materials kopiert/entwendet werden und mit einem eigenen, die Urheberschaft beweisenden Wasserzeichen versehen werden.

Angriffe Unter einem Angriff versteht man Manipulationen, die das Wasserzeichen zerstören. Man unterscheidet dabei zwischen blinden Angriffen, bei denen das Ziel die Zerstörung des Wasserzeichens ist und nicht-blinden Angriffen, bei denen das Wasserzeichen unbeabsichtigt zerstört wird. Diese Unterscheidung ist jedoch technisch nicht eindeutig, sondern bezieht sich auf die Intention des „Angreifers“. Die verlustbehaftete Komprimierung einer Audiodatei (Audio-CD zu MP3) kann einerseits nur dazu dienen, die Musik auf einem anderen Abspielgerät nutzen zu können, sie kann jedoch auch zur gezielten Zerstörung eines Wasserzeichens verwendet werden.

Transparenz Die Transparenz ist ein Maß für die Wahrnehmbarkeit eines Wasserzeichens. Ein Wasserzeichen ist transparent, wenn mit einem durchschnittlichen Hör- bzw. Sehvermögen kein Unterschied zwischen einem markierten und unmarkierten Datenstrom erkennbar ist.

Nach Dittmann et al. [12] ist ein allgemein anerkanntes Verfahren, Probanden zufällig ausgewählte nicht markierte und markierte Materialien vorzuspielen. Wenn die Zuordnung markiert oder nicht markiert eine Erfolgsrate von 50% erreicht hat, könne das Wasserzeichenverfahren als transparent betrachtet werden. Zu diesem Verfahren ist jedoch anzumerken, dass die Testmaterialien den später zu markierenden Materialien in ihrer Struktur ähneln müssen, denn gerade bei niederfrequenten Datenströmen sind durch das Wasserzeichen hervorgerufene Veränderungen leichter wahrzunehmen.

Detektierbarkeit Die Detektierbarkeit gibt Aufschluss darüber, wie leicht erkennbar ist, dass ein Datenstrom (mit einem beliebigen unbekanntem) Wasserzeichen markiert ist. Bei einem nicht detektierbaren Wasserzeichen darf durch die Markierung kein signifikanter statistischer Unterschied zwischen Original und markiertem Material eingebracht werden.

Komplexität Die Komplexität ist ein Maß für den zur Einbettung des Wasserzeichens benötigten Aufwand.

Kapazität Die Kapazität gibt an, wieviele Informationseinheiten (Bits) sich theoretisch mit einem Verfahren in das Trägermaterial einbringen lassen.

2.3 Anwendungsgebiete

Durch die hauptsächlichlichen Eigenschaften von Wasserzeichentechniken, dass sie Informationen transparent für den Konsumenten, untrennbar und unauffindbar in Daten einbetten können, sind sie im Gegensatz zum einfachen Einbetten der Informationen (z.B. in Dateihedern) besonders für die in diesem Kapitel vorgestellten Anwendungsgebiete geeignet.

Broadcast Monitoring

Ziel des Broadcast Monitoring ist es, im Radio oder Fernsehen ausgestrahlte Inhalte zu überwachen bzw. zu einem Sender zurück verfolgen zu können. Dazu werden die zu sendenden Daten durch ein Wasserzeichen markiert, um es später im ausgestrahlten Signal wieder auffinden zu können.

Eine Anwendung des Broadcast Monitorings ist zum Beispiel, automatisiert prüfen zu können, ob ein Werbespot wie vertraglich vereinbart gesendet wurde. So erschütterte 1997 ein Skandal um nicht ausgestrahlte Werbespots die Japanische Medienwelt. Der

Sender „Fukuoka Broadcasting System“ verkaufte zwischen 1975 und 1997 mehr Werbeplatz als tatsächlich verfügbar war, weswegen mehrere TV-Spots nicht gesendet, aber trotzdem abgerechnet wurden. Der Betrug wurde damals durch ‚manuelles‘ Broadcast Monitoring - der Überprüfung des ausgesendeten Programms durch Menschen - entdeckt [5].

Die Robustheit der Wasserzeichen für diese Anwendung ist vom Störverhalten des Übertragungsmediums abhängig. Wenn die Ausstrahlung eines Werbespots in einem Internetradio (somit Bit-genaue Übertragung) überwacht werden soll, genügt schon ein fragiles Wasserzeichen. Für die Überwachung eines FM-Radio-Werbespots sind jedoch robustere Verfahren notwendig, da dort mit Digital-Analog-Umwandlungen (im Playout-Center) und atmosphärischen Störungen gerechnet werden muss .

Urheberidentifikation

Die früher üblichen Techniken der Urheberidentifikation, den Urheberhinweis in Textform auf einem Bild oder dem Trägermedium anzubringen, hat sich als nicht wirksam herausgestellt. Ein sehr prominentes Beispiel, bei dem einfach der entsprechende Urhebervermerk weggeschnitten wurde, ist das oft in der Bildverarbeitung verwendete „Lena“-Bild (siehe Abbildung 2.3). Bei digitalen Audiodaten, wie MP3-Dateien aus einem Onlineshop, ist sogar gar kein Trägermedium vorhanden, auf dem sich ein Hinweis anbringen ließe. Die Speicherung des Urhebers innerhalb eines ID3-Tags¹ wiederum ließe sich zu leicht verändern oder entfernen.

Bringt man die Urheberinformationen jedoch mittels eines Wasserzeichens in die Daten ein, können sie nicht mehr einfach entfernt werden. Werden sie mehrmals, also redundant in das Material eingebracht, können auch Teile des markierten Werks wieder erkannt werden. Wäre das „Lena“-Bild mit einem redundanten Wasserzeichen versehen worden, hätte auch der verbreitete Ausschnitt des Gesamtbilds leicht seinem Urheber zugeordnet werden können.

Kundenidentifikation

Wasserzeichen können auch zur Identifikation eines Kunden verwendet werden, um ihn im Falle einer unerlaubten Weitergabe der Inhalte identifizieren zu können. Diese Anwendung, auch Fingerprinting genannt, ist zumindest zur Zeit (Februar 2008) bei deutschen

¹Mit Hilfe von ID3-Tags lassen sich in MP3-Dateien zusätzliche Informationen wie Titel, Interpret oder Albumcover speichern. Diese sind formal kein Bestandteil des MP3-Formats und lassen sich entfernen, ohne die Dateiintegrität zu gefährden. (Siehe <http://www.id3.org>)



Abbildung 2.3: Das in der Bildverarbeitung oft verwendete „Lena“-Bild und sein Urheberhinweis. [6] ©1972 Dwight Hooker/Playboy Enterprises

Audio-Onlineshops noch nicht weit verbreitet, oder ihre Verwendung wurde nicht publik gemacht. Lediglich der Hörbuch-Download-Shop von Libri.de bettet bei jedem Download ein personalisiertes Wasserzeichen ein [8]. Einen anderen Ansatz hatte die Firma DIVX² für ihren Konkurrenten des DVD-Formats gewählt. Beim DIVX-System hat jeder Player in seine Ausgangssignale ein Wasserzeichen eingebettet. Vom Player aufgenommene Inhalte waren so zu einem Player zurück verfolgbar, wodurch auch die Identität des Kundens festgestellt werden konnte [1].

Authentizitätsbeweis

Durch die zunehmende Digitalisierung von Archiven und Aufnahmegeräten und die Zulassung digitaler Beweise bei Gerichtsverfahren wird die Authentizität digitaler Daten wichtig. Um sie zu beweisen, können hochfragile Wasserzeichen in die Daten eingebettet werden, um jede Manipulation entdecken zu können. Da nicht nur die Trägerdaten, sondern auch das Wasserzeichen den Manipulationen unterworfen werden, lassen sich je nach Verfahren teilweise sogar die vorgenommenen Veränderungen identifizieren.

²Die Firma DIVX stellte 1999 ihren Geschäftsbetrieb ein [7]. Die heute im Videosektor bekannte Firma DiVX steht in keiner Verbindung zu ihr.

Kopierschutz

Um mit Hilfe von Wasserzeichen einen Kopierschutz zu realisieren, können generell zwei Ansätze verfolgt werden:

Der nichttechnische Ansatz beruht auf der Abschreckung potentieller Kopierer. Da bei einem ausreichend robusten Kundenidentifikations-Wasserzeichen der ursprüngliche Besitzer zurückverfolgt werden kann, geht man davon aus, dass dieser alles in seiner Macht stehende tun wird, dass seine Dateien nicht kursieren.

Beim technischen Ansatz müsste in jedes aufnahmefähige Gerät ein Wasserzeichencoder eingebaut werden. Dieser würde dann die Aufnahme unterbrechen, sobald ein Kopierverbot-Wasserzeichen an einem Eingang auftaucht. Dieser Ansatz ist jedoch problematisch, denn es müsste sichergestellt werden, dass jeder am Markt verfügbare Recorder das entsprechende Wasserzeichen auswertet. Dies lässt sich jedoch schlecht über Gesetze vorschreiben, weswegen verschiedene Herstellerinitiativen die Verwendung von Wasserzeichencodern in Patentierungsbedingungen aufnehmen [1]. Zusätzlich wäre die Frage, wie lange ein Kopierverbot-Wasserzeichen am Eingang anliegen müsste, bis die Aufnahme gestoppt wird. Theoretisch wäre es ja möglich, „aus Versehen“ ein Wasserzeichen im Hintergrund mittels eines Camcorders/Diktiergeräts aufzunehmen [10].

3 Verfahren

3.1 Allgemeines

Allen Verfahren für Audiodaten ist gemein, dass sie mit der zeitlichen Komponente von Audioströmen arbeiten können. So muss im Gegensatz zu Wasserzeichen für Standbilder nicht zu jedem Zeitpunkt das komplette Wasserzeichen vorhanden sein. Je nach Anwendungsfall kann daher entschieden werden, wie hoch die tatsächliche Datenrate sein muss um das Ziel, innerhalb des kürzesten zu schützenden Abschnitts das komplette Wasserzeichen unterbringen zu können, zu erreichen.

3.2 Least-Significant-Bit-Wasserzeichen

Der Datenstrom des Wasserzeichens wird beim Least-Significant-Bit-Verfahren (LSB-Verfahren) in den niederwertigsten Bits der Samples einer unkomprimierten PCM-Datei kodiert. Dadurch bietet es eine hohe theoretische Bitrate. Bei einer Samplingfrequenz von 44kHz und Verwendung jedes LSBs lassen sich theoretisch 44kBit/s einbetten. Da für die meisten Anwendungsgebiete keine so hohe Datenrate benötigt wird, kann die Nichtdetektierbarkeit auf Kosten der Bitrate erhöht werden. Dazu werden mit Hilfe eines geheimen Schlüssels die zur Markierung verwendeten Samples ausgewählt.

Ein LSB-Wasserzeichen ist zwar schnell und einfach einzubetten und auszulesen, jedoch ist seine Transparenz stark von der Bittiefe eines Samples abhängig. Ein weiterer Nachteil ist seine Fragilität. Die Umwandlung der Audiodaten mittels einer verlustbehafteten Komprimierung, wie MP3, wird das Wasserzeichen zerstören, ebenso wie eine Digital-Analog-Wandlung.

3.3 Echo-Wasserzeichen

Beim Echo-Wasserzeichenverfahren wird die temporale Maskierung des menschlichen Gehörs ausgenutzt, um dem Audiosignal durch Hinzufügen von Echos die Wasserzeichen-

bits hinzuzufügen. Bender et al. [11] geben für das Verfahren eine erreichbare Bitrate von 16Bit/s an.

Die temporale Maskierung des menschlichen Gehörs tritt auf, wenn zwei unterschiedlich starke Signale zeitnah oder zeitgleich auftreten. Die Pre-Maskierung beschreibt den Effekt, dass ein schwächeres Signal, das zeitlich vor dem stärkeren zweiten Signal aufgenommen wird, maskiert und somit nicht mehr bewusst wahrgenommen wird. Bei der Post-Maskierung wird ein schwächeres Signal nach einem stärkeren Signal nicht wahrgenommen, sofern es eine bestimmte Schwelle nicht überschreitet (siehe Abbildung 3.3). [9]

Bei der Einbettung eines Echo-Wasserzeichens wird zuerst der zu markierende Strom in einzelne Teile zerlegt. Diese Teile werden dann mit Echos versehen. Dabei entscheidet die Zeit zwischen dem Beginn des Original- und des Wasserzeichensignals, ob eine Null oder Eins codiert wird. Um zu verhindern, dass vor der Markierung existierende Echos fälschlicherweise als Wasserzeichenbits interpretiert werden und um die Transparenz zu verbessern, führen Bender et al. in [11] eine „Decay-Rate“ ein. Sie stellt einen Faktor dar, der die Amplitude des eingefügten Echos entsprechend seiner Wertigkeit (Null oder Eins) mit der des Originalsignals in Verbindung setzt. Zusätzlich stellt der Faktor sicher, dass die Amplitude des Echos sich nicht über der Maskierungsschwelle befindet.

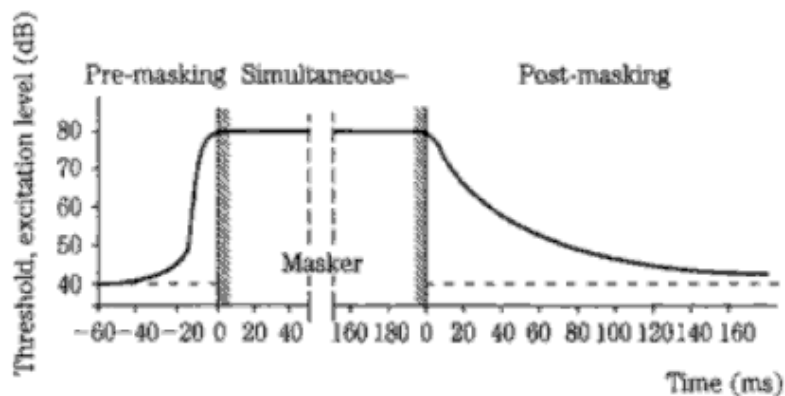


Abbildung 3.1: Temporale Maskierung des menschlichen Gehörs (aus [9]).

Echo-Wasserzeichen sind robuster als LSB-Verfahren und können in komprimierten und unkomprimierten Audiodaten eingebettet werden. Sie sind jedoch fragil im Bezug auf verlustbehaftete Kompressionsverfahren, die ein psychoakustisches Modell verwenden, da diese oft darauf beruhen, für Menschen nicht wahrnehmbare Bestandteile des Audiosignals zu entfernen.

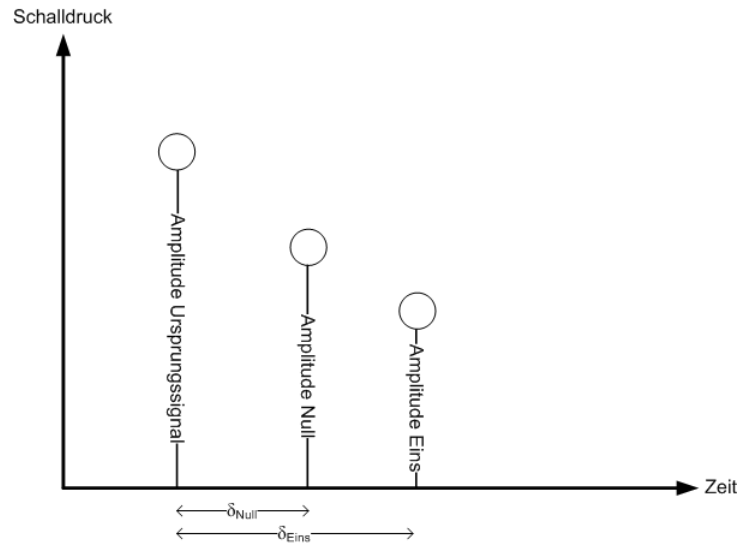


Abbildung 3.2: Echo-Wasserzeichen: Amplituden von Null und Eins im Vergleich

3.4 MPEG2-Scale-Factor-Wasserzeichen

Dittman et al. beschreiben in [12] ein blindes Verfahren, um Wasserzeichen in MPEG2-komprimierte Audiodaten einzubetten. Dabei werden die Wasserzeichenbits in Differenzmuster kodiert und in die Scalefaktoren der Datei eingebracht. Da das Verfahren auf der Bitstruktur der MPEG2-Frames aufsetzt, ist es fragil im Bezug auf Formatkonvertierungen. Bei Veränderungen des MPEG2-Datenstroms ist es sehr robust, da es eine eingebaute Redundanz besitzt. Die zu erwartende Datenrate beträgt ungefähr 0.5 Bits/Frame, bei einer minimalen Gruppenlänge von $n = 1$.

Definitionen

Um das Verfahren verdeutlichen zu können, müssen folgende Definitionen vorgenommen werden:

Längenfaktor Der Längenfaktor l beschreibt die Anzahl von Werten bzw. Scalefaktoren innerhalb eines Musters.

Redundanzfaktor Der Redundanzfaktor r beschreibt, wie viele Muster innerhalb einer Gruppe enthalten sein müssen.

Muster Ein Muster wird zur Kodierung der Wasserzeichenbits ($E = 1$, $N = 0$) und zur Synchronisierung (S) verwendet. Es besteht aus einer Folge von Ganzzahlwer-

ten, deren Wertebereich (MPEG2: -62 bis +62) durch die möglichen Scalefaktoren (MPEG2: 0 bis 62) definiert wird. Die Findung der zur Kodierung verwendeten Muster wird in [12] nicht beschrieben, es wird lediglich auf einen »geheimen Schlüssel« verwiesen, der zu Hilfe genommen werden kann.

„Falsche“ Muster sind beliebige Muster, die vor der Einbettung des Wasserzeichens bereits im MPEG2-Datenstrom enthalten sind.

Das Muster M wird dann erkannt, wenn die Scalefaktoren $x_{1\dots(l+1)}$ folgende Bedingung erfüllen:

$$M_i = x_1 + x_{i+1}$$

Gruppe Eine Gruppe ist eine Menge von n aufeinander folgenden MPEG2-Frames, in der ein Wasserzeichenbit kodiert wird. Innerhalb einer Gruppe darf nur eine Musterart auftreten. Treten mehrere auf, wird die Gruppe als gestört betrachtet und das am häufigsten auftretende Muster wird als Wert interpretiert.

Eine Gruppe wird durch ein Synchronisations-Muster beendet.

Einbettung

Zur Erklärung der Einbettung wird angenommen, dass eine 1 mit dem Muster $E = 22, 4, -3$ ($l = 3$) eingebracht werden soll. Eine 0 hat das Muster $N = 10, 10, 10$. Alle Muster werden in horizontaler Richtung gelesen. Eine Gruppe umfasst 3 Frames, der Redundanzfaktor r ist 2.

Zuerst werden vom Algorithmus die Scalefaktoren aller Frames (mit allen Subbändern) extrahiert und in Reihe zusammengefügt (siehe Tabelle 3.1).

	Frame 1			Frame 2			Frame 3		
Subband 1 Links	13	35	-	-	17	10	-	-	-
Subband 1 Rechts	-	13	37	-	-	17	10	-	-
Subband 2 Links	9	-	19	-	29	39	-	-	-
Subband 2 Rechts	-	-	-	-	-	-	-	-	-

Tabelle 3.1: Extrahierte Scalefaktoren der ersten drei Frames.

Danach wird überprüft, ob sich in der Gruppe N - und S -Muster befinden, die unkenntlich gemacht werden müssen. Im linken Kanal des zweiten Subbands beginnt beim ersten Scalefaktor des ersten Frames ein N -Muster, das durch Erhöhung des ersten Wertes um 1 maskiert wird. Als nächstes werden die ursprünglich enthaltenen E -Muster in der Gruppe gesucht. Wenn bereits r Muster enthalten sind, muss keines erzeugt werden. Im Beispiel

ist dies nicht der Fall, die Faktoren im linken Kanal von Subband 1 beschreiben zwar ein E -Muster, die geforderte Redundanz ist jedoch 2, weswegen beim ersten - für das Muster zählende - Scalefaktor (37) im rechten Kanal des ersten Subbands 2 subtrahiert werden muss (siehe Tabelle 3.2). Um die Transparenz zu erhöhen, wird bei der Anpassung der Scalefaktoren versucht, dem Zielmuster ähnliche, bereits existierende Scalefaktormuster auszuwählen.

	Frame 1			Frame 2			Frame 3		
Subband 1 Links	13	35	-	-	17	10	-	-	-
Subband 1 Rechts	-	13	35	-	-	17	10	-	-
Subband 2 Links	9	-	20	-	29	39	-	-	-
Subband 2 Rechts	-	-	-	-	-	-	-	-	-

Tabelle 3.2: Scalefaktoren nach der Einbringung eines zusätzlichen E -Musters und Maskierung des N -Musters.

Auslesen

Beim Auslesen des Wasserzeichens müssen dieselben Parameter (E, N, S, l, r, n) wie beim Einbettungsprozess bekannt sein, das unmarkierte Original wird nicht benötigt. Theoretisch ist es auch möglich, ohne die Kenntnis von n das Wasserzeichen zu restaurieren und sich nur auf die Synchronisationsmuster zur Taktung des Wasserzeichenstroms zu beziehen. Dies setzt jedoch voraus, dass alle S -Muster noch intakt sind. Sobald inhomogene Gruppen auftreten oder Synchronisationsinformationen fehlerhaft sind, kann von einer Manipulation des Datenmaterials ausgegangen werden. Dank der eingebrachten Redundanz innerhalb der Gruppen lässt sich aber statistisch auswerten, welchen Bitwert eine Gruppe ursprünglich hatte. Somit kann das Wasserzeichen trotz Manipulationen noch auslesbar sein und seinem Zweck dienen.

4 Zusammenfassung und Ausblick

Im Rahmen dieser Arbeit wurden die Grundlagen von digitalen Wasserzeichen in Audiodaten vorgestellt. Neben dem historischen Kontext der Entwicklung wurden mögliche Anwendungsgebiete aufgezeigt, sowie zum Vergleich verschiedener Verfahren notwendige Begriffe erläutert.

Die drei vorgestellten Verfahren zeigen die unterschiedlichen Möglichkeiten, Wasserzeichen einzubetten. So wurde ein einfaches auf Bitebene und ein auf der Psychoakustik arbeitendes Verfahren vorgestellt, sowie Techniken zur Robustheitsmaximierung in einem komplexeren Algorithmus präsentiert.

Die steigende Intensität der Forschungsaktivitäten in den letzten Jahren zeigt, dass digitale Wasserzeichen in Zukunft immer wichtiger werden. Auch durch die Tatsache, dass sich gerade im Audio-Download-Markt restriktive, inoperable Digital-Rights-Management-Systeme nicht durchsetzen konnten [13], werden digitale Wasserzeichen und ihre Algorithmen in Zukunft auch kommerziell eine wichtige Rolle spielen.

Abbildungsverzeichnis

2.1	Ausschnitt aus Gentleman's Magazine, Volume 49, von 1779 [2].	2
2.2	Anzahl der Veröffentlichungen des IEEE zum Thema digitale Wasserzeichen und Steganographie [4].	3
2.3	Das in der Bildverarbeitung oft verwendete „Lena“-Bild und sein Urheberhinweis. [6] ©1972 Dwight Hooker/Playboy Enterprises	7
3.1	Temporale Maskierung des menschlichen Gehörs (aus [9]).	10
3.2	Echo-Wasserzeichen: Amplituden von Null und Eins im Vergleich	11

Literaturverzeichnis

- [1] I. Cox, M. Miller, J. Bloom: *Digital Watermarking*
Morgan Kaufmann Publishers, San Francisco, 2002
- [2] Gentleman's Magazine, Volume 49, 1779,
Verfügbar unter: <http://books.google.com/books?id=70IDAAAAMAAJ&q=water-mark+%22gentleman's+magazine%22+method+counterfeiting&pgis=1>
Abgerufen: 8. Februar 2008, 19:02 MEZ
- [3] E.F. Hembrooke: *Identification of Sound and Like Signals.*
United States Patent 3,004,104, Gewährt am 10. Oktober 1961
- [4] I. Cox, M. Miller, J. Bloom, j. Fridrich, T. Kalker: *Digital Watermarking and Steganography, Second Edition*
Morgan Kaufmann Publishers, Amsterdam/Boston, 2008
- [5] D. Kilburn: *Dirty Linen, Dark Secrets*
In: ADWEEK, November 1997
Verfügbar unter: <http://www2.gol.com/users/kilburn/dirty.htm>
Abgerufen: 12 Februar 2008, 19:06 MEZ
- [6] C. Rosenberg: *The Rest of the Lenna Story*
Verfügbar unter: <http://www.lenna.org/>
Abgerufen: 17. Februar 2008, 13:17 MEZ
- [7] Digital Video Express: *Digital Video Express, LP to discontinue operations*
URL: <http://www.divx.com/>
Version vom 16. Juni 1999
Verfügbar unter: <http://web.archive.org/web/19991013054000/http://divx.com/>
Abgerufen: 21. Februar 2008, 12:47 MEZ
- [8] Libri.de: *MP3-Hörbuch Download Einführung*
URL: http://www.libri.de/shop/action/magazine/6252/mp3_hoerbuch_download.html
Abgerufen: 3. Januar 2008, 16:21 MEZ

- [9] K. C. Pohlmann: *Principles of Digital Audio*
McGraw-Hill, New York, 2005
- [10] Heise Zeitschriftenverlag: *Warner entwickelt „Audio-Wasserzeichen“ für HD DVDs*
URL: <http://www.heise.de/newsticker/meldung/65687>
Version vom 2. November 2005 20:16 MEZ
Abgerufen: 3. Januar 2008 16:22 MEZ
- [11] Bender, Gruhl, Morimoto, Lu: *Techniques for data hiding*
In: IBM Systems Journal, Volume 35, NOS 3&4, 1996
- [12] J. Dittmann: *Digitale Wasserzeichen*, Springer-Verlag, Berlin/Heidelberg/New York, 2000
- [13] Catherine Holahan: *Sony BMG Plans to Drop DRM*
In: Business Week, 4. Januar 2008
URL: http://businessweek.com/print/technology/content/jan2008/tc2008013_398775.htm
Abgerufen: 21. Februar 2008 14:20 MEZ