Digitale Audiowasserzeichen im Archivbereich – Das H2O4M Projekt

Martin Steinebach[1], Enrico Hauer[1], Jana Dittmann[2]

[1]C4M
Fraunhofer IPSI
Dolivostr.15
64293 Darmstadt
martin.steinebach@ipsi.fraunhofer.de
enrico.hauer@ipsi.fraunhofer.de

[2]PLATANISTA GmbH
Heinz-Röttger-Str. 12
06846 Dessau
Jana.Dittmann@platanista.de

Abstract: Im dem vom BMBF geförderten Projekt H2O4M wurden am Fraunhofer IPSI digitale Wasserzeichen zum Nachweis der Authentizität und Integrität von Multimediadokumenten und -objekten klassifiziert und bewertet. Es wurden in der Literatur und der Praxis vorgefundene Verfahren, Konzepte und Ideen in einem Klassifikationsschema zusammengefasst, welches Anwendungsgebiete und Verfahrensabläufe berücksichtigt. Durch die Projektpartner, das Deutsche Rundfunkarchiv (DRA) und die tecmath AG wurde eine Praxisbezug hergestellt. Es galt, die anstehende Öffnung des DRA für einen Webzugriff auf den Archivbestand hinsichtlich der verbreiteten Mediendaten zu schützen. Für Problemstellungen im Video- und Audiobereich wurden neue Algorithmen entwickelt oder bestehende Verfahren verbessert.

1 Projektszenario H2O4M

In dem Projekt H2O4M [DSK+00] konnten wir praktische Erfahrungen mit den Anforderungen an digitale Wasserzeichen [D00] im Archivbereich sammeln: Digitalisierte Medien des Deutsche Rundfunkarchivs (DRA) sollen über das Internet sicher für Anwender zugänglich werden. In der Testphase handelt es sich dabei um verteilt arbeitende Archivare. Letztendlich soll aber das Archiv jedem Internetteilnehmer offen stehen. Das Archiv enthält Audio- und Videodaten, beide Medientypen wurden im Projekt betrachtet. Wir konzentrieren uns in der vorliegenden Arbeit auf den Schutz der Audiodaten, bei denen auch die Digitalisierung weiter vorangeschritten ist.

Das DRA stellte folgende Anforderungen hinsichtlich der Sicherheit, welche auf verschiedene Weise durch Audiowasserzeichen befriedigt werden sollten:

- **Möglichkeit des Urhebernachweises** - In jeder weitergegebenen Datei soll ein Hinweis auf das DRA vorhanden sein, um bei illegaler Weitergabe des Materials das DRA als ursprüngliche Quelle nachweisen zu können.
- **Medienidentifikation** - Jede weitergegebene Datei soll einen Hinweis auf deren Inhalt enthalten. Dabei wird eine Art Katalognummer verwendet, die ein eindeutiges Identifizieren des Material ermöglicht.
- **Integritätsschutz** - Material soll nicht unerkannt im Nachhinein veränderbar sein. Da das vom DRA bereitgestellte Material für Fernsehübertragungen und die Forschung verwendet wird, kann es zu Fälschungen oder Inhaltsveränderungen kommen. Um dies zu verhindern, soll ein Schutzmechanismus Veränderungen im Original nachweisen.
- **Verfallsdatum** - Die Verwendung des Materials durch Fernsehsender wird durch die entrichtete Gebühr nur für einen bestimmten Zeitraum erlaubt. Bei einer weiteren Verwendung des Materials sind erneute Zahlungen notwendig. Um diesen Prozess zu unterstützen, ist das Einbetten des Verfallsdatums in das Medium notwendig.

2 Einsatz von digitalen Audiowasserzeichen

Aus den in Kapitel 1 aufgeführten Anforderungen an die Sicherheit können in Verbindung mit der Betrachtung des Szenarios verschiedene Anforderungen an die Eigenschaften der eingesetzten Wasserzeichen abgeleitet werden. Eine allgemeine Betrachtung der Eigenschaften von Wasserzeichen erfolgt hier aus Platzgründen nicht, kann aber beispielsweise in [D00] nachgeschlagen werden. Wir stellen im Folgenden die wichtigsten Anforderungen vor und bewerten den Grad der Umsetzung durch unsere Algorithmen. Dabei kommen zwei Algorithmen zum Einsatz:

- **PCM-Wasserzeichen –** Der Algorithmus bettet Wasserzeichen in PCM (Pulse Code Modulation)-Audiodaten ein. Diese bestehen aus einer nicht komprimierten Folge von Abtastwerten mit wechselnder Abtastrate und Bitbreite und stellen die Rohform von in Rechnersystem betrachteten Audiodaten dar.
- **Mp2-Wasserzeichen –** Das Verfahren bettet Informationen in mp2-Dateien ein, basierend auf unseren in [D+99] vorgestellten Algorithmus. Mp2-Dateien stellen verlustbehaftet komprimierte Audiodaten da, aus denen für Hörer nicht relevante Anteile entfernt wurden, um eine niedrigere Datenrate zu erreichen. Mp2 ist das übliche Austauschformat für Audiodaten im DRA.

Urheberschutz und Medienidentifikation wurden gemeinsam durch ein PCM-Wasserzeichen eingebettet. Zwar waren die Anforderungen an die Medienidentifikation hinsichtlich der Robustheit niedriger als beim Urheberschutz, ein gemeinsames Einbetten bei hohen Anforderungen an die Robustheit ließ sich aber problemlos umsetzen. Es zeigte sich, dass die Wasserzeichen alle vom DRA als im einsatztypisch angesehene Operationen, wie Entrauschen, Filtern und leichtes Timestretching (<2%) problemlos überstehen, hier traten keine Fehler beim Auslesen der eingebetteten

Informationen auf. Auch hinsichtlich der Datenrate konnten alle Anforderungen erfüllt werden: Die Kennung des DRA sollte mindestens in jedem 30 Sekunden langen Stück Audio gefunden werden können, in der Praxis konnte die Kennung in jedem mindestens 9 Sekunden langem zusammenhängenden Stück Audio detektiert werden.

Die durch das Wasserzeichen verursachten Verluste in der Qualität waren minimal: Sowohl Hörtests durch geschultes Personal als auch automatisierte Systeme zur Qualitätskontrolle von Audioübertragungen zeigten, dass es zu keiner wahrnehmbare Verschlechterung der Audiodaten durch die Wasserzeichen kommt. Ein Sonderfall bildet der Einsatz der Wasserzeichen für stark komprimierte Dateien, die für Vorhör-Funktionen eingesetzt werden. Hier musste ein wahrnehmbarer Qualitätsverlust in Kauf genommen werden, der allerdings durch den deutlich stärkerer Klangverlust, verursacht durch die starke Kompression, maskiert wird.

Neben den technischen Anforderungen musste auch eine geeignete Stelle innerhalb der Arbeitsabläufe des DRA identifiziert werden, an der das Wasserzeichen eingebettet werden soll. Da Urheberinformation und Medienidentifikation untrennbar mit dem weitergegeben Medium verknüpft sein sollen und für jede Kopie einer Quelle gleich sind, kann hier das Einbetten bereits bei dem Übertragen vom Archiv in den Server der Webschnittstelle geschehen. Ein unmarkiertes Original ist somit nur im Archiv selbst vorhanden, wodurch keine Kopien ohne Kennung ins Internet gelangen können.

Das **Verfallsdatum** wurde in der praktischen Evaluierung des Projektes nicht betrachtet, es wurde aber ein Verfahren identifiziert, welches für die aus der Anwendung abgeleiteten Anforderungen erfüllt. Das Datum soll ebenfalls in jedem 30 Sekunden langem Stück Audio vorhanden sein. Bei einer groben Darstellung des Datums ist eine Angabe von Jahr und Monat ausreichend, wodurch sind eine minimale notwendige Datenrate ergibt: Auch bei nur einem Bit Wasserzeicheninformation pro Sekunde könnten mehrere tausend Jahre abgedeckt werden. Allerdings kann das Verfallsdatum erst eingebettet werden, wenn der Zeitpunkt des Bereitstellens bekannt ist, da die Medien über einen zeitlich begrenzten, vom Datum der Ausgabe beginnenden Zeitraum genutzt werden dürfen. Daher ist hier ein zweites Verfahren notwendig, welches bei Ausgabe der Datei über das Internet in Echtzeit ein weiteres Wasserzeichen mit dem Verfallsdatum als Information einbetten kann. Hier kann unser mp2-Verfahren eingesetzt werden, welches das zu diesem Zeitpunkt bereits eingebettete PCM-Wasserzeichen nicht merklich beeinflusst.

Die Funktion der Verfallsdatumskontrolle erfordert ein Auslesen des Wasserzeichen während des Einsatzes bei den Anwendern, z. B. durch eine Warnfunktion. Während des Ladens von Audiodaten kann das Wasserzeichen gesucht und das Verfallsdatum angezeigt werden. Dazu muss aber ein Detektor für das Wasserzeichen mitsamt dem entsprechenden Schlüssel an die Anwender weitergegeben werden. Ein Angreifer kann dadurch aber das Wasserzeichen gezielt angreifen. Eine Lösung ist ein zweifaches Einbetten mit einem öffentlichen und einem internen Schlüssel. Der Angreifer kann so zwar die Warnhinweise deaktivieren, das DRA kann aber mit dem zweiten Schlüssel weiterhin das Verfallsdatum erkennen, z.B. bei Ausstrahlung der Medien.

Der **Integritätsschutz** als letzte Sicherheitsanforderung wurde nur innerhalb der Forschungsumgebung evaluiert, da hier nur grundlegende Untersuchungen durchgeführt wurden. In der Versuchsumgebung konnte ein Verfahren entwickelt und getestet werden, welches auf inhaltsfragilen Wasserzeichen (siehe hierzu [DS+00]) basiert. Hier werden Prüfsummen von aus Audiodaten extrahierten Inhaltsmerkmalen [DSS+01] berechnet und mittels einer angepassten Variante unseres PCM-Wasserzeichens in die Audiodaten eingebettet. Diese können später extrahiert und mit Prüfsummen aktueller Inhaltsmerkmale verglichen werden. In unserer Versuchen konnten wir anhand dieses Verfahrens in Zeitfenstern von ca. 3 Sekunden Audio erkennen, starke Veränderungen oder schwache Veränderungen der Inhalte auftraten. Eine Manipulation durch starke Veränderung oder auch durch Schneiden des Materials wird somit erkannt.

Wir können zusammenfassend feststellen, dass durch digitale Audiowasserzeichen einige Sicherheitsanforderungen des DRA bereits vollständig erfüllt werden können, während in anderen Bereichen nach Ende des Projektes noch weiterer Forschungsbedarf besteht: Während Urhebernachweis heute problemlos möglich ist, sind Verfahren zum Integritätsschutz, die nicht auf Kryptographie, sondern auf Wasserzeichen beruhen, noch Forschungsthema. Für eine ausführlichere Betrachtung der einzelnen Punkte sei auf die Auswahl unserer innerhalb des Projektes entstandener Referenzen verwiesen.

Literaturverzeichnis

[DDS+01] Dappa, Artur; Dittmann, Jana; Steinebach, Martin; Vielhauer, Claus: Eine Sicherheitsarchitektur auf der Basis digitaler Wasserzeichen und kryptographischer Ansätze. In: Verlässliche IT-Systeme 2001, Sicherheit in komplexen IT-Infrastrukturen, Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, pp. 209 - 224, ISBN 3-528-05782-3, 2001.

[DSK+00] Dittmann, Jana; Steinebach, Martin; Kunkelmann, Thomas; Stoffels, Ludwig: H2O4M - Watermarking for Media: Classification, Quality Evaluation, Design Improvements. In: Proceedings ACM Multimedia 2000 Workshops, November 4, Los Angeles, California, pp. 107 - 110, ISBN 18113-311-1, 2000.

[DSS+99] Dittmann, Jana; Steinebach, Martin; Steinmetz, Ralf (1999): Digitale Wasserzeichen für MPEG Audio. ITG-Fachbericht 156 Multimedia Anwendungen, Technologien, Systeme. Vorträge des 8. Dortmunder Fernsehseminars vom 27. bis 29. September in Dortmund. Berlin: VDE Verlag, 1999, S. 185 - 190, ISBN: 3-8007-2488-X.

[D00] Dittmann: Digitale Wasserzeichen, Springer Verlag, ISBN 3 - 540 - 66661 - 3, 2000

[DSS+01] Dittmann, Jana; Steinebach, Martin; Steinmetz, Ralf: Merkmale digitaler Audiodaten zur Verwendung in inhaltsfragilen digitalen Wasserzeichen. In: Verlässliche IT-Systeme 2001, Sicherheit in komplexen IT-Infrastrukturen, Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, pp. 193 - 208, ISBN 3-528-05782-3, 2001

[DS+00] Dittmann, Jana; Steinebach, Martin: Manipulationserkennung bei digitalem Bildmaterial mit fragilen Wasserzeichen. In: Datenschutz und Datensicherheit; Verlag Vieweg, 10/2000, pp. 593 - 597, 2000