Robustheit digitaler Audiowasserzeichen gegen Pitch-Shifting und Time-Stretching

Martin Steinebach, Sascha Zmudzinski

Fraunhofer Institut für
Integrierte Publikations- und Informationssysteme (IPSI)
Dolivostr. 15
64293 Darmstadt
{martin.steinebach|sascha.zmudzinski}@ipsi.fraunhofer.de

Zusammenfassung: Die Robustheit digitaler Wasserzeichen ist neben der Transparenz das am häufigsten diskutierte und evaluierte Charakteristikum. Im Bereich der Audiowasserzeichen sind inzwischen eine Reihe von Algorithmen bekannt, die Operationen wie verlustbehaftete Kompression oder DA/AD-Wandlung überstehen. Eine größere Herausforderung ist derzeit noch die Robustheit gegen Pitch-Shifting und Time-Stretching, die oft zur Nicht-Auslesbarkeit der Wasserzeichen führen. Wir beschreiben eine Serie von Versuchen zu diesen Angriffen und zeigen, dass die Angriffe das Wasserzeichen oft nicht zerstören, sondern nur deren Auslesen erschweren.

1 Motivation

Digitale Wasserzeichen werden heute vermehrt zum Schutz von Audiodaten vor Urheberrechtsverletzungen eingesetzt. Dabei sind derzeit in erster Linie zwei Aspekte von Bedeutung: Die Wasserzeichen dürfen die Qualität der geschützten Audiodaten nicht vermindern und sie sollen auch nach starken Veränderungen der Audiodaten noch aus diesen ausgelesen werden können.

Derzeit kann bei einem aktuellen Audiowasserzeichenalgorithmus davon ausgegangen werden, dass er, ohne die Klangqualität wahrnehmbar zu beeinträchtigen, robust gegen starke verlustbehaftete Kompression wie mp3 oder WMA sowie DA/AD-Wandlung ist [St03]. Angreifer müssen dementsprechend entweder unter Kenntnis des Wasserzeichenverfahrens gezielte Angriffe gegen den Algorithmus ausführen oder sich allgemeine Bearbeitungsschritte suchen, die das Wasserzeichen zerstören.

Geeignete Bearbeitungen sind hier in erster Linie solche, die die Audioeigenschaften kaum hörbar verändern, trotzdem aber starke Auswirkungen auf die Wasserzeichen haben. Dazu gehören insbesondere Veränderungen an der Tonhöhe (engl. Pitch-Shifting) oder der Abspieldauer (engl. Time-Stretching) der Audiodaten [SPR+01], welche heute zur Anpassung an gewünschte Spiellängen verbreitet eingesetzt werden. Abbildung 1 zeigt ein entsprechendes Werkzeug. Aber auch durch Ungenauigkeiten in analogen Abspielgeräten können entsprechende Effekte schnell auftreten.

Für die Anwender digitaler Wasserzeichen ist es auf der anderen Seite von großer Bedeutung, die eingebetteten Informationen nach Angriffen wieder auslesen zu können. Ein Beispiel sind hier Musikstücke, die in Online-Shops beim Kauf individuell markiert werden und somit beim Auftauchen illegaler Kopien auf deren Quelle zurückverfolgt werden können. Ist der verursachte Schaden hoch, kann sich ein aufwändiges Suchen nach dem Wasserzeichen lohnen. Hier können dann auch die oft als zu komplex angesehenen nicht-blinden Wasserzeichen verwendet werden, die zum Auslesen die Originaldatei benötigen [SF05].

Wir beschäftigen uns im Folgenden damit, ob die Angriffe Pitch-Shifting und Time-Stretching (siehe dazu auch [VLB04]) Wasserzeichen tatsächlich zerstören oder ob durch ausgefeilte Suchstrategien auch nach diesen Angriffen die Wasserzeichen ausgelesen werden können. Dazu erläutern wir in Abschnitt 2 die Grundlagen der Technologie der digitalen Wasserzeichen und gehen näher auf die technischen Details von Time-Stretching und Pitch-Shifting ein. In Abschnitt 3 beschreiben wir einen Versuchsaufbau, der eine Datei zuerst mittels Time-Stretchin und Pich-Shifting angreift und anschließend wieder in ihre ursprüngliche Spieldauer und Tonhöhe zurückversetzt. Danach wird in Abschnitt 4 festgestellt, ob das Wasserzeichen noch auslesbar ist oder die Auswirkungen der doppelt aufgetretenen Veränderungen das Wasserzeichen zerstören. Zusätzlich wird hierbei untersucht, welche Auswirkungen die durchgeführten Operationen auf die Klangqualität besitzen. In Abschnitt 5 diskutieren wir, ob und welche Strategien zu einer verbesserten Detektion von Wasserzeichen entwickelt werden können, wenn die Audiodaten mittels Picht-Shifting oder Time-Stretching verändert wurden und geben in Abschnitt 6 eine Zusammenfassung.

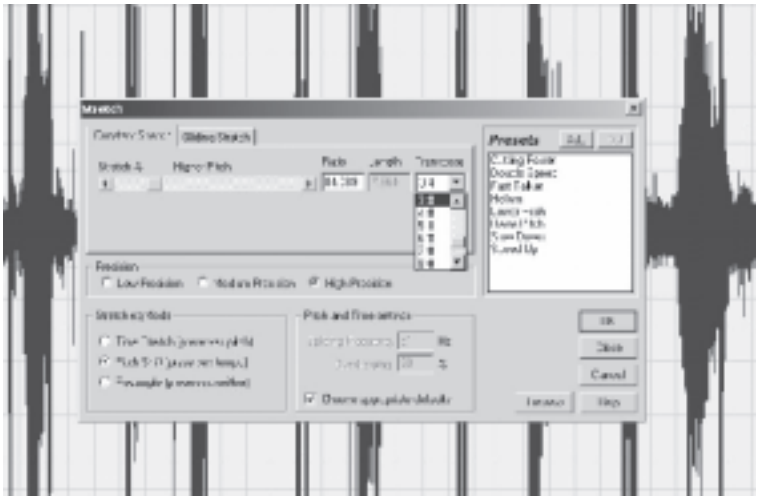

Abbildung 1: Pitch-Shifting und Time-Stretching sind heute verbreitete Funktionen in Audiobearbeitungssoftware, wie beispielsweise dem hier gezeigten CoolEdit.

2 Digitale Wasserzeichen und der Begriff der „Robustheit“

Nach [Di00] verstehen wir unter einem digitalen Wasserzeichen ein transparentes, nicht wahrnehmbares Muster, welches in das Datenmaterial (Bild, Video, Audio, 3D-Modelle) mit einem Einbettungsalgorithmus unter Verwendung eines geheimen Schlüssels eingebracht wird. Digitale Wasserzeichen sind passive Schutzmechanismen und in den meisten Fällen sogar völlig transparent für die menschliche Wahrnehmung.

Jeder Wasserzeichenalgorithmus besteht in Analogie zur Steganographie aus:

- Einem Einbettungsprozess (Watermark Embedding)
- Einem Abfrageprozess/Ausleseprozess (Watermark Retrieval)

Das eingebettete Muster repräsentiert die eingebrachte Information. Typischerweise stellt das Muster eine von zwei Arten von Informationen dar: Entweder ein von einem Schlüssel abhängiges Muster zur Identifizierung des Urhebers/Autors/Senders oder kodierte Informationen. Hier handelt es sich im Allgemeinen um Urheberdaten, Kundendaten oder Metadaten.

Nach [CMB2002] ist die Verbindung zwischen Trägerdatei und Wasserzeichen ein wichtiges Unterscheidungskriterium zwischen Wasserzeichen und Steganographie. In der Steganographie stehen Trägerdatei und versteckte Information im Allgemeinen nicht miteinander in Beziehung, die Trägerdatei dient nur zur Tarnung der Informationen. Bei digitalen Wasserzeichen hingegen sagt die in der Trägerdatei eingebettete Information etwas über die Trägerdatei aus.

Jeder Wasserzeichenalgorithmus hat bestimmte Eigenschaften. Die wichtigsten Eigenschaften sind nach [D2000] und [CMB02] Robustheit, Nicht-Wahrnehmbarkeit, Sicherheit, Komplexität, Kapazität, Verifikation und Invertierbarkeit.

In der vorliegenden Arbeit wird in erster Linie die Robustheit betrachtet. Die eingebrachte Wasserzeicheninformation ist robust, wenn die Information zuverlässig aus dem Datenmaterial ausgelesen werden kann, auch wenn das Datenmaterial modifiziert (aber nicht vollständig zerstört) wurde. Robustheit bezeichnet somit die Widerstandsfähigkeit der in ein Datenmaterial eingebrachten Wasserzeicheninformation gegenüber blinden, d.h. ungezielten Veränderungen des Datenmaterials, legitimen Medienverarbeitungen (z.B. Bild-, Tonverarbeitung oder 3D-Modellierungen) oder gegenüber Fehlern bei der Datenübertragung. Robustheit bezieht sich nicht auf Angriffe, die auf der Kenntnis des Einbettungs- und Abfrageprozesses oder gar des geheimen Schlüssels basieren. Gezielte Angriffe auf den Algorithmus deckt der Parameter Sicherheit ab.

2.1 Pitch-Shifting und Time-Stretching

Pitch-Shifting und Time-Stretching sind vor allem deshalb als Angriff geeignet, weil sie Frequenzen verändern und den zeitlichen Ablauf von Audiodaten beeinflussen. Viele Audiowasserzeichenverfahren sind zwar beispielsweise in der Lage, zufällige Veränderungen in den Audiodaten, wie es beispielsweise Rauschen bewirkt, zu

überstehen, können aber nach dem Verschieben ganzer Frequenzbänder das Wasserzeichen nicht mehr auslesen.

Der Grund dafür liegt in dem verbreiteten Konzept, Wasserzeichen im Spektrum von diskreten Audioblöcken einzubetten. Beispiele sind das Überlagern mit schwachem Rauschen oder das Herstellen von statistisch detektierbaren Energieverhältnissen zwischen den einzelnen Spektralbändern. Um das Wasserzeichen wieder auszulesen, werden die gleichen Spektralbänder wie beim Einbetten benötigt. Diese sind aber durch die Angriffe entweder im Spektrum verschoben oder zeitlich verzerrt. Dabei entstehen je nach verwendetem Algorithmus weitere Artefakte, die die Detektion erschweren.

In Abbildung 2 zeigen wir, wie sich Pitch-Shiftig auf einen Akkord auswirkt. Dabei wird offensichtlich, dass es sich nicht um ein bloßes Verschieben von Frequenzen handelt, sondern dass diese gespreizt werden.

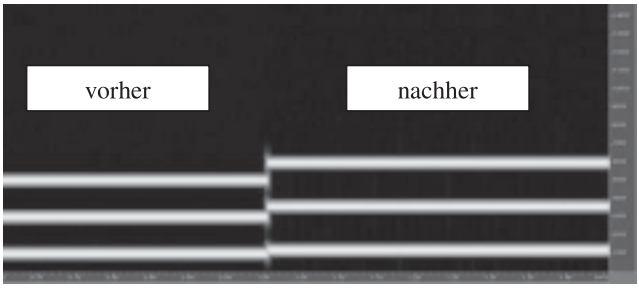

Abbildung 2: Auswirkung eines Pitch-Shiftings um 3 Halbtonschritte nach oben auf einen Akkord aus 3 Sinuswellen (Spieldauer 0,8 Sekunden, Frequenzbereich 0-15 kHz).

3 Versuchsbeschreibung

Zur Evaluierung wurden 92 Testdateien zu je 30 Sekunden, 44,1 kHz, mono, eingesetzt, deren Qualität von sehr guten Klassikaufnahmen bis hin zu Videomitschnitten reicht. Es sind auch alleinstehende Instrumente, Drumloops und Testsignale enthalten. Durch das Testmaterial wird somit ein umfassendes Spektrum an Audiomaterial geboten.

Die Bewertung der Auswirkung der Angriffe auf die Klangqualität des Audiomaterials wurde durch Opera [1], ein System zum objektiven Bewerten von Klangverlusten, durchgeführt. Anhand verschiedener Hörmodelle werden hier Unterschiede zwischen zwei Versionen einer Audiodatei erkannt und gemeinsam zu einem Differenzwert zusammengerechnet. Dieser wird mit ODG (Objective Difference Grade) bezeichnet und zur Bewertung herangezogen.

[1] http://www.opticom.de/, eingesetzt wird das Perceptual Evaluation of Audio Quality (PEAQ) Modell, basierend auf der ITU Recommendation BS.1387-1

Unterschieden wird zwischen den folgenden Einstufungen:

0,0	Nicht wahrnehmbar
-1,0	Wahrnehmbar, aber nicht störend
-2,0	Leicht störend
-3,0	Störend
-4,0	Sehr störend

Wichtig zu beachten ist noch, dass die Vergleiche zwischen der markierten Ausgangsdatei und der Datei, die zum Auslesen des Wasserzeichens verwendet wurde, durchgeführt wurden. Somit hat zum einen das Wasserzeichen selbst keine Auswirkungen auf die hier gemessene Klangqualität. Zum anderen ist der Vergleich nur zwischen den Dateien vor dem Angriff und nach dem invertierten Angriff, der das Material wieder in die Ausgangstonlage oder –spieldauer bringt, möglich. Somit sind die Artefakte der Angriffe stärker als die in der angegriffenen Datei wahrnehmbar, dafür sind natürlich die Auswirkungen der Angriffe auf die Ausgangstonlage oder –spieldauer nicht mehr vorhanden. Dieser Umstand ist nicht optimal zur Analyse geeignet, durch die in Abschnitt 4 beschriebenen sehr prägnanten Ergebnisse bezüglich der Klangqualität kann aber allgemein von einem hohen Qualitätsverlust ausgegangen werden.

Die Auswirkungen der Wasserzeichen auf die Klangqualität werden nicht betrachtet, detaillierte Analysen hierzu sind in [St03] zu finden.

3.1 Versuchsablauf

In unserem Versuch gingen wir nach dem folgenden Schema vor:

1. Markieren der Dateien
2. Auslesen des Wasserzeichens aus der markierten Datei
3. Angriff
4. Invertierter Angriff
5. Auslesen des Wasserzeichens aus der resultierenden Datei
6. Ermitteln des ODG-Wertes (siehe oben) aus markierter und resultierender Datei

Für (1), (2) und (5) wurde ein von uns entwickelter und in [St03] vorgestellter Wasserzeichenalgorithmus verwendet.

Um Pitch-Shifting und Time-Stretching in (3) und (4) durchzuführen, wurden die Werkzeuge Sound Forge und CoolEdit eingesetzt, beides gebräuchliche Werkzeuge zum Nachbearbeiten von Audiodaten.

Damit wurden die folgenden Angriffe durchgeführt:

- Pitch-Shifting: Hier wurde die Tonhöhe um einen, zwei, drei und sechs Halbtonschritte erhöht und danach wieder auf den Ursprungswert zurückgesetzt.
- Time-Stretching: Hier wurde die Ausgangsspieldauer um 1%, 5%, 10%, 30% und 50% erhöht und danach wieder erniedrigt.

Es wurden vier unterschiedliche Abläufe gestestet: In zweien wurden beide Werkzeuge für sich allein für die Schritte (3) und (4) eingesetzt, in zwei anderen wurden die Werkzeuge zwischen Schritt (3) und (4) ausgetauscht. Dadurch wird der realistische Fall simuliert, dass beim Auslesen zwar beispielsweise die Originalspieldauer eines markierten Musikstücks bekannt ist, aber nicht, mit welchem Werkzeug diese durch einen Angreifer verändert wurde.

4. Ergebnisse

Der in Abschnitt 3 beschriebene Versuchsaufbau liefert eine Reihe von aufschlussreichen Ergebnissen bezüglich der Robustheit digitaler Wasserzeichen gegenüber den Angriffen Pitch-Shifting und Time-Stretching. Im Folgenden werden zuerst die einzelnen Ergebnisse beschrieben und zum Ende des Abschnitts diskutiert.

Für beide Angriffstypen werden sowohl der durchschnittliche absolute Erfolg als auch die durchschnittliche Anzahl der ausgelesenen Wasserzeichen angegeben. Ersterer besagt, in wie viel Prozent der Dateien zumindest ein Wasserzeichen wieder ausgelesen werden konnte. In die Originaldaten wurden jeweils 5 Wasserzeichen eingebettet.

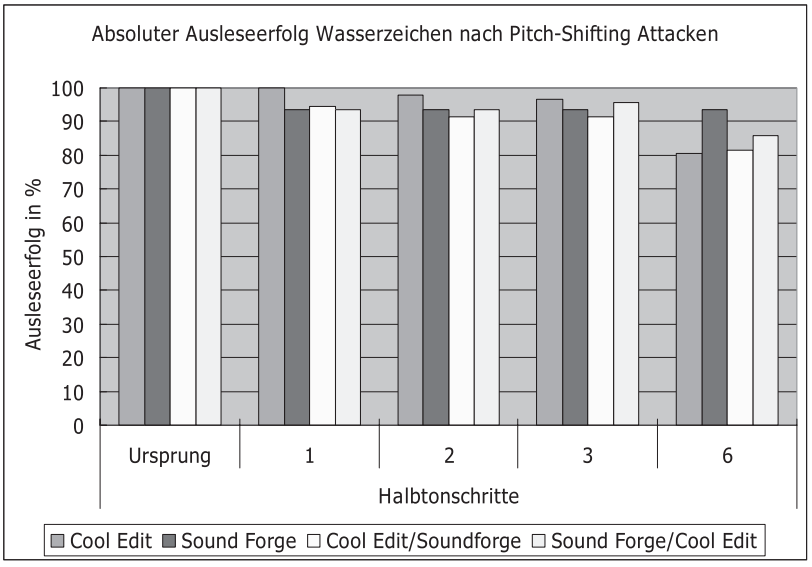

Abbildung 3: Die Anzahl von Dateien, aus denen mindestens ein Wasserzeichen erfolgreich ausgelesen werden konnte, sinkt erwartungsgemäß mit dem Anstieg der Tonhöhenunterschiede. Allerdings ist das Erfolgsniveau selbst bei 6 Halbtonschritten noch bei mindestes 80%.

4.1 Robustheit gegen Pitch-Shifting

Die Ergebnisse im Pitch-Shifting zeigen eine hohe Robustheit des Wasserzeichens gegen die Veränderungen auf, die durch das Erhöhen und erneute Vermindern der Audiodaten entsteht. Nach einem Halbtonschritt können aus über 90% der Dateien noch Wasserzeichen ausgelesen werden, wie Abbildung 3 zeigt. Bei sechs Halbtonschritten sind es noch immer mindestens 80%. Die Werkzeuge haben keinen starken Einfluss auf die Ergebnisse, auch nach einem Wechsel zwischen ihnen bleibt das Erfolgsniveau ähnlich. Interessant ist, dass CoolEdit bei geringen Angriffen bessere Ergebnisse liefert, während Sound Forge bei starken Angriffen bessere Ausleseerfolge mit sich bringt.

Die in Abbildung 4 gezeigte Anzahl der durchschnittlich ausgelesenen Wasserzeichen verhält sich ähnlich. Aus der Ausgangsdatei können durchschnittlich 4 Wasserzeichen ausgelesen werden, was für Wasserzeichenverfahren aufgrund der teilweise unvorteilhaften Eigenschaften einzelner Passagen im Audiomaterial typisch ist. Nach den Angriffen mit einem, zwei und drei Halbtonschritten können noch immer im Durchschnitt mehr als 3 Wasserzeichen detektiert werden. Erst sechs Halbtonschritte lassen den Schnitt unter 2 Wasserzeichen fallen.

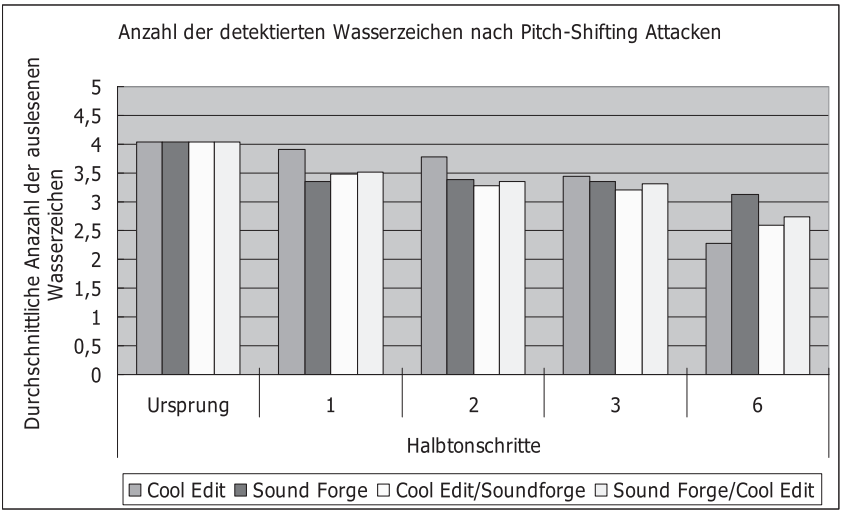

Abbildung 4: Die Anzahl der Wasserzeichen, die durchschnittlich aus den Dateien ausgelesen werden konnte, sinkt ebenfalls kontinuierlich mit dem Erhöhen der Angriffsstärke.

4.2 Robustheit gegen Time-Stretching

Time-Stretching hat stärkere Auswirkungen auf die Ausleserate als Pitch-Shifting. Hier wird nur dann ein hohes Niveau erreicht, wenn ausschließlich mit CoolEdit gearbeitet wird, zumindest bei den Angriffsstärken 1% und 5%. Ansonsten sinkt der Ausleseerfolg

(siehe Abbildung 5) sofort unter 90%. Bei einem Angriff mit 50% liegt der Erfolg nach Angreifen durch CoolEdit und inversem Angriff durch Sound Forge bei nur ca. 65%. Interessant ist noch, dass auch hier Sound Forge bei stärkeren Angriffen bessere Ergebnisse liefert.

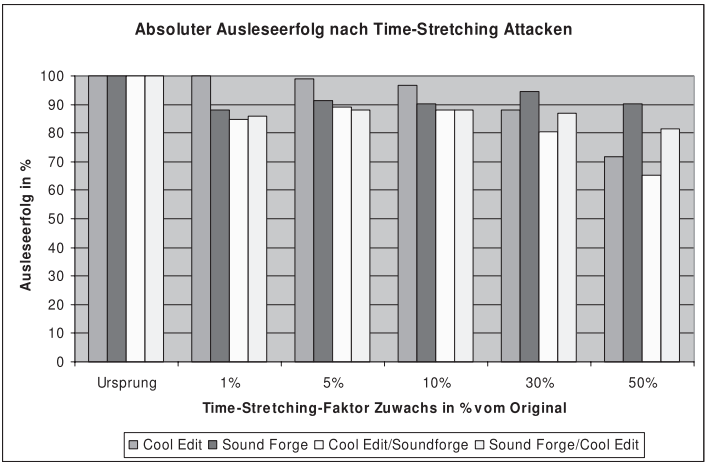

Abbildung 5: Time-Stretching hat stärkere Auswirkungen als Pitch-Shifting. Hier Sind bereits 1% Veränderung ausreichend, um den Ausleseerfolg auf ca. 85% zu senken

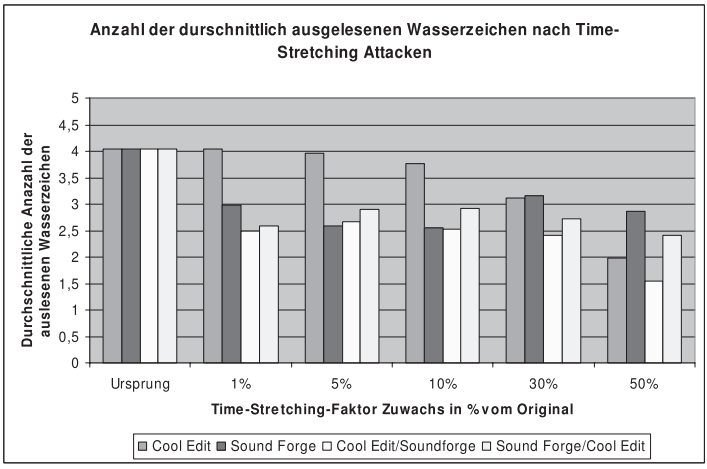

Abbildung 6: Die durchschnittliche Anzahl der ausgelesen Wasserzeichen nach Time-Stretching-Angriffen sinkt schnell unter 3.

Bei den in Abbildung 6 gezeigten durchschnittlich ausgelesenen Wasserzeichen verhält es sich ebenso. Allerdings werden Fall von CoolEdit bei den niedrigen Angriffsstärken durchschnittlich mehr Wasserzeichen ausgelesen werden können als nach den Pitch-Shifting Angriffen.

4.3 Klangverlust durch die Angriffe

Die Auswirkungen der Angriffe auf die Klangqualität waren allgemein sehr hoch. Nach fast allen Angriffen und mit allen Werkzeugen und deren Kombination wurden die Qualitätsverluste von Opera als störend beurteilt (Abbildungen 7 und 8). Einzige Ausnahme ist Time-Stretching von einem Prozent mit CoolEdit, wo nur ein Klangverlust bemerkt wurde, der wahrnehmbar bis leicht störend ist (Abbildung 8).

Bemerkenswert ist, dass eine niedrige Klangqualität nicht mit schwer auszulesenden Wasserzeichen gleichzusetzen ist. So klingt CoolEdit bei einem Angriff mit 2 Halbtonschritten zwar schlechter als Sound Forge, es können aber mehr Wasserzeichen aus der angegriffenen Datei ausgelesen werden. Ebenso sind die Klangverluste zwischen CoolEdit und Sound Forge auch bei hohen Angriffen ähnlich, während der Ausleseerfolg hier bei Sound Forge höher ist.

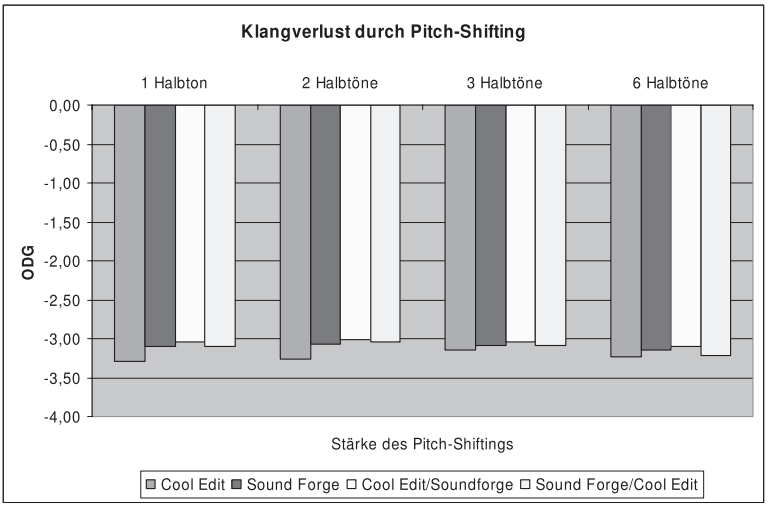

Abbildung 7: Die Klangverluste durch das zweifach ausgeführte Pitch-Shifting sind hoch. In allen Fällen sind die Auswirkungen als störend erkannt worden.

4.4 Diskussion der Ergebnisse

Die in den vorherigen Abschnitten aufgezeigten Ergebnisse zeigen eine Reihe von Eigenschaften von Pitch-Shifting und Time-Stretching Angriffen:

1. Werden die Angriffe wieder rückgängig gemacht, kann aus einer großen Anzahl von markierten Dateien das Wasserzeichen wieder ausgelesen werden. Das Wasserzeichen wird also nicht zerstört, sondern befindet sich nur an einer Position, die bei der Detektion des Wasserzeichens nicht beachtet wird.

2. Die Angriffe führen zu einem hohen Qualitätsverlust. Ein Angreifer wird die Angriffe nur ausführen, wenn er ganz bewusst Wasserzeichen zerstören will oder wenn es das Einsatzgebiet der Audiodaten mit sich bringt.
3. Beide Angriffstypen führen mit einer höheren Angriffsstärke zu einer schlechteren Detektion der Wasserzeichen. Gleichzeitig bleiben die Klangverluste ähnlich hoch. Würde ein Angreifer also gegen Wasserzeichen vorgehen wollen, würde er eher einen starken Angriff wählen und diesen wieder rückgängig machen, da der Klangverlust gleich bleibt, die Wasserzeichen aber eher zerstört werden. Der Angreifer wird das Material sicher nicht in dem stark veränderten Zustand lassen, da eine Tonhöhenverschiebung von 6 Halbtonschritten oder ein Erhöhen der Abspieldauer um 50% qualitativ nicht akzeptabel sind.
4. Es ist nicht notwendig, das Werkzeug zu kennen, mit dem ein Angreifer vorgegangen ist. Die Ergebnisse zeigen, dass die Auslesequalität annähernd unabhängig von den eingesetzten Werkzeugen ist und auch die Verwendung verschiedener Werkzeuge zu keinen deutlichen Verschlechterungen führt.

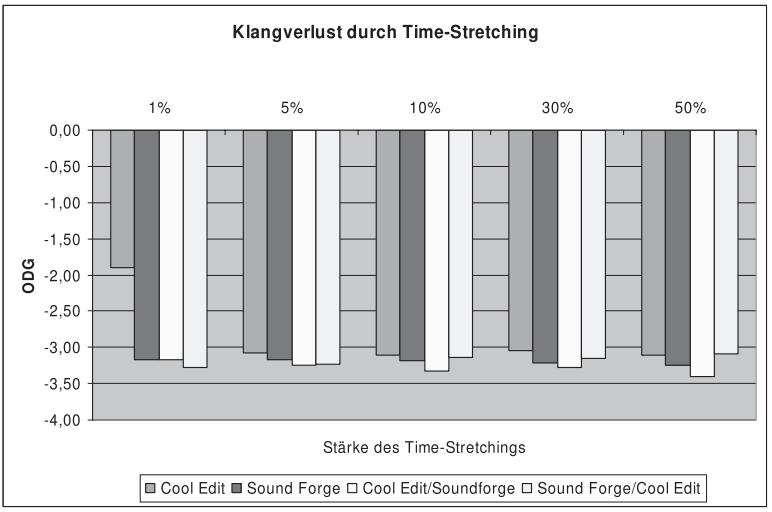

Abbildung 8: Auch Time-Stretching reduziert die Qualität wahrnehmbar. Nur CoolEdit liefert bei einem Angriff mit 1% eine akzeptable Qualität.

Zusammenfassend kann gesagt werden, dass das getestete digitale Wasserzeichen durchaus robust gegen Pitch-Shifting und Time-Stretching ist, aber im angegriffenen Zustand nicht detektiert werden kann. Werden aber Strategien zum Rückgängigmachen der Angriffe eingesetzt, kann das Wasserzeichen auch wieder ausgelesen werden.

Im folgenden Abschnitt diskutieren wir, welche Strategien hier denkbar sind und mit welchem Aufwand diese verbunden sein werden.

5. Strategien zur Detektion

In den vorhergehenden Abschnitten wird deutlich, dass Wasserzeichen auch nach Pitch-Shifting und Time-Stretching wieder ausgelesen werden können, wenn die Auswirkungen dieser Angriffe wieder rückgängig gemacht werden können. Dazu sind drei Methoden denkbar:

1. **Nicht-Blinde Wasserzeichen**: Hier können Abspieldauer oder Tonhöhe der angegriffenen Datei mit dem Original verglichen werden. Danach kann mittels eines geeigneten Werkzeugs die Veränderung rückgängig gemacht und das Wasserzeichen ausgelesen werden. Dieser Prozess kann automatisiert werden. Eine Herausforderung sind allerdings das Aufbewahren und das Identifizieren des Originals. Außerdem können weitere Angriffe, wie beispielsweise die Ausschnittsbildung die Strategie stark stören. In einzelnen Fällen ist es trotzdem denkbar, entsprechend vorzugehen. Bei einer Raubkopie eines Films beispielsweise sind der Aufwand für das Identifizieren des Originals und auch der Position im Vergleich mit dem entstandenen Schaden akzeptabel.

2. **Schrittweise Rückgängigmachen des Angriffs**: Erste von uns durchgeführte Versuche haben gezeigt, dass das Wasserzeichen aus nur leicht angegriffenen Kopien wieder ausgelesen werden kann. Diese können sich beispielsweise um bis zu fünf Prozent eines Halbtonschrittes vom Original unterscheiden. Denkbar ist folglich, eine Datei in kleinen Schritten durch Pitch-Shifting und Time-Strechting zu modifizieren und immer wieder zu versuchen, das Wasserzeichen auszulesen. Das kann in einem vorher definierten Bereich geschehen, der beispielsweise +/- sechs Halbtonschritte und +/-50 % Abspieldauer umfasst. Dieser Prozess ist zwar zeitaufwändig, kann aber ohne das Original durchgeführt werden und wird durch weitere Angriffe auf das markierte Material nicht gestört. Diese Strategie lässt sich einfach umsetzen und benötigt keinen weiteren Entwicklungsaufwand neben der Steuerung der Pitch-Shifting und Time-Stretching Werkzeuge. Für Schadensfälle von hohem Wert ist der hohe Rechenaufwand akzeptabel.

3. **Scanner**: Unter Kenntnis der Einbettungsstrategie des Wasserzeichens und der Auswirkungen der Angriffe kann ein Verfahren entworfen werden, welches gezielt versucht, das Wasserzeichen in den resultierten Frequenzbändern und Positionen zu suchen. Es wird letztendlich die ursprünglich verwendete Frequenz- und Zeitzuordnung des Wasserzeichens während dem Auslesen modifiziert, um die Auswirkungen der Angriffe rückgängig zu machen, ohne die Angriffswerkzeuge erneut einzusetzen. Auch hier muss wie in (2) ein schrittweises Durchsuchen der Inhalte in gewissen Grenzen erfolgen. Allerdings ist der Aufwand deutlich geringer, da nur innerhalb des Wasserzeichenalgorithmus eine Zuordnung von Positionen stattfindet. Die zeitaufwändigen Algorithmen für Pitch-Shifting und Time-Stretching müssen nicht erneut durchgeführt werden.

6. Zusammenfassung

Wir haben in einem umfangreichen Test gezeigt, dass digitale Wasserzeichen durch Time-Stretching und Pitch-Shifting Angriffe nicht zerstört werden, sondern nach gezielter Nachbearbeitung mit einer hohen Erfolgschance wieder ausgelesen werden können. Dementsprechend sind in der Zukunft Mechanismen zu entwickeln, die effizient nach durch die Angriffe nicht auslesbaren Wasserzeichen suchen. Dazu stellen wir drei Vorgehensweisen vor, welche sich hinsichtlich Entwicklungsaufwand und Rechenaufwand unterscheiden.

Danksagung

Die Arbeiten und Ergebnisse, die in dieser Veröffentlichung beschrieben sind, werden teilweise von der Europäischen Kommission innerhalb des IST Programms, Vertrag IST-2002-507932 *ECRYPT*, unterstützt.

Teile der Forschungsergebnisse wurden gemeinsam mit den Studenten Bussmann, El-Seoud und Sailer der TU Darmstadt und der FH Darmstadt erarbeitet.

Literaturverzeichnis

[CMB02] I. Cox, M. Miller, J. Bloom, “Digital Watermarking”, 2002 Academic Press, San Diego, USA, ISBN 1-55860-714-5, 20002

[Di00] Dittmann, Jana, „Digitale Wasserzeichen“, Springer Verlag, ISBN 3-540-66661-3, 2000

[SF05] Steinebach, Lucilla Croce-Ferri: „Einsatzgebiete nicht-blinder Wasserzeichen", D-A-CH-Security 2005, Verlag Patrick Horster (Hrsg.), ISBN 3-0001-5548-1, 2005

[SPR+01] Steinebach, Petitcolas, Raynal, Dittmann, Fontaine, Seibel, Fates, Croce-Ferri; “StirMark Benchmark: Audio watermarking attacks”. In: Int. Conference on Information Technology: Coding and Computing (ITCC 2001), April 2 - 4, Las Vegas, Nevada, S. 49 - 54, ISBN 0-7695-1062-0, 2001

[St03] Steinebach, „Digitale Wasserzeichen für Audiodaten“, Dissertationsschrift, Shaker Verlag Aachen, ISBN 3-8322-2507-2, 2003

[VLB04] Van der Veen, Lemma, Beauge, “Informed detection of audio watermark for resolving playback speed modification”, ACM Multimedia and Security Workshop, 20.-21. September 2004, Magdeburg, Proceedings of the Multimedia and Security Workshop 2004