4. Digitale Wasserzeichen zum Integritätsschutz von Multimediadaten (Thiemert, S., Smudzinski, S., Ferri, L.C., Steinebach, M.)

Dank der Entwicklung neuer digitaler Technologien und der weiten Verbreitung des Internets kann man heutzutage auf Informationen und Daten sehr einfach zugreifen, diese verändern, kopieren und wieder veröffentlichen. Daraus ergeben sich neue Aspekte im Umgang mit Multimediadaten. Neben dem Zugriff auf eine Vielfalt von Informationen besteht die Möglichkeit der Nutzung von Diensten, die Informationen und Daten in hoher Qualität anbieten. Dies führt jedoch in verschiedenen Fällen zum verstärkten Missbrauch bei der Verwendung digitaler Informationen.
Auf dem Gebiet der Sicherheit von Multimediadaten beschäftigt man sich heute nicht nur mit dem Schutz urheberrechtlich geschützter Daten, sondern geht auch auf den Bedarf nach Technologien zur Authentifizierung des Datenmaterials ein. Lösungen werden hier insbesondere von Produzenten und Anbietern multimedialer Inhalte gewünscht. Besonders die Integrität von Daten muss hier betrachtet werden, wenn es um Material mit einem hohen Bedarf an Sicherheit geht: Nur wenn der Benutzer eines digitalen Dokuments die Möglichkeit hat, unerlaubte Veränderungen zu erkennen, wird er es auch als vertrauenswürdig einstufen (z.B. als Beweismittel vor Gericht).

Bestehende Lösungen zur Integritätsüberprüfung von Daten basieren auf der Kryptographie. Der Schutz digitaler Medien mit Hilfe kryptografischer Techniken bedeutet in der Regel, dass die Integrität eines Dokuments nur dann gegeben ist, wenn eine exakte Übereinstimmung auf Bitebene vorliegt. Die Authentifizierungsnachricht, die Informationen über die Integrität enthält, wird im Allgemeinen von den zu authentifizierenden Daten getrennt oder in deren Headern gespeichert. Dies bedeutet jedoch eine Zunahme der Datenmenge und der Gefahr, dass die Authentifizierungsnachricht verloren geht. Darüber hinaus gestaltet sich die Lokalisierung der manipulierten Stellen (z.B. manipulierter Details in digitalen Bildern) mit kryptografischen Ansätzen als sehr schwierig. Da digitale Medien durch Formatumwandlung, Unterabtastung und andere Operationen, die im Post-Production-Prozess üblich sind, ständig verändert werden, kann eine Prüfung der Integrität nicht mehr auf einem bitgenauen Vergleich beruhen.

Integritätswasserzeichen stellen hier eine Alternative zur Kryptographie dar. Dabei wird die Authentifizierungsnachricht untrennbar in den zu schützenden Inhalt eingebettet. Existierende Wasserzeichen-verfahren können in drei Klassen unterteilt werden:

- *Fragile Wasserzeichen* reagieren auf jegliche Veränderung. Verändert sich ein Bit innerhalb eines Pixelwertes, so wird bereits das gesamte Wasserzeichen zerstört.
- *Semi-fragile Wasserzeichen* sind teilweise robust gegen Post-Production-Operationen. Die Schwierigkeit bei diesem Ansatz besteht in der eingeschränkten Möglichkeit zwischen erlaubten und nicht erlaubten Veränderungen zu unterscheiden.
- *Inhalts-fragile Wasserzeichen* sind demgegenüber nur empfindlich gegenüber Veränderungen am Inhalt und ermöglichen so eine Authentifizierung von Audio- und Bilddaten.

Eine Vielzahl der existierenden Wasserzeichenverfahren befasst sich mit dem Problem der Robustheit gegenüber Kompression. Geometrische Transformationen und

Schnitte, resultierend aus der Bildbearbeitung, werden jedoch als Integritätsverletzung erkannt, obwohl diese Operationen den Inhalt des Bildes nicht verändern. Die Aufgabe bei der Entwicklung ist in diesem Fall die Unterscheidung zwischen inhaltserhaltenden und inhalts-verändernden Operationen zu ermöglichen. Dies erfordert anspruchsvollere Ansätze.

Wir diskutieren in der vollständigen Version dieser Arbeit zunächst die drei Klassen von Integritäts-Wasserzeichen, analysieren anschließend die wichtigsten Anforderungen an ein effizientes inhalts-fragiles Wasserzeichen und die dazugehörige Auswahl von inhaltsbeschreibenden Merkmalen. Hierbei setzen wir unseren Schwerpunkt auf die Medientypen Audio, Bild und Video. Ziel dieses Artikels ist es Kriterien herauszuarbeiten, die für alle drei Medientypen gleichermaßen wichtig sind. Darüber hinaus stellen wir spezielle Ansätze für den Integritätsschutz von Mediendaten vor, welche den speziellen Charakteristiken der einzelnen Medientypen angepasst sind.