B. Technische Grundlagen und Anbieter von Content-Identification-Technologien

Content-Identification-Technologien basieren darauf, digitale Multimediawerke anhand von Merkmalen zu identifizieren, die Rückschlüsse auf deren sinnlich wahrnehmbaren Inhalt ermöglichen. Die hierzu eingesetzten sogenannten „perceptual hash functions" wurden auf der Grundlage von Technologien aus dem Bereich der Kryptographie entwickelt.

I. Cryptographic Hash Functions

„Digital Fingerprinting" ist eine andere Bezeichnung für die „cryptographic hash function", die aus dem Bereich der Kryptographie stammt. Diese wird beispielsweise zusammen mit *public-key*-Algorithmen zur Verschlüsselung von Daten und digitalen Signaturen sowie im Bereich der Integritäts- und Authentizitätskontrolle eingesetzt.[601] Die Funktion steht für einen Transformationsvorgang in Bezug auf einen Eingabewert (beispielsweise eine digitale Nachricht oder ein digitales Dokument), nach dessen Durchführung der Eingabewert in Form eines „fixed-size bit string" wiedergegeben wird, der auch als „hash value" oder „digitaler Fingerabdruck" bezeichnet wird.[602] Die beiden am weitesten verbreiteten *cryptographic hash functions* sind die von Ron Rivest 1992 erfundene sogenannte „MD5"[603]-Funktion, sowie die „SHA-1"[604]-Funktion, die 1993 von der US-amerikanischen National Security Agency veröffentlicht wurde.[605]

601 Vgl. 4. Kapitel, Teil B.II.1; *Schneier*, Cryptanalysis of MD5 and SHA: Time for a New Standard, Computerworld, 19.08.2004, http://schneier.com/essay-074.html (zuletzt abgerufen am 01.07.2010).

602 Vgl. *Wikipedia*, Stichwort „cryptographic hash function", Version vom 29.04.2010, 21:37 h, http://en.*Wikipedia*.org/w/index.php?title=Cryptographic_hash_function&oldid=359138309 (zuletzt abgerufen am 01.07.2010).

603 Akronym für „Message Digest 5".

604 Akronym für „Secure Hash Algorithm 1".

605 Im Jahr 2004 wurden bei beiden Funktionen Sicherheitslücken entdeckt, woraufhin das US-amerikanische National Institute of Science and Technology im Jahr 2007 das „cryptographic hash project" ausrief mit dem Ziel, anhand eines Wettbewerbs zwischen innovativen Hash-Algorithmen die Grundlage für eine neue, sicherere sogenannte „New Cryptographic Hash Algorithm (SHA-3) Family" zu schaffen; vgl. die Ankündigung des Projekts auf der Webseite der NIST, abrufbar unter http://csrc.nist.gov/groups/ST/hash/ (zuletzt abgerufen am 01.07.2010).

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Cryptographic hash functions sind grundsätzlich hochsensibel für geringste Abweichungen der digitalen Zusammensetzung des jeweiligen Eingabewerts. Dies bedeutet, dass sich ein völlig anderer *hash value* ergibt, wenn am ursprünglichen Eingabewert auch nur ein einziges Bit abgeändert wird. Dies bedeutet jedoch auch, dass die Identifizierung eines Eingabewerts durch eine *cryptographic hash function* bereits dann fehlschlägt, wenn nur eine geringfügige Veränderung an der betroffenen Datei vorgenommen wurde, die so minimal sein kann, dass sie sich nicht in einer Veränderung des sinnlich wahrnehmbaren Inhalts der Datei niederschlägt.[606] Daher sind herkömmliche *crpytographic hash functions* für die Identifikation von digitalen Multimediawerken ungeeignet. Denn insoweit spielt gerade nicht das Format, die Kompression oder die Bitanzahl einer Datei, die ein digitales Multimediawerk enthält, die entscheidende Rolle, sondern vielmehr deren sinnlich wahrnehmbarer Inhalt.

Daher basieren die im Multimediabereich eingesetzten Content-Identification-Technologien auf „perceptual hash functions“[607] und damit auf einem digitalen Fingerabdruck, der eigens auf Medieninhalte abgestimmt ist. *Perceptual hash functions* folgen ebenso wie *crpytographic hash functions* dem Prinzip, dass unterschiedliche Eingabewerte (hier: unterschiedliche digitale Multimediawerke) unterschiedliche *hash values* generieren müssen. Jedoch sind für die Verschiedenheit der zu errechnenden Werte nicht rein technisch-formale Unterschiede wie Bitanzahl oder Dateiformat maßgeblich, sondern allein die Unterschiede im sinnlich wahrnehmbaren Inhalt der in den Dateien verkörperten Multimediawerke. Eine *perceptual hash function* stützt sich im Rahmen des durchgeführten Transformationsvorgangs zur Errechnung des *hash value* daher auf Merkmale wie Akustik, Farben und Bewegungen. Die spezielle Funktionsweise und Stärke von Content-Identification-Technologien besteht somit im Ergebnis darin, dass sie digitale Multimediawerke anhand ihrer sinnlich wahrnehmbaren, charakteristischen Ton- und Bildsignale identifizieren können.[608] Hierdurch sind Content-Identification-Technologien in der Lage, ein Multimediawerk auch dann wiederzuerkennen, wenn die das Werk enthaltende Datei verändert, komprimiert, konvertiert, neu aufgenommen oder an ihr anderweitige Manipulationen vorgenommen wurden. Denn solche

606 *Evans*, Perceptual Image Hashing: Methods, Image Hashing Research, University of Texas in Austin, http://users.ece.utexas.edu/~bevans/projects/hashing/methods.html (zuletzt abgerufen am 01.07.2010).

607 Vgl. die Beschreibung des “Perceptual Hashing”-Projekts der Polytechnic University, Information Systems and Internet Security Lab, http://isis.poly.edu/projects/percephash (zuletzt abgerufen am 01.07.2010).

608 *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93; vgl. auch die Ausführungen zu der als „Fuzzy Hashing“ betitelten Technologie bei *Haber/Horne/Pato/Sander/Tarjan*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 224, 229.

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Modifikationen lassen regelmäßig den charakteristischen, sinnlich wahrnehmbaren Inhalt des Multimediawerks unangetastet.[609] Anders ausgedrückt ist eine funktionierende Content-Identification-Technologie dazu in der Lage, ein multimediales Werk auch trotz etwaiger Manipulationen solange wiederzuerkennen, wie auch ein menschlicher Rezipient, der das digitale Multimediawerk ansieht oder anhört, in der Lage wäre, darin das originäre Werk wiederzuerkennen.[610] Anders als beispielsweise beim Einsatz von Wasserzeichentechnologien werden im Zusammenhang mit Content-Identification-Technologien dem jeweiligen digitalen Werk somit auch keine Informationen zum Zwecke der Identifikation hinzugefügt, sondern die Identität des jeweiligen multimedialen Inhalts unmittelbar aufgrund einer Analyse von dessen besonderen Eigenschaften, wie sie in den entsprechenden Ton- oder Bildsignalen zum Ausdruck kommen, ermittelt.[611]

609 *Bechtold*, DRM, 2002, S. 92. Ein Nutzer möchte über einen Web 2.0.-Dienst in der Regel anderen Nutzern den Konsum eines bekannten, urheberrechtlich geschützten Werks ermöglichen; dieses Ziel wird jedoch nicht erreicht, wenn die digitale Version dieses Werks so stark modifiziert wird, dass die anderen Nutzer das ursprünliche Werk nicht mehr wiedererkennen können. Daher müssen solche Modifikationen den wahrnehmbaren "Kern" des Multimediawerks weitgehend unangetastet lassen; es ist jedoch gerade dieser Kern, auf den sich Content-Identification-Technologien bei der Identifikation von digitalen Inhalten konzentrieren.

610 Solange somit ein menschlicher Hörer in der Lage wäre, eine Tonaufnahme wiederzuerkennen, obwohl an den Tonhöhen oder der Geschwindigkeit der Tonfolge dieser digitalen Tonaufnahme manipuliert wurde, kann auch eine Content-Identification-Technologie den Titel identifizieren.

611 Sogenannter „non-invasive approach". Der Prozess der Datenanalyse durchläuft zwei Stadien, die sogenannte „training"- und die „recognition"-Phase. In der *training phase* werden die charakteristische Besonderheiten, die das zu analysierende Multimediawerk in Bezug auf bestimmte Ton- oder Bildmerkmale – wie beispielsweise Tonspektrum und zeitliche Abfolge der einzelnen Töne bei einer Tonaufnahme bzw. Farbe, Form und Bewegung innerhalb der einzelnen Bilder bei einem Filmwerk – aufweist, durch eine Software extrahiert und auf diese Weise eine einzigartige Kombination an Referenzdaten geschaffen, anhand derer das Multimediawerk von allen anderen unterschieden werden kann. Dabei werden nur diejenigen Merkmale berücksichtigt, die von menschlichen Rezipienten sinnlich wahrgenommen werden, um auf diese Weise das Datenvolumen des Fingerabdrucks des Multimediawerks möglichst gering zu halten. Dieser Fingerabdruck, dessen Datenvolumen im Vergleich mit demjenigen der analysierten Datei, beispielsweise einer Tonaufnahme im MP3-Format, extrem komprimiert ist, wird sodann zusammen mit einigen den Inhalt beschreibenden Metadaten (beispielsweise Werktitel, Name des Rechtsinhabers) in einer Datenbank abgespeichert. Im zweiten Verfahrensabschnitt, während der *recognition phase*, wird die auf Identität mit einem Multimediawerk, dessen Fingerabdruck in der Datenbank gespeichert wurde, zu überprüfende Datei durch die Content-Identification-Technologie auf gleiche Weise analysiert wie im Rahmen der *training phase*, d.h. ein Fingerabdruck erstellt, der mit dem in der Datenbank abgespeicherten Fingerabdrücken abgeglichen wird. Ergibt dieser Abgleich einen hohen Grad an Übereinstimmung mit einem dieser Fingerabdrücke, meldet die Technologie diese Übereinstimmung unter Angabe des Grads der Übereinstimmung mit dem möglicherweise betroffenen Multimediawerk. Vgl. hierzu *Bechtold*, DRM, 2002, S. 92; *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93, 94.

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

III. Qualitätsmerkmale und Treffsicherheit von Content-Identification-Technologien

Die Qualität einer Content-Identification-Technologie bemisst sich daran, ob sie in Bezug auf ihre Treffsicherheit bestimmte Anforderungen erfüllt. Sie muss zum einen robust sein, was bedeutet, dass die Technologie den Inhalt einer Datei auch dann identifizieren können muss, wenn an der Datei bestimmte Manipulationshandlungen vorgenommen wurden, wie beispielsweise eine Veränderung der Formatierung der Datei oder Änderung des in der Datei enthaltenen Inhalts selbst, beispielsweise der Tonhöhe oder der Geschwindigkeit der Ton- oder Bildfolge etc.[612] Auch muss eine Identifikation möglich sein, wenn nur Bruchstücke des Multimediawerks vorliegen. Weiterhin müssen *false positives* ausgeschlossen sein, d.h. es dürfen keine Übereinstimmungen angezeigt werden, obwohl der zu prüfende Inhalt mit keinem der in der Datenbank hinterlegten Fingerabdrücke von urheberrechtlich geschützten Multimediawerken übereinstimmt.

Ein weiteres Erfordernis ist die „signature compactness", d.h. ein möglichst geringes Datenvolumen des extrahierten Fingerabdrucks, da eine Content-Identification-Technologie regelmäßig große Mengen unterschiedlicher Multimediawerke zu erkennen in der Lage sein muss, wofür Voraussetzung ist, dass Fingerabdrücke all dieser Multimediawerke in der zugehörigen Datenbank hinterlegt werden. Dennoch muss das Datenvolumen der Datenbank technologisch beherrschbar bleiben. Dabei steht diese Notwendigkeit der Minimierung der Daten des Fingerabdrucks im Spannungsfeld mit der Anforderung, die Inhalte möglichst sicher zu identifizieren, was wiederum die Unterschreitung einer gewissen Mindestmenge an Referenzdaten in Bezug auf den gespeicherten Fingerabdruck verbietet.[613] Weiterhin ist eine gewisse Schnelligkeit in Bezug auf die Analyse der zu prüfenden Inhalte und den Vergleich mit den in der Datenbank eingespeisten Fingerabdrücken notwendige Voraussetzung für die Effizienz und damit für die praktischen Einsetzbarkeit der Content-Identification-Technologie.[614]

Generell ist die Treffsicherheit von Content-Identification-Technologien umstritten. Nach der Information Technology & Innovation Foundation sind Content-Identification-Technologien „mature, highly accurate and widely available".[615]

612 *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93, 95. Manipulationen wie die Rotation des Bildwinkels, Verfälschungen von Einzelbildern oder die Abänderung des Farbabgleichs machen Content-Identification-Technologien vor allem im Zusammenhang mit der Identifikationen von Film- und Videowerken für Fehler anfällig, vgl. *Germain*, Dusting for Copyright Clues With Digital Fingerprinting Tech, TechNewsWorld, 22.08.2008, http://www.technewsworld.com/story/64249/.html.?wlc=1247835959 (zuletzt abgerufen am 01.07.2010).

613 *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93, 95, 96.

614 *Herre* s.o.

615 *Castro/Bennett/Andes*, Steal these Policies, ITIF, 2009, S. III.

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Auch nach Angaben des Internetdienstes iMesh liegt die Trefferquote der von diesem Dienst eingesetzten Content-Identification-Technologie des Anbieters Audible Magic bei 99 Prozent und sind insbesondere keine Probleme mit *false positives* bekannt.[616] Ebenso beansprucht YouTube für seine proprietär entwickelte Content-ID-Technologie[617] eine hohe Treffsicherheit. Allerdings wird gerade die Trefferquote dieser Content-Identification-Technologie oftmals in Zweifel gezogen.[618]

IV. Anbieter

Da die Verfahren für die Identifikation von Tonaufnahmen einerseits und von Filmwerken andererseits stark voneinander abweichen, ist in Bezug auf die Anbieter von Content-Identification-Technologien zu unterschieden, ob es sich um eine Technologie zur Erkennung von Audio- oder Videoinhalten handelt. Zwar ist es grundsätzlich möglich, ein Filmwerk auch auf der Grundlage einer reinen Audio-Filtertechnologie identifizieren zu lassen, allerdings sind die Anhaltspunkte zur Identifikation dann zwangsläufig auf die darin enthaltenen Audioelemente begrenzt. Naheliegend ist eine in dieser Weise beschränkte Identifikation für Musikvideos, da es den Rechtsinhabern hier grundsätzlich nur um die Durchsetzung ihrer Rechte in Bezug auf die darin verwendete Tonaufnahme geht, da solche Videos vornehmlich der Vermarktung der der Tonaufnahme dienen.[619] Für die Identifikation „reiner" Filmwerke wurden jedoch mittlerweile spezielle Technologien entwickelt.

Im Audiobereich gehört das Unternehmen Audible Magic Corp. („Audible Magic") zu den wichtigsten Anbietern. So bekannte Unternehmen wie die sozialen Netzwerke Facebook und MySpace, der Sender MTV sowie die Videoplattformen Veoh und YouTube gehören zu den Kunden, die innerhalb ihrer Dienste die Tech-

616 *Ohne Autor*, The End of Free Trade? How YouTube and MySpace will stop users from sharing copyrighted content, Newsweek Web Exclusive, 20.10.2006, http://www.newsweek.com/id/45365 (zuletzt abgerufen am 01.07.2010).

617 Vgl. 7. Kapitel, Teil B.I.4.c.

618 Vgl. beispielsweise *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 3.

619 Daher finden sich auf YouTube beispielsweise oftmals „stumme" Musikvideoclips, da die Rechtsinhaber nur den Audioteil ausfiltern lassen. Durch diese Vorgehensweise bezwecken die Rechtsinhaber, das technisch mögliche isolierte Ausschneiden des Audioteils aus einem gestreamten Videoclip zu verhindern. Der stumme Videoclip wird jedoch auf dem Internetdienst belassen, um dessen Marketingeffekt auszunutzen, d.h. Musikfans durch den Videoclip auf das Musikstück neugierig zu machen und dazu zu animieren, dass zugehörige Musikstück auf legalem Wege zu erwerben.

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

nologie dieses Anbieters einsetzen,[620] deren Ergebnisse angeblich zu 98 Prozent zutreffend sind.[621] Die von Audible Magic im Zusammenhang mit seiner Technologie geschaffene Datenbank enthält mittlerweile Informationen über mehr als sechs Millionen verschiedene Tonaufnahmen, Filmwerke und Softwareprogramme und wird auf der Grundlage neuer Informationen, die Audible Magic von den Rechtsinhabern zur Verfügung gestellt werden, ständig erweitert und aktualisiert.[622] Im Anschluss an die Identifizierung stellt die Content-Identification-Technologie von Audible Magic den Rechtsinhabern verschiedene Optionen zur Verfügung, wie mit einem Multimediawerk nach dessen Identifikation weiter zu verfahren ist (beispielsweise Nachverfolgung der Nutzung, Zuschaltung von Werbung, Hinzufügung von Erwerbsoptionen).

Für den Filmbereich galt die Entwicklung von Content-Identification-Technologien noch bis vor kurzem als höchst problematisch. Denn aufgrund der Komplexität von Filmdateien und der damit einhergehenden Bandbreite an Manipulationsmöglichkeiten bereitet die Erstellung von digitalen Fingerabdrücken von Filmwerken größere Schwierigkeiten als bei Tonaufnahmen.[623] Zudem werden weit mehr filmische Inhalte ständig neu veröffentlicht als Tonaufnahmen, weswegen es angesichts der ständig wachsende Menge an neuen Inhalten eine große Herausforderung darstellt, die zur effektiven Filterung erforderlichen Datenbanken zu aktualisieren.[624] Im Jahr 2007 zeichnete sich jedoch ab, dass auch die Rechtsinhaber im Filmbereich zunehmend auf Content-Identification-Technologien beim Schutz von Urheberrechten im Internet setzen, als Motion Picture Laboratories, Inc. („MovieLabs") ein Projekt initiierte, in dessen Rahmen die Effizienz der zu dieser Zeit verfügbaren Content-Identification-Technologien getestet wurde.[625] Dabei wurde in einer ersten Versuchsreihe die Treffsicherheit der Technologien der teilnehmenden Anbieter bei der Identifikation von 1000 Videoclips unterschiedlichster Formate und Qualität geprüft. Unter den teilnehmenden Technologieanbietern

620 Vgl. die Auflistung der „Content Identification Services Customers" des Unternehmens, http://audiblemagic.com/clients-partners/contentsvcs.asp (zuletzt abgerufen am 01.07.2010). Für eine ausführliche Beschreibung der Funktionsweise der von Audible Magic angebotenen Technologie vgl. *Wilkinson*, Musical Fingerprints, Electronic Musician, 01.09.2003, http://www.emusician.com/mag/tech/emusic_musical_fingerprints/index.html (zuletzt abgerufen am 01.07.2010).

621 *Wilkinson* s.o.

622 Vgl. die Beschreibung der „Content Identification Services" des Unternehmens, http://audiblemagic.com/products%2Dservices/contentsvcs (zuletzt abgerufen am 01.07.2010).

623 *Rosenblatt*, 2006 Year in Review: DRM Technologies, DRM Watch, 21.12.2006, http://www.drmwatch.com/drmtech/article.php/3650401 (zuletzt abgerufen am 01.07.2010).

624 *Rosenblatt* s.o.

625 *Rosenblatt*, MovieLabs Shows Results of Fingerprint Testing, DRM Watch, 27.09.2007, http://www.drmwatch.com/watermarking/article.php/3702101 (zuletzt abgerufen am 01.07.2010).

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

schnitt das Unternehmen Vobile[626] am besten ab, gefolgt von den Technologien etablierter Anbieter wie Audible Magic und Gracenote. Nach dieser ersten Testreihe erklärte sich Harry Weinstein, der Präsident von MovieLabs, dass er Digital-Fingerprinting Technologien für den Schutz urheberrechtlich geschützter Filmwerke einsatzbereit halte.[627]

Das Unternehmen Auditude bietet eine Video-Fingerprinting-Technologie an, mit deren Hilfe Rechtsinhaber digitale Kopien von Filmwerken im Internet aufspüren[628] und die identifizierten Filmdateien mit Werbebotschaften und weiterführenden Informationen versehen können.[629] Im Rahmen einer Kooperation zwischen Auditude, dem Sozialen Netzwerk MySpace und dem Unternehmen MTV Networks wird diese Technologie dazu eingesetzt, die auf MySpace eingestellten Inhalte auf urheberrechtlich geschützte Inhalte von MTV Networks zu durchsuchen.[630] Zu diesem Zweck werden die von den Nutzern auf den Web 2.0-Dienst hochgeladenen Videoclips mit einer von Auditude erstellten Datenbank abgeglichen, die Informationen über ca. 250 Millionen Filmwerke enthält.[631] Ergibt dieser Abgleich eine Übereinstimmung, wird die betroffene Filmdatei mit einem Hinweis auf die Originalquelle, einem Verweis auf eine Kaufmöglichkeit und/oder einer Werbebotschaft versehen.[632] Die daraus gewonnen Einnahmen teilen sich MTV und MySpace.[633]

Ein Beispiel für einen deutschen Anbieter einer Video-Fingerprinting-Technologie ist die iPharro Media GmbH mit Sitz in Darmstadt, ein im Jahr 2006 gegründeter Ableger des Fraunhofer Instituts für Graphische Datenverarbeitung.[634] iPharros bisher erfolgreichstes Produkt ist die „MediaSeeker"-Software, die es ihren

626 *Stone*, One Anti-Piracy System to Rule Them All, New York Times, Bits Weblog, 21.9.2007, http://bits.blogs.nytimes.com/2007/09/21/one-anti-piracy-system-to-rule-them-all/(zuletzt abgerufen am 01.07.2010).

627 *Stone* s.o.

628 *Sandoval*, Feature films coming to YouTube, CNET News, 06.11.2008, http://news.cnet.com/8301-1023_3-10083481-93.html?part=rss&tag=feed&subj=News-Digital-Media (zuletzt abgerufen am 01.07.2010).

629 *Rosenblatt*, Auditude's Fingerprinting Powers Contextual Ad Service on MySpace, DRM Watch, 06.11.2008, www.drmwatch.com/watermarking/article.php/3783336 (zuletzt abgerufen am 01.07.2010).

630 *Heise Online*, MySpace und MTV testen neues Vermarktungsmodell für Online-Videos, heise online, 03.11.2008, http://www.heise.de/newsticker/meldung/118328 (zuletzt abgerufen am 01.07.2010); *Chartier*, MySpace inks advertising deal with MTV networks, Ars Technica, 03.11.2008, http://arstechnica.com/news.ars/post/20081103-myspace-inks-advertising-deal-with-mtv-networks.html (zuletzt abgerufen am 01.07.2010).

631 *Heise Online*, MySpace und MTV testen neues Vermarktungsmodell für Online-Videos, heise online, 03.11.2008, http://www.heise.de/newsticker/meldung/118328 (zuletzt abgerufen am 01.07.2010).

632 *Heise Online* s.o.

633 *Heise Online* s.o.; *Rosenblatt*, Auditude's Fingerprinting Powers Contextual Ad Service on MySpace, DRM Watch, 06.11.2008, www.drmwatch.com/watermarking/article.php/3783336 (zuletzt abgerufen am 01.07.2010).

634 http://www.igd.fraunhofer.de.

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Nutzern erlaubt, mehrere Fernsehkanäle mithilfe einer Video-Fingerprinting-Technologie auf rechtlich geschützte Inhalte hin zu überwachen. Zu den Kunden des Unternehmens zählt unter anderem das Unternehmen Nielsen Media Research, die eine iPharro-Technologie zur weltweiten Überwachung und Nachverfolgung von Werbebotschaften im Rahmen der werbestatistischen Datensammlung einsetzt, sowie das Zweite Deutsche Fernsehen (ZDF). Im Juni 2009 kündigte iPharro ein neues Produkt an, den „iPharro Enterprise Server", mit dessen Hilfe es nach Angaben des Unternehmens möglich sein soll, die Funktionen der Video-Fingerprinting-Technologie zur Indexierung und Identifizierung von Filmwerken effizient und umfassend in den Betriebsablauf von medienabhängigen Unternehmens zu integrieren.[635]

V. Die „ContentID"-Technologie der Videoplattform YouTube

Im Oktober 2007 verkündete Google auf seiner Webseite[636] die Implementierung einer Technologie auf seiner Videoplattform YouTube, mit deren Hilfe Videoclips mit urheberrechtlich geschützten Inhalten identifiziert und daraufhin je nach Wunsch des jeweils betroffenen Rechtsinhabers entweder entfernt oder aber durch die Hinzufügung von Werbebotschaften kommerzialisiert werden können sollen.[637] Diese sogenannte „ContentID-Technologie"[638] besteht aus zwei Komponenten: einer Audio-Fingerprinting-Technologie des Anbieters Audible Magic,[639] sowie einer Video-Fingerprinting-Technologie, die von Googles Ingenieuren intern entwickelt wurde (nachfolgend „Video-ID" genannt). Anfang 2007 hatte YouTube mit dem Einsatz der Audio-Fingerprinting-Technologie von Audible Magic im Zusammenhang mit seiner Kooperation mit einigen Musikunternehmen

635 Vgl. die Ankündigung des Unternehmens anlässlich der DAM (Digital Asset Management) 2009, abrufbar unter http://www.ipharro.com/all_Images/PDFs/english/iPharro_DAM_ES_1_6_09.pdf (zuletzt abgerufen am 01.07.2010.).

636 *King*, Latest Content ID Tool for YouTube, The Official Google Weblog, 15.10.2010 http://googleblog.blogspot.com/2007/10/latest-content-id-tool-for-youtube.html (zuletzt abgerufen am 01.07.2010).

637 *Heise Online*, YouTube startet automatische Video-Identifizierung, 16.10.2007, http://www.heise.de/newsticker/meldung/97434 (zuletzt abgerufen am 01.07.2010); *Hendrickson*, YouTube Tries a Little Harder to Protect Copyright Holders, TechCrunch, 15.10.2007, http://www.techcrunch.com/2007/10/15/youtube-tries-a-little-harder-to-protect-copyright-holders (zuletzt abgerufen am 01.07.2010.).

638 Vgl. die Beschreibung der ContentID-Technologie auf YouTube, http://www.youtube.com/t/contentid (zuletzt abgerufen am 01.07.2010); vgl. auch die frühere Ankündigung der Beta-Version, YouTube-Videoidentifizierung - Beta-Version, http://www.youtube.com/t/video_id_about (zuletzt abgerufen am 01.07.2010).

639 Vgl. vorhergehendes Kapitel.

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

begonnen, darunter Warner Music, Sony und Universal.[640] Die Technologie überprüft, sobald ein Nutzer einen Videoclip auf die Plattform hochzuladen versucht, ob der Audio-Teil des Videoclips mit dem digitalen Fingerabdruck einer der in der Datenbank von Audible Magic gespeicherten Tonaufnahmen übereinstimmt.

YouTubes Entscheidung, zur Identifizierung urheberrechtlich geschützter Inhalte in Videoclips anders als bei der Identifizierung von reinen Audioelementen nicht auf einen externen Anbieter zurückzugreifen, sondern eine eigene Technologie zu entwickeln geht angeblich darauf zurück, dass ein Testlauf ergeben hätte, dass die in Betracht kommenden bereits existierenden Technologien YouTubes Anforderungen nicht entsprechen würde.[641] Die daraufhin intern entwickelte Video-ID-Technologie basiert auf der Prämisse, dass jedes Filmwerk bestimmte charakteristische, einzigartige Eigenschaften besitzt, die es ermöglichen, dieses Werk oder Teile davon mit Hilfe eines Algorithmus, der diese Eigenschaften verkörpert, auch in kurzen Videoclips wieder zu erkennen. Über die Details der Technologie hält sich YouTube jedoch sehr bedeckt. So beschränken sich die Pressemitteilungen insoweit auf die eher vage Aussage, dass „key visual aspects" verwendet würden, um die hochgeladenen Videoclips mit Referenzmaterial von urheberrechtlich geschützten Werken, welches die Rechtsinhaber YouTube zunächst zur Verfügung stellen müssen, wenn sie ihre Werke durch die Video-ID-Technologie schützen lassen wollen, abzugleichen.[642] Auf der Grundlage dieses Referenzmaterials erstellt YouTube einen digitalen Fingerabdruck, der in eine Datenbank eingespeist wird.[643] Findet die ContentID-Technologie geschütztes Material auf, so wird dieses je nach Wunsch des betroffenen Rechtsinhabers entweder von der Plattform gelöscht, seine Nutzung zur Erstellung statistischer Daten überwacht (Anzahl der Abrufe etc.) oder aber Werbung zugeschaltet, deren Erlös zwischen YouTube und dem Rechtsinhaber geteilt wird. Nach Angaben von YouTube entscheidet sich mittlerweile die überwiegende Mehrheit der Rechtsinhaber, ihre Inhalte auf der Webseite zu belassen, d.h. ihre Nutzung an YouTube zu lizenzieren und von den

640 *Delaney*, YouTube to Test Software To Ease Licensing Fights, The Wall Street Journal, 12.06.2007, http://online.wsj.com/article/SB118161295626932114.html (zuletzt abgerufen am 01.07.2010); *Li/Auchard*, YouTube to test video ID with Time Warner, Disney, Reuters, 12.06.2007, http://www.reuters.com/article/wtMostRead/idUSWEN871820070612 (zuletzt abgerufen am 01.07.2010).

641 *Delaney* s.o.

642 *Chen*, The state of our video ID tools, The Official Google Weblog, 14.06.2007, http://googleWeblog.Weblogspot.com/2007/06/state-of-our-video-id-tools.html (zuletzt abgerufen am 01.07.2010).

643 *Associated Press*, For YouTube, a System to Halt Copyright-Infringement Videos, The New York Times, 28.07.2007, http://www.nytimes.com/2007/07/28/business/28google.html (zuletzt abgerufen am 01.07.2010).

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

im Zusammenhang mit den Inhalten erzielten Werbeeinnahmen zu profitieren.[644] Weiterhin ist Google nach eigenen Angaben dabei, eine Technologie zu entwickeln, die es Rechtsinhabern ermöglicht, Werbebotschaften unmittelbar in die von Nutzern hochgeladenen Inhalte einzubetten.[645]

Umstritten ist, wie treffsicher die ContentID-Technologie tatsächlich ist; YouTube selbst äußert sich dazu nicht, ebensowenig wie zu der Höhe der Umsätze, die es durch die Zuschaltung von Werbung zu den Videoclips erzielt. So war beispielsweise ein Videoclip mit einem in den USA sehr populären Sketch der „Saturday Night Live"-Show betreffend die Gouverneurin Sarah Palin noch tagelang nach seiner Erstausstrahlung über den Fernsehsender NBC auf YouTube abrufbar, obwohl NBC Universal zu denjenigen Medienunternehmen gehört, die ihre geschützten Inhalte von der Videoplattform entfernen lassen, um interessierte Nutzer auf ihre eigenen Webseiten bzw. die in Gemeinschaft mit anderen Medienunternehmen betriebene, konkurrierende Videoplattform Hulu umzusteuern.[646] Es ist somit davon auszugehen, dass die Technologie derzeit jedenfalls noch nicht völlig fehlerfrei arbeitet.[647]

C. Einsatzmöglichkeiten für Content-Identification-Technologien im Web 2.0

Content-Identification-Technologien können entweder rein repressiv zur Beseitigung von Multimediawerken eingesetzt werden, die auf einem Web 2.0-Dienst unerlaubt der Öffentlichkeit zugänglich gemacht werden. Darüber hinaus ermöglichen sie jedoch auch die Kommerzialisierung von Multimediawerken in Web 2.0-Diensten im Zusammenhang mit sogenannten *ad-supported business models*.

644 *King*, Making money on YouTube with Content ID, The Official Google Weblog 27.08.2009, http://googleblog.blogspot.com/2008/08/making-money-on-youtube-with-content-id.html (zuletzt abgerufen am 01.07.2010).

645 *Sandoval*, Could peace be near for YouTube and Hollywood?, CNET News, 23.07.2008, http://news.cnet.com/8301-1023_3-9996905-93.html (zuletzt abgerufen am 01.07.2010).

646 *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 3.

647 *Steinert-Threlkeld*, s.o. Google selbst die Entwicklung der Technologie einmal als *„one of the most technologically complicated tasks that we have ever undertaken"* bezeichnet, vgl. The state of our video ID tools, The Official Google Weblog, 14.06.2007, abrufbar unter http://googleblog.blogspot.com/2007/06/state-of-our-video-id-tools.html (zuletzt abgerufen am 01.07.2010) .

https://doi.org/10.5771/9783845233727-145, am 02.10.2024, 10:32:05
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb