MULTIMEDIA AND SECURITY
ECRYPT – EUROPEAN NETWORK OF EXCELLENCE IN CRYPTOLOGY

Jana Dittmann

Die Abkürzung ECRYPT /1/ steht für „European Network of Excellence in Cryptology". Das Netzwerk ist ein Zusammenschluss von ca. 180 europäischen Forschern und Entwicklern, an dem auch Informatiker der Otto-von-Guericke-Universität Magdeburg beteiligt sind. Das Projekt, in dessen Mittelpunkt die Forschungen zur Sicherung von Multimediadaten (Digital Rights Management) stehen, wird von der Europäischen Union über einen Zeitraum von vier Jahren gefördert. Die Forscher wollen Methoden entwickeln, um Musik, Bilder oder Videos mit zusätzlichen Schutzmechanismen zu versehen, mit dem Ziel Manipulationen zu erkennen oder bspw. Raubkopien zu verhindern oder aufzuspüren.

Das Advanced Multimedia and Security Lab (AMSL) der Arbeitsgruppe Multimedia and Security an der Otto-von-Guericke-Universität leitet zusammen mit Stefan Katzenbeisser (TU München) seit Anfang 2004 das „Watermarking Virtual Lab" (WAVILA), einen Teilbereich des Netzwerkes ECRYPT. In diesem Verbund arbeiten verschiedene Arbeitsgruppen, zum Beispiel aus Italien, Spanien, Frankreich, Deutschland, Belgien, der Schweiz und den Niederlanden, zusammen. Der Fokus der gemeinsamen Arbeit liegt dabei im Bereich der digitalen Wasserzeichen. Ihre Eigenschaften und Einsatzgebiete werden analysiert und es werden theoretische Grundlagen für Sicherheitsmodelle und für die Definitionen digitaler Wasserzeichen erarbeitet. In diesem Beitrag sollen die Motivation und die neuen Herausforderungen von ECRYPT, sowie die Ziele des Netzwerkes vorgestellt werden. Des Weiteren werden Arbeiten aus dem Bereich Wasserzeichen Benchmarking sowie Algorithmenentwurf präsentiert, um einen Einblick in das Umfeld zu ermöglichen.

MOTIVATION UND HERAUSFORDERUNGEN

Kryptologie ist eine Wissenschaft die mathematische Methoden und Techniken erforscht, um Vertraulichkeit, Integrität und Authentizität von digitalen Daten sicherstellen zu können. Sie ist somit ein fundamentaler Baustein um Sicherheit, Verlässlichkeit und Datenschutz in der modernen Informationsgesellschaft zu erzielen. In diesem Kontext spielen auch digitale Wasserzeichen, die zusätzliche Informationen direkt in das Datenmaterial einbetten, eine wesentliche Rolle und werden oftmals mit kryptologischen Mechanismen kombiniert. Zielsetzung ist hier, dass die eingebettete Information unsichtbar, schwer fälschbar und zur Sicherung der Authentizität robuste bzw. zur Sicherung der Integrität fragile Eigenschaften aufweist.

Kryptologie und **digitale Wasserzeichen** können somit als Herzstücke heutiger Konzepte der Computer-, Netzwerk- und Datensicherheit verstanden werden. Die grundlegenden Methoden werden zum Beispiel zur Identifizierung von Daten und Benutzern, für digitale Signaturen, im Digital Rights Management (DRM), für inhaltsbasiertes Suchen oder zum Fälschungsnachweis eingesetzt und bedienen eine Vielzahl von Anwendungen, welche von E-Business, M-Business, E-Voting und Online-Bezahlsystemen bis hin zu kabellosen Netzwerken und so genannten Ambient Intelligence Applikationen reichen. Wir finden heute Kryptologie in unseren GSM Mobiltelefonen, in Kreditkarten, im Pay-TV, in Datei- und Betriebssystemen, in unserer Browsersoftware, in WLAN-Verbindungen, und manche Europäer haben sie bereits in ihren Ausweisdokumenten.

Als eine besondere Technik hat sich in den letzten Jahren der so genannte inhaltsbasierte Hash – **Perceptual Hash** oder Content-based Hash, manchmal auch als passiver Fingerabdruck oder Perceptual Fingerprint bezeichnet, entwickelt, der als eine Kombination von Wasserzeichen und Kryptographie angesehen werden kann und der einer der Forschungsschwerpunkte der Arbeitsgruppe Multimedia and Security ist. Zielsetzung hier ist es, besonders wahrnehmungsrelevante Informationen eines Objektes abzusichern, zum Beispiel zu signieren, um die Objektauthentizität und -integrität zu garantieren. Während herkömmliche kryptographische Signaturen bei einer einzigen Veränderung das Objekt als verfälscht bzw. nicht authentisch ansehen, erlauben inhaltsbasierte Signaturen auch nach Medienoperationen wie Formatwechseln oder Formatbrüchen, die keine wahrnehmbaren Veränderungen des Originals zur Folge haben, eine korrekte Überprüfung der Signatur. Vorteile bieten sich darüber hinaus für inhaltsbasierte Schlüsselgeneratoren, um speziellen Angriffen in Wasserzeichensystemen zu begegnen, und für persistente Identifikatoren (zum Beispiel MPEG-21), um eine inhaltsbasierte Suche in Datenbeständen zu ermöglichen.

In Europa findet man eine Vielzahl von wissenschaftlichen Aktivitäten zu diesem Thema, genannt sei beispielsweise die International Asso-

ciation of Cryptologic Research (IACR, 1 200 Mitglieder), welche pro Jahr drei führende Konferenzen mit hoch qualitativen Beiträgen organisiert. Der europäische Erfolg auf den Gebieten zeigt sich auch bei der Entwicklung des AES (Rijndael, eine Entwicklung aus Belgien), im UMTS/3GPP, in der Smartcard Industrie und im NESSIE-IST-Projekt.

Auf dem Gebiet der Wasserzeichen spielt Europa ebenfalls eine große Rolle. Die Stärken liegen hier im Algorithmendesign und der Evaluation, wie Ergebnisse in anerkannten Konferenzen und Workshops zeigen. Ziel der Magdeburger Informatiker der Arbeitsgruppe Multimedia and Security und ihrer Partner an der Technischen Universität München, der Technischen Universität Dresden und der Universität Salzburg ist es, an der Stärkung des europäischen Knowhows in diesem Bereich mitzuwirken.

Im Bereich der Kryptographie fließen Techniken aus verschiedenen Gebieten der Mathematik und der Informatik sowie aus der Physik und der Elektrotechnik ein. Als Beispiele ließen sich hier die Algebra, Komplexitätsberechnungen, formale Modelle, Informationstheorie, Zahlentheorie, Kombinatorik, Statistik, Signalverarbeitung, Quantenphysik, Halbleitertheorie und viele weitere anführen. Außenstehenden, die nur eine begrenzte Vorstellung von der Komplexität dieser Gebiete haben, sollte der weit verbreitete Einsatz der Techniken einen Eindruck von deren Potenzial vermitteln. Kryptographische Algorithmen und Protokolle werden oftmals als „black box" bezeichnet, so dass man glauben könnte, dass sich die Forschung exklusiv auf das Bauen von sicheren und vertrauenswürdigen Infrastrukturen und mit der Integration von Sicherheitsmechanismen in Applikationen beschäftigen würde. Dieser (nicht korrekte) Eindruck wird verstärkt durch die (korrekte) Beobachtung, dass Sicherheitssysteme gewöhnlich durch kryptographische Schwächen gebrochen werden (wie eine inkorrekte Spezifikation oder Implementierung, schlechtem Management, Viren, Social Engineering Angriffen, …). Während Kryptologie eine im hohen Maße ausgereifte wissenschaftliche Disziplin ist, gibt es noch einen großen Bedarf an Forschung zum Thema ihrer Integration – auf der Grundlagen- als auch auf der Anwendungsebene.

Die Einsatzbedingungen, für die Kryptosysteme entwickelt wurden sind, ändern sich stetig und die Sicherheitsbedrohungen im Einsatz steigen. Dies fordert ein kontinuierliches Überwachen des aktuellen Standes der Technik zum Brechen von Kryptosystemen, um die Sicherheit existierender Systeme zuverlässig einschätzen zu können. Die Erhaltung der Sicherheit ist entscheidend, um unsere Informationsinfrastrukturen zu sichern. Auf der anderen Seite fordern zukunftsweisende Entwicklungen (wie Ambient Intelligence) neue, herausfordernde Anwendungen, welche mit anderen oder besseren kryptographischen Methoden bedient werden müssen. Die Kombination von Kryptographie und Wasserzeichen einschließlich des Perceptual Hashing eröffnen hier interessante und neue Fragen, um die Systemsicherheit zu erhöhen. Das grundlegende Problem, welches sich jedoch durch solche hybriden Ansätze eröffnet, ist die Herausforderung ein sicheres Protokoll zu finden, das eine Bit-präzise kryptographische Methode mit einer so genannten „fuzzy Signalverarbeitung" (also einer unscharfen und toleranten Signalverarbeitung) wie Wasserzeichen und/oder Perceptual Hashing zusammenarbeiten lässt.

Die wichtigsten Forschungsfragen in diesem Bereich, an denen die Arbeitsgruppe Multimedia and Security der Otto-von-Guericke-Universität Magdeburg zur Zeit arbeitet, können wie folgt aufgegliedert werden:

- Bedarf an Niedrig-Preis- und Strom-sparenden Lösungen;
- Bedarf an hoch effizienten Lösungen für Applikationen wie Busverschlüsselung oder Verschlüsselung von Hochgeschwindigkeitsnetzwerken, wo der zusätzliche Aufwand durch die Verschlüsselung so gering wie möglich gehalten werden muss;
- Bedarf an Hochsicherheitslösungen, insbesondere im Bereich kryptographischer Protokolle wie für das E-Voting, im Gesundheitswesen oder bei der nationalen Sicherheit, wenn eine Schutzgarantie von mehr als 50 Jahren zugesagt werden muss;
- Bedarf an sicheren digitalen Wasserzeichenverfahren, die auf einem formalen, theoretisch abgesichertem Fundament basieren und deren Integration auf sicheren Protokollen für DRM aufbaut;
- sowie Bedarf der Erforschung an geeignetem Zusammenwirken von Perceptual Hashing-Techniken und Informationssuche sowie Inhaltsidentifizierung als Alternative zu DRM.

ZIELSETZUNGEN

ECRYPT orientiert sich an den strategischen Zielen des IST (Information Society Technologies der EU) Work Programme *„Towards a global dependability and security framework"*. Kryptologie und Wasserzeichen stellen ein hochgradig interdisziplinäres Forschungsgebiet dar. Die wesentlichen Ziele des ECRYPT-Projektes sind deshalb:

- Erhalt und Stärkung von Kompetenzen der europäischen Forschung und der Industrieaktivitäten im Bereich Kryptologie und Wasserzeichen;
- Bündelung der Aktivitäten durch Etablierung einer Forschungsinfrastruktur und Aufbau von so genannten *Virtual Laboratories*, um die gemeinsamen Forschnugsaktivitäten zu strukturieren und gewinnbringend zusammenzuführen.

Erzielt werden soll eine verbesserte Aufbereitung des Standes der Technik in Theorie und Praxis, um:

- das Verständnis über die existierenden Algorithmen und Protokolle zu verbessern,
- die theoretischen Grundlagen zu erweitern,
- bessere Algorithmen, Protokolle und Implementierungen bezüglich niedrigerer Kosten, höherer Performanz und Sicherheit zu entwickeln,
- eine gemeinsame Infrastruktur zu schaffen, mit Werkzeugen zur Evaluation von Algorithmen und deren Benchmarking bezüglich verschiedener Anforderungen und Randbedingungen.

Darüber hinaus können folgende konkrete Zielsetzungen zusammengefasst werden:

- Verstärkt werden soll die Interaktion zwischen den einzelnen Forschungsgruppen in Kryptologie und Wasserzeichen, um deren Austausch untereinander, als auch mit der Industrie, den verschiedenen Regierungen sowie Standardisierungsgreminen, zu unterstützen, um das Wissen schneller weitergeben zu können und die Entwicklungen zügiger in praktische Anwendungen zu überführen.
- Jährlich sollen Empfehlungen über Algorithmen, Protokolle und Parameter gegeben werden.
- Die existierenden Tutorialreihen in Kryptologie und Wasserzeichen sollen koordiniert und erweitert werden (z. B. die der K. U. Leuven, Eindhoven-EIDMA, UCL, ...).
- Die interdisziplinäre Kollaboration zwischen den unterschiedlichen Forschungsdisziplinen soll stimuliert und intensiviert werden. Angestrebt ist, dass sich die Anzahl an Doktoranden und Postdoktoranden in Kryptologie und Wasserzeichen deutlich erhöht und deren Austausch untereinander gefördert wird. Des Weiteren sollen die angebotenen Kurse an den beteiligten Universitäten ausgebaut werden und von nationalen sowie internationalen Workshops und Summer Schools begleitet werden, um aktuelle Ergebnisse zu diskutieren.

ECRYPT-AKTIVITÄTEN

Die ECRYPT-Aktivitäten sind in fünf *Virtual Laboratories* (Virtual Labs) aufgegliedert:

1. *Symmetric techniques virtual lab (STVL)* für symmetrische Kryptosysteme,
2. *Asymmetric techniques virtual lab (AZTEC)* für asymmetrische Kryptosysteme,
3. *Protocols virtual lab (PROVILAB)* für Protokollaspekte,
4. *Secure and efficient implementations virtual lab (VAMPIRE)* für Aspekte der Implementierung in Software und Hardware,
5. *Watermarking and perceptual hashing virtual lab (WAVILA)* für digitale Wasserzeichen und Aspekte der inhaltsbasierten Signaturen.

Letzteres wird durch Prof. Dr. Jana Dittmann von der Otto-von-Guericke-Universität Magdeburg geleitet. Die detaillierten Zielsetzungen der einzelnen Virtual Labs können unter www.ecrypt.eu.org/ nachgelesen werden. Im Folgenden wird WAVILA genauer vorgestellt, da sich dort der größte Teil des Magdeburger Engagements in diesem Projekt wiederfindet.

WAVILA – Wasserzeichen und Aspekte von inhaltsbasierten Signaturen

WAVILA erweitert das Aktivitätsspektrum klassischer kryptographischer Techniken um Aspekte der Signalverarbeitung und so genannter unscharfer („fuzzy“) Logik. Unter einem digitalen Wasserzeichen im engeren Sinne versteht man ein transparentes, nicht wahrnehmbares Muster, welches in das Datenmaterial (Bild, Video, Audio, 3D-Modell) meist unter Verwendung eines geheimen Schlüssels eingebracht und ausgelesen wird /2/. Dieses Muster wird dazu benutzt, entweder das Vorhandensein einer Kennzeichnung anzuzeigen oder textuelle Informationen zu kodieren. In Abbildung 1 sieht man zum Beispiel unter a) ein Original und ein markiertes Bild wobei in einem Differenzbild die Unterschiede sichtbar gemacht werden. Das Wasserzeichen ist über das gesamte Bild gleichmäßig verstreut. Beim genauen Hinsehen, lassen sich auch kleine visuelle Störungen in der Kopie mit dem Wasserzeichen feststellen, da hier die Markierung besonders stark aufgebracht wurde. Unter b) sieht man ein block-basiertes Wasserzeichen im Luminanzbereich. Es wurde zur Visualisierung ebenfalls extrem verstärkt und ausschnittsweise vergrößert.

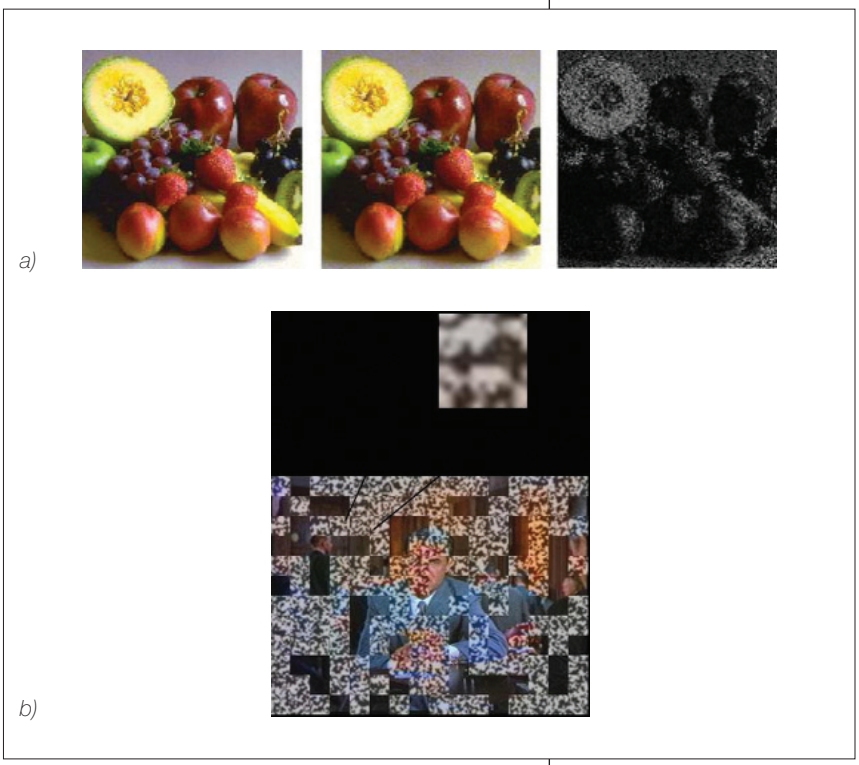

Abbildung 1
a) Original (links) und Kopie mit Wasserzeichen (Mitte), Differenzbild (links) mit sichtbaren Veränderungen;
b) Block-basiertes Wasserzeichenmuster im Luminanzbereich – stark verstärkt und vergrößert

Digitale Wasserzeichen als auch inhaltsbasierte Signaturen haben in den letzten Jahren einen enormen Aufschwung erhalten und spielen in DRM-Systemen eine bedeutende Rolle. Erstaunlicherweise fehlt es aber oft an systematischen Sicherheitsanalysen und ausgereiften Protokollen, wie man sie aus der Kryptographie her kennt.

Zielsetzung ist deshalb:
- Werkzeuge und Techniken zu entwickeln, die die Sicherheitsaspekte von Wasserzeichen und inhaltsbasierten Signaturen abschätzbar machen,
- verbesserte Algorithmen mit einem wohldefinierten Sicherheitsniveau zu designen,
- Protokolle unter Nutzung bekannter kryptographischer Mechanismen zu entwerfen, die eine überprüfbare Sicherheit bieten.

Des Weiteren stehen Implementierungsaspekte im Vordergrund, um effiziente und sichere Umsetzungen zu garantieren.

Um die verschiedenen Aspekte systematisch zu untersuchen, haben sich in WAVILA sechs Arbeitsgruppen (Working Groups; WG) gebildet, die sich folgenden Themen widmen: Erforschung theoretischer Grundlagen, Analyse und Verbesserung praktischer Systeme, Erforschung asymmetrischer Wasserzeichenansätze, Systeme die neben Wasserzeichentechniken andere Sicherheitstechniken nutzen (Hybride Systeme), Wasserzeichen zur Überprüfung der Datenauthentizität und -integrität (fragile Wasserzeichen in deren verschiedenen Ausprägungen), sowie Erforschung der Methoden des Perceptual Hashings zur forensischen Analyse.

Aus der Vielzahl von Forschungsarbeiten werden im Folgenden zwei Aspekte zu Praktischen und Hybriden Systemen herausgegriffen, um die Arbeiten, die an der Otto-von-Guericke-Universität Magdeburg durchgeführt werden, auszugsweise vorzustellen.

Herausforderung – Evaluation von Wasserzeichen

Im Rahmen der Arbeitsgruppe zum Thema Analyse und Verbesserung Praktischer Systeme werden Methoden zur Evaluation von digitalen Wasserzeichen untersucht, die deren Qualität abhängig vom Anwendungsszenario der Wasserzeichen bewerten. Jeder digitale Wasserzeichenalgorithmus sollte evaluiert werden, damit die Vor- und Nachteile bzw. die detaillierten Wasserzeichenparameter zum einen untersucht und zum anderen vergleichbar gemacht werden (siehe Ausführungen dazu auch in /3/). Das Advanced Multimedia and Security Lab (AMSL) der Universität Magdeburg beschäftigt sich dabei speziell mit der Evaluation von Audio-Wasserzeichen.

Bei der Evaluierung gibt es verschiedene Ansätze, welche in der Literatur Anwendung finden. Wie in /4/ dargelegt, wird oftmals die verlustbehaftete Kompression (zum Beispiel im MP3-Format) bis zu einer bestimmten Bit-Rate /5/ oder digital-analogen Wandlung /6/ verwendet. Darüber hinaus gibt es Werkzeuge, die eine Sammlung von Angriffen auf das Datenmaterial und somit auf das digitale Wasserzeichen bereitstellen – um dessen Robustheit und Fragilität zu bestimmen. Beispiele dafür sind StirMark (www.petitcolas.net/fabien/watermarking/stirmark/index.html), OPTIMARK (www.optimark.com), CHECKMARK (www.checkmark.com), CERTIMARK (www.certimark.org), OpenWatermark (www.openwatermark.org) oder WET (www.datahiding.org/).

Bei den genannten Evaluierungsumgebungen wird oftmals der Fokus auf Bilder gesetzt. In unseren Arbeiten steht Audio im Vordergrund und das entwickelte Werkzeug /7/ ist der Ausgangspunkt für die Arbeiten innerhalb von ECRYPT. Auf der Basis von StirMark können verschiedene Angriffstypen mit den Angriffsparametern individuell eingestellt werden. Aufgabe in ECRYPT ist es, einerseits die Angriffe performanter zu gestalten, um Tests über eine große Anzahl von Wasserzeichenverfahren und über eine große Anzahl von Testmaterialien zu führen, andererseits, auch die Angriffsparameter zu optimieren. Unser Schwerpunkt liegt hier beispielsweise in der Untersuchung des Einflusses des Audio-Datenmaterials auf die Angriffsparameter. Will man Wasserzeichen im Bereich E-Commerce einsetzen, bedeutet dies, dass auch die Wasserzeichenparameter datenmaterialabhängig parametrisiert werden müssen, so dass deren anwendungsspezifische Evaluation von besonderer Bedeutung ist.

In /4/ finden sich dazu unsere ersten Ergebnisse für Musik und Sprache. StirMark für Audio erlaubt die individuelle Einstellung von verschiedenen Angriffstypen mit Angriffsparametern. Basierend auf unseren Untersuchungen konnten wir feststellen, dass es wesentlich ist zu erkennen, welche Art von Audiomaterial verwendet wird. Ein großer Unterschied ist zwischen Musik (Rock, Pop, Jazz, …) und Sprache (weibliche, männliche Stimme, englisch, deutsch, …) festzustellen. Hat man Kenntnis über die Art des Datenmaterials, können die Angriffe zum einen effektiver (in Hinblick auf Transparenz und Angriffsstärke) durchgeführt werden und zum anderen kann entschieden werden, ob es überhaupt Sinn macht, den jeweiligen Angriff durchzuführen. Dies impliziert auch, in wieweit Wasserzeichenalgorithmen selbst entsprechend des Datenmaterials parametrisiert werden können.
Um einen Eindruck über die Arbeitsweise von StirMark for Audio (SMBA) zu erhalten, sei auf Abbildung 2 verwiesen.

SMBA stellt eine Sammlung von verschiedenen Angriffen bereit, welche jeweils kleine Veränderungen am Signalverlauf vornehmen. Ein eingebettetes Wasserzeichen wird durch diese Veränderung ebenfalls modifiziert und somit geschwächt oder zerstört /8/. Aufbauend darauf lassen sich verschiedene Wasserzeichenparameter, wie beispielsweise Robustheit, Transparenz oder Sicherheit, untersuchen.

Die allgemeine Funktionsweise von StirMark for Audio, welche ebenfalls in Abbildung 2 verdeut-

Glossar (1)

Digital Rights Management (DRM)
DRM beschreibt die digitale Verwaltung von Rechten, die sich meist aus dem Urheberrecht ergeben. Es umfasst alle Prozesse der Aufnahme oder Erstellung und Produktion, Verarbeitung, Vertrieb und Konsumtion.

Digitale Wasserzeichen
Unter einem digitalen Wasserzeichen im engeren Sinne versteht man ein transparentes, nicht wahrnehmbares Muster, welches in das Datenmaterial (Bild, Video, Audio, 3D-Modell) meist unter Verwendung eines geheimen Schlüssels eingebracht und ausgelesen wird /2/. Je nach Eigenschaft des Wasserzeichens unterscheiden wir nach robusten und fragilen, die entweder verschiedene Transformationen des Datenmaterials zulassen bzw. durch die Transformationen verändert werden.

Wasserzeichen Benchmarking
Unter dem Benchmarking versteht man die Evaluation von wichtigen Qualitätsparametern bezüglich der Eigenschaften Robustheit, Fragilität, Wahrnehmbarkeit, Kapazität, Komplexität.

Digitale Signaturen
Eine digitale Signatur wird oft auch als elektronische Signatur bezeichnet. Ziel ist es, die Sicherheitseigenschaften der handschriftlichen Unterschrift in der digitalen Welt nachzubilden. Das kann einerseits mit der Digitalisierung der eigenhändigen Unterschrift erfolgen oder aber mittels kryptographischer Funktionen. Im Allgemeinen wird letzteres darunter verstanden, wenn man heute von digitalen oder elektronischen Signaturen spricht.

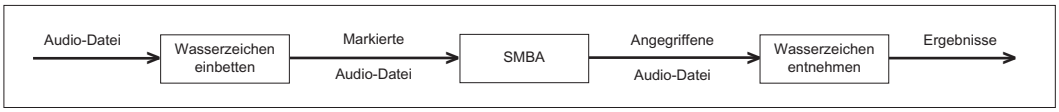

Abbildung 2
Arbeitsweise von StirMark for Audio (SMBA) aus /9/

licht wird, besteht darin, dass in eine originale Audiodatei mit einem Wasserzeichenverfahren eine Information eingebettet wird. Anschließend wird die markierte Audiodatei mit StirMark for Audio angegriffen und die angegriffene Audiodatei dem Wasserzeichenverfahren zur Detektion bzw. zum Auslesen eines Wasserzeichens übergeben. Dabei ist es generell möglich, die verschiedenen Angriffe einzeln auszuführen oder rekursiv miteinander zu verknüpfen. Der Angriff führt derzeit weder eine Analyse des vorliegenden Audioinhaltes noch eine psychoakustische Untersuchung /9/ durch. Das bedeutet, dass der Angriff mit der als Parameter übergebenen Angriffsstärke auf den gesamten Audioinhalt angewandt wird.

In unseren Untersuchungen im Rahmen des ECRYPT-Projektes (siehe /4/) konnten wir feststellen, dass die Transparenz bei der Evaluierung digitaler Audiodateien nicht nur von den Angriffsparametern abhängt. Einen wichtigen Aspekt dabei spielt der Inhalt (Kontext) der Audiodaten selber. Wenn Kenntnisse über die Audiodaten vorhanden sind, können die Angriffsparameter in Hinblick auf Transparenz optimiert werden. Deshalb haben wir gezeigt, welche Methoden bzw. Algorithmen des Data Mining existieren, damit eine Klassifizierung der Audiodaten vorgenommen werden kann. Bei den durchgeführten Tests wurde als Evaluierungswerkzeug StirMark for Audio verwendet und mit den Standardangriffsparametern in Hinsicht auf Transparenz mit dem SQAM (Sound Quality Assessment Material) Dateien untersucht. Dabei wurden subjektive Hörtests durchgeführt, welche die Standardwerte der Angriffe in Hinblick auf den Audiokontext verbesserten. Wir haben dabei primär zwischen Sprache und Musik unterschieden. Als nächstes wollen wir die Verbindung zwischen Data Mining und den Angriffen der digitalen Wasserzeichenevaluierung herstellen und umsetzen.

Sicherung der Integrität und Authentizität von Medien mit hybriden Systemen

Wie bereits einleitend ausgeführt, liegt ein Hauptaugenmerk auf der Sicherung der Integrität, der Authentizität und der Verbindlichkeit multimedialer digitaler Daten. Generell erfüllen elektronische Signaturen als kryptographische Mechanismen diese besonderen Anforderungen der Sicherung einer Nachricht bzw. einer Datei, z. B. für Dokumente, Bilder, Audio- und Videodaten. Wie in /10/ dargestellt, wird die Erkennung – jedoch nicht die Verhinderung – jeder Art von aktiver oder passiver Manipulation ermöglicht. Darüber hinaus kann die elektronische Signatur die Verbindlichkeit im Sinne der Nicht-Abstreitbarkeit der Identität von Sender bzw. Besitzer oder Urheber und Empfänger einer Nachricht bzw. Datei sichern, siehe dazu auch weitere Ausführungen in /10/.

In den bisher üblichen Anwendungsszenarien wird die elektronische Signatur an eine Nachricht oder Datei angefügt. Jedoch auch die direkte Einbettung dieser Informationen in den Inhalt, durch ein digitales Wasserzeichenverfahren, ist möglich. Lösungsmöglichkeiten für diese Problematik der Sicherung der Authentizität und Integrität digitaler Mediendaten wurde in /11/ erstmals vorgestellt. Erste Sicherheitsanalysen dazu können in /12/ gefunden werden. Aufgabe ist es nun in ECRYPT ein formales Protokoll zu diesem Ansatz zu entwickeln, welches, mit aus der Kryptographie bekannten Methoden, beweisbar ist.

An dieser Stelle wollen wir kurz die grundlegende Vorgehensweise beim Einbetten einer Signatur als digitales Wasserzeichen skizzieren.

Die wasserzeichenbasierten Verfahren entscheiden die Integrität über Fragilität auf Schwellwertbasis. Dabei wird das Wasserzeichen meist mit geringer Stärke eingebracht. Man evaluiert auf der Basis des Vorhandenseins von Restinformationen aus dem Wasserzeichen, ob Manipulationen aufgetreten sind. Kann das eingebrachte Wasserzeichen gefunden werden, ist mit großer Wahrscheinlichkeit keine Manipulation erfolgt. Kann das Wasserzeichen nicht mehr gefunden werden, wurde es durch Angriffe zerstört – eine Manipulation kann somit indirekt nachgewiesen werden.

Wie in /10/ dargelegt, verfälschen diese fragilen Wasserzeichen das Original durch das direkte Integrieren der Informationen in das Medium. In Hochsicherheitsbereichen, wie der Medizin oder dem Militär, bei denen selbst kleinste Änderungen am Inhalt aus Gründen der Fehlinterpretation vermieden werden müssen, kann somit ein herkömmliches digitales Wasserzeichen zur Absicherung nicht zum Einsatz kommen. Aus dieser Motivation heraus wurden detaillierte Überlegungen zu so genannten invertierbaren Wasserzeichen angestellt (siehe in /13/), welche nicht nur die Integrität (und mittels eines geheimen Schlüssels auch die Authentizität) überprüfen, sondern auch das Wasserzeichen entfernen lassen. Diese Verfahren werden deshalb auch als reversibel bezeichnet.

Um die Problematik der öffentlichen Überprüfbarkeit zu lösen, findet man ein invertier-

Glossar (2)

Kryptologie
ist eine Wissenschaft, die mathematische Methoden und Techniken erforscht, um Vertraulichkeit, Integrität und Authentizität sowie Nachweisbarkeit von digitalen Daten sicherstellen zu können.

E-Business
Von Begriffen wie E-Mail, der elektronischen Post, leitet sich das Wort E-Business ab und umfasst die Vielzahl der im Internet ablaufenden Geschäfte, vom Kaufen/Verkaufen bis hin zur Kundenbetreuung.

M-Business
bezeichnet E-Business über das Mobilfunknetz.

E-Voting
Abgeleitet von E-Business, werden hierunter elektronische Wahlen über das Internet verstanden.

Ambient Intelligence
Der Begriff entstammt der Advisory Group zum 6. Rahmenprogramm der EU (ISTAG, www.cordis.lu/ist/istag.htm). Grob umfasst das Aufgabengebiet die intelligente Interaktion von Benutzern mit der jeweiligen Umgebung (Ambience), wobei im Vordergrund die Intelligenz, die sich in den von dem Anwender verwendeten Zugangsgeräten, in einem Netzwerk, in den zugegriffenen Medien/Informationen oder der Umgebung befinden kann, steht.

Perceptual Hash
inhaltsbasierter Hash, Content-based Hash, manchmal auch passiver Fingerabdruck oder Perceptual Fingerprint genannt

Virtual Laboratories
(Virtual Labs)
Virtuelle Labore

bares Wasserzeichen kombiniert mit elektronischen Signaturen, um die Integrität und Authentizität nachzuweisen bei gleichzeitiger Möglichkeit, das Original durch das invertierbare Wasserzeichen zu schützen /11/. Die Überprüfung der Integrität und Authentizität von Bilddaten erfolgt durch ein öffentlich verifizierbares elektronisches Signaturprotokoll. Die Invertierfunktion ist nur autorisierten Personen zugänglich, wobei zusätzliche Sicherheitsfunktionen wie Zeitstempel ebenfalls denkbar sind.

Das Protokoll kann aus /12/ wie folgt beschrieben werden:
a) Das Original O wird in zwei Teilmengen A und B zerlegt, die Zerlegung ist abhängig vom Medientyp und vom konkret verwendeten Wasserzeichenverfahren.
(Zum Beispiel basiert ein Ansatz für digitales Bildmaterial darauf, im Blaukanal des Bildes (im Farbanteil Blau) eine Bit-Ebene auszuwählen, die für das menschliche Auge nur bedingt bei Veränderungen, d. h. Einbettung von Informationen, Artefakte hervorruft. Dazu wird beim Einbetten des Wasserzeichens der Grad zugelassener visueller Veränderungen bestimmt und entsprechend der einzubettenden Nachrichtenlänge eine oder mehrere Bit-Ebene(n) als Wasserzeichen-Positionen für die Menge B bestimmt.)
b) Die Menge A wird unverändert gelassen und die Menge B wird als Wasserzeichenträger benutzt. Um Invertierbarkeit zu erreichen, muss die Menge B verlustfrei komprimierbar sein. Nach der Kompression von B nach C entsteht somit Platz für das Einbetten einer Nachricht M.

Die Abbildung 3 verdeutlicht das prinzipielle Vorgehen hierzu. Einerseits wird somit das Original geschützt (nur O' wird weiterverteilt) und andererseits ist Platz geschaffen, eine Signatur direkt einzubetten, um eine öffentliche Überprüfbarkeit des Originals zu erhalten. Diese Überprüfung erfolgt mit folgender Konstruktion:

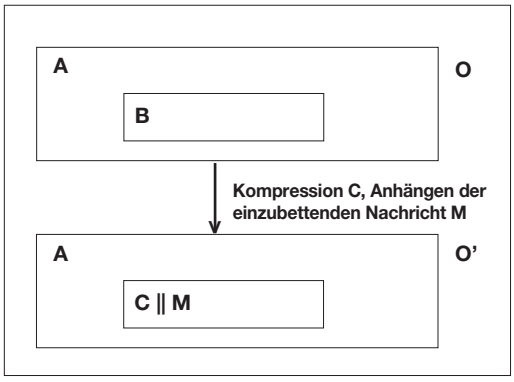

Abbildung 3
Invertierbare Wasserzeichen: Schematisiertes Vorgehen der Einbettung

- Über das Original O wird ein Hashwert gebildet und mit dem Kompromat C konkateniert: C|H(O)
- Um den Schutz des Originals zu garantieren, wird dieser Nachrichtenteil mit einem Verschlüsselungsalgorithmus (z. B. symmetrische Kryptographie) mit einem geheimen Schlüssel verschlüsselt: Encrypt(C|H(O))
- Über dieses Chriffrat und der Menge A wird eine kryptographische Signatur gebildet, wobei der Ersteller seinen privaten Schlüssel nutzt: s = Sign(A | Encrypt(C|H(O)))
- Die einzubettende Nachricht M wird mit weiteren Synchronisationsinformationen bestückt und sieht dann wie folgt aus: M = Encrypt(C|H(O)) | s | datainfo

Im Prüfungsfall, wird die Signatur detektiert, ausgelesen und mit dem zugehörigen öffentlichen Schlüssel verifiziert. Nur bei Kenntnis des symmetrischen (geheimen) Schlüssels, kann auch das Original rekonstruiert werden. Details zur Prüfung und zur Rekonstruktion können in /10/ für Bilddaten nachgelesen werden.

Innerhalb des ECRYPT Projektes, in der Arbeitsgruppe Hybride Systeme, wird das Protokoll zusammen mit der Technischen Universität München weiter formalisiert und verifiziert, sowie auf weitere Medientypen mit kontinuierlichen Eigenschaften wie Video und Audio erweitert.

AUSBLICK

Das Network of Excellences ECRYPT strukturiert und organisiert die Forschung zu Kryptologie und Wasserzeichen, in dem allgemeine Forschungsziele gesetzt und *roadmaps* definiert werden, um offene Probleme systematisch anzugehen. ECRYPT beherbergt Forscher unterschiedlicher Herkunft – aus der Informatik, aus der Mathematik, aus der Elektrotechnik –, sowohl Akademiker als auch Experten aus der Industrie.

Experten und Laien müssen den Anwendungen, die sie nutzen, vertrauen können.

Die Entwicklung von sicheren und vertrauenswürdigen Infrastrukturen ist von fundamentaler Wichtigkeit für die globale, digitale Informationsrevolution. In unserem Beitrag haben wir die brennenden Herausforderungen von ECRYPT zusammengefasst und am Beispiel digitaler Wasserzeichen einige offene Fragestellungen exemplarisch verdeutlicht.

Idealerweise werden erreichte technologische Fortschritte ebenfalls in Aus- und Weiterbildungen reflektiert und integriert. Die Weitergabe des Wissens ist somit wesentlicher Bestandteil und stellt einem wichtigen Arbeitspunkt innerhalb ECRYPT dar. Aktuelle Veranstaltungen und Neuigkeiten aus ECRYPT und auch von der Arbeitsgruppe AMSL können unter: wwwiti.cs.uni-magdeburg.de/iti_amsl/veranstaltungen/ und amsl-smb.cs.uni-magdeburg.de/ecrypt/ nachgelesen werden.

Referenzen

/1/ ECRYPT Network of Excellence in Cryptology, IST-2002-507932, http://www.ecrypt.eu.org/

/2/ Dittmann, Jana: Digitale Wasserzeichen, Springer Verlag, ISBN 3-540-66661-3, 2000

/3/ Macq, Benoit; Dittmann, Jana; Delp, Edward J.: Benchmarking of Image Watermarking Algorithms for Digital Rights Management, Proceedings of the IEEE, Special Issue on: Enabling Security Technology for Digital Rights Management, pp. 971-984, Vol. 92 No. 6, June 2004

/4/ Andreas Lang, Marcus Holley, Jana Dittmann: StirMark for Audio: Unterschiede zwischen Musik und Sprache, Erscheint in 12. Leipziger Informatik-Tage, LIV-Jahrestagung 2004, Von e-Learning bis e-Payment – Das Internet als sicherer Marktplatz, September 2004

/5/ Martin Steinebach, Andreas Lang, Jana Dittmann, StirMark Benchmark: Audio watermarking attacks based on lossy compression, Photonics West 2002 SPIE, San Jose, CA, USA Bellingham, Washington, USA, vol. 4675, ISBN 0-8194-4415-4

/6/ Martin Steinebach, Andreas Lang, Jana Dittmann, Audio Watermarking Quality Evaluation: Robustness to DA/AD Processes, Int. Conference on Information Technology: Coding and Computing, ITCC 2002, Las Vegas, Nevada, USA, IEEE Computer Society, Piscataway, NJ, USA, ISBN 0-7695-1506-1

/7/ StirMark for Audio: http://amsl-smb.cs.uni-magdeburg.de

/8/ Andreas Lang; Stefan Thiemert; Martin Steinebach; Jana Dittmann, Ausgewählte Angriffe der Stirmark Benchmark Suite, Sichere Geschäftsprozesse – Grundlagen, Konzepte, Anwendungen, Perspektiven, Patrick Horster (Eds.) it Verlag für Informationstechnik GmbH, Höhenkirchen, pp. 320-332, ISBN 3-936052-07-7, 2002

/9/ Andreas Lang; Jana Dittmann; Martin Steinebach; Psycho-akustische Modelle für StirMark Bechmark – Modelle zur Transparenzevaluierung; Informatik 2003 – Mit Sicherheit Informatik, Beiträge des Schwerpunktes „Sicherheit – Schutz und Zuverlässigkeit"; Proceedings; Rüdiger Grimm; Hubert B. Keller, Kai Rannenberg (Hrsg.), pp. pp 399-410, Informatik 2003, 29.09.-02.10.2003, Frankfurt/Main, ISBN 3-88579-365-2, 2003

/10/ Dittmann, Jana; Steinebach, Martin; Pharow, Peter: Neue Perspektiven zur Manipulationserkennung in digitalen Medien, In: D-A-CH Security IT Security & IT Management; Patrick Horster (Eds.) Proceeding D-A-CH Security; syssec, pp. 117-129, D-A-CH Security, 25.-26.03., Erfurt, Germany, ISBN 3-00-010941-2, 2003

/11/ J. Dittmann, M. Steinebach, L. Ferri: „Watermarking protocols for authentication and ownership protection based on timestamps and holograms", in Security and Watermarking of Multimedia Contents IV, Proceedings of SPIE vol. 4675, pp. 240-251, 2002

/12/ Katzenbeisser, Stefan; Dittmann, Jana: Malicious attacks on media authentication schemes based on invertibe watermarks, To appear in Security and Watermarking of Multimedia Contents VI, Electronic Imaging – Science and Technology, Edward J. Delp III, Ping Wah Wong, SPIE, 18.-22. January, Santa Clara, CA USA, 2004

/13/ J. Fridrich, with M. Goljan and Rui Du: Invertible Authentication, Proc. SPIE Photonics West, vol. 3971, Security and Watermarking of Multimedia Contents III, San Jose, California January (2001), pp. 197-208, 2001

Dank
Dank geht an dieser Stelle an die Arbeitsgruppe AMSL für die Unterstützung im ECRYPT-Projekt. Insbesondere gilt dieser Dank Andreas Lang, Christian Krätzer und Marcus Holley (welcher sich mit der Audiowasserzeichenevaluation beschäftigt) und Stefan Katzenbeisser (TU München; der bei der Erweiterung des invertierbaren Wasserzeichenprotokolls konstruktiv mitgearbeitet hat) – durch diese Kooperation konnten viele neue Erkenntnisse gewonnen werden.

Prof. Dr.-Ing. Jana Dittmann
studierte Wirtschaftsinformatik an der Technischen Universität in Darmstadt und promovierte am GMD-Forschungszentrum Informationstechnik in Kooperation mit der TU Darmstadt zum Thema *Digitale Wasserzeichen – Sicherheit in Medienströmen* im Oktober 1999. Von November 1999 bis Februar 2002 leitete sie am Fraunhofer IPSI, Darmstadt in verantwortlicher Position eine Forschungsgruppe zum Thema Sicherheit in Multimedia und betreute die dortigen Projekte sowie Dissertationsvorhaben. Darüber hinaus war sie am Aufbau und der Eröffnung (März 2001) des Kompetenzzentrums: C4M – Competence for Multimedia Security maßgeblich beteiligt, welches sie bis Februar 2002 leitete.
Im September 2002 nahm sie den Ruf auf die C3-Professur für Angewandte Informatik an der Otto-von-Guericke-Universität Magdeburg, Institut für Technische und Betriebliche Informationssysteme (ITI), an und leitet seit dem die Arbeitsgruppe „Multimedia and Security". Das Forschungsspektrum ist interdisziplinär mit den Gebieten Informatik, Mathematik und Elektrotechnik und umfasst fünf wesentliche inhaltliche Schwerpunkte: digitale Wasserzeichen für Einzel- und Bewegtbild, Audio, 3D-Modelle sowie für kombinierte Medien zum Nachweis der Urheberschaft und der Unversehrtheit bis hin zu neuen elektronischen Geschäftsmodellen für die Medienwirtschaft; steganographische Techniken und kryptographische Protokolle; multimediale biometrische Erkennungstechniken zur Benutzerauthentifizierung; Vertrauensmodelle, Sicherheitsevaluierungen und Securityscans; Multimedia in Applikationen: Human Computer Interfaces und Mobile Multimedia.