ECRYPT - European Network of Excellence in Cryptology
Aspekte der Sicherheit von Mediendaten

Jana Dittmann[1], Andreas Lang[1], Martin Steinebach[2], Stefan Katzenbeisser[3]
[1]Otto-von-Guericke Universität Magdeburg, ITI/AMSL
[2] Fraunhofer Institut IPSI, Darmstadt
[3]Technische Universität München, Institut für Informatik

Abstract: Die Abkürzung ECRYPT steht für „European Network of Excellence in Cryptology". Das Netzwerk ist ein Zusammenschluss von ca. 180 europäischen Forschern in Industrie und Wissenschaft. Das Projekt, in dessen Mittelpunkt Forschungen auf dem Gebiet der Kryptographie und der digitalen Wasserzeichen steht, wird von der Europäischen Union über einen Zeitraum von vier Jahren gefördert. In dieser Arbeit werden die Ziele von ECRYPT zusammengefasst und exemplarisch zwei Forschungsvorhaben von ECRYPT auf dem Gebiet der Multimedia-Sicherheit vorgestellt.

1 ECRYPT – Projektziele

Kryptologie und digitale Wasserzeichen können als Herzstücke aktueller Konzepte der Computer- und Netzwerksicherheit 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. Diese Techniken haben eine Vielzahl von Anwendungen, welche von E-Business, M-Business, E-Voting und On-line Bezahlsystemen bis hin zu kabellosen Netzen reichen. Wir finden heute Kryptologie in unseren GSM Mobiltelefonen, in Kreditkarten, in unserer Browsersoftware, in WLAN Verbindungen, und manche Europäer finden kryptographische Techniken bereits in ihren Ausweisdokumenten.

ECRYPT orientiert sich an den strategischen Zielen des IST Work Programme 2.3.1.5 "Towards a global dependability and security framework". Da Kryptologie und Wasserzeichen inzwischen interdisziplinäre Forschungsgebiete darstellen, befasst sich ECRYPT speziell auch mit den Wechselwirkungen dieser Techniken. Die wesentlichen Ziele von ECRYPT sind:

- Stärkung der europäischen wissenschaftlichen und industriellen Forschung auf dem Gebiet der Kryptologie und der digitalen Wasserzeichen.

- Stärkung und Integration der Forschung in Kryptologie und im Bereich digitaler Wasserzeichen; Bündelung der Aktivitäten durch den Aufbau so genannter Virtual Laboratories, die die Forschungsaktivitäten strukturieren und gewinnbringend zusammenführen sollen.

- Erzielt werden soll ein verbessertes Verständnis des Standes der Technik in Theorie und Praxis, um die theoretischen Grundlagen zu erweitern, sichere Algorithmen und Protokolle zu entwerfen sowie effiziente Implementierungen (niedrigere Kosten, hohe Performanz) zu entwickeln.

Die Forschungsaktivitäten innerhalb von ECRYPT gliedern sich in fünf Virtual Labs, die sich mit symmetrischer und asymmetrischer Kryptographie, Protokolldesign und -analyse, Implementierungsfragen sowie digitalen Wasserzeichen beschäftigen. Eine detaillierte Beschreibung der einzelnen Virtual Labs kann auf der Homepage von ECRYPT (www.ecrypt.eu.org) gefunden werden. Wir stellen im Folgenden das WAVILA Lab genauer vor, welches sich mit digitalen Wasserzeichen beschäftigt. Unter einem digitalen Wasserzeichen versteht man ein transparentes, nicht wahrnehmbares Muster, welches in ein Datenmaterial (Bild, Video, Audio, 3D-Modell), meist unter Verwendung eines geheimen Schlüssels, eingebracht wird. Dieses Muster wird dazu benutzt, applikationsabhängige textuelle Information (wie etwa den Urheber eines Medienobjekts) zu codieren. Digitale Wasserzeichen haben in den letzten Jahren einen enormen Aufschwung erlebt und spielen in DRM Systemen eine bedeutende Rolle.

Erstaunlicherweise fehlt es aber bei digitalen Wasserzeichen oft an systematischen Sicherheitsanalysetechniken und ausgereiften Protokollen, wie man sie aus der Kryptographie kennt. Eine Hauptzielsetzung von WAVILA ist es deshalb, Werkzeuge und Techniken zu entwickeln, die die Sicherheit von Wasserzeichen abschätzbar machen. Aufbauend auf diesen Erkenntnissen sollen verbesserte Algorithmen mit einem wohldefinierten Sicherheitsniveau entwickelt werden. Zudem stehen Implementierungsaspekte im Vordergrund, um eine effiziente und sichere Umsetzung in praktischen Systemen zu garantieren. Innerhalb von WAVILA existieren mehrere Arbeitsgruppen, die sich unter anderem mit theoretischen Grundlagen, Aspekten des Protokolldesigns sowie der Analyse und Verbesserung bestehender Wasserzeichenverfahren befassen. Aus der Vielzahl dieser Forschungsthemen werden im Folgenden exemplarisch zwei Arbeiten herausgegriffen, die im Rahmen von ECRYPT an der Universität Magdeburg in Zusammenarbeit mit dem Fraunhofer IPSI sowie der TU München durchgeführt werden.

2 Evaluierung von Wasserzeichen

In der Arbeitsgruppe „Practical Systems“ innerhalb von WAVILA werden Methoden zur Evaluierung digitaler Wasserzeichen untersucht, die deren Qualität aufgrund von realistischen Anwendungsszenarien bewerten. Die Ergebnisse der Evaluation können einerseits die Vor- und Nachteile einzelner Algorithmen aufzeigen, andererseits aber auch für Vergleichszwecke herangezogen werden. Das Advanced Multimedia and Security Lab (AMSL) der Universität Magdeburg beschäftigt sich mit der Evaluation von Audio-Wasserzeichen. Grundsätzlich gibt es bei der Evaluierung verschiedene Ansätze, die von naiven Verfahren (wie die Verwendung von analog-digital Wandlern) bis hin zum Einsatz komplexer, vielschichtiger Testroutinen reichen. Inzwischen sind mehrere Werkzeuge verfügbar, die eine Sammlung von spezifischen Angriffen auf digitale Wasserzeichen bereitstellen, um deren Robustheit zu bestimmen. Beispiele dafür sind StirMark (www.petitcolas.net/fabien/watermarking/stirmark), 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 den Arbeiten von AMSL stehen Audiowasserzeichen im Vordergrund. Auf der Basis von „StirMark for Audio“ (SMBA, amsl-smb.cs.uni-magdeburg.de), das von der Gruppe AMSL mit entwickelt wurde, wird der Einfluss bestimmter Angriffe sowie Angriffsparameter auf Audiowasserzeichen untersucht. SMBA stellt eine Sammlung von

verschiedenen Angriffen bereit, welche jeweils kleine Veränderungen am Audiosignalverlauf vornehmen. Ein eingebettetes Wasserzeichen wird durch diese Veränderung ebenfalls modifiziert und somit geschwächt oder zerstört. Aus diesen Veränderungen am Datenmaterial lassen sich Schlüsse über sicherheitskritische Wasserzeichenparameter (wie etwa Robustheit oder Transparenz) ziehen.

SMBA [DSZL04] geht dabei wie folgt vor: In eine originale Audiodatei wird mit einem Wasserzeichenverfahren eine Information eingebettet. Dann wird die markierte Datei mit SMBA angegriffen, wobei entweder die Angriffe einzeln ausgeführt oder rekursiv miteinander verknüpft werden können. Anschließend wird versucht die eingebettete Information aus der resultierenden Datei wieder auszulesen. SMBA führt derzeit weder eine Analyse des Audioinhaltes noch eine psychoakustische Untersuchung [LDS03] durch. Der Angriff wird somit gleichermaßen auf den gesamten Audioinhalt angewandt.

Aufgabe eines Teilprojekts von WAVILA ist es, einerseits die Angriffsroutinen performanter zu gestalten, um Tests über eine große Anzahl von Wasserzeichenverfahren und über eine große Anzahl von Testmaterial führen zu können, und andererseits die Angriffsparameter zu optimieren. Ein weiterer Schwerpunkt liegt in der Untersuchung des Einflusses des Inhalts des Audiomaterials (Musik, Sprache, Geräusche oder entsprechende Mischformen) auf die Angriffsparameter. In [LHD04] finden sich dazu erste Ergebnisse für Musik und Sprache. In unseren Untersuchungen stellten wir fest, dass die Art des Audiomaterials wesentlichen Einfluss auf den Erfolg bestimmter Angriffe hat. Wird dies beachtet, können einerseits die Angriffe zukünftig effektiver gestaltet werden. Andererseits kann SMBA selbst hinsichtlich seiner Laufzeit optimiert werden.

Die gewonnenen Resultate spielen ebenfalls in der Entwicklung von neuartigen Wasserzeichen eine entscheidende Rolle. Parametrisiert man das Einbettungsverfahren eines Wasserzeichenalgorithmus entsprechend des Datenmaterials, so kann man etwa optimal auf das Auftreten von Stille oder eines schmalbandigen Frequenzverlaufs reagieren und damit spezifische Angriffe durch entsprechendes Design abwehren.

3 Sicherung der Integrität von Medien durch digitale Wasserzeichen

Die Verfügbarkeit von mächtiger Bildbearbeitungssoftware erlaubt eine einfache Manipulation an Bildern oder Videosequenzen auf jedem aktuellen Industrie-PC. Obwohl die Fortschritte in der Bildbearbeitung verschiedene Applikationen (wie beispielsweise den Videoschnitt am PC) erst ermöglichen, stellen sie prinzipiell die Vertrauenswürdigkeit und Beweiskraft von digitalen Bildern sowie von Videosequenzen stark in Frage. Beispielsweise gibt es keine Garantie, dass ein (Beweis-)Foto ein exaktes Abbild der Realität darstellt, da es prinzipiell durch Bildverarbeitungssoftware modifiziert worden sein könnte. Ähnliche Probleme stellen sich etwa bei Videosequenzen aus Überwachungskameras, digitalisierten amtlichen Dokumenten sowie bei digitalisierten Zahlscheinen und Verträgen. Traditionell wurde dieses Problem durch den Einsatz von digitalen Signaturen gelöst, die jedoch separat von der Mediendatei gespeichert werden mussten.

Die Verfügbarkeit von ausgereiften digitalen Wasserzeichenalgorithmen erlaubt es nun, digitale Signaturen direkt in ein Medienobjekt zu codieren, um dessen Integrität und Authentizität sicherzustellen. Da in diesem Fall das Medienobjekt selbst alle Informationen in sich trägt, die zur Verifikation seiner Integrität benötigt werden, können derartige Integritätstests leicht in bestehende Softwaresysteme eingebettet werden.

Im Rahmen von WAVILA wurde ein Authentifikationsverfahren für digitale Medien entwickelt, das auf digitalen Signaturen und auf „fragilen invertierbaren“ Wasserzeichen beruht [DSF02, KaDi04, DKSV05]. Diese spezielle Klasse von Wasserzeichen ist einerseits nicht robust gegen Modifikationen des Medienobjekts, erlaubt jedoch andererseits die restlose Entfernung eines Wasserzeichens aus einem unmodifizierten Medienobjekt. Durch die Fragilität werden Modifikationen an den Mediendaten erkannt; die Invertierbarkeit ermöglicht die Verifikation der eingebetteten Signatur.

Das Verfahren arbeitet dabei wie folgt. Um ein Medienobjekt O zu signieren, wird in einem ersten Schritt festgestellt, welche Änderungen sich durch Einbringung eines Wasserzeichens im Objekt ergeben werden. Wir bezeichnen jene Teile von O, die sich durch das Einbetten des Wasserzeichens potentiell ändern können mit O_A, den Rest mit O_B. Um die unbefugte Rekonstruktion des Originals zu verhindern, wird O_A mit symmetrischer Kryptographie verschlüsselt. Danach wird die digitale Signatur $S=SIG(O_B|E(O_A))$ berechnet und die Zeichenkette $O_A|S$ als Wasserzeichen in O eingebettet. Diese Operation erzeugt das authentifizierte Medienobjekt O'.

Um die Authentizität und Integrität eines Objekts O' nachzuweisen, wird zuerst das Wasserzeichen vollständig aus O' entfernt, d.h. es wird analog zur Einbettung das Objekt O' in seine Teile O'_A und O'_B zerlegt. Falls O' mit dem vorgestellten System signiert war und O' nicht verändert wurde, hat O'_A die Form $O_A|S$. Aus dieser Information lässt sich das Original O rekonstruieren, in dem man den Teil O'_A von O durch den rekonstruierten Teil O_A ersetzt. Mit Kenntnis des Originals O kann schließlich die Korrektheit der Signatur S verifiziert werden.

Das vorgestellte Verfahren kann sowohl für kleine Medienobjekte als auch für Video- und Audioströme implementiert werden und ist (relativ zu den klassischen kryptographischen Annahmen) beweisbar sicher. Im Falle von Video- und Audioströmen wird das Authentifikationsschema blockweise auf den Medienstrom angewendet. Zudem kann es leicht in bestehende Multimedia-Anwendungen integriert werden, da der Integritätstest gänzlich von der restlichen Anwendung getrennt ist.

Danksagung. Die Autoren bedanken sich an dieser Stelle bei allen Mitarbeitern der Arbeitsgruppe AMSL für ihr Engagement im ECRYPT-Projekt. Die Arbeiten und Ergebnisse, die in dieser Veröffentlichung beschrieben sind, werden von der Europäischen Union innerhalb des IST-Programms, Vertrag IST-2002-507932 ECRYPT, unterstützt.

Literaturverzeichnis

[DKSV05] J. Dittmann, S. Katzenbeisser, C. Schallhart, H. Veith: „Ensuring media integrity on third-party infrastructures”, in 20th IFIP Information Security Conference (SEC05).

[DSF02] J. Dittmann, M. Steinebach, L. Ferri: „Watermarking protocols for authentication and ownership protection based on timestamps and holograms“, in Proceedings of the SPIE vol. 4675, pp. 240-251, 2002.

[DSZL04] J. Dittmann, M. Steinebach, S. Zmudzinsky, A. Lang, „Advanced audio watermarking benchmarking“, in Proceedings of the SPIE vol. 5306, 2004.

[KaDi04] S. Katzenbeisser, J. Dittmann: „Malicious attacks on media authentication schemes based on invertible watermarks“, in Proceedings of the SPIE vol. 5306, 2004.

[LDS03] A. Lang, J. Dittmann, M. Steinebach, „Psycho-akustische Modelle für StirMark Bechmark - Modelle zur Transparenzevaluierung“, in Informatik 2003, pp 399 – 410.

[LHD04] A. Lang, M. Holley, J. Dittmann, „StirMark for Audio: Unterschiede zwischen Musik und Sprache“, in „Von e-Learning bis e-Payment 2004“; Proceedings LIT’04, 2004.