PIK, Praxis der Informationsverarbeitung und Kommunikation 20/3 (1997), 134-137.

Vertrauliche Kommunikation mit Steganographie

Hannes Federrath, Guntram Wicke

TU Dresden, Fakultät Informatik, 01062 Dresden
{federrath, wicke}@inf.tu-dresden.de

Zusammenfassung. Mit Steganographie ist es möglich, geheime Daten über Kommunikationsnetze zu übermitteln, ohne daß überhaupt etwas über deren Existenz bekannt wird. Hierzu werden in unverdächtigen Daten die geheimen Nachrichten eingebettet.

Hannes Federrath, Diplom-Informatiker, seit 1994 wissenschaftlicher Mitarbeiter an der TU Dresden, Institut für Theoretische Informatik. Mitarbeit im Ladenburger Kolleg „Sicherheit in der Kommunikationstechnik“ der Gottlieb-Daimler- und Karl-Benz-Stiftung Ladenburg. Arbeitsgebiete: Sicherheit in verteilten Systemen, Technischer Datenschutz in Mobilkommunikationssystemen.

Guntram Wicke, Dipl.-Wirtsch.-Inf., Wiss. Mitarbeiter an der TU Dresden, Institut für Theoretische Informatik seit 1996, Mitarbeit im BMBF-Projekt SSONET (Sicherheit und Schutz in offenen Datennetzen) mit dem Schwerpunkt Architekturentwurf für mehrseitige Sicherheit.

1 Kryptoreglementierung

Sowohl die Anbieter wie auch die Nachfrager von kryptographischen Verfahren bewegen sich in einem gesellschaftlichen Rahmen, der von vielfältigen Interessengegensätzen geprägt ist. Es ist nie auszuschließen, daß vertraulicher Nachrichtenaustausch mißbräuchlich oder illegal angewendet wird. Mit der freien Verfügbarkeit von Kryptographie steigt neben der Anzahl der Nutzer, die aus bestimmten Gründen Kryptographie für tolerierte bzw. gewünschte Zwecke einsetzen, auch die Zahl derer, die nicht tolerierbare Zwecke verfolgen.

Die Notwendigkeit einer gesetzlichen Kryptoreglementierung wird mit der Bekämpfung insbesondere des organisierten Verbrechens begründet. In diesen Kreisen wird, so nimmt man an, Kryptographie verwendet, die es den Verfolgungsbehörden unmöglich macht, an derart geschützte Informationen durch Brechen von Verfahren zu gelangen. Per Gesetz

„regulierter“ Einsatz von Kryptographie könnte einen Zugriff auf geheime Informationen für berechtigte Behörden ermöglichen, so die Argumentation.

Es sollen nur kryptographische Systeme zum Gebrauch zugelassen werden, die den sog. Bedarfsträgern, d.h. den Geheimdiensten, der Kriminalpolizei, dem Verfassungsschutz etc. eine Hintertür offen lassen, über die ihnen eine nachträgliche Entschlüsselung gespeicherter bzw. übermittelter Informationen möglich wird.

Ein Verbot oder eine Reglementierung von Kryptographie kann nicht verhindern, daß sie unerlaubt verwendet wird. Wenigstens ist ihr Einsatz aber noch erkennbar und könnte geahndet werden, auch wenn sich die Nachrichten nicht entschlüsseln lassen.

2 Steganographie

Steganographie dient zur Sicherung der Vertraulichkeit der Existenz von geheimen Daten und liefert Verfahren, bei denen nicht einmal erkennbar ist, daß geheime Nachrichten ausgetauscht wurden. Falls diese Verfahren gut sind, ist Kryptoreglementierung völlig ineffektiv.

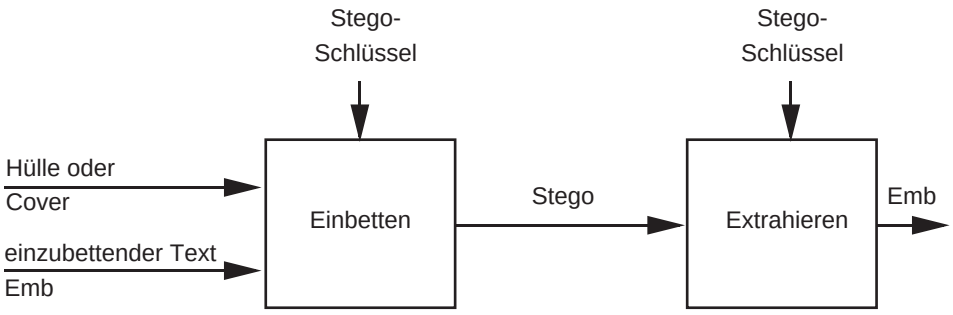

Abbildung 1: Prinzipieller Aufbau eines Stegosystems

Abbildung 1 zeigt den prinzipiellen Aufbau eines Stegosystems. Bei Steganographie wird eine geheimzuhaltende Nachricht in eine Hülle derart eingebettet, daß

1. dem Ergebnis (in der Abbildung mit Stego bezeichnet) die minimalen Veränderungen nicht anzusehen sind und
2. die Veränderungen nicht mit Meßmethoden nachweisbar sind.

Um dies zu erreichen, wird die Einbettung in einem „Unsicherheitsbereich“ (genauer: in Bereichen maximaler Entropie) durchgeführt, der auf natürlichen Ursachen beruht. Ein Beispiel soll dies verdeutlichen: Scannt man ein Foto mehrmals ein, entstehen stets unterschiedliche digitale Bilddaten. Die Ursachen hierfür liegen

- einerseits in Toleranzen der Scannermechanik,
- andererseits aber auch im stets vorhandenen Quantisierungsrauschen des Analog-Digital-Umsetzers.

Die Einbettung geschieht nun derart, daß sich die ergebenden Veränderungen der digitalisierten Hülle stets innerhalb des oben beschriebenen Unsicherheitsbereiches bewegen.

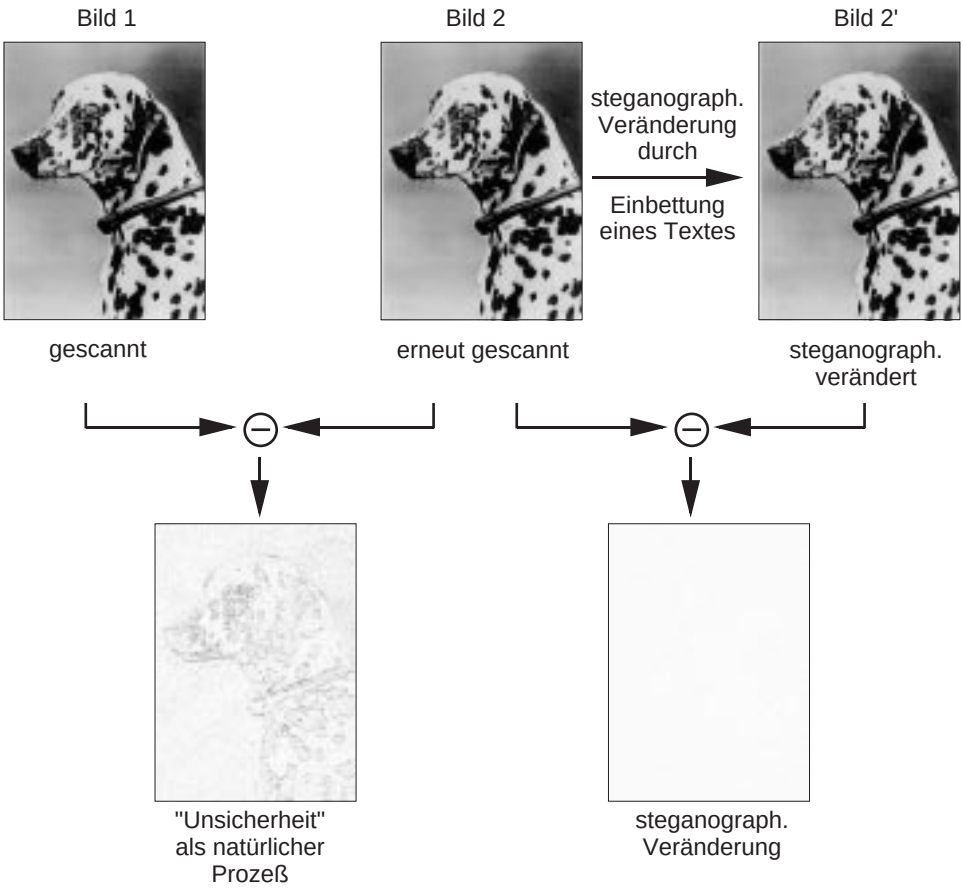

Abbildung 2: Veränderungen einer Hülle, basierend auf natürlichen Prozessen

Abbildung 2 zeigt ein zweimal eingescanntes Foto sowie eine steganographisch veränderte Version des Bildes 2 (mit Hilfe des Programms S-Tools [WWW_97], maximale Menge an Text eingebettet, Fotos aus [Fran_96, FrPf_97]). Die jeweils dargestellten Differenzbilder zeigen, daß die steganographische Veränderung von Bild 2 so minimal ist, daß sie auch natürliche Ursachen gehabt haben kann; es handelt sich zwar um ein verändertes Bild, dessen natürliche Eigenschaften wurden jedoch nicht verändert.

Die obigen Ausführungen zeigen, daß nicht jede Hülle gleichermaßen geeignet ist, um Steganographie zu betreiben. Insbesondere digitale Hülldaten, die *keinen* solchen natürlichen „Unsicherheits“-Prozeß (Scannen, Quantisieren) durchlaufen haben, eignen sich nicht besonders gut als Hülle (beispielsweise ausschließlich am Rechner erstellte Grafiken, Sounds und Animationen). In der Praxis stellt sich diese Einschränkung für die Betreiber von Steganographie jedoch nicht als Hindernis dar, da sie die Hülldaten selbst wählen können. Gerade multimediale Rohdaten (digitalisierte Sounds, Videos, gescannte

Bilder etc.) eignen sich hervorragend als Hülldaten für Steganographie. Selbst ISDN-Telefongespräche sind geeignet, um Steganographie zu betreiben [MöPS_94].

Falls nicht bewiesen werden kann, daß sich die Einbettung stets innerhalb des Unsicherheitsbereiches bewegt, muß beispielsweise durch eine vorgeschaltete Analyse (der Hülle und ggf. des einzubettenden Textes) und probeweise Einbettung mit nachgeschalteter Bewertung des Ergebnisses festgestellt werden, ob die Unbeobachtbarkeit der verdeckten steganographischen Kommunikation noch erhalten bleibt (vgl. auch [ZFPW_97]).

Die Algorithmen „Einbetten“ und „Extrahieren“ sollten immer öffentlich bekannt sein, wie man das von starker Kryptographie her kennt. Deshalb müssen sie mit einem Schlüssel „parametrisiert“ werden, um eine Entdeckung zu verhindern.

Interessant ist, daß der einzubettende Text nicht unbedingt verschlüsselt vorliegen muß. Da gute Steganographie ja nicht erkennbar ist, kommt auch niemand (außer dem gewünschten Empfänger) in Kenntnis des eingebetteten Textes. Trotzdem kann es sinnvoll sein, einen einzubettenden Text vor dem eigentlichen Einbettungsprozeß zu verschlüsseln. Hierbei steht allerdings weniger das „Unleserlichmachen“ eines Textes im Vordergrund. Vielmehr besitzen gute Verschlüsselungssysteme die Eigenschaft, daß verschlüsselter Text die Eigenschaften von gleichverteilten Zufallszahlen besitzt und von natürlichem Rauschen nicht unterscheidbar ist.

Nutzt man aber gerade ein in der Hülle enthaltenes natürliches Rauschen (beispielsweise der niederwertigsten Bits, sog. Least Significant Bits, LSBs) aus, um Steganographie zu betreiben, gestaltet sich der eigentliche Einbettungsprozeß sehr einfach, indem das natürliche Rauschen durch das künstliche Rauschen (d.h. den verschlüsselten Text) ersetzt wird (siehe Abbildung 3). Ein Stego-Schlüssel erübrigt sich in diesem Fall bzw. dessen Funktion wird von dem Kryptoschlüssel erbracht. Nur der intendierte Empfänger kann den Klartext extrahieren, da nur er den kryptographischen Schlüssel der vorgeschalteten Verschlüsselung besitzt.

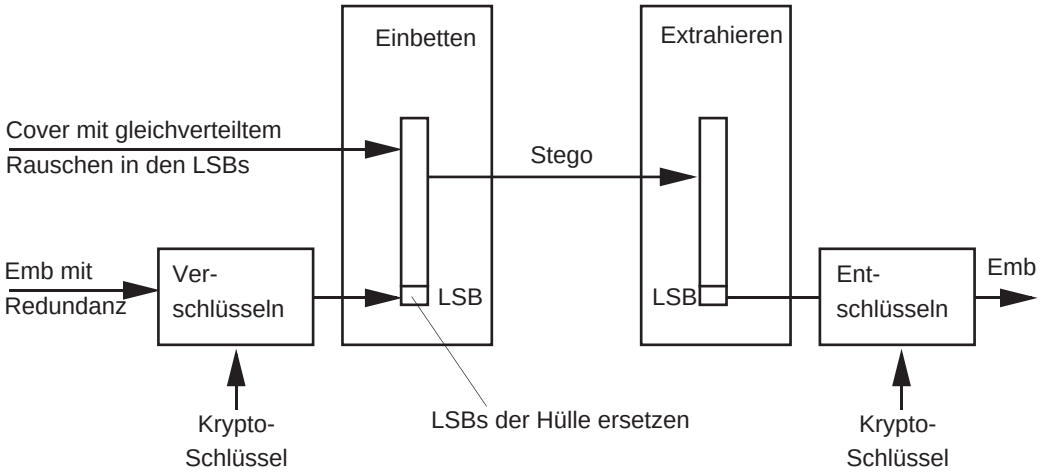

Abbildung 3: Stegosystem mit vorgeschalteter Verschlüsselung

Selbst mit leistungsfähiger Hard- und Software ist Steganographie nicht erkennbar. Der Nutzer von Steganographie muß jedoch unbedingt beachten, daß er die Hülle unwiederbringlich vernichtet. Ein direkter Vergleich gäbe sofort Anhaltspunkte für die Verwendung von steganographischer Nachrichtenübermittlung.

3 Steganographie und Multimediakommunikation

Welche Möglichkeiten Steganographie im Kontext multimedialen Informationsaustausches bietet, wurde auf der CeBit im Rahmen der Ausstellung des Kollegs „Sicherheit in der Kommunikationstechnik“ vorgeführt.

Mit Hilfe eines simulierten Videokonferenzsystems wurde demonstriert, wie in bewegten Bildern Steganographie betrieben werden kann. Die einzubettenden Informationen konnten vom Messebesucher über die Tastatur eingegeben werden und wurden sofort in das Videobild eingebettet.

Da der implementierte Algorithmus nur dann einbettet, wenn die Eigenschaften des Bildes dies zulassen, konnte sich der Besucher ebenfalls davon überzeugen, daß nicht jede Hüllinformation gleichermaßen geeignet ist, um Steganographie zu betreiben.

Um die Wirkung der Einbettung noch deutlicher sichtbar zu machen, wurde im vorgestellten Demonstrator nebenbei ein Differenzbild des originalen, digitalisierten Kamerabildes und des steganographisch veränderten Bildes berechnet und angezeigt.

Abbildung 4 zeigt einen Screenshot des Steganographie-Demonstrators. Der vorgestellte Demonstrator beruht auf einer Entwicklung von Andreas Westfeld, die im Rahmen seines Informatikstudiums [West_96] entstand. Für die CeBit wurden von ihm einige

Veränderungen vorgenommen, um die intern ablaufenden Prozesse besser sichtbar zu machen.

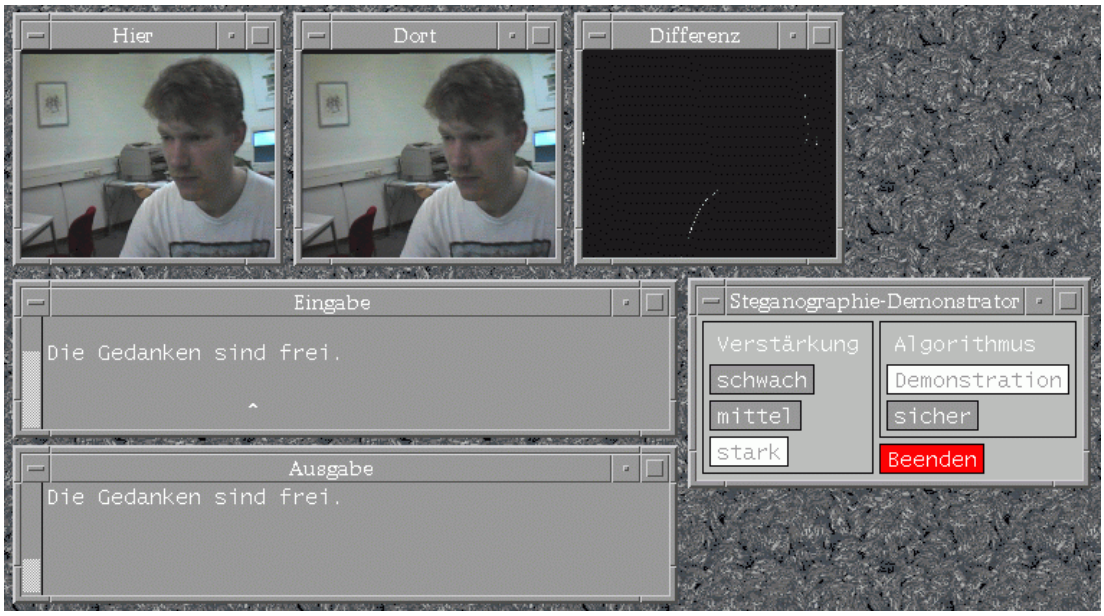

Abbildung 4: Der Steganographie-Demonstrator auf der CeBit'97

4 Steganographie in komprimierten Videoströmen

Im folgenden Abschnitt wird das in [West_96] entwickelte und implementierte Verfahren kurz erläutert. Alle neu entwickelten Teile der steganographischen Videokonferenz wurden in Software unter UNIX realisiert.

Das Verfahren basiert auf einer H.261-Videokonferenz. H.261 [CCITT_90] ist ein Standard zur symmetrischen Echtzeitkompression und -dekompression von Videosequenzen. Die Funktionsblöcke einer H.261-Videokonferenz werden in Abbildung 5 dargestellt. Es wurde gleichzeitig gekennzeichnet, an welcher Stelle des Signalweges die Einbettung und Extraktion erfolgt.

Die Einbettung der steganographischen Informationen in das Videobild erfolgt nach der Diskreten Kosinustransformation (DCT) und der verlustbehafteten Quantisierung. Die DCT und Quantisierung entfernt die für das menschliche Auge unwesentlichen Teile eines Bildausschnittes (im konkreten System aus einem 8×8 Pixelfeld). Auf der Empfängerseite kann deshalb nicht das originale 8×8 Pixelfeld rekonstruiert werden, sondern nur eine Annäherung dessen. Die nachfolgenden Teile der Kodierung sind verlustfrei (Huffman- bzw. Lauflängenkodierung).

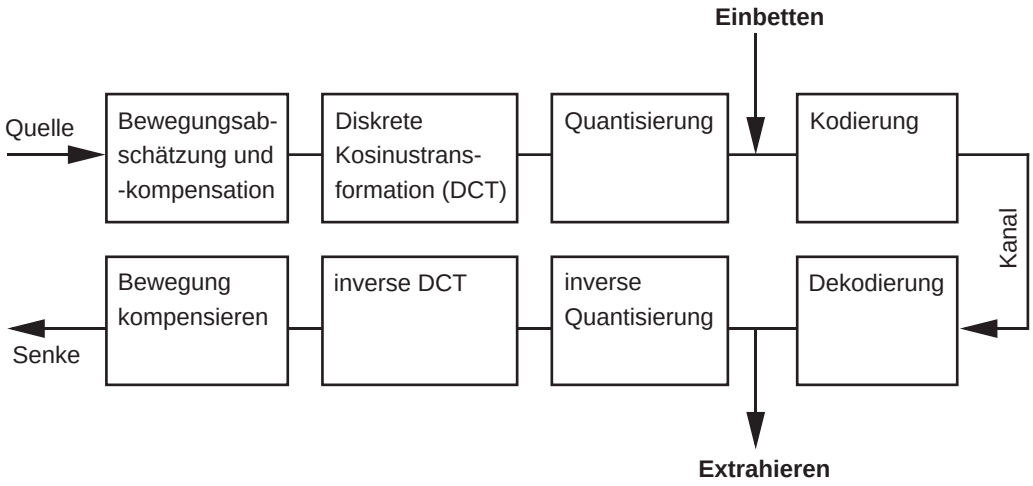

Abbildung 5: H.261-Funktionsblöcke (vereinfacht)

Der natürliche Prozeß, der zur Einbettung steganographischer Informationen ausgenutzt wird, beruht primär

- auf der natürlichen Reproduktionsungenauigkeit einer CCD-(Charge Coupled Device)-Kamerazeile: Eine minimale horizontale Verschiebung des Bildes um Bruchteile eines Pixels führt zu deutlichen Änderungen des Frequenzspektrums und damit der Koeffizienten der DCT. Entsprechende Berechnungen finden sich in [West_96].
- auf der Phasenverschiebung und Dämpfung sowie dem Einfluß von externen Störungen auf der Verbindungsleitung zwischen Kamera und Video-In-Karte des Rechners: Die horizontalen Bildinformationen des von der Kamera gelieferten analogen Videosignals sind sehr breitbandig (6 MHz) und daher auch recht störanfällig.

Weitere, für die spezielle Implementierung eher untergeordnete „Unsicherheitsprozesse“, z.B. Halbleiterrauschen der analogen Bauelemente des Signalweges, Unsauberkeiten des Objektivs etc. tragen dazu bei, daß der implementierte Einbettungsalgorithmus eher defensiv bzgl. der Menge einbettbarer Daten arbeitet. Trotzdem gestattet der Algorithmus bereits die Einbettung mit einer Datenrate von mehreren kBit/s, so daß ein komprimiertes Telefongespräch in einer Videokonferenz Platz hätte.

5 Watermarking

Mit Steganographie können neben der geheimen Nachrichtenübermittlung auch Urheberrechte in digitalen Informationen geschützt werden.

Watermarking bezeichnet einen Vorgang, bei dem ein digitales Objekt mittels steganographischer Techniken verändert wird, um Rechte an diesem Objekt zu schützen. Das Objekt, welches z.B. ein Text, eine Grafik, eine Audiodatei bzw. ein Video sein

kann, wird dabei möglichst *robust* (persistent gegenüber Transformationen) und *nicht beeinträchtigend* gekennzeichnet, ähnlich wie Papier mit einem Wasserzeichen (daher „Watermark“). Das Kennzeichen muß trotzdem *nachweisbar* sein.

Damit sind schon die Kriterien gegeben, die ein „digitales Watermark“ zu erfüllen hat. Sie ähneln in gewissem Maße denen, die bei steganographisch geschützter Kommunikation zu erfüllen sind, weisen dazu aber auch charakteristische Unterschiede auf, wie folgender Vergleich zeigt.

Watermarking zum Schutz von Rechten an dig. Objekten	**Steganographie** zur vertraulichen Kommunikation
Robustheit des eingebetteten Watermarks	**Robustheit** der eingebetteten (zu schützenden) Nachricht
Beeinträchtigungslosigkeit gegenüber dem (zu schützenden) Objekt	**Beeinträchtigungslosigkeit** gegenüber dem Träger
Nachweisbarkeit des Watermarks durch Dritte	**Nichtnachweisbarkeit** der eingebetteten Nachricht durch Dritte

Tabelle 1: Kriterien bei Watermarking und Steganographie

Die Zielstellungen des Watermarking unterscheiden sich grundlegend von denen der vertraulichen Kommunikation mittels Steganographie. Letztere kann dahingehend präzisiert werden, daß hier die Tatsache der Existenz von Kommunikation (und damit insbesondere auch deren Vertraulichkeit) geschützt wird, während Watermarking Rechte, insbesondere Urheber- oder Eigentumsrechte, an digitalen Dokumenten schützt. Die Bedeutung eines solchen Schutzes digitaler Objekte, die ja identisch kopierbar und damit in Originalform verbreitbar sind, gewinnt besonders bei kommerzieller Nutzung digitaler Medien an Bedeutung.

Um zu gewährleisten, daß ein mit einem Watermark versehenes Dokument nicht unberechtigterweise so transformiert werden kann, daß das Watermark dabei entfernt wird und das Original (nahezu) unversehrt zurückbleibt, muß es eine große Widerstandsfähigkeit gegen Bearbeitungsschritte wie Formatkonvertierung, verlustbehaftete Kompression, Filterung, Resampling, Subtraktion (z.B. durch Abschneiden), Rotation, Spiegelung usw. aufweisen.

Es ist klar, daß das Watermark möglichst so in das digitale Objekt eingebracht werden muß, daß es nicht zu Beeinträchtigungen des Dokumentes kommt. Wann eine Beeinträchtigung vorliegt, wird durch den Nutzungszweck und die daraus folgende Rezeptionsweise des Dokumentes bestimmt. So sollten Watermarks in Grafiken bzw. Videos nicht sichtbar, in Sounddateien nicht hörbar sein. Voraussetzung ist, daß das Dokument selbst genügend Irrelevanz aufweist, die ein schadloses Einbetten zuläßt.

Ein eingebettetes Watermark muß nachweisbar sein, damit illegale Kopien aufgedeckt werden und in der Folge z.B. Konventionalstrafen verhängt werden können. Davon zu trennen ist die Warnfunktion, die z.B. durch eine Mitteilung wie „dieses Werk ist

urheberrechtlich geschützt“ erfüllt wird. Während die Warnfunktion jedem zugänglich sein muß, ist der Nachweis eines Watermarks nur dazu bestimmten Instanzen, z.B. einer dem Patentamt vergleichbaren Registrierungsinstanz, vorbehalten. Denkbar ist jedoch eine Verkettung der Warnfunktion mit dem Watermark, je nachdem, ob jeweils zum Nachweis, zum Aufbringen bzw. zum Entfernen geheime Schlüssel im Sinne der Kryptographie notwendig sind oder nicht.

Die Kriterien, die ein Watermarkingsystem erfüllen muß, stellen hohe Anforderungen an die Algorithmen, da sie untereinander um so stärker konkurrieren, je weniger Redundanz durch das Original zur Verfügung gestellt wird. Technisch gesehen können wie bei Steganographie zufällige Rauschanteile im Original für Watermarking genutzt werden.

Gegenwärtige Watermarkingtechniken arbeiten bevorzugt im Frequenzbereich (neben Raum- und Zeitbereich), den die digitalen Objekte abdecken [Zhao_97]. Dazu werden sog. Spread Spectrum Techniken eingesetzt. Die Information zur Authentikation, die das Watermark trägt, ist vom Einsatzzweck (Urheberrechts- oder Eigentumrechtsschutz) und der zur Verfügung stehenden Infrastruktur abhängig. Das kann eine Dokument-ID sein (z.B. *Fingerprint*) oder der Name des Autors.

6 Zusammenfassung

Steganographische Verfahren sind in der Lage, noch weitergehende Schutzziele als Datenverschlüsselung mit Hilfe von Kryptographie zu erreichen.

Steganographie zur Konzelation kann folgende Schutzziele erfüllen:
- vertraulicher Austausch von Nachrichteninhalten,
- Unbeobachtbarkeit des Austausches der eingebetteten Nachrichten.

Während aus der Literatur bekannte Verfahren zur Unbeobachtbarkeit der Kommunikation (z.B. [Chau_81, Chau_88, Pfit_90]) das gewünschte Schutzziel *direkt* erreichen, nimmt Steganographie den „Umweg“ über eine unverfängliche, für jeden lesbare und beobachtbare Hülle.

Steganographie zur Authentikation leistet folgenden Schutz:
- Schutz der Authentizität digitaler Objekte,
- Nachweisbarkeit der Urheberschaft digitaler Werke.

Dabei bleibt die Nachweisbarkeit der Urheberschaft digitaler Objekte selbst bei digitaler (und ggf. auch analoger) Veränderung des zu schützenden Werkes erhalten (vgl. auch die in [BGML_96] formulierten Eigenschaften). Dies kann beispielsweise durch sog. Spread Spectrum Watermarking erreicht werden [CKLS_95].

Der wirksame Schutz von Geschäfts-, Berufs- und Privatgeheimnissen wird durch Kryptoreglementierung stark abgeschwächt oder gar unmöglich gemacht. Trotz einer Reglementierung oder eines Verbotes von Kryptographie können mittels Steganographie unbeobachtbar und unbeweisbar geheime Nachrichten ausgetauscht werden. Man müßte also Steganographie in die Reglementierung einbeziehen. Die Einhaltung der Bestimmungen eines solchen Gesetzes wäre allerdings nicht umfassend kontrollierbar. Folglich lohnt sich Kryptoreglementierung nicht.

Dank

Diese Arbeit wurde finanziell unterstützt von der Gottlieb-Daimler- und Karl Benz-Stiftung Ladenburg sowie dem Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF). Für Kommentare, Anregungen und Diskussionen danken wir besonders Elke Franz, Herbert Klimant, Marit Köhntopp, Andreas Pfitzmann und Dagmar Schönfeld. Besonders danken möchten wir Andreas Westfeld, dessen Demonstrator viel dazu beigetragen hat, Steganographie anschaulich zu machen.

Literatur

BGML_96 W. Bender, D. Gruhl, N. Morimoto, A. Lu: Techniques for Data Hiding. IBM Systems Journal, 35/3&4 (1996).

CCITT_90 CCITT Recommendation H.261: Video Codec for Audiovisual Services at $p \times 64$ kbit/s, Genf 1990.

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology 1/1 (1988) 65-75.

CKLS_95 I. Cox, J. Kilian, T. Leighton, T. Shamoon: Secure Spread Spectrum Watermarking for Multimedia. NECI Technical Report 95-10, NEC Research Institute, Princeton, NJ (1995).

Fran_96 Elke Franz: Untersuchung von Bewertungsmöglichkeiten für Bilder bezüglich eingebettteter steganographischer Daten. Großer Beleg, TU Dresden, Institut für Theoretische Informatik, Dezember 1996.

FrPf_97 Elke Franz, Andreas Pfitzmann: Ableitung eines neuen Stegoparadigmas mit Hilfe empirischer Untersuchungen. Arbeitspapier, 1997.

MöPS_94 Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist. Datenschutz und Datensicherung DuD 18/6 (1994) 318-326.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Berlin 1990.

West_96 Andreas Westfeld: Steganographie am Beispiel einer Videokonferenz. erscheint in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley 1997.

WWW_97 Eric Milbrandt: Steganography Info and Archive. http://www.iquest.net/~mrmil/stego.html, 1997.

ZFPW_97 J. Zöllner, H. Federrath, A. Pfitzmann, A. Westfeld, G. Wicke, G. Wolf: Über die Modellierung steganographischer Systeme. Eingereicht für VIS'97, 30.9.-2.10.97, Freiburg/Brsg.

Zhao_97 Jian Zhao: Look, it's not there. Byte 22/1 (1997) 7-12.