IT-Sicherheit 3/3 (1997) 10-13.

Steganographie zur vertraulichen Kommunikation

Hannes Federrath, Elke Franz, Andreas Westfeld, Guntram Wicke

TU Dresden, Fakultät Informatik, 01062 Dresden

Zusammenfassung

Auf der CeBit'97 zeigten Mitarbeiter der Fakultät Informatik der TU Dresden im Rahmen einer Ausstellung des Ladenburger Kollegs „Sicherheit in der Kommunikationstechnik“ der Gottlieb Daimler - und Karl Benz-Stiftung einen Demonstrator für Steganographie. Er veranschaulicht, daß sich mit Steganographie eine nicht nachweisbare vertrauliche Kommunikation realisieren läßt.

Motivation

Motivation für die Entwicklung eines Steganographie-Demonstrators war die aktuelle politische Diskussion in Deutschland über das Verbot bzw. die Reglementierung von Verschlüsselung zum Zwecke der effektiveren Verbrechensbekämpfung. Es sollte gezeigt werden, daß es trotz Kryptoreglementierung möglich wäre, geheime Daten unbeobachtet über Kommunikationsnetze zu senden, und daß die Situation der Strafverfolgungsbehörden damit sogar erheblich verschärft würde, da Kriminelle auf solche unbeobachtbaren Kommunikationsmittel ausweichen könnten.

Funktionsweise steganographischer Systeme

Nachrichten vor unerwünschter Kenntnisnahme zu schützen, ist nicht ausschließlich durch Verschlüsselung möglich: Eine weitere Methode besteht darin, die Nachricht bei der Übertragung so zu tarnen, daß sie von Dritten gar nicht bemerkt wird (Steganographie). Solche Techniken lassen sich effizient bei modernen Kommunikationsmedien einsetzen, z.B. bei einer Videokonferenz. Sie könnten eine durch Kryptoreglementierung eingesetzte kostspielige Überwachung wirkungslos werden lassen [HuPf_96]. Durch effektive Steganographie wird es Dritten unmöglich, vertrauliche Nachrichten zu finden. Die zu schützende Nachricht Emb wird vom Sender in einer anderen, längeren harmlosen Nachricht Cover (z.B. GIF-Bild oder Videodatenstrom) geeignet versteckt, siehe Abb. 1. Im Ergebnis dieses Einbettens wird Stego übertragen. Der Empfänger gewinnt durch Extrahieren Emb zurück.

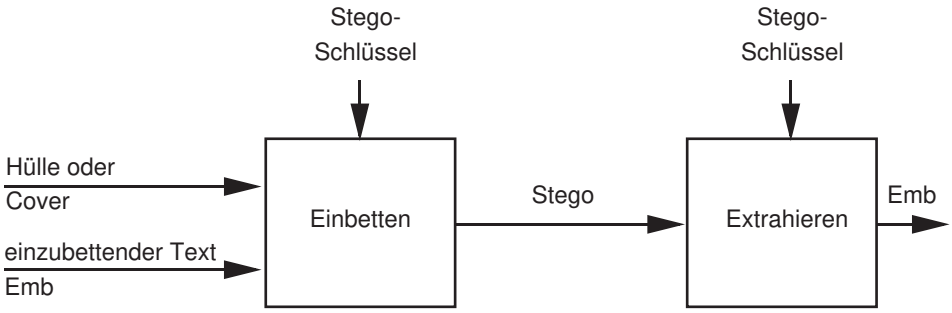

Abb. 1: Stegosystem

Bei Parametrisierung durch Schlüssel sind solche Verfahren auch in offenen Benutzergruppen wie bisherige Verschlüsselungstechniken verwendbar, da das Verfahren öffentlich bekannt sein darf und die Teilnehmer über geheime Schlüssel verfügen.

Abb. 2 demonstriert das Ergebnis eines in Software implementierten steganographischen Systems (kurz: Stegosystems). Das linke Bild ist das Original; das Ergebnis des Einbettens einer geheimzuhaltenden Nachricht, hier bestehend aus ASCII-Text, zeigt das Stegobild in der Mitte. Ein Differenzbild rechts verdeutlicht die Unterschiede zwischen beiden Bildern. Wie man sieht, wurden die Änderungen vom Stegoprogramm auf dem ganzen Bild verteilt. Da es sich dabei nur um geringe Änderungen handelt, sind die Differenzen mit bloßem Auge gar nicht zu erkennen.

Abb. 2: Vergleich zwischen Cover und Stego

Bei dem verwendeten Bild handelt es sich um ein sehr günstiges Medium für Steganographie. Die Farben sind nicht klar, es gibt keine scharfen Konturen. Ein Bild, das aus einfarbigen Flächen besteht, stellt ein größeres Problem für ein Stegoprogramm dar – abweichende Pixel können viel eher auffallen. Ganz extrem ist natürlich ein reines Schwarzweißbild, etwa eine technische Zeichnung. Meist ist der Sender einer geheimen Nachricht jedoch in der Lage, ein „passendes“ Cover zu wählen.

Angriffe auf Stegosysteme

Um dem Ziel der Steganographie – Gewährleistung einer unbemerkten und vertraulichen Kommunikation – gerecht zu werden, müssen Stegoprogramme verschiedenen Angriffen widerstehen. Die folgende Abbildung demonstriert mögliche Angriffspunkte.

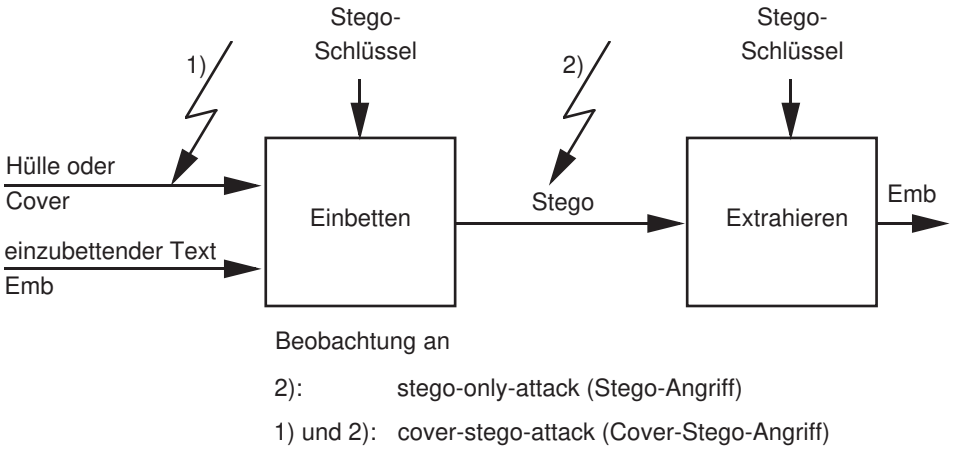

Abb. 3: Angriffspunkte auf Stegosysteme

Es ist naheliegend, diese Angriffe mit entsprechenden Angriffen auf Kryptosysteme zu vergleichen (Tab. 1).

Stegosystem	**Kryptosystem**
stego-only-attack (Stego-Angriff)	ciphertext-only-attack (Reiner Schlüsseltext-Angriff)
cover-stego-attack (Cover-Stego-Angriff)	known-plaintext attack (Klartext-Schlüsseltext-Angriff)

Tab. 1: Vergleich der Angriffsarten

Bei der Verwendung von Steganographie muß auf alle Fälle mit einem Stego-Angriff gerechnet werden. Beim Übertragen der Stegodaten kann es natürlich passieren, daß diese einem Angreifer in die Hände fallen. Dieser steht nun vor dem Problem, zu entscheiden, ob es sich bei den abgefangenen Daten wirklich um Stegodaten handelt, d.h. ob in den Daten wirklich etwas eingebettet ist. Diese Form des Angriffs stellt geringere Anforderungen an die Stegosysteme, denn ohne Vergleichsdaten ist eine solche Entscheidung schwierig zu treffen.

Würde es sich bei den verwendeten Hülldaten beispielsweise um Bilddateien handeln, so müßte der Angreifer aus der Kenntnis eines einzelnen Bildes heraus entscheiden, ob es eingebettete Daten enthält. Die Schwierigkeit besteht darin zu definieren, wie ein Bild

„normalerweise“ aussehen soll. Auf einem Bild könnte jedes beliebige Motiv dargestellt werden, die Helligkeiten und die Farben können beliebig und zur Erreichung besonderer Effekte sogar besonders ungewöhnlich gewählt werden. An einem einzelnen Bild könnten lediglich Einzelheiten entdeckt werden, welche dem Betrachter auffällig erscheinen. Das könnten z.B. farblich stark abweichende Pixel einer ansonsten einfarbigen Fläche oder ausgefranste Linien in einem Bild mit ansonsten klaren Konturen sein.

Damit ein Stegosystem Stego-Angriffen widerstehen kann, darf es also keine Änderungen an den Hülldaten vornehmen, welche einem Angreifer auffallen könnten.

Schärfere Anforderungen an das Stegosystem ergeben sich bei Betrachtung eines Cover-Stego-Angriffs. Dem Angreifer könnte es beispielsweise gelungen sein, in den Rechner des Benutzers des Stegosystems einzubrechen und dort an die nicht vernichteten Hülldaten zu gelangen. Nun kann er leicht einen bitweisen Vergleich durchführen und jede Änderung feststellen. Natürlich kann der Angreifer nicht sicher sein, daß es sich bei den beiden Exemplaren wirklich um Cover und Stego handelt. Um bei den Bilddateien zu bleiben, könnte man sich vorstellen, daß er (statt Cover und Stego) zwei Bilddateien vergleicht, die durch mehrmaliges Scannen entstanden sind. Da der Scanprozeß mit einem Indeterminismus behaftet ist, werden sich die bei mehrmaligem Scannen entstehenden Bilddateien nie exakt gleichen.

Die Chance des Stegosystems besteht nun darin, mit dem Einbetten einen natürlichen Prozeß nachzubilden, so daß die Differenzen zwischen Hülldaten und Stegodaten auch durch eben diesen Prozeß entstanden sein könnten. Um auch Cover-Stego-Angriffen widerstehen zu können, muß das Stegosystem also so operieren, daß seine Änderungen plausibel erscheinen.

Steganographische Videokonferenz

Mit Steganographie ist es auch möglich, vertrauliche Daten in einer Videokonferenz zu verstecken. Die Bilder der Videokonferenz werden dabei so verändert, daß es für einen Angreifer unmöglich ist zu entscheiden, ob in den Videosequenzen zusätzliche Daten verborgen wurden.

Auf der CeBit’97 wurde eine Lösung zu Demonstrationszwecken vorgestellt.

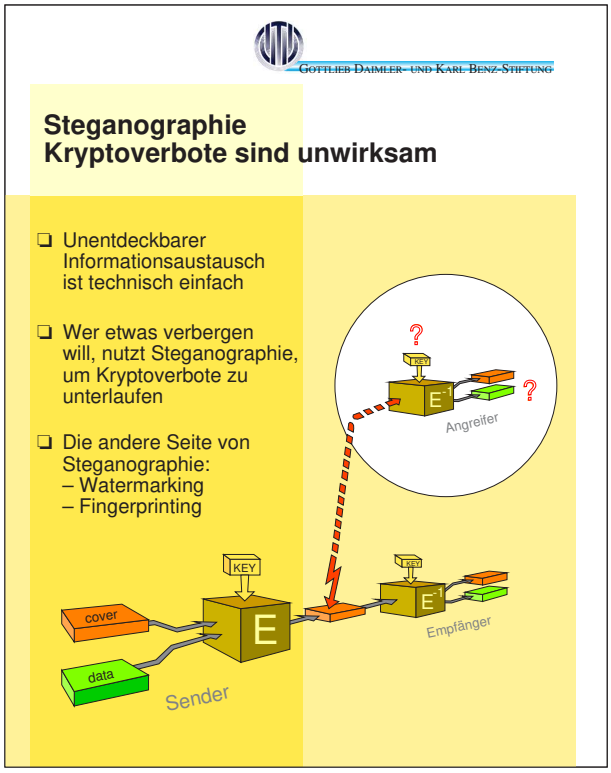

Abb. 4: Zweck des Demonstrators war die Sensibilisierung der Messebesucher

Videokonferenzen verwenden verlustbehaftete Kompressionsverfahren, um das Datenvolumen für die Übertragung zu reduzieren. Für das menschliche Auge unwesentliche Signalanteile sowie Rauschanteile werden dadurch entfernt. Das erschwert einen unentdeckbaren Eingriff in das Signal. Dennoch kann man nichtdeterministische Eigenschaften des Signals ausnutzen, die vom Kompressionsalgorithmus nicht beeinflußt werden. Solche Eigenschaften wurden z. B. bei der Untersuchung der Kamera gefunden, denn Kompressionsalgorithmen werden anpassungsfähig konstruiert und sind unabhängig von den Eigenheiten der Eingabegeräte.

Fügt man in ein steganographisches System eine bestimmte Videokamera ein, so kann man Eigenschaften dieser Kamera für das Einbetten von geheimen Daten ausnutzen.

Da die Kamera das Bild zeilenweise aufbaut, werden die Bildpunkte vertikal im festen Raster der Zeilen positioniert, während sie horizontal nur durch Zeilensynchronimpulse aneinander ausgerichtet werden und keine diskrete Position erhalten. Für die Darstellung von zwei vertikal benachbarten Bildpunkten steht 800 mal mehr Zeit zur Verfügung wie für die Darstellung zweier horizontal benachbarter Bildpunkte. Deshalb ist eine wesentlich größere Bandbreite für horizontale Videofrequenzen nötig. Sowohl das von der Bandbreite bestimmte größere Rauschen als auch die Synchronisierungstoleranzen wirken sich auf die horizontale Lage der Bildpunkte aus.

Als Bildwandler wird ein CCD-Element verwendet, eine Matrix lichtempfindlicher Sensoren, die hinter einem Filter mit feinen Farbstreifen angeordnet sind. Je drei

nebeneinander liegende Sensoren für rot, grün und blau werden zu einem Bildpunkt zusammengefaßt. Auch hier wird ein horizontaler Abstand vernachlässigt.

Diese Effekte werden für steganographische Zwecke künstlich nachgebildet, indem die horizontale Lage der Bildinhaltes in gewissen Grenzen verändert wird. Es entstehen dabei nur Bilder, die die Kamera ohnehin hätte liefern können. Das Signal wird weder untypisch noch auffällig verändert. Das unveränderte Bild wird nicht mit übertragen, so daß ein Angreifer diese Veränderung nicht wahrnehmen kann.

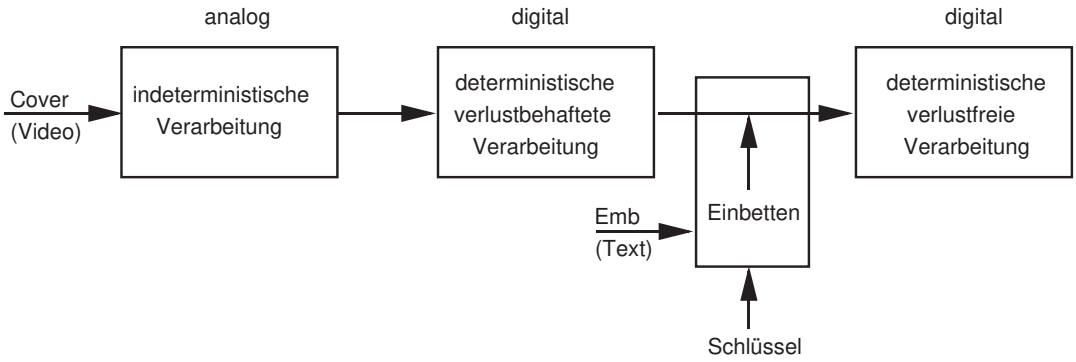

Abb 5: Einbetten in einer Videokonferenz

Die geheimen Daten werden nach der verlustbehafteten Kompression eingebettet (siehe Abb. 5). So spart man eine fehlerkorrigierende Kodierung für den einzubettenden Text. Dabei ist allerdings zu beachten, daß das Bild durch die diskrete Kosinustransformation [Mild_96], die den Kern der gängigen Kompressionsstandards wie MPEG, JPEG oder H.261 bildet, in Frequenzanteile gewandelt wird. Die Videofrequenzen des Bildes liegen nach der Kompression in kleineren Blöcken variabler Größe von 1-64 Koeffizienten vor.

Nicht in jeden dieser Blöcke kann etwas eingebettet werden. Ideal geeignet sind die Koeffizientenblöcke kontrastreicher Bilder. Sowohl beim Sender als auch beim Empfänger werden die Koeffizientenblöcke in „gute“ (steganographisch verwendbare) und „schlechte“ (zu ignorierende) Blöcke eingeteilt. Jeder gute Block trägt ein eingebettetes Bit als Modulo-2-Summe (Parität) seiner Koeffizienten vom Sender zum Empfänger. Nur wenn die Parität vom einzubettenden Bit abweicht, muß der Block geändert werden. Dabei wird der Koeffizient ausgesucht, der sich bei horizontaler Verschiebung des Bildinhaltes am stärksten ändert. Man kann zeigen, daß das nie der betragsmäßig größte Koeffizient im Block ist. Dadurch bleibt das Kriterium „guter Block“ für den Empfänger von der Veränderung unangetastet. Der ausgesuchte Koeffizient wird um 1 verändert und damit die Parität des Blockes gekippt. Der Empfänger extrahiert die steganographisch übermittelte Nachricht, indem die Modulo-2-Summen der guten Blöcke aneinandergereiht werden.

Vertrauenswürdig sind nur öffentliche, wohluntersuchte Algorithmen. Bei öffentlichen Verfahren ist es nötig, das Geheimnis vom Algorithmus zu trennen. Die einfachste Möglichkeit ist, eine Pseudozufallsbitfolge durch einen geheimen Schlüssel gesteuert zu

erzeugen, die sowohl beim Sender als auch beim Empfänger mit den einzubettenden Bits verknüpft wird. Die Paritätsbits sind statistisch gleichmäßig zufällig verteilt (sowohl mit als auch ohne die eingebetteten Daten), so daß ein Angreifer durch Untersuchung der übertragenen Daten nicht entscheiden kann, ob es sich um eine gewöhnliche Videokonferenz handelt oder ob vertrauliche Daten eingebettet wurden.

In eine ISDN-Videokonferenz (H.261) läßt sich ein GSM-Telefonat (8 kbit/s) einbetten. Aus Abb. 6 wird die Oberfläche des auf der CeBIT'97 gezeigten Demonstrators ersichtlich.

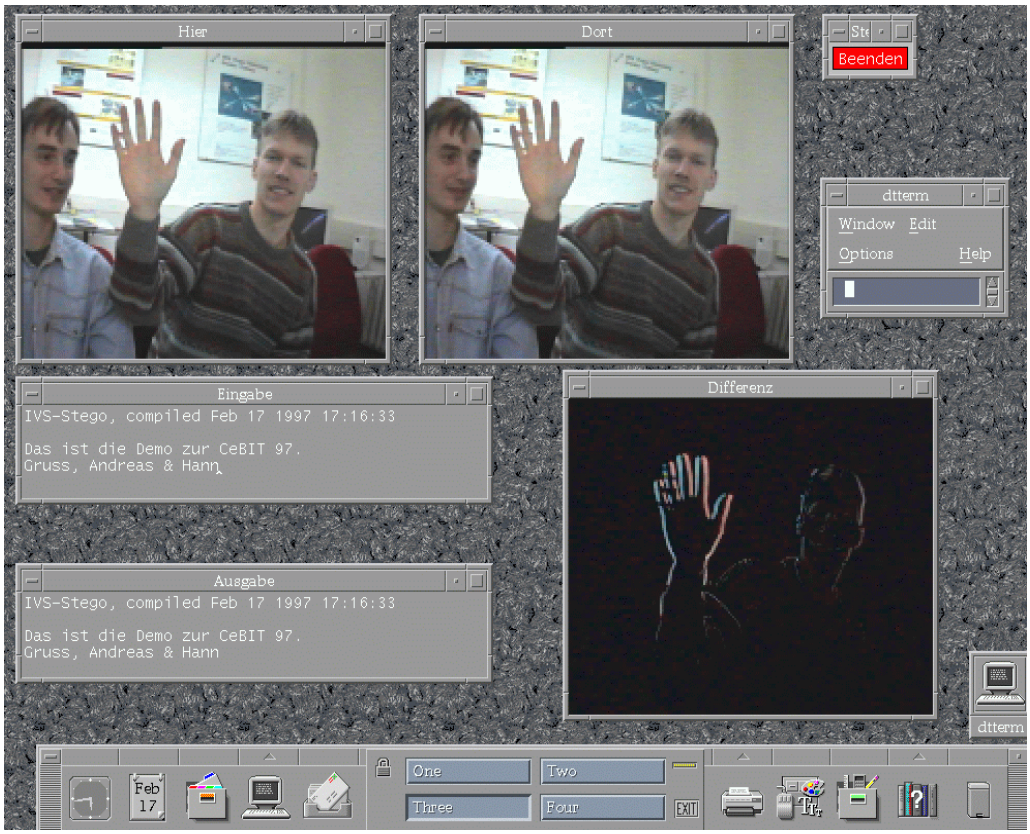

Abb. 6: Oberfläche des Demonstrators

Schlußbemerkungen

Wie das anhand einer Videokonferenz beispielhaft umgesetzte Steganographiesystem gezeigt hat, ist es realistisch, davon auszugehen, daß Steganographie effektiv und effizient zur vertraulichen Kommunikation eingesetzt werden kann. Stegosysteme können so implementiert werden, daß sie gegen die dargestellten Angriffe wirksam schützen und keinen wesentlich erhöhten Aufwand in der Kommunikation mit sich bringen. Steganographie stellt deshalb ein ernstzunehmendes Argument gegen eine gesetzliche Reglementierung von Kryptographie dar. Die Einhaltung eines Verbotes würde sich gerade in den kritischen Fällen der Nutzung von Steganographie durch die organisierte

Kriminalität jeglicher Kontrolle entziehen. Sanktionen, die nicht greifen können offenbaren, daß Kryptoreglementierung zur effektiven Verbrechensbekämpfung ungeeignet ist.

Literatur

[HuPf_96] Michaela Huhn, Andreas Pfitzmann: Technische Randbedingungen jeder Krypto-regulierung. In: Datenschutz und Datensicherheit (DuD) 20/1 (1996) 23-26.

[Mild_96] Torsten Milde, Videokompressionsverfahren im Vergleich: JPEG, MPEG, H.261, Verlag Dpunkt, Heidelberg, 1996.