Proc. Verläßliche IT-Systeme (VIS'97), DuD Fachbeiträge, Vieweg-Verlag 1997, 211-223

Über die Modellierung steganographischer Systeme[♣]

J.Zöllner, H.Federrath**, A.Pfitzmann**, A.Westfeld**, G.Wicke**, G.Wolf**
Technische Universität Dresden, 01062 Dresden
**Institut für Betriebssysteme, Datenbanken und Rechnernetze*
***Institut für Theoretische Informatik*
{zoellner, federrath, pfitza, westfeld, wicke, g.wolf}@inf.tu-dresden.de

Zusammenfassung

Nach einer kurzen Einführung in die Steganographie und der Abgrenzung zu kryptographischen Systemen werden verschiedene Modellierungsmöglichkeiten für steganographische Systeme vorgestellt und hinsichtlich ihrer Allgemeingültigkeit diskutiert. Es wird ein allgemeines Modell für steganographische Konzelationssysteme abgeleitet. Weiterhin werden Bedingungen für sichere Steganographie formuliert.

1 Einführung

Sicherheitsanforderungen an Kommunikationssysteme werden meist durch eine Kombination von Vertraulichkeits-, Integritäts- und Verfügbarkeitseigenschaften beschrieben. Die Einhaltung bzw. Realisierung dieser Sicherheitseigenschaften wird durch Sicherheitsmechanismen garantiert. Mit Hilfe kryptographischer Systeme können vor allem die Eigenschaften Vertraulichkeit und Integrität gewährleistet werden. In diesem Kontext spielen vor allem Konzelationssysteme und Authentikationssysteme eine bedeutende Rolle. Konzelation beschreibt Funktionen zur Sicherung der *Vertraulichkeit des Inhaltes* geheimer Daten, während Authentikation die Richtigkeit (und Echtheit) von Information sicherstellen soll. Die zugrundeliegenden Mechanismen arbeiten mit der Verschlüsselung von Daten. Dieser Problematik widmet sich insbesondere die Kryptographie. Demgegenüber beschreibt Steganographie Funktionen zur Sicherung der *Vertraulichkeit der Existenz* von geheimen Daten.

[♣] Wir danken den Teilnehmern der „Stegorunde“ in Dresden, die nicht als Autoren auf diesem Papier erscheinen. Viele der hier dargestellten Ideen wurden in gemeinsamen Diskussionen erarbeitet und präzisiert. Diese Arbeit wurde finanziell unterstützt vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF) sowie der Gottlieb-Daimler- und Karl-Benz-Stiftung Ladenburg.

1.1 Steganographie - was ist das?

Bruce Schneier kennzeichnet Steganographie folgendermaßen [Schn_96, S. 10]: „Steganographie hat den Zweck, Nachrichten in anderen Nachrichten zu verstecken, um die bloße Existenz einer geheimen Botschaft zu verbergen“. Als historische Beispiele nennt er „...unsichtbare Tinte, winzige Einstiche in ausgewählten Buchstaben, kleinste Unterschiede in handgeschriebenen Zeichen, handschriftliche Markierungen auf getippten Buchstaben...“.

Steganographie ist also nicht neu, sie erfährt jedoch durch den Einsatz von Computer- und Multimediatechnik eine Renaissance. Besonders gilt dies für Grafik- und Audiodaten. In Abbildung 1 wird die Anwendung von Steganographie auf Grafikdaten veranschaulicht.

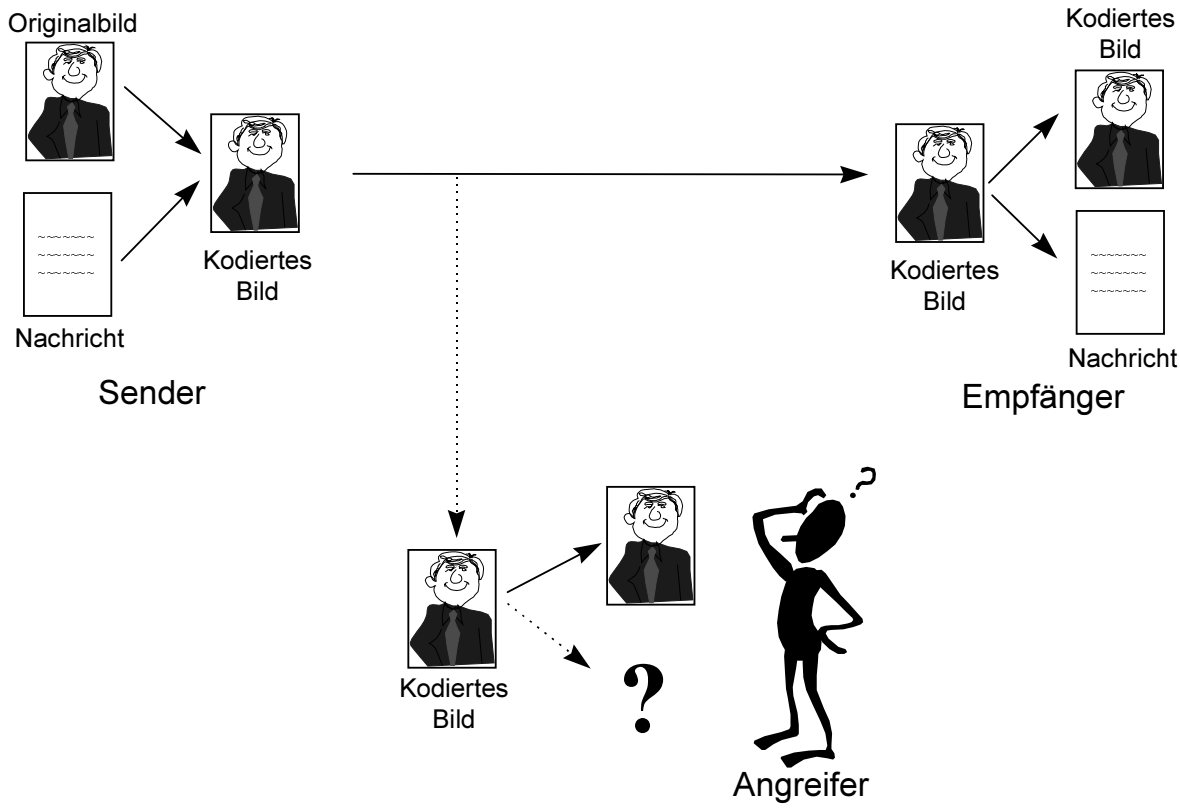


Abbildung 1: Steganographie am Beispiel von Grafikdaten

Auf der linken Seite ist zu sehen, daß der Sender der Nachricht diese in eine Grafikdatei einbettet. Die hier als „kodiertes Bild“ bezeichnete modifizierte Grafik wird zum rechts symbolisierten Empfänger übertragen. Dabei wird sie durch den Angreifer (unten) abgehört. Der Empfänger kann die eingebettete Nachricht aus dem kodierten Bild extrahieren, der Angreifer nicht. Das gelingt selbstverständlich nur, wenn zwischen Sender und Empfänger ein gemeinsames „Geheimnis“ existiert. Dies könnte der

Algorithmus zum Extrahieren sein oder bestimmte Algorithmenparameter, z.B. Schlüssel.

Wie sich bei Kryptosystemen schon oft zeigte, können Varianten, die sich auf die Geheimhaltung des Algorithmus zur Realisierung der Konzelation verlassen, in offenen Anwendungen nicht als langfristig sicher betrachtet werden. Vor allem bei großer Teilnehmerzahl ist die Geheimhaltung des Algorithmus schwierig. Es ist also notwendig, den (öffentlichen) Algorithmus mittels eines Schlüssels zu parametrisieren. Die Geheimhaltung dieses Schlüssels ist analog zu kryptographischen Systemen: sie ist essentiell für die sichere Anwendung des Systems.

Bei steganographischen Systemen kann man zwischen zwei Varianten mit unterschiedlichen Zielrichtungen unterscheiden:

1. Steganographie zum vertraulichen und versteckten Datenaustausch (siehe Abbildung 1) und
2. sogenanntes Watermarking, dessen Ziel es ist, mittels der eingebetteten Informationen Urheberschaft von digitalen Daten nachzuweisen.

Beide Varianten zielen darauf ab, die Originaldaten möglichst geringfügig zu verändern. Während jedoch bei 1. die Geheimhaltung der eingebetteten Daten oberste Priorität hat, kommt es bei den Watermarkingsystemen auf die robuste Anbringung des eingebetteten Kennzeichens an. Es darf durchaus sehr einfach nachweisbar sein, seine Entfernung soll jedoch ohne signifikante Beeinträchtigung der Originaldaten für alle außer den Eigentümer schwierig sein. Watermarking wird in diesem Papier nicht betrachtet.

1.2 Vertraulichkeit durch Geheimhaltungssysteme

Vertrauliche Nachrichtenübermittlung ist sowohl mit Steganographie als auch mit Kryptographie möglich. In beiden Fällen spielt Geheimhaltung eine bedeutende Rolle. Bei Konzelation im Sinne von Inhaltsdatenverschlüsselung soll eine geheime Botschaft vor einem Außenstehenden (Angreifer) vertraulich bleiben, während bei Steganographie sogar die Existenz einer solchen Botschaft verborgen bleiben soll.

Entsprechend lassen sich zwei Eigenschaften von Geheimhaltung definieren:

1. Konzelationseigenschaft: Ein Angreifer ist ohne Kenntnis eines Geheimnisses nicht in der Lage, an den Inhalt einer geheimen Botschaft zu gelangen.
2. Steganographische Eigenschaft: Ein Angreifer ist ohne Kenntnis eines Geheimnisses nicht in der Lage, in einer offenen Übermittlung (von Daten) die Existenz einer verborgenen Nachricht zu entdecken.

Durch diese Eigenschaften läßt sich beschreiben, wann ein Geheimhaltungssystem gebrochen ist. Bei Konzelationssystemen ist dies einfach: Ein Konzelationssystem ist gebrochen, wenn die Konzelationseigenschaft verletzt ist. Im Gegensatz dazu ist dieses Brechen bei einem steganographischen Konzelationssystem zweistufig:

1. Stufe: Ein steganographisches System ist gebrochen, wenn die steganographische Eigenschaft verletzt ist. Dies bedeutet jedoch nicht, daß der Angreifer den Inhalt der verborgenen Nachricht besitzt. Erst in einer zweiten Stufe kommt er in Kenntnis des Inhaltes:
2. Stufe: Zusätzlich gelingt es dem Angreifer, den Inhalt der verborgenen Nachricht aufzudecken. Dies entspricht der Verletzung der Konzelationseigenschaft.

Wir wollen annehmen, daß ein Brechen der 1. Stufe bereits genügt, um ein steganographisches System als unsicher zu bezeichnen. Ist das Brechen der 2. Stufe erfolgt, ist automatisch auch die 1. Stufe gebrochen, d.h. es ist nicht möglich, die Konzelationseigenschaft zu verletzen, ohne auch die steganographische Eigenschaft zu verletzen. Anders formuliert: Die steganographische Eigenschaft ist die weitergehende Eigenschaft eines Geheimhaltungssystems. Folglich muß jedes Stegosystem auch ein Konzelationssystem sein.

1.3 Was bezwecken Modelle?

Um das Phänomen Steganographie zu erfassen und Eigenschaften steganographischer Systeme beschreiben zu können, werden im folgenden Modelle aufgestellt. Als abstrakte Systeme beschreiben sie nicht nur die wesentlichen Objekte (Sender, Empfänger, Angreifer) und ihre Beziehungen untereinander (z.B. „unentdeckt kommunizieren“), sondern sie erheben den Anspruch, eine homomorphe Abbildung des betrachteten Ausschnitts der Welt der sicheren Kommunikation zu sein. In [Klir_89] findet man einen Überblick über die Systemmodellierung.

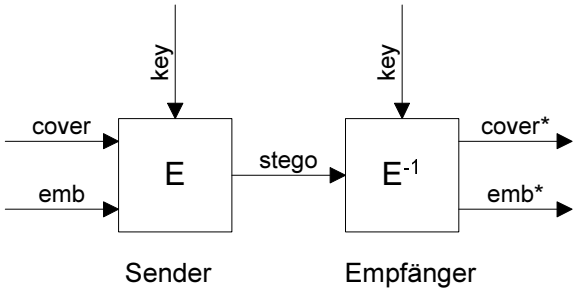
Dies geschieht mit dem Ziel zu zeigen, was einerseits notwendige, andererseits auch hinreichende Bedingungen für diese besondere Art der vertraulichen Kommunikation sind, so daß letztlich Aussagen darüber getroffen werden können, ob ein gegebenes steganographisches System dem allgemeinen Modell entspricht und die Modellannahmen, insbesondere zur Sicherheit, erfüllt sind. Ein weiterer Aspekt der Modellierung ist es, Steganographie in den größeren Zusammenhang der Geheimhaltung zu stellen.

Während der Modellierung eines allgemeinen steganographischen Systems wird besonderer Wert auf die Abgrenzung der Objekte gelegt. Das geschieht mit dem Ziel, die Außensicht auf das System mit der Sicht des Angreifers abzustimmen.

2 Modellierungsmöglichkeiten für steganographische Konzelationssysteme

2.1 Das Einbettungsmodell

Ausgangspunkt der folgenden Überlegungen zur Modellierung steganographischer Konzelationssysteme soll Abbildung 2 sein, eine leichte Erweiterung von [Pfit_96].



E: steganographische Funktion „Einbetten“
E^{-1}: steganographische Funktion „Extrahieren“
cover: Hüllnachricht
emb: einzubettende Nutzdaten
stego: Hüllnachricht mit eingebetteten Daten
key: Parameter für E und E^{-1}
cover*: Hüllnachricht nach dem Extrahieren (meist: cover* = stego)
emb*: erhaltene Nutzdaten nach dem Extrahieren (Ziel: emb* = emb)

Abbildung 2: Das Einbettungsmodell

Die im Folgenden angeführten Modelle sind prinzipiell Erweiterungen dieses Modells oder beinhalten detailliertere Darstellungen des Schrittes E, wobei die Abgrenzung „gehörig zu Schritt E oder nicht“ oft nicht leichtfällt. Im Schritt E wird die zu verbergende Nachricht *emb* in die Hüllnachricht eingebettet. Das Ergebnis dieser Operation ist das kodierte Bild *stego* (vgl. Abbildung 1). E^{-1} ist die Umkehroperation zu E, die *emb* wieder extrahiert. Es gilt also *stego* = E(*cover*, *emb*, *key*) und $emb^* = E^{-1}(stego, key)$. Dabei wird natürlich angestrebt, daß *emb* und emb^* identisch sind, da sonst das Einbetten nicht umkehrbar ist.

In diesem Modell wird vorausgesetzt, daß E beim Sender ausgeführt wird und E^{-1} beim Empfänger der Nachricht. Dazwischen findet eine Übertragung von *stego* zum Empfänger statt. Diese Annahmen sind auch für alle folgenden Modelle gültig.

Da es momentan noch keine echte asymmetrische Steganographie gibt (Ansätze sind in [Ande_96] und [HuPf_96] zu finden), befassen wir uns auch bei der Modellbildung ausschließlich mit symmetrischen Systemen. Aus diesem Grunde wird in Abbildung 2 im Gegensatz zu *cover* und *emb* auch keine Unterscheidung zwischen den in E und E^{-1} verwendeten Schlüsseln getroffen.

Anmerkung: Es ist ohne weiteres ein Stegosystem vorstellbar, das ohne *cover* auskommt, indem es sich ein in E zu verwendendes *cover* generiert bzw. alleine aus *emb* ein *stego* erzeugt (das dann implizit ein *cover* enthält). Daraus ergibt sich zwangsläufig die Frage: Braucht man für ein allgemeines Modell ein *cover*?

In einem solchen Modell (vgl. Abbildung 3) kann *stego* als *emb* plus eine bestimmte hinzugefügte Datenmenge (Redundanz) betrachtet werden. Diese hinzugefügten Daten müssen so gestaltet sein, daß das resultierende *stego* einem Angreifer plausibel er-

scheint. Ein Beispiel dafür sind z.B. Programme, die in fraktalen Bildern Daten unterbringen.

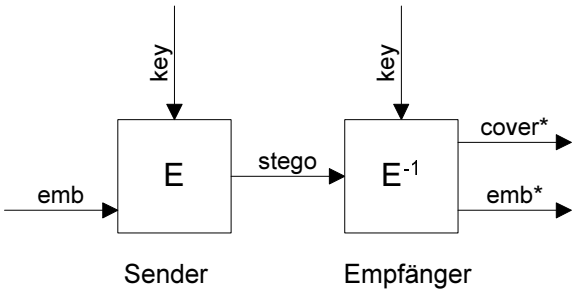
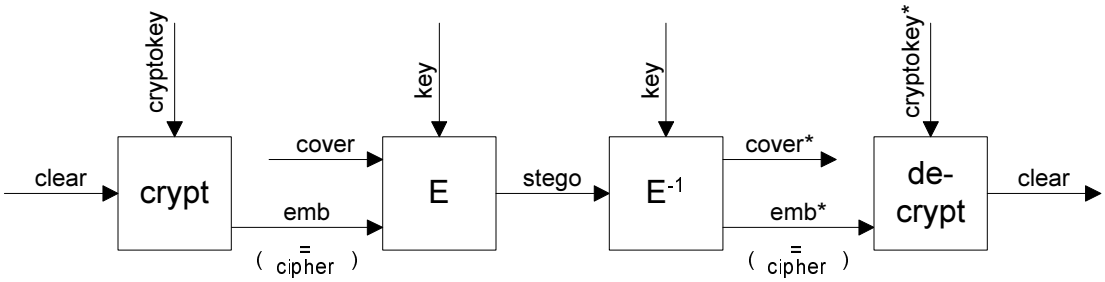


Abbildung 3: Modell eines Stegosystems ohne die Eingangsgröße cover

Dieses Modell setzt die Möglichkeit voraus, *cover* weitgehend frei generieren zu können. Ein allgemeines Modell muß aber alle Anwendungsfälle abdecken und kann daher nicht von dieser speziellen Freiheit ausgehen. Das in diesem Papier herausgearbeitete allgemeine Modell (vgl. Abschnitt 2.4) schließt auch den eben angeführten Spezialfall ein und zeigt damit seine umfassendere Anwendbarkeit.

2.2 Erweiterung um Kryptographie

Die Anwendung kryptographischer Systeme ist für die Verschlüsselung von *emb* interessant. Es gibt also die der eigentlichen Stegofunktion vor- bzw. nachgelagerten Schritte Verschlüsseln und Entschlüsseln (Abbildung 4).



crypt:	Verschlüsseln
decrypt:	Entschlüsseln
clear:	Klartext
cipher:	verschlüsselter Klartext
cryptokey:	Parameter für die Funktion Verschlüsseln
cryptokey*:	Parameter für die Funktion Entschlüsseln

Abbildung 4: Erweiterung des Modells um Kryptographie

Der Einsatz eines asymmetrischen Kryptosystems bei crypt bzw. decrypt führt nicht zu einer asymmetrischen Steganographie, wie man vermuten könnte; ebensowenig wie ein

mit asymmetrischer Kryptographie ausgeführter Austausch des (symmetrischen) Steganographie-Schlüssels *key* (z.B. Diffie-Hellman-Schlüsselaustausch).

So lassen sich mehrere vorgeschlagene Systeme, die asymmetrische Schlüssel verwenden, auf eine Erweiterung schlüsselloser symmetrischer steganographischer Funktionen um asymmetrische Verschlüsselung zurückführen.

Wie in Abschnitt 1.2 dargelegt wurde, ist das Ziel eines Stegosystems die Wahrung der steganographischen Eigenschaft. Mit der zusätzlichen Anwendung von Kryptographie wird nur die Wahrung der Konzelationseigenschaft eines Stegosystems unterstützt, die steganographische Eigenschaft jedoch nicht. Daher wird diese um kryptographische Verfahren erweiterte Variante nicht als allgemeingültiges Modell für steganographische Systeme betrachtet, wenngleich der Einsatz von Kryptographie durchaus sinnvoll sein kann.

2.3 Erweiterung um Vorverarbeitungsfunktionen

2.3.1 Analyse der Ein- und Ausgangsgrößen

Das in Abbildung 5 dargestellte Modell ist eine Erweiterung des allgemeinen Falles durch eine dem Schritt E vorgelagerte Analysephase. Während der Analysephase wird anhand des angenommenen Angreifermodells zu bewerten versucht, ob die vorliegende *cover*/*emb*-Kombination sichere Steganographie ermöglicht. Auf diese Art und Weise wird das System von den Eingangsgrößen unabhängiger und insgesamt sicherer, da es die Möglichkeit zur Zurückweisung unsicherer Datenkombinationen hat.

Hier zeigt sich ein wesentlicher Unterschied zwischen Steganographie und Kryptographie: während kryptographische Systeme als Schlüsseltext möglichst ideales weißes Rauschen erzeugen sollen, muß *stego* anderen Anforderungen genügen. Insbesondere muß es dem verwendeten *cover* genügend ähnlich sein (abhängig vom Angreifermodell). Das heißt, daß Annahmen über das Wissen des Angreifers gemacht werden, die in hohem Maße die Sicherheit des Stegosystems bestimmen.

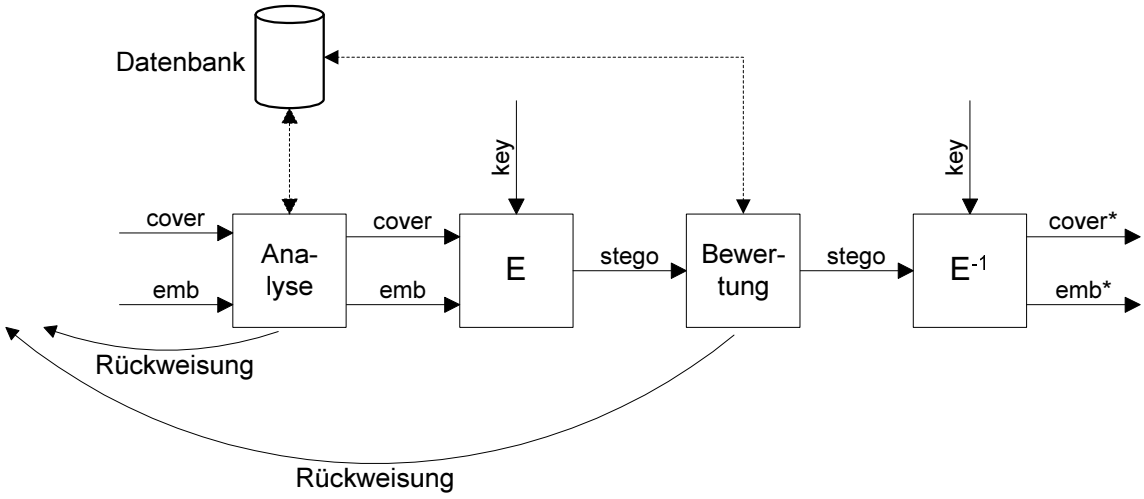


Abbildung 5: Analyse der Eingangsdaten und Ergebnisbewertung

Wie weiterhin in Abbildung 5 gezeigt, kann auch eine Datenbank zum System hinzugefügt werden. Diese Datenbank ist ein Hilfsmittel für den Analyseschritt. Sie kann zur Sicherstellung der einmaligen Verwendung eines bestimmten *cover* genutzt werden.

Eine weitere Rückweisung ist im Schritt „Bewertung“ nach der Erzeugung von *stego* und damit vor dem Transfer zum Empfänger vorgesehen. Hier ist eine gute Überprüfung des Einbettungsergebnisses möglich, da man sämtliche bekannten, vom Angreifer verwendeten Methoden selbst anwenden kann. Die Bewertungskriterien ergeben sich aus dem Angreifermodell, also insbesondere aus dem Wissen über *cover*, das dem Angreifer zugebilligt wird, wie etwa bestimmte statistische Kenntnisse. Hält *stego* diesen Überprüfungen stand, kann es als sicher betrachtet werden. Auch dieser Schritt kann, wie in Abbildung 5 zu sehen ist, durch eine Datenbank unterstützt werden.

Die beiden Schritte Analyse und Bewertung bedingen einander nicht, d.h. es sind auch Systeme realisierbar, die nur mit einem der beiden auskommen.

2.3.2 Wann ist ein Stegosystem sicher?

Wenn dem Angreifer das verwendete *cover* und das daraus erzeugte *stego* bekannt sind, ist es für ihn trivial zu erkennen, daß Steganographie verwendet wurde, da er Unterschiede zwischen *stego* und *cover* feststellen kann. Aus diesem Grund darf ihm das konkrete *cover* nicht bekannt sein. Die dann für den Angreifer existierende Unsicherheit (Entropie) über *cover* wird vom Stegosystem ausgenutzt (siehe auch [KlPi_96]).

Ein allgemeines sicheres Stegosystem bei gleichzeitiger Kenntnis von *cover* und *stego* durch den Angreifer ist also nicht realisierbar.

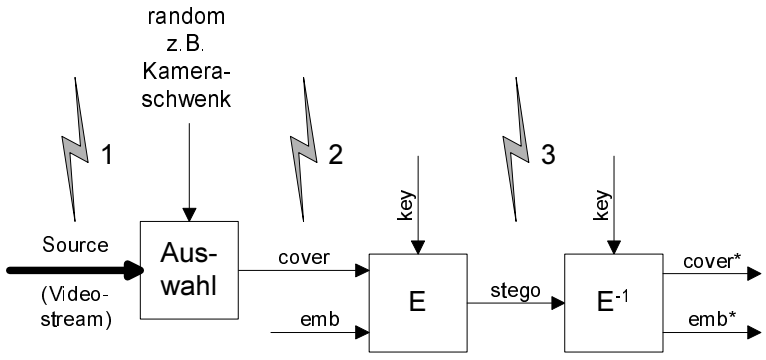
Eine Ausnahme gilt es zu beachten: Im Fall *cover* ≡ *stego*, d.h. *cover* enthält bereits steganographische Daten (auch als „selective steganography“ bezeichnet), wäre theo-

retisch sichere Steganographie möglich. Voraussetzung ist jedoch, daß es dem Sender gelungen ist, in einem *echt zufälligen Prozeß* ein *cover* zu finden, das die gewünschten eingebetteten Daten bereits enthält. Die systematische Ausnutzung dieses Sachverhalts ist jedoch praktisch nicht möglich.

2.3.3 Auswahl aus breiten Eingabeströmen am Beispiel einer Videoaufnahme

Als ein interessanter Ansatz erweist sich die Idee, nicht mehr ein einzelnes *cover* zu betrachten, sondern eine große Anzahl von *covers*, die dann als *Source* bezeichnet wurden.

Ein Beispiel dafür ist die Aufnahme eines Videobildes mit einer Kamera (vgl. Abbildung 6), die durch viele Parameter beeinflußt wird. Einige Parameter sind nicht reproduzierbar (oder nur mit einer bestimmten Genauigkeit), woraus die nötige Unsicherheit (Entropie) über *cover* selbst bei vollständiger Kenntnis von *Source* für einen Angreifer erzielt wird. Aus *Source* wird eine Auswahl getroffen, in die ggf. noch zufällige Parameter eingehen, über die keiner (auch der Nutzer des Stegosystems nicht) hundertprozentige Aussagen treffen kann.



Source:	Menge an Eingangsdaten
Auswahl:	Auswahlprozeß
random:	Zusammenfassung der in die Auswahl eingehenden Zufälligkeiten
1, 2, 3:	mögliche Angriffspunkte

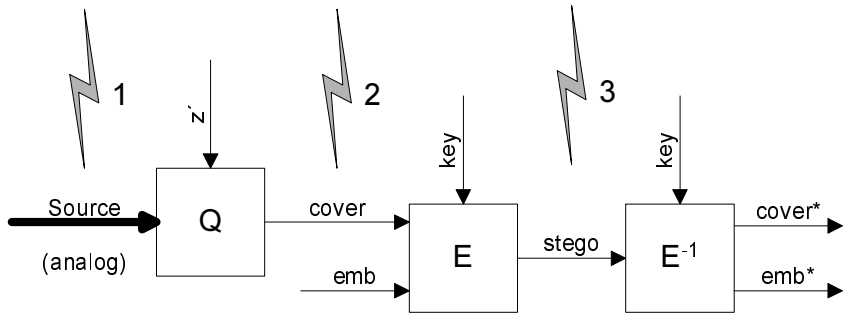
Abbildung 6: Auswahl aus breiten Eingabeströmen (*Source*) am Beispiel Videoaufnahme

Der Vorteil eines solchen Verfahrens ist die extreme Erschwerung der Ermittlung des konkret verwendeten *cover* durch den Angreifer. Diese wird durch die eingehenden Zufallsgrößen noch verstärkt.

In Abbildung 6 bedeutet das konkret: beim Angriff an Stelle 1 ist Steganographie möglich (der Angreifer kennt nur *Source*); beim Angriff an Stelle 2 nicht (Angreifer kennt *cover*). Stego (Punkt 3) ist ihm in beiden Fällen bekannt. Selbstverständlich darf die Kenntnis von *stego* durch den Angreifer keine Schwächung des Stegosystems darstellen.

2.3.4 Vorgelagerte Quantisierung

Wie bereits in den Abschnitten 2.3.2 und 2.3.3 aufgeführt wurde, muß für den Angreifer eine bestimmte Ungenauigkeit in seinem Wissen über *cover* existieren, die z.B. auch durch Digitalisierung/Quantisierung eines analogen Signals erreicht werden kann. Der Angreifer darf Wissen über das analoge Signal haben und auch das analoge Signal *Source* selbst ganz genau kennen, und dennoch ist Steganographie möglich.



Source: analoge Eingangsgröße
Q: Quantisierungsschritt
z´: sich durch die Indeterminiertheit von Q ergebende Zufälligkeit
1, 2, 3: mögliche Angriffspunkte

Abbildung 7: Modell mit Quantisierungsschritt

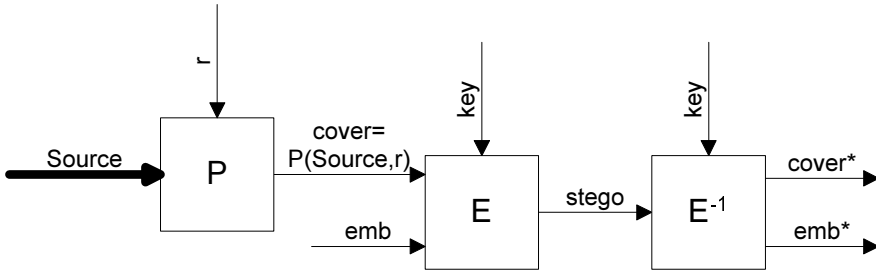
Ein Beispiel für das Modell in Abbildung 7 ist ein ISDN-Telefon mit in den Digital/Analog-Wandler integrierter Stegofunktion: Der Angreifer darf das eingehende Analogsignal (*Source*) beliebig genau kennen (Punkt 1) und die Ausgabe des Bausteins beobachten (Punkt 3), und dennoch ist es der Stegofunktion möglich, das (indeterministische) Quantisierungsrauschen des Wandlers für sichere Steganographie zu nutzen.

Einem Angriff an Punkt 2 entspricht es, wenn der Angreifer Zugriff auf die digitalisierten Daten vor dem Einbetten erhält. Das könnte z.B. der Fall sein, wenn Digitalisiereinheit und Stegofunktion auf getrennten Bausteinen untergebracht sind und die Verbindung zwischen ihnen abgehört werden kann.

2.4 Ergebnis der Diskussion

Die Hauptbedingung für sichere Steganographie ist, daß dem Angreifer *cover* nicht bekannt sein darf. Das Modell aus Abschnitt 2.1. beschreibt somit die steganographische Kernfunktion eines Stegosystems, die von genau dieser Annahme ausgeht. Will man analog zur Kryptographie davon ausgehen, daß dem Angreifer alle Ein- und Ausgangsgrößen außer dem Schlüssel bekannt sind, erweist sich dieses Modell als unzureichend, wenngleich es nichts von seiner Gültigkeit einbüßt.

Der Funktion Einbetten muß ein Schritt vorangestellt werden, der sicherstellt, daß dem Angreifer *cover* nicht beliebig genau bekannt ist (vgl. Abschnitt 2.3.2 ff.). Das führt uns zu folgender Darstellung:

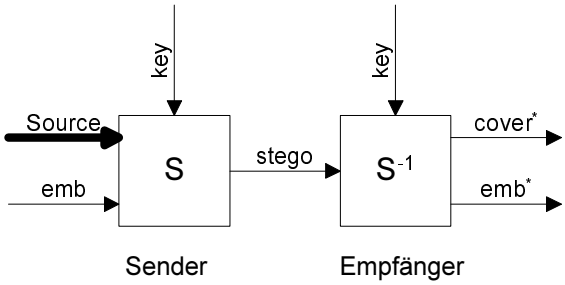


P: Preprocessing; Vorverarbeitungsfunktion
r: durch P entstehender zufälliger Anteil von cover (kann Eingangsgröße von P sein, muß aber nicht)

Abbildung 8: Modell mit Vorverarbeitungsfunktion

Die Funktion P kann z.B. ein Auswahlprozeß analog Abschnitt 2.3.3 oder die Digitalisierung eines Analogsignals (vgl. 2.3.4) sein.

Faßt man die Funktionen E und P zusammen, kommt man zum Modell eines symmetrischen steganographischen Konzelationssystems:



S: indeterministische steganographische Gesamtfunktion „Verbergen“
S^{-1}: Umkehroperation zu S

Abbildung 9: Modell eines symmetrischen steganographischen Konzelationssystems

Der Unterschied zur anfänglichen Betrachtungsweise besteht darin, daß jetzt nicht mehr nur die steganographische Kernfunktion, sondern das gesamte System betrachtet wird. Mittels der Eingangsgröße *Source* wird die Unbestimmtheit des Parameters *cover* der Einbettungsfunktion modelliert und nicht mehr nur einfach vorausgesetzt. Die Gesamtfunktion S ist damit indeterministisch, die Kernfunktion E dagegen deterministisch.

Mit dieser Modelldarstellung wird eine weitgehende Analogie zur Modellierung von Kryptosystemen dahingehend erreicht, daß das Kerckhoff-Prinzip gilt. Dieses besagt, „... daß die Sicherheit eines Verschlüsselungsverfahrens nur von der Geheimhaltung des Schlüssels abhängen darf“ [Schn_96, S. 6]. Ein Angreifer darf also alle Eingangs-

größen und Ausgangsgrößen eines Systems sowie die Algorithmen selbst kennen, nur den Schlüssel nicht. Das ist bei dem in Abbildung 9 dargestellten Modell der Fall, beim ursprünglichen Einbettungsmodell (Abbildung 2) dagegen nicht.

3 Zusammenfassung und Ausblick

Besondere Beachtung verdient bei steganographischen Konzelationssystemen die Hüllnachricht (*cover*). Diese darf dem Angreifer nicht bis ins letzte Detail bekannt sein, da sonst sichere Steganographie unmöglich ist. Wir können daher zwei Anforderungen an ein Stegosystem nennen:

1. Dem Angreifer bleibt der Schlüssel *key* unbekannt.
2. Dem Angreifer ist das *konkrete cover* unbekannt; er hat jedoch eine gewisse Menge an Wissen über *cover* (z.B. Verteilungen).

Die Geheimhaltung des Schlüssels *key* entspricht der von symmetrischen Kryptosystemen.

Punkt 2 kann zunächst nur als Voraussetzung für sichere Steganographie formuliert werden. Alternativ besteht jedoch die Möglichkeit, eine als *Source* bezeichnete Menge an Eingangsdaten zu betrachten, aus der das Stegosystem ein konkretes *cover* auswählt (wobei für einen Angreifer die auswählbaren *cover* die gleiche Wahrscheinlichkeit haben). Dem Angreifer ist dann nur *Source* bekannt. Diese Herangehensweise ist für die Modellierung und Implementierung realer Systeme besser geeignet, da Aussagen über die Preprocessing-Funktion P getroffen werden können und die Einbettungsfunktion E optimal auf die eingehenden Datenströme abgestimmt werden kann. E nutzt dabei die im Verlauf von P entstehende Zufälligkeit in *cover* zum Verbergen von Daten. Für eine gute Realisierung der Funktion E ist also eine genaue Kenntnis bezüglich der Indeterminiertheit von P notwendig.

Es gibt etliche offene Probleme und Fragestellungen auf dem Gebiet der Steganographie, die weiteren Arbeiten vorbehalten bleiben bzw. in diesem Papier nicht betrachtet werden. Einige davon sind:

- die Beschreibung und Bewertung der Sicherheit von Stegosystemen mit den Mitteln der Informationstheorie (dieser Punkt wir ausführlich in [KlPi_97] diskutiert),
- die möglichst umfassende Modellierung und Bewertung von Angriffen auf Stegosysteme,
- die Betrachtung von existierenden oder zu realisierenden Stegosystemen unter den beiden o.a. Gesichtspunkten sowie der Konformität zum erarbeiteten allgemeinen Modell für steganographische Konzelationssysteme.

Darüber hinaus hat Steganographie zum Urheberrechtsschutz seine Bedeutung, die in diesem Papier nicht betrachtet wurde. Bezüglich der hier vorgenommenen Modellbil-

dung kann man davon ausgehen, daß existierende Watermarkingsysteme ebenfalls nach den hier vorgestellten Modellen arbeiten. In Zukunft ist jedoch zu erhoffen, daß auch „echte“ asymmetrische Systeme entstehen werden.

4 Literatur

[Ande_96] Ross Anderson: Stretching the limits of Steganography. In: Proceedings: Information Hiding. Workshop, Cambridge, U.K., May/June, 1996, LNCS.

[HuPf_96] Michaela Huhn, Andreas Pfitzmann: Erste Gedanken zu Steganographie mit öffentlichen Schlüsseln. Internes Arbeitspapier TU Dresden, Dresden 1996.

[Klir_89] G. J. Klir: Inductive Systems Modelling: An Overview. In: M. S. Elzas, T. I. Ören, B. P. Zeigler (Hrsg.): Modelling And Simulation Methodology, Knowledge Systems' Paradigms. Elsevier Science Publishers B.V., North Holland 1989, 55-75.

[KlPi_97] Herbert Klimant, Rudi Piotraschke: Informationstheoretische Bewertung steganographischer Konzelationssysteme. eingereicht für: VIS ´97, Freiburg/Brsg.

[Pfit_96] Birgit Pfitzmann: Information Hiding Terminology. In: Proceedings: Information Hiding. Workshop, Cambridge, U.K., May/June, 1996, LNCS.

[Schn_96] Bruce Schneier: Angewandte Kryptographie, Addison-Wesley, Bonn 1996.