Steganographie

Lukas Sikorski

mail@lukassikorski.de

Inhaltsverzeichnis

1. Einleitung

Seit der Einführung des Internet in den neunziger Jahren spielt die computervermittelte Kommunikation eine sehr wichtige Rolle. Dabei sind auch die Methoden zur vertraulichen Kommunikation immer mehr im Blickfeld von Untersuchungen über die Sicherheit. Nicht nur die Militärdaten, Wirtschaftsdaten, Bankdaten sondern auch Daten bei Vertragsverhandlungen, bei Forschung und Entwicklung und der Politik erfordern ein hohes Maß an Vertraulichkeit.

Überall dort, wo vertrauliche Daten übermittelt werden sollen, kommt die sog. Steganographie zum Einsatz. Das Wort „Steganographie“ kommt aus dem Griechischen und heißt übersetzt „verdeckt Schreiben“. Dabei geht es um die verborgene Übermittlung oder Speicherung von Informationen. Die Existenz der Nachricht wird verborgen und dem Angreifer fällt nicht auf, dass eine geheime Nachricht existiert.

Im Rahmen dieser Arbeit wird die Steganographie beschrieben. Zuerst werden die Grundlagen dieser Methode dargestellt. Darüber hinaus werden die Zusammenhänge zwischen Steganographie und Kryptographie sowie die Eigenschaften und die Arten der Steganographie analysiert. Weiterhin werden die Besonderheiten des Steganographie-Systems beschrieben. Es werden die dabei verwendeten Hülldaten und Einbettungstechniken näher betrachtet. Anschließend werden Angriffe auf steganographische Nachrichten dargestellt.

2. Grundlagen der Steganographie

Steganographie ist eine Variante des Konzepts, Informationen zu verbergen. Es ist „die Lehre vom verdeckten Schreiben.“[1] Das Verfahren gilt dann als Sicher, wenn nach Anwendung des Verfahrens keinerlei Rückschlüsse Dritter darauf zu

[1] Vgl. Westfeld, A.: Angriffe auf steganographische Systeme, S.2; http://os.inf.tu-dresden.de/~westfeld/publikationen/vis99.pdf, Stand: 03.02.07

ziehen sind, ob im vorliegenden Medium eine Nachricht verborgen wurde oder nicht.

Ein einfaches Prinzip am Beispiel eines Urlaubsgrußes:[2]

Liebe Kolleginnen!
Wir genießen nun endlich unsere Ferien auf dieser Insel vor Spanien.
Wetter gut, Unterkunft auch, ebenso das Essen. Toll!
Gruß, J. D.

Die Regel zum extrahieren der Nachricht ist, dass die Buchstaben bis zum nächsten Leerzeichen gezählt werden, und falls die Anzahl ungerade ist eine 0 ausgegeben wird, sonst eine 1. Die ersten 8 Wörter liefern uns 01010011, was dezimal 83 und im ASCII dem Buchstaben **S** entspricht. Die nächsten 8 Wörter ergeben 01001111 (79, Buchstabe **0**), letzten acht Wörter wieder 01010011 (also den Buchstaben **S**). Damit wird aus dem positiven Urlaubsgruß ein versteckter Hilferuf „**SOS“**.

Anhand dieses Beispiels ergeben sich folgende Eigenschaften, die insbesondere grundlegend für Steganographie sind: Die Nachricht ist versteckt, d.h. es ist nicht zu erkennen, dass eine andere Nachricht als die Offensichtliche übermittelt werden soll. Es wurde ein harmlos erscheinendes Trägermedium, hier der nette Urlaubsgruß, zum Verstecken der Botschaft benutzt. Außerdem ist die Entzifferung des Geheimnisses nur demjenigen möglich, der den entsprechenden „Algorithmus“ zur Auflösung der Mitteilung besitzt. Bei Verdacht auf eine versteckte Nachricht lassen sich immer noch verschiedene Botschaften herauslesen. Die Menge der versteckten Informationen ist zumeist sehr viel geringer, als die Nachricht in der sie verpackt ist.

[2] Vgl. Breetzmann, R. (2000). Die Methoden der Steganographie, S.1; http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/rbreetzmann/einf.html, Stand: 03.02.07

2.1. Steganographie und Kryptographie im Vergleich

Steganographie und Kryptographie sind eng verwandte Wissenschaften. Sie unterscheiden sich in ihren Ansätzen. Bei der Steganographie soll eine Nachricht dadurch vor dem Zugang Unbefugter geschützt sein, dass nicht erkennbar ist, dass eine versteckte Nachricht überhaupt vorhanden ist.[3] Der geheime Text wird verborgen, nicht verschlüsselt, hier existiert also scheinbar gar keine Nachricht. Die Sicherheit kryptographischer Verfahren basiert auf der Komplexität der eingesetzten Transformationen und der Geheimhaltung der Schlüssel. Für mögliche Angreifer die den Schlüssel nicht kennen ist der Schlüsseltext unleserlich. Der Text wird verschlüsselt und nicht verborgen, hierbei existiert eine Nachricht kann aber nicht gelesen werden.

Beide Techniken lassen sich auch kombinieren, indem man eine versteckte Nachricht zusätzlich verschlüsselt. Verschlüsseln und Verbergen bedeutet mehr Sicherheit. Ziele der Steganographie sind, das verstecken von Nachrichten und die Prüfung des Ursprungs von Gütern oder Dokumenten (durch Wasserzeichen), aber auch zum Nachweis von Veränderungen der Ware beziehungsweise des Dokuments.

Wie auch bei der Kryptographie spricht man bei der Steganographie von symmetrischer und asymmetrischer Steganographie.[4] Bei der symmetrischen Steganographie tauschen Sender und Empfänger einer Nachricht vor der verdeckten Kommunikation einen geheimen Schlüssel aus. Dabei ist es bekannt, auf welche Art und Weise und an welcher Stelle eine Nachricht versteckt ist. Bei sicheren Verfahren ist nur durch Kenntnis dieses Schlüssels die Erkennbarkeit gewährleistet. Bei der asymmetrischen Steganographie stellt der Empfänger einer verdeckten Nachricht einen (möglichst authentischen) öffentlichen Schlüssel zur Verfügung. Dieser wird zum verdecken der Nachricht verwendet. Der Empfänger selbst ist nicht in der Lage herauszufinden, ob sich in einem Medium (s)eine Nachricht verbirgt, sofern er das Trägermedium nicht direkt mit dem Steganogramm ver-

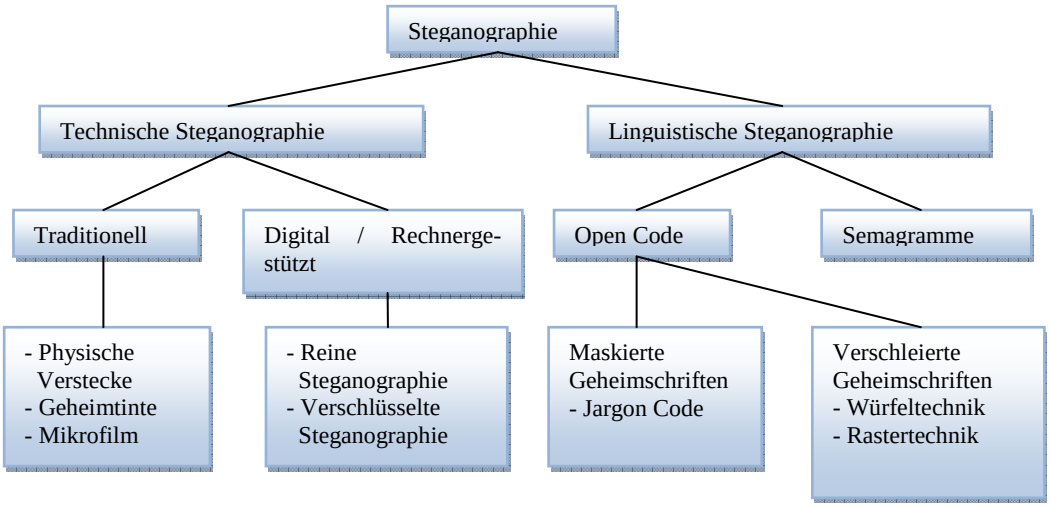
[3] Vgl. Schuster, M. (2002/03). Steganographie, S.2; http://www.logic.at/people/schuster/stego _ms. pdf, Stand: 03.02.2007
[4] Wikipedia: Steganographie; http://de.wikipedia.org/wiki/Steganografie, Stand: 03.02.07

gleicht. Durch die zuletzt aufgeführte Methode wird deutlich, dass asymmetrische Steganographie nur sehr schwer realisiert werden kann.

2.2. Arten der Steganographie

Steganographie teilt sich in zwei große Hauptrichtungen, die Technische und die Linguistische Steganographie (vgl. Abbildung 1).[5]

Abbildung 1: Arten der Steganographie



Die linguistische Steganographie teilt sich wieder in zwei große Klassen. Die erste Klasse ist der Open Code (unersichtlich getarnte Geheimschriften). Die zweite Klasse sind die Semagramme (sichtlich getarnte Geheimschriften).

Beim Open Code wird die Nachricht als unverfänglich oder offen verständlich ausgegeben (natürlich mit anderer Bedeutung) oder in eine Nachricht dieser Art eingebettet. Die Nachricht ist unersichtlich getarnt, z.B. wird ein sinnvoller Text verfasst indem ein weiterer unersichtlicher Text enthalten ist. Es wird zwischen zwei Methoden zum verstecken einer Nachricht unterschieden, den maskierten Geheimschriften und den verschleierten Geheimschriften. Die maskierten Geheimschriften benutzen nicht allgemein bekannte Codewörter. Sowohl Sender als auch Empfänger müssen sich über die Bedeutung dieser Geheimschrift austauschen, bevor sie sie benutzen können. Zu den maskierten Geheimschriften gehört unter

[5] Vgl. Breetzmann, R. (2000). Die Methoden der Steganographie; S.2; http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/rbreetzmann/einf.html, Stand: 03.02.07

Anderen auch der Jargon Code. Hierbei wird ein vorher, von den Teilnehmern vereinbartes Vokabular, zur Kommunikation benutzt, z.B. entsprechen Zigarren den Kriegsschiffen, Loch steht für Gefängnis, usw. Bei den verschleierten Geheimschriften wird die zu übermittelnde Nachricht unverändert in eine offene, unverfängliche Nachricht eingebettet. Dazu müssen die Plätze zwischen den Partnern vereinbart werden, an denen die eigentlichen Nachrichten zu finden sind. Hierzu gibt es zwei Möglichkeiten, die Würfeltechnik und die Rastertechnik.

Bei der Rastertechnik haben Sender und Empfänger die gleichen Schablonen (vgl. Abbildung 2). Die unverdächtige Nachricht muss so abgefasst sein, dass die Schablonen den gleichen Text zeigen. Demgegenüber bilden bei der Würfeltechnik ausgewählte Buchstaben die geheime Nachricht, z.B. jeder dritte Buchstabe nach einem Satzzeichen (vgl. Abbildung 3).

Abbildung 2: Rastertechnik
(Quelle: Schuster 2002/03, S.8)

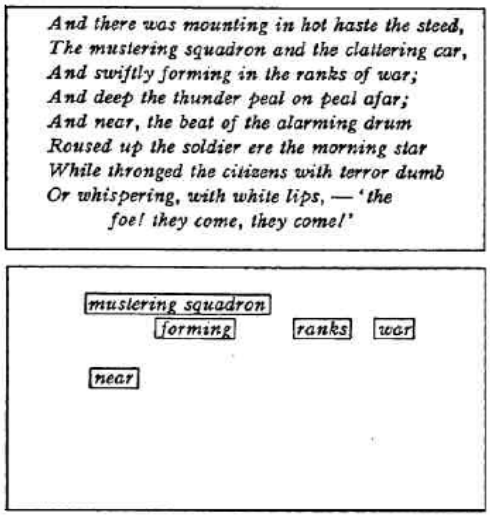
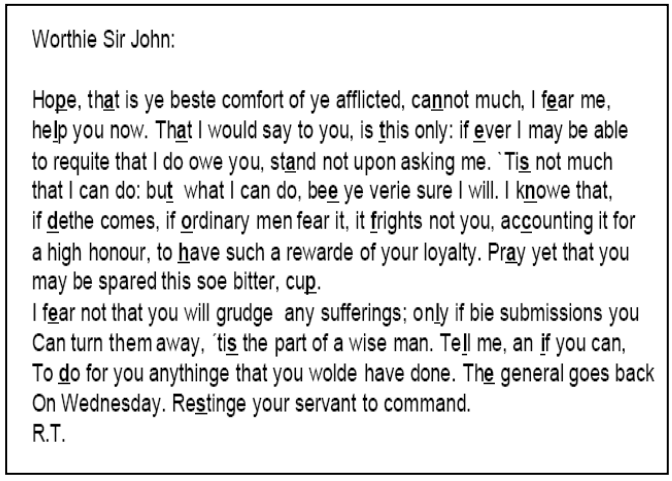
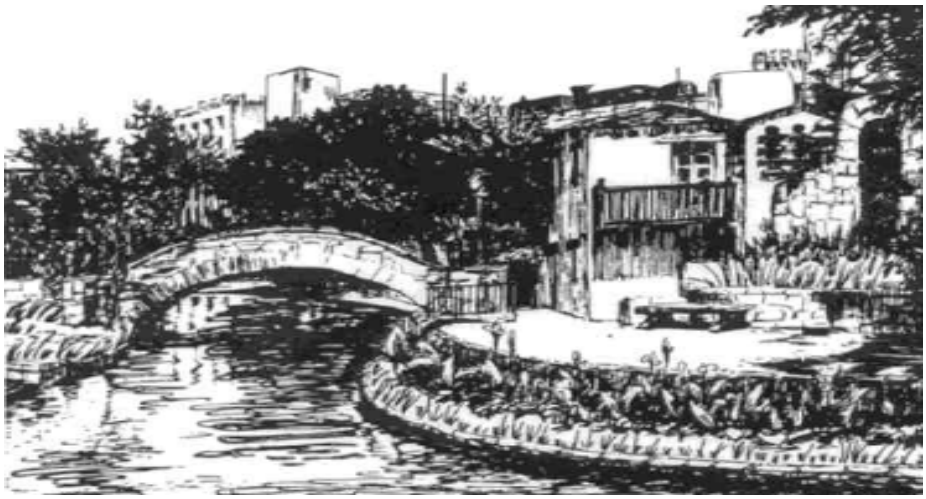


Abbildung 3: Würfeltechnik (geheime Botschaft Sir John: „panel at east end of chapel slides“)
(Quelle: Schuster 2002/03, S.7)



Weiterhin bilden die zweite Klasse der linguistischen Steganographie die sog. Semagramme. Diese verstecken die Botschaft in sichtbaren Elementen von Bildern, Zeichnungen oder Schriften. Ein Prinzip zeigt Abbildung 4.

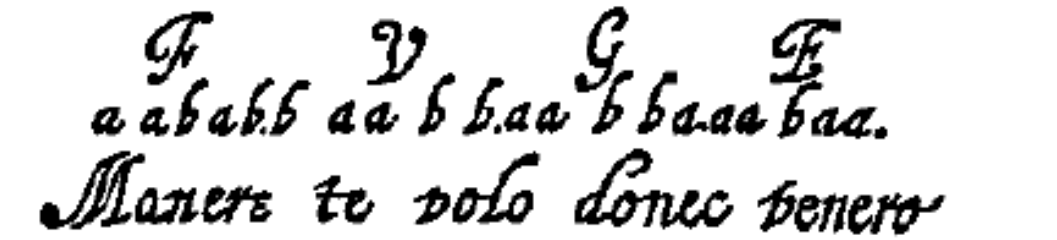
Abbildung 4: Semagramm: Grashalme als Morsezeichen
(Quelle: Schuster 2002/03, S.4)



Im Vordergrund sind kurze und lange Grashalme erkennbar, die als Morsezeichen verstanden und zu einer Nachricht zusammengesetzt werden können. Die Nachricht ist zwar offen aber getarnt, und so nur für den Eingeweihten erkennbar. Die Nachricht ist im Gegensatz zum Open Code sichtlich getarnt.

Ein weiteres Prinzip ist die Verwendung von zwei Schriftarten (vgl. Abbildung 5), hier werden auch zwei Botschaften vermittelt, die eine die offensichtlich ist und die andere die im Verborgenen bleibt und nur dem Wissenden klar ersichtlich ist. So lenkt also die eine Nachricht jeweils von einer möglichen anderen ab.

Abbildung 5: Semagramm: Verschiedene Schriftzeichen
(Quelle: Steurer, S.4)



Francis Bacon: Sichtbare Tarnung eines binären Codes ('biliteral cipher') mittels zweier verschiedener Schriftzeichen-Formen. Man beachte die beiden verschiedenen /e/ in Manere.

Die zweite große Hauptrichtung der Steganographie ist die technische Steganographie. Die technische Steganographie verwendet traditionell, Geheimtinten, physische

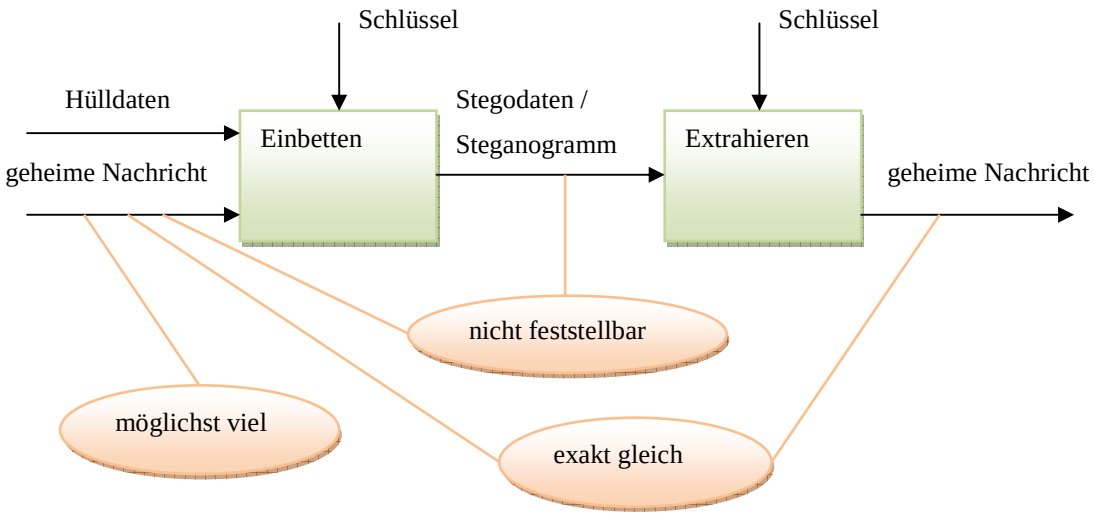
Verstecke wie doppelte Böden oder Briefumschläge, hohle Absätze von Schuhen und ähnliches. Schnelltelegraphie (gespeicherte Morsecode-Botschaft mit 20 Zeichen pro Sekunde) oder der Microdot im Zweiten Weltkrieg (Mikrophotographische Informationsträger die, obwohl so klein sind wie z.B. ein Punkt über dem Buchstaben "i", große Mengen an Information beinhalten können), gehören auch zur traditionellen Steganographie.

Bei der digitalen oder rechnergestützten Steganographie handelt es sich um nicht erkennbare Einbettung von Nachrichten in digitale Inhalte (stehende oder bewegte Bilder, Audiodaten, Multimedia). Dabei verwendet Pure oder Reine Steganographie nur ein Stego-Schlüssel für das Einbetten und Extrahieren einer geheimen Nachricht. Die Verschlüsselte Steganographie steht in Verbindung mit Kryptographie und verwendet deshalb zwei Schlüssel. Vor dem Einbetten und nach dem Extrahieren wird der Krypto-Schlüssel angewendet.

3. Stegosystem

Steganographie basiert auf dem Stegosystem. Dabei werden folgende Parameter verwendet: Hülldaten, Stegodaten oder Steganogramm (Hülle mit geheimer Nachricht), geheime Nachricht, Schlüssel (Passwort). die Funktionen Einbetten und Extrahieren (vgl. Abbildung 6).

Abbildung 6: Modell des Stegosystems
(Quelle: In Anlehnung an Schuster 2002/03, S.13)

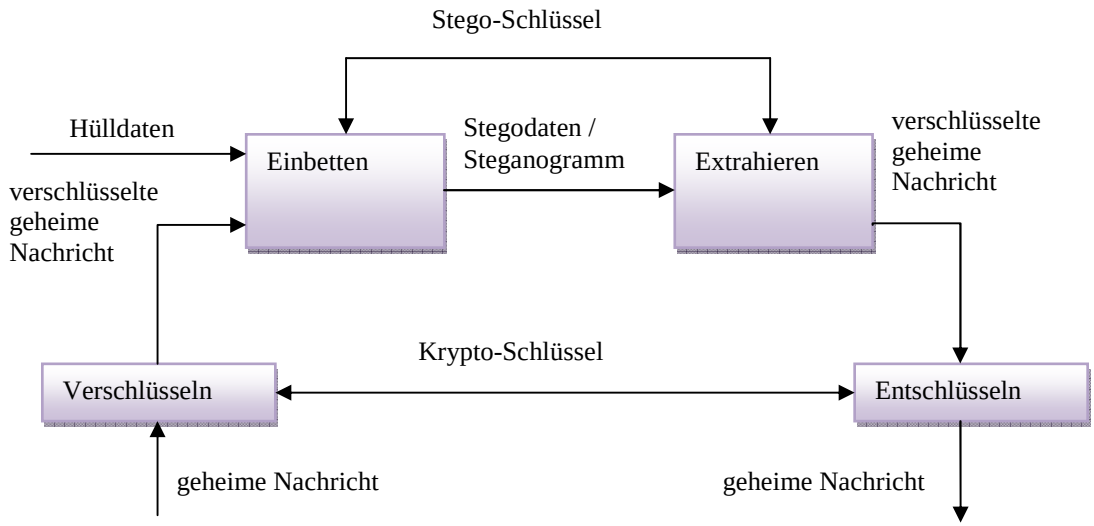


Durch die Funktion Einbetten und unter einem frei gewähltem Passwort bekommen wir aus den Hülldaten und der geheimen Nachricht die Stegodaten. Durch die Funktion Extrahieren und dem zuvor für die Einbettung benutztem Passwort können wir aus den Stegodaten die geheime Nachricht wieder sichtbar machen.

Der Schutzgegenstand bei dem Stegosystem ist die vertrauliche Nachricht. Die primäre Anforderung an das System ist die Unentdeckbarkeit der Existenz der Nachricht. Eine weitere Anforderung ist, dass die erzeugten Stegodaten plausibel sein müssen, dabei kann man die Hülldaten frei wählen. Die geheime Nachricht sollte am Eingang und am Ausgang des Systems exakt gleich sein. Weiterhin sollte das Geheime in den Stegodaten nicht feststellbar sein. Zusätzlich möchte man möglichst viel geheime Nachricht einbetten.

Um die Sicherheit des Systems zu erhöhen wird die geheime Nachricht vor dem Einbetten mit einem kryptographischen Verfahren verschlüsselt und nach dem Extrahieren entschlüsselt (vgl. Abbildung 7).

Abbildung 7: Modell des Stegosystems mit Kryptographie
(Quelle: In Anlehnung an Westfeld 2000, S.7)



3.1. Hülldaten

Für die fehlerfreie Funktion des Stegosystem werden geeignete Hülldaten benötigt. Da Steganographie nur möglich ist wenn dem Angreifer die Hülldaten bzw. deren charakteristischen Merkmale nicht exakt bekannt sind, spielt bei der Wahl der Hülldaten die Zufälligkeit eine entscheidende Rolle. Bei digitalisierten Medien wie Bild- und Audiodaten sind die exakten Werte auf Grund des Digitalisierungsrauschens unbekannt. Es sind Daten vorhanden, die zufällig bzw. unberechenbar sind. Ein gescanntes Foto ist eine stark verrauschte Datei und deshalb als Trägermedium geeignet. Anders ist es bei einer CAD-Zeichnung, die kein Rauschen enthält. In diesem Fall ist Steganographie nicht möglich. Weitere geeignete Medien zur Übermittlung von Nachrichten sind ungenutzter Speicherplatz auf Datenträgern, der Aufbau von Textdokumenten (Zeilenabstand, Wortabstand) oder auf anderer Ebene die Wortwahl (Auswahl aus einer Menge von Synonymen). Auch der Aufbau von IP-Headern und die Reihenfolge der gesendeten Nachrichtenpakete können für Steganographie verwendet werden. Insgesamt je verrauschter das Trägermedium ist, desto schwieriger ist das Auffinden der versteckten Information.

Textdateien (Textnachrichten, wie E-Mail-Texte, elektronische Briefe, Skripte usw.) eignen sich sehr schlecht zur Steganographie da sie relativ klein sind und wenige Informationen aufnehmen können. Weiterhin ist es sehr schwer Informationen zu verstecken ohne die Textdatei erkennbar zu verändern.
Bilddateien (BMP, GIF, JPEG) hingegen eignen sich sehr gut und werden derzeit wohl als häufigstes Medium für die Steganographie eingesetzt. Hier lassen sich Informationen bequem hinzufügen ohne merkliche Veränderungen zu verursachen (ähnliche Vorgehensweise: JPEG-Format: Daten vom Bild werden absichtlich nicht mit gespeichert, um die Größe der Datei zu senken). Der Unterschied zwischen dem Original und dem Steganogramm ist mit freiem Auge nicht erkennbar.

Bei Audiodateien (WAF, MP3) können die Hintergrundgeräusche (Rauschen etc.), die durch das Analog-Digital-Wandeln entstanden sind, genutzt werden um Information darin zu verstecken. Audiodateien eignen sich auch sehr gut zur Steganographie.

3.2. Einbettungstechniken

Auch die Einbettungstechniken spielen bei dem Stegosystem eine wichtige Rolle. Sie können danach unterschieden werden, wie die Hülldaten beim Einbetten verändert werden. Es gibt nichtadaptive Algorithmen, die die Nachricht ohne Beachtung der Hülle einbetten und adaptive Algorithmen bei denen die Eigenschaften der Hülldaten untersucht und berücksichtigt werden. Nichtadaptive Algorithmen sind jedoch leicht angreifbar.

Im Folgenden werden Einbettungstechniken für Bilddateien sowie Audiodateien detailierter analysiert.

3.2.1. Einbettungstechniken bei Bilddateien

Das Schema zum Einbetten einer Nachricht hängt von dem Format der Datei ab in die eingebettet wird. Bei Bilddateien gibt es die verlustfrei nichtkomprimierten Formate, wie das BMP-Format, die verlustfrei komprimierten Formate, wie das GIF (Indexfarbenbilder) und die verlustbehaftet komprimierten Formate, wie das JPEG-Format. Bei dem Schema für verlustfrei nichtkomprimierte Formate, wie das BMP-Format wird die LSB-Methode (Least Significant Bits) zum Einbetten verwendet. Diese Methode verbirgt die Information im jeweils niederwertigsten Bit jedes einzelnen Pixels. Das Bild hat eine Farbtiefe von 24 Bit, dabei stehen jeweils 8 Bit für den Rot-, Grün- und Blauanteil (RGB). Im Folgenden seien drei Bildpunkte durch folgende Farbwerte definiert:

Rot	Grün	Blau
(00100111	11101001	11001000)
(00100111	11001000	11101001)
(11001000	00100111	11101001)

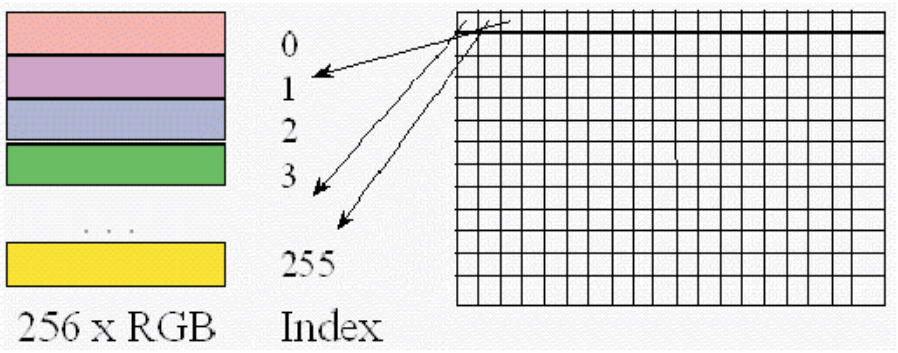
Das Verstecken des ASCII-Zeichen S (01010011) in diesen Bildpunkten liefert das folgende Steganogramm:

Rot	Grün	Blau
(00100110	11101001	11001000)
(00100111	11001000	11101000)
(11001001	00100111	11101001)

Dabei werden nur drei Bits verändert. Für das menschliche Auge ist keine Änderung feststellbar, da sich die Farbwerte des Bildes allenfalls um eine Farbstufe ändern. Insgesamt können in einem 24-Bit Image pro Pixel 3 Bits an Information verborgen werden. Das liefert 3 x Höhe x Breite [Bits] zum Einbetten. Bei einem 200 x 200 Pixel Bild sind das 117 KB. Ein Nachteil bei Bildern im BMP-Format ist, dass diese schnell die Größe von einigen Megabytes erreichen und als E-Mail-Anhang häufig zu groß und deshalb zu auffällig für Steganographie sind. Die LSB-Methode ist einfach zu implementieren, sie ist aber nicht sehr widerstandsfähig gegenüber Angriffen. Zusätzlich bewirkt eine leichte Bildmanipulation, dass die geheime Nachricht nicht wieder ermittelt werden kann. Die Konvertierung von BMP oder GIF in JPEG zerstört die in den LSBs verborgene Information.

Das Schema für verlustfrei komprimierte Formate (Indexfarbenbilder, wie das GIF-Format) verwendet auch die LSB-Methode, jedoch mit einer durch die Komprimierung bedingten Änderung. Beim GIF-Format werden die 256 wichtigsten Farben in einer eigenen Farbpalette gespeichert (vgl. Abbildung 8).

Abbildung 8: GIF-Format
(Quelle: Hübner 2003, S.8)

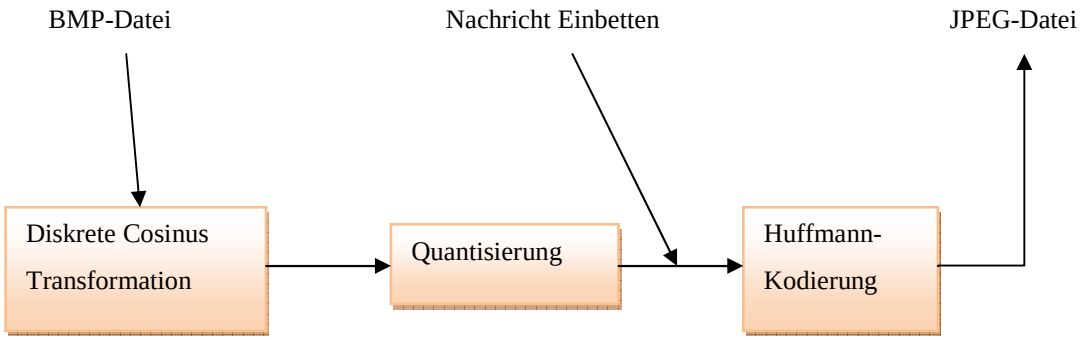


Jedes Pixel verweist auf den entsprechenden Indexeintrag in der Palette. Damit ergibt sich eine Speicherung von nur noch 1 Byte pro Bildpunkt. Der Algorithmus

muss beim Einbetten des LSB´s die Farbpalette neu sortieren, damit die hervorgerufene Farbänderung möglichst gering erscheint. Diese Indexfarbenbilder sind nur rund ein Drittel so groß wie True Color Bilder. Insgesamt sind bei dieser Methode nur noch Höhe x Breite [Bits] zum Einbetten verfügbar. Folglich ergibt das bei einem 200 x 200 Pixel-Bild nur noch 39 KB. Vorteilhaft bei dem GIF-Format ist, dass es wohl das verbreitetste und damit unauffälligste Format im Internet und somit z.B. als E-Mail Anhang geeignet ist.

Weiterhin gibt es bei Bilddateien die verlustbehaftet komprimierten Formate. Diese Formate erreichen sehr hohe Kompressionsraten, wobei das Bild geringfügig geändert wird. Ein digitales Bild, das mit JPEG komprimiert und wieder dekomprimiert wird, bei dem wird das Ergebnis nicht genau das Bild sein, das man anfangs hatte. Diese Änderung beeinflusst die niederwertigsten Bits und somit auch die Nachrichtenbits, deshalb muss hierbei eine andere Technik verwendet werden. Das JPEG verwendet das DCT-Verfahren (Diskrete-Kosinus-Transformation), um eine Datenreduktion und Kompression zu erreichen (vgl. Abbildung 9).

Abbildung 9: Entstehung eines Steganogramms bei einer JPEG-Datei
(Quelle: Hübner 2003, S.8)



Das zu bearbeitende Bild wird in Blöcke von 8x8 Bits unterteilt. Über die Pixel wird die Kosinus-Funktion gelegt um diese darzustellen. Nun werden die Frequenzkoeffizienten (Häufigkeiten) dieser Kosinus-Funktion zur Beschreibung der Pixelblöcke als Abfolge von Nullen und Einsen gespeichert (Quantisierung). In dieser Frequenz können jetzt wiederum die niederwertigsten Bits genutzt werden, um Informationen zu speichern. Zum Abschluss erhält das Bild eine Farbtabelle mit sehr ähnlichen, benachbarten Farbeinträgen. Da die Huffmann-Kodierung verlustfrei

arbeitet, kann die Nachricht auf dem Rückweg durch die entsprechende Dekodierung extrahiert werden.

3.2.2. Einbettungstechniken bei Audiodateien

Audiodateien haben die Eigenschaft, dass durch die Digitalisierung Rauschen entsteht. Ursachen für dieses Rauschen können Hintergrundgeräusche analoger Daten sein, oder das elektrische Rauschen. Auch dadurch, dass die Konvertierung von Stimmen und Tönen zu Bits nicht perfekt ist, entsteht Rauschen. Informationen können in diesem Rauschen versteckt werden. Wie bei Bilddateien wird auch hier unter anderen die LSB-Methode verwendet. Audiodateien im WAV-Format arbeiten nicht nach dem Prinzip der Datenreduktion, deshalb wird hier die LSB-Methode verwendet. Dabei liegt die Datenaufnahme bei 1/8 bis 1/16 der Trägerdatei.

Zusätzliche Methoden bei Audiodateien sind: Das Ausschneiden von Passagen und durch akustisch gleichwertige ersetzen, Passagen mehrfach duplizieren oder Ein künstliches Echo einfügen. Es gibt auch Verfahren, die auf Basis menschlicher Psychoakustik basieren, z.B. überschatten lautere Töne leisere Töne. Hierbei könnte man die leiseren Töne als Versteck für geheime Informationen nutzen. Eine andere Eigenschaft menschlicher Psychoakustik ist, dass für kurze Zeit nach einem lauten Ton das Gehör „taub“ ist. Diese kurze Zeit könnte auch als Versteck dienen.

Das MP3 (MPEG3) Verfahren benutzt zur Datenkompression und -reduktion das Huffmann-Verfahren. Dabei werden Daten Paketweise in einer Tabelle gespeichert. Die Reduktion erfolgt durch das Zusammenfassen gleicher Passagen in einer Zelle der Tabelle. Die Wiederholung der Passagen wird durch eine Referenz zum entsprechenden Tabelleneintrag realisiert. Informationen werden, z.B. durch das Ersetzen Psychoakustisch unrelevanter Zellen oder durch das Einfügen neuer Zellen, die nicht gespielt werden, eingebettet.

4. Angriffe

In der Steganographie wird bei Bilddateien zwischen zwei Arten von Angriffen unterschieden, den visuellen und den statistischen Angriffen.

Beim visuellen Angriff wird das Hintergrundrauschen eines Trägermediums untersucht. Eine Nachricht die nicht über das gesamte Trägermedium verteilt wurde, kann dadurch relativ einfach entdeckt werden. Dabei wird die vermutliche steganogrphische Nachricht vom Trägermedium getrennt. Bleibt die Struktur des Trägermediums erhalten so ist die Wahrscheinlichkeit gering, dass es sich um ein Steganogramm handelt. Ist jedoch keine Struktur erkennbar, dann kann man davon ausgehen, dass geheime Daten im Träger enthalten sind. Im Steganogramm (vgl. Abbildung 10) ist eine horizontal verlaufende Grenze sichtbar, diese lässt darauf schließen, dass Daten versteckt wurden.

Abbildung 10: Visueller Angriff
(Quelle: Westfeld 2000, S.8)

Trägerdaten

Steganogramm

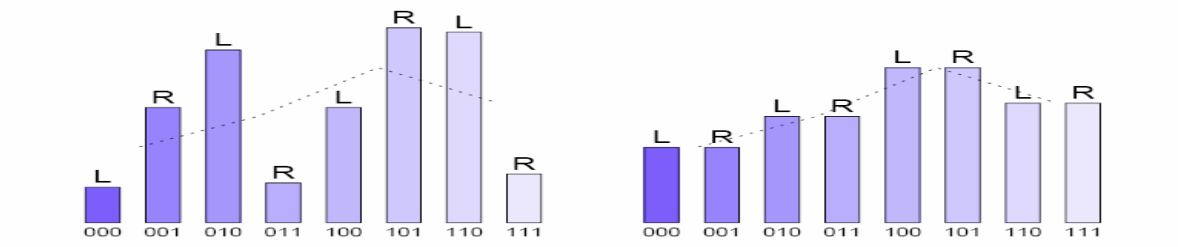
Durch die folgende Methode lässt sich beweisen, dass ein Steganogramm vorliegt. Es wird jedes Pixels durch das LSB des Pixels ersetzt. Ist das LSB 0, wird das Pixel schwarz und sonst weiß gefärbt. Bei einem natürlichen Bild ist das LSB von den anderen Bits des Pixels und somit vom Bildinhalt abhängig. Besteht das LSB-Bild nur aus rauschen, so ist die Wahrscheinlichkeit groß, dass es sich um

eingebettete Daten handelt. Die obere Hälfte des rechten Bildes ist stark verrauscht (vgl. Abbildung 11).

Abbildung 11: Färbung der Pixel beim visuellen Angriff
(Quelle: Westfeld 2000, S.9)

Beim statistischen Angriff wird nur der Vergleich zwischen Farbhäufigkeiten und Verteilung der Mittelwerte durchgeführt, da keine Veränderungen des Mittelwertes durch den Algorithmus entstehen. Es werden die Farbwerte untersucht, die sich nur im letzten Bit unterscheiden, z.B. 000 und 001. Diese beiden Farbwerte kommen in einem normalen Bild unterschiedlich häufig vor. In einem Steganogramm gleichen sich die Häufigkeiten dieser beiden Farbwerte durch den steganographischen Algorithmus an (vgl. Abbildung 12).

Abbildung 12: Farbverteilung beim statistischen Angriff
(Quelle: Westfeld 2000, S.11)



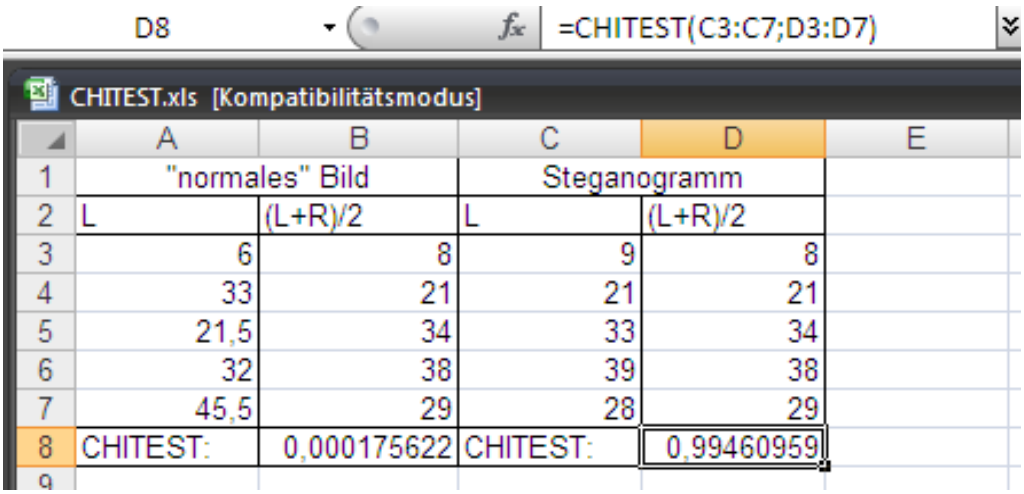
Farbverteilung in einem normalen Bild

Farbverteilung in einem „unsauberen“ Bild

Erkennung eines Steganogramms erfolgt durch die Angleichung der Farbpärchen. Dabei listet man die L-Farbwerte aller Paare (L) und die Mittelwerte aller Paare

((L+R)/2) auf (vgl. Abbildung 13). Die Mittelwerte ändern sich durch die Einbettung von Daten nicht. Dann werden die L-Werte mit den Mittelwerten mit dem Chi-Quadrat-Test verglichen. Das Ergebnis des Tests liefert die Wahrscheinlichkeit für das Vorliegen eines Steganogramms.

Abbildung 13: Chi-Quadrat-Test beim statistischen Angriff



	A	B	C	D	E
1	"normales" Bild		Steganogramm		
2	L	(L+R)/2	L	(L+R)/2	
3	6	8	9	8	
4	33	21	21	21	
5	21,5	34	33	34	
6	32	38	39	38	
7	45,5	29	28	29	
8	CHITEST:	0,000175622	CHITEST:	0,99460959	

5. Schlussfolgerungen

Die Möglichkeiten, die die Steganographie bietet, spielen bei den Sicherheitstechniken der Kommunikation eine bedeutende Rolle. Die vertrauliche Kommunikation besteht darin, dass außer dem Sender und dem Empfänger keine dritte Person an die vertrauliche Information gelangt. Die Besonderheit zum Schutz des Vertraulichen bei der Steganographie ist, dass die geheime Information versteckt wird. Das Geheime muss also erstmal entdeckt werden und außerdem lassen sich bei dem Verdacht auf eine versteckte Nachricht immer noch verschiedene Botschaften herauslesen.

Die Steganographie wird die Kryptographie keinesfalls ersetzen. Vielmehr gilt sie als ihre Ergänzung, da die Steganographie nicht so robust gegenüber Angriffen wie die Kryptographie ist. Deshalb ist es sinnvoll beide Techniken zu verbinden. Maximale Sicherheit gegenüber „Angreifern“ erreicht man, indem die Nachricht mit

krypto-graphischen Verfahren verschlüsselt und zudem durch Steganographie versteckt wird.

Die Güte eines Stegosystems hängt entscheidend von der Wahl der Hülldaten und einer dazu passenden Einbettungstechnik ab. Hülldaten sollten Stellen enthalten die zufällig bzw. unberechenbar sind. Einbettungstechniken sollten adaptive Algorithmen verwenden bei denen die Eigenschaften der Hülldaten untersucht und berücksichtigt werden.

Zurzeit gibt es sehr viele Steganographie-Programme, die im Internet frei verfügbar sind.[6] Mit diesen Programmen kann also jeder Steganographie betreiben. Dabei sollte man allerdings beachten, dass nicht jede Software gegenüber bekannten Angriffen sicher ist.

Literaturverzeichnis

Breetzmann, R. (2000). Die Methoden der Steganographie; http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/rbreetzmann/ einf.html, Stand: 03.02.07

Hübner, C. (2003). Grundlagen der Steganographie; http://www-ra.informatik.uni-tuebin-gen.de/lehre/ws02/pro_sicherheit_ausarbeitung/Huebner_Steganographie.pdf, Stand: 03.02.07

Schuster, M. (2002/03). Steganographie; http://www.logic.at/people/schuster/stego _ms. pdf, Stand: 03.02.2007

Steurer, J. Steganographie; http://wwwspies.in.tum.de/lehre/seminare/SS00/prosem/steurer.pdf, Stand: 03.02.07

Westfeld, A. (2000). Prinzipien sicherer Steganographie; http://os.inf.tu-dresden.de/~westfeld/publikationen/kurz.pdf, Stand: 03.02.07

[6] Beispiele zur Steganographie-Software sind im Internet zu finden (siehe: http://www.cipherbox.de/down-stegano.html).

Westfeld, A.: Angriffe auf steganographische Systeme; http://os.inf.tu-dresden.de/~westfeld/publikationen/vis99.pdf, Stand: 03.02.07

Wikipedia: Steganographie; http://de.wikipedia.org/wiki/Steganografie, Stand: 03.02.07