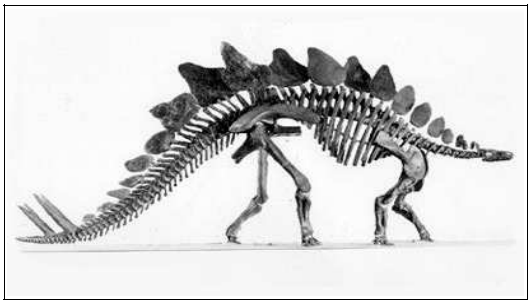


Steganographie
im Wandel der Zeit

Nils Babion
MT 99, 29652

29.07.2003

Ergänzungslehrgebiet „IT-Sicherheit und Datenschutz“
Dipl.-Wirtsch.-Inf. Jana False, Martin Heise
SS 2003
TU Ilmenau

Zusammenfassung

Diese Arbeit hat die Steganographie zum Thema. Es soll erläutern werden, was der Begriff bedeutet und was man unter Steganographie versteht. Einige Beispiele aus der Geschichte sollen zeigen welche unterschiedlichen Arten für angewandte Steganographie es gab und gibt. Um zu verdeutlichen, wie die Steganographie heute Anwendung findet, werde ich das Verfahren der rechnergestützten Steganographie erläutern. Der letzte Abschnitt soll verdeutlichen was ein gutes Steganogramm ausmacht und was beim Erstellen zu beachten ist. Abgeschlossen wird die Arbeit mit einem Fazit.

1. Einleitung

Der Begriff Steganographie kommt aus dem Griechischen, von den Worten 'steganos' für heimlich oder verdeckt und 'graphein' was schreiben bedeutet, zusammen ergibt sich die Kunst des geheimen Schreibens. Bis 1967 wurde Steganographie gleichbedeutend mit Kryptographie gebraucht. Der Historiker David Kahn definierte damals den Begriff neu, demnach ist die Steganographie das Verfahren um die Existenz einer geheimen Botschaft zu verbergen, diese kann chiffriert sein, muss sie allerdings nicht notwendigerweise sein. Anders als bei der Kryptographie soll also eine Nachricht Dritten entgehen, indem allein ihre Existenz verschleiert wird.

Die Steganographie ist eine der ältesten und effektivsten Verfahren, um Nachrichten vor Dritten zu verbergen. Schon die Ägypter versteckten geheime Warnungen und Nachrichten in Grabbeigaben und Inschriften.
Ob nun das Schreiben mit unsichtbarer Tinte in Agentenmanier oder das Verbergen einer Nachricht im Rauschen eines Audio-Files, Möglichkeiten für das verstecken von Informationen in Trägermedien gibt es viele.

Um das Prinzip der Steganographie zu verstehen hier ein kleines Textbeispiel aus dem 17. Jahrhundert. Den folgenden Text bekam Sir John Trevanion, ein überzeugter Royalist zu Zeiten Oliver Cromwells, als er auf Colchester Castle auf seine Hinrichtung wartete.

> Worthie Sir John:-Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much that I can do: but what I can do, bee ye verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honour, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if bie submission you can turn them away, 'tis the part of a wise man. Tell me, an if you can, to do for you anythinge that you woulde have done. The general goes back on Wednesday. Restinge your servant to command.-R.T.

In diesem Fall war es so, dass die Nachricht in jedem dritten Buchstaben nach einer Interpunktion versteckt war. Sir John muss einen Tipp bekommen haben, er entschlüsselte folgende Nachricht „panelateastendofchapelslides“, auf deutsch „Die Täfelung am östlichen Ende der Kapelle kann verschoben werden“. Er bat darum eine Stunde in der Kapelle in sich gehen zu dürfen und wart nie wieder gesehen.
Wenn man sich den Text durchliest und den Schlüssel nicht kennt, wird man in diesem Text auf Anhieb keine Nachricht vermuten. Auch Sir Johns Häscher ließen die Nachricht zu ihm passieren.

An diesem Beispiel werden vier Eigenschaften des steganographischen Verfahrens deutlich:

- Es ist eine riesige Vielfalt von steganographischen Verfahren denkbar
- Die verborgene Nachricht ist um einiges kleiner als das Trägermedium
- Auch wenn ein Verdacht besteht, dass in einem Medium eine Nachricht enthalten ist, kann sie ohne den erforderlichen Schlüssel nur schwer aufgespürt werden.
- Ein Problem der Steganographie ist immer auch, dass die Nachricht übersehen werden kann.

2. Klassische Steganographie

Die Steganographie ist eines der ältesten Verfahren, um Nachrichten vor Dritten zu verbergen. Schon in der Antike kam sie vor allem im militärischen Bereich und der Politik zum Zuge. Im folgenden Abschnitt möchte ich einen Überblick über verschiedene Anwendungen der Steganographie geben und diese an Hand von historische n Beispielen illustrieren.

2.1 Verdeckte Nachrichten

Um 500 v. Chr. berichtet der griechische Geschichtsschreiber Herodot über den Konflikt zwischen Griechenland und Persien, der um 480 v. Chr. seine Hoch-Zeit hatte. Damals vergrößerte der despotische Anführer der Perser, Xerxes, das Persische Reich durch aggressive Expansion. Um einer Vernichtung zu entgehen und den König der Könige milde zu stimmen, sandten die umliegenden Staaten Geschenke und Abgaben an Xerxes. Nur Sparta und Athen weigerten sich, sich dem Persischen Herrscher zu unterwerfen. Gegen 480 v. Chr. hatte Xerxes eine riesige Streitmacht aufgestellt, um die Griechen durch einen Überraschungsangriff zu unterjochen.
Einem verstoßenen Griechen, Demaratos, der in der persischen Stadt Susa im Exil lebte, war die Aufrüstung der Perser nicht entgangen. Um seine Landsleute zu warnen und die Nachricht unbemerkt übermitteln zu können, bediente er sich eines Tricks, er schabte das Wachs von einer Schreibtafel ab, dem damals gebräuchlichen Mittel zum Austausch von Schriften, und gravierte eine Warnung in das dahinter liegende Holz, dann deckte er das Ganze erneut mit Wachs ab.
Die Nachricht erreichte unentdeckt ihren Bestimmungsort und konnte von den Griechen ausgewertet werden. Binnen kürzester Zeit stellten sie eine Gegenstreitmacht auf und als schließlich der Angriff der Perser erfolgte konnte Xerxes Streitmacht innerhalb eines Tages vernichtend geschlagen werden.

In einer anderen Episode berichtet Herodot über Histiaeus, der Aristagoras von Milet zum Aufstand gegen den persischen König anstacheln wollte. Histiaeus rasierte dazu einem Boten den Kopf und brannte seine Nachricht in die Kopfhaut des Kuriers. Nachdem die Haare nachgewachsen waren, brach der Kurier auf, bei Aristagoras angelangt, rasierte er sich den Kopf und präsentierte die Nachricht im Klartext.

Man kann sich natürlich noch viele weitere Orte ausdenken an denen man eine Nachricht verstecken kann. So sind z.B. auch Berichte aus dem alten China bekannt, in denen beschrieben wurde, dass Texte auf Seide verfasst in Wachs ummantelt wurden und dann von Boten geschluckt wurden.
Ob nun der Magen eines toten Tieres, eine Truhe mit einem doppelten Boden oder ein Geheimfach im Schuhabsatz eines Kuriers, der Phantasie sind keine Grenzen gesetzt. Wird der Ort allerdings entdeckt liegt die Nachricht sofort im Klartext vor.

2.2 Unsichtbare Tinte

Schon im alten Rom war man mit dem Gebrauch von unsichtbarer Tinte vertraut um Nachrichten in harmlos erscheinenden Texten zu verbergen.
So berichtet der römische Schriftsteller Plinius der Ältere in seinem Werk „Naturgeschichte“ (23-79 n. Chr.) vom Gebrauch der Milch der Thithymallus-Pflanze, die man benutzte um Nachrichten auf Pergament zu schreiben. Nach dem Trocknen war von dem Text nichts mehr zu sehen. Erst wenn das Pergament vom Empfänger über eine offene Flamme gehalten wurde und so die organischen Verbindungen in der unsichtbaren Tinte denaturierten, wurde die Botschaft mit bräunlicher Färbung wieder sichtbar. Viele andere organische Flüssigkeiten, die Kohlenstoffverbindungen enthalten, sind ebenfalls für den Gebrauch als unsichtbare Tinte einsetzbar. Dies wären z.B. Milch, Essig, Zitronensaft, Zwiebelsaft und auch Urin.

Im 15. Jahrhundert beschrieb der italienische Wissenschaftler Giovanni Porta, wie man eine Nachricht auf der Oberfläche eines hart gekochten Eis verstecken kann. Wenn man eine Unze Alaun[1] in einem Becher Essig auflöst, ergibt sich eine Art Tinte. Schreibt man nun mit diesem Gemisch auf eine Eierschale eines hart gekochten Eis, so dringt die Flüssigkeit durch die poröse Kalkschale und schlägt sich auf dem gehärteten Eiweiß nieder und hinterlässt eine Botschaft.

Im ersten Weltkrieges kam die „unsichtbare Tinte“ noch zum Einsatz. Agenten verwendeten sog. sympathetische Tinten (z.B. Kupfersulfat oder Natriumhypochlorid) um Nachrichten vor den Augen des Feindes zu verbergen. Anders als bei den organischen Verbindungen, bei denen meist einfaches Erwärmen ausreichte, um die Nachricht wieder sichtbar zu machen, musste man die so verfassten Botschaften z.B. dem Ammoniak-Dampf-Test unterziehen.

Auch heutzutage kommt unsichtbare Tinte noch zum Einsatz. Dank der modernen Chemie ist es möglich Flüssigkeiten zu erstellen die nur bei Einsatz von UV-Licht und Bestrahlung mit einer ganz bestimmten Wellenlänge sichtbar sind. Ohne Licht dieser speziellen Wellenlänge und ohne das UV-Licht bleibt die Nachricht verborgen.

2.3 Verbergen durch Miniaturisieren

Im Jahre 1941 entdeckte das FBI den ersten Mikropunkt. Auf einen anonymen Hinweis versandte Briefe auf schimmernde Punkte zu untersuchen. Nach diesem Fund tauchten regelmäßig sog. '*Microdots*' auf. Man fand sie in Telegrammen, in Briefen und unter Briefmarken. Es handelte sich dabei um ein Verfahren der Mikrophotographie, das deutsche Wissenschaftler in den 20er Jahren des 20. Jahrhunderts entwickelt hatten. Mit Hilfe dieses Verfahrens war es möglich die Inhalte ganzer DIN A-4-Seiten auf die Größe eines i-Punktes zu bringen. Die Mikropunkte wurden dann auf die Oberfläche eines harmlosen Briefs aufgeklebt. Sie wurden vor allem von deutschen Agenten in Süd-Amerika zur Kommunikation benutzt.

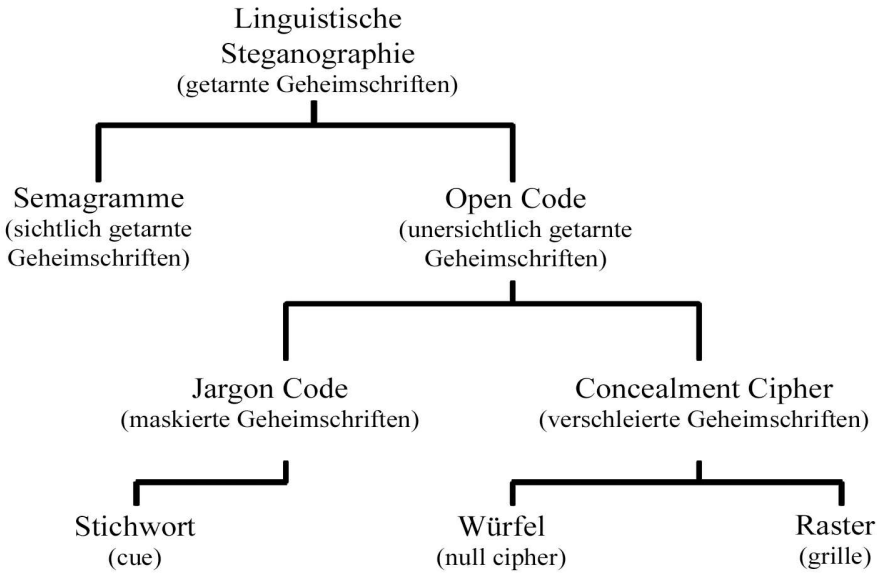
1Alaun: Kalium-Aluminium-Sulfat, wird zum Beizen von Stoffen und zum Gerben von Leder verwendet.

Die Mikrophotographie hatte schon eine wichtige Rolle im 19. Jahrhundert gespielt. Im Krieg zwischen Preussen und Frankreich wurden wichtige Informationen auf Mikrofilm übertragen und dann mit Hilfe von Brieftauben versandt.

Durch die Weiterentwicklung der Lasertechnik sind ganz neue Varianten des Verbergens von miniaturisierten Nachrichten möglich. Der CIA hat z.B. mit Hilfe eines Mikrolasers chiffrierte verkleinerte Botschaften in ganz gewöhnlichen Zeitschriften und neben Annoncen eingebrannt. Nur mit Hilfe von leistungsfähigen Vergrößerungsgeräten war es möglich diesen Text wiederherzustellen.

2.4 Linguistische Steganographie

Neben den traditionellen, technischen Methoden der Steganographie gibt es einen Zweig der sich mit dem Verbergen von Inhalten in Texten, Bildern und Symbolen beschäftigt, die sog. Linguistische Steganographie.

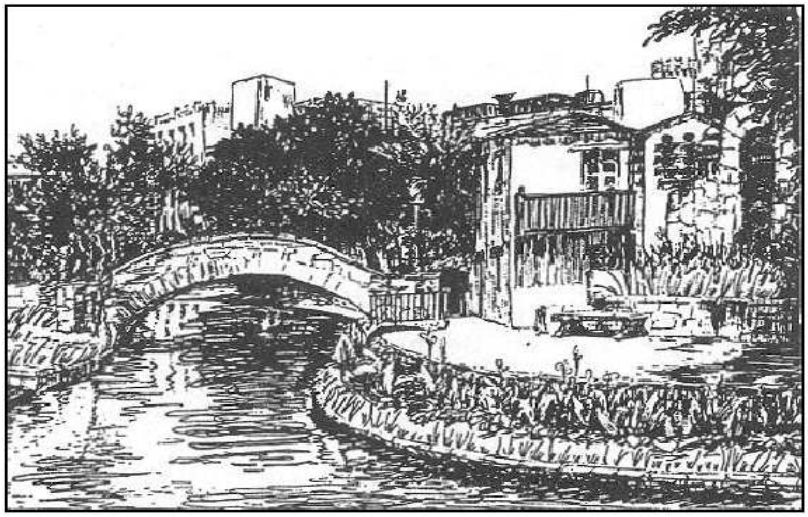


Diese gliedert sich in zwei große Gruppen, zum einen das Verbergen von Botschaften in Details einer Schrift oder eines Bildes (Semagramm) und dem Verbergen einer Nachricht innerhalb einer unverfänglichen Botschaft (Open Code).

2.4.1 Semagramm

Unter einem Semagramm versteht man das Verbergen einer geheimen Nachricht in den Eigenheiten einer Schrift oder in Details eines Bild. So machten sich Steganographen die Angewohnheit von Schreibern zu Nutze in längeren Worten die einzelne Buchstaben nicht zu verbinden. Ebenso konnte ein nach oben gerichteten Aufschwung eines Buchstabens das Ende einer Buchstabengruppe bedeuten.
Um Nachrichten in Texten zu verbergen wurde auch die Möglichkeit genutzt einzelne Buchstaben tiefer zu stellen als andere oder zwei verschieden Schriftarten zu verwenden. Ein klassisches Beispiel ist auch einzelne Buchstaben in einem Text mit Nadelstichen zu versehen, wird das so präparierte Material gegen ein Licht gehalten, erscheint die Botschaft.

Ein Beispiel für eine verborgene Botschaft in einem Bild kommt aus '*The Codebreakers*' von David Kahn.



Die Nachricht in diesem Bild von 1945 steckt in den Grashalmen im Vordergrund, im Morse-Code bedankte sich der Künstler für einen schönen Aufenthalt in San Antonio. Man kann sich natürlich leicht vorstellen, dass Semagramme in Zeiten des Krieges benutzt wurden, um Landkarten und taktische Informationen über Truppenaufstellungen an die Heimat weiterzuleiten.

2.4.2 Open Code

Von weitaus größerem Interesse als die sichtlich getarnten Semagramme sind allerdings unersichtlich getarnten Geheimschriften. Bei einem Semagramm kann auch ein uneingeweihter Betrachter auf eine verborgen Nachricht aufmerksam werden. Bei den Open-Code-Verfahren ist dies nicht so einfach. Sie beruhen zum großen Teil auf Absprachen zwischen Sender und Empfänger und die Verwendung von Spezialausdrücken.

2.4.2.1 Jargon Code

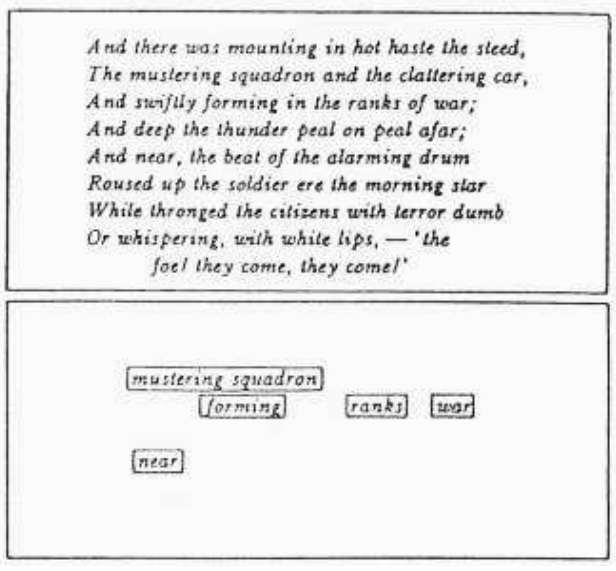
Schon in alten Kulturen war es Gang und Gebe Nachrichten durch die Verwendung von Geheimausdrücken zu übertragen und diese zu Maskieren. Die Maskierung bedient sich einer gesellschaftlicher und beruflicher Sondersprache.
Besonders im militärischen Bereich, aber auch im kriminellen Milieu ist dieses auch heute noch normal. So können '*Zigarren*' für Kriegsschiffe stehen und '*Schnee*' für Heroin. Einem geübten Leser fallen solche Botschaften leicht auf, der Text kann gekünstelt und gestelzt wirken. Durch einfaches Umformulieren und Ersetzen von Begriffen durch Synonyme geht die Botschaft verloren.
Ein wichtiger Spezialfall des Jargon Codes ist das '*Stichwort*'. Ein im Vorfeld ausgemachter Satz kann somit ein eingetretenes Ereignis bestätigen oder eines herauf beschwören. So kann die Wettermeldung '*...Ostwind und starker Regen ...*' für einen Angriff auf Japan stehen. Im zweiten Weltkrieg verwendete das amerikanische Oberkommando diese Möglichkeiten um geheime Botschaften an ihre Generäle der Westfront zu übertragen.

2.4.2.2 Würfelverfahren

Anders als beim Jargon Code, in dem die Nachricht sich hinter einzelnen Begriffen verbirgt, ist die Botschaft beim Würfelverfahren in Teile eines unverfänglichen Textes eingebettet und mit Nieten, Blendern und Füllzeichen versehen. Die einzelnen Zeichen sind im Text '*verwürfelt*'.
Das erste Beispiel für Steganographie aus der Einleitung, durch das Sir John Trevanion so glanzvoll die Flucht gelang, ist ein Beispiel für das Würfelverfahren. Die Botschaft war hier in jedem dritten Zeichen nach einer Interpunktion enthalten. Es ist klar, dass die Regeln dieses Verfahrens im Vorfeld zwischen dem Sender und dem Empfänger abgemacht sein müssen. Auch diese Art der Tarnung ist von einem geübter Leser recht leicht an der zum Teil recht künstlichen Art des Textstils zu bemerken.
Eine Sonderform des Würfelverfahrens ist das Akrostichon[2]. Die Botschaft ist in den ersten Buchstaben, Silben oder Worten aufeinander folgender Verse, Strophen, Abschnitte oder Kapitel eines Textes enthalten. Das Akrostichon war sicher gegen Einfügung von neuen Textpassagen in bestehende Texte, es stellt somit die erste Form einer fehlerresistenten Codierung da.

2.4.2.3 Rastertechnik

Die Rastertechnik geht auf den berühmten italienische Arzt und Mathematiker Gerolamo Cardano zurück (1501-1576). Dabei wird eine Schablone verwendet um einen geheimen Text zu schreiben, der dann mit Fülltext umrandet wird. Diese Methode ist recht unhandlich, außerdem muss sowohl auf Sender- wie auf Empfänger-Seite die gleiche Schablone vorliegen.



Ein Beispiel ist dieser hypothetische Text von Lord Byron (1788-1824).

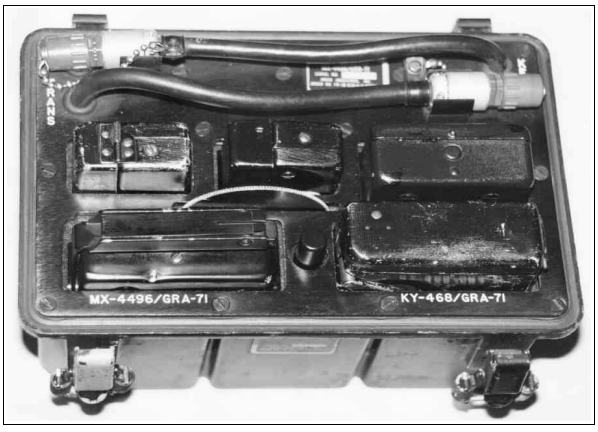
2 Akrostichon (grch.: *akros Spitze*; *stichos* Vers) ist die Versform, bei der die Anfänge (Buchstaben bei Wortfolgen, oder Worte bei Versfolgen) hintereinander gelesen einen Sinn ergeben. (aus http://de.wikipedia.org)

2.5 Gegenmaßnahmen zu Kriegszeiten

Es sollte klar sein, dass für jede Möglichkeit des Verbergens von Informationen eine Gegenmaßnahme existiert, um diese zu unterbinden. In den USA und Großbritannien nahmen diese Maßnahmen fast paranoide Formen an. Nach dem Angriff auf Pearl Habor erließ die amerikanische Zensurbehörde einige Restriktionen, diese betrafen Zeitungsartikel und Anzeigen, ebenso wie Kommentare in Schulzeugnissen. Lose Briefmarken wurde durch neue ersetzt, oder an andere Stellen geklebt um z.B. den Microdot vorzubeugen.
Das Verschicken von Schachaufgaben, Kreuzworträtseln, Zeitungsausschnitten, Strickmustern und Kinderzeichnungen war komplett untersagt. Liebesbriefe und Nähanleitungen wurden auf die Häufigkeit der enthaltenen 'X' und 'O' hin untersucht. Zum Teil wurden abgefangene Briefe sogar umformuliert, um Nachrichten, die mit dem Open-Code-Verfahren kodiert waren, unschädlich zu machen. Überseetelegramme waren nur noch sehr begrenzt nutzbar und stark überwacht. Blumenbestellungen mit ihren unterschiedlichen und mannigfaltigen Namen waren in allen alliierten Ländern verboten.

2.6 Technische Verfahren der Steganographie

Mit dem Aufkommen der modernen Nachrichtentechnik wollte man auch eine sichere Kommunikation über das Fernsprechnetz ermöglichen. Vor allem das Militär aber auch Geschäftsleute waren sehr daran interessiert das Fernsprechgeheimnis zu bewahren. Mit Hilfe von Verzerrergeräten und Stimmen-Modifikatoren sollte die Verschleierung von mündlichen Mitteilungen erreicht werden. Diese Art der Fernsprechverschlüsslung bezeichnet man als '*Ciphony*'[3], durch Möglichkeiten der Frequenzmodulation, aber auch dem Vertauschen einzelner Frequenzen und dem Vertauschen einzelner Segmente des Audiomaterials mittels eines Scramblers konnte eine gewisse Sicherheit gewährleistet werden.



Das Bild zeigt ein AN/GRA-71-'B*urst-Coder*'-Gerät.

Ende der 70er Jahre wurde in den USA das AN/GRA-71 entwickelt, ein Gerät das neben Impulsmodulation auch die Hochfrequenztechnik nutzte um Nachrichten zu verbergen. Die Nachricht wurde auf einem Tonband im Morse-Code aufgezeichnet.

3 Ciphony : Kunstwort aus '*cipher*', Chiffre und '*telephony*', Fernsprechwesen

Nun erfolgte eine starke Kompression der Information mit Hilfe des AN/GRA-71. Dazu wurde die Aufzeichnung um bis zu 40 Mal schneller aufgezeichnet und übertragen. Somit war es möglich eine einminütige Morse-Sendung in 1,5 Sekunden zu übertragen. Sendungen dieser Art waren nur sehr schwer abzufangen und zu entschlüsseln, da die Übertragung nur sehr kurz war. Mit einem gewöhnlichen Empfänger war es nicht möglich alle Frequenzen, die Informationen enthielten, abzufangen. Mit dem AN/GRA-71 war es möglich, dass viele unterschiedliche Teams den gleichen Kanal nutzen konnten. Diese Technik wurde von Agenten der CIA und von in Feindgebiet operierenden Spezialeinheiten genutzt (z.B. Rangers der US-Armee).

Eine weitere Technik die genutzt wird, um Kommunikation zu verschleiern und Daten sicher zu übertragen, ist die sog. Spektrumserweiterung. Bei diesem Verfahren wird ein größerer Anteil des Frequenzspektrums genutzt. Digitale Datenpackete werden dabei in scheinbar zufälliger Abfolge über eine Vielzahl von Kanälen bei ständigem Wechsel der Frequenz gesendet. Wird diese Sendung von einem gewöhnlichen Empfänger abgehört bekommt dieser nur Wellensalat. Durch die Entwicklung von immer schnelleren Signalprozessoren sind immer schnellere Wechsel der Frequenz möglich, dadurch ist die Wahrscheinlichkeit einer Entschlüsslung immer geringer.

2.7 Rechnergestützte Steganographie

Nach diesem historischen Überblick der steganographischen Techniken sieht man ganz klar, dass diese Art der verdeckten Kommunikation vor allem im militärischen und politischen Sektor zur Anwendung kam.
Mit der zunehmenden Technisierung der Gesellschaft und der Durchdringung aller Lebensbereiche mit moderner Rechentechnik und deren Vernetzung stehen allerdings auch dem gewöhnlichen Menschen immer mehr Möglichkeiten der steganographischen und kryptographischen Kommunikation offen.
Die Übertragung von Bilden, Texten und Sprache findet heute oft nur noch digital statt. Mit rechnergestützter Steganographie ist es nun möglich in diese digitalen Inhalte weitere geheime Botschaften zu packen, ohne dass ein potentieller Lauscher eine Veränderung des Materials wahrnehmen würde. Immer schnellere Computertechnik erledigt die steganographische Verschlüsslung in einem Bruchteil der Zeit, die früher einmal für solch komplizierte Verschlüsslung notwendig war. So kann heute der einfache Bürger kommunizieren ohne, dass es staatlichen Geheimdiensten möglich ist diese Inhalte einzusehen. Natürlich muss man unter diesem Licht die Steganographie und ihre Möglichkeiten auch kritisch sehen. Zum einen bietet sie dem Privatmann sehr sichere Möglichkeit zu kommunizieren, zum anderen ermöglicht sie auch einem Feind eines Staatssystems eine verdeckte, nicht wahrnehmbare Kommunikation.
Heute unterscheidet man zwei Einsatzfelder in denen Steganographie zum Tragen kommt. Zum einen in dem Bereich der **unsichtbaren Kommunikation**, in diesen fallen all die oben aufgezählten Beispiele und Ausführungen. Hierzu zählen auch die '*Covert Channels*'[4] aus dem Bereich der Betriebssystem und das Verbergen von Nachrichten in Bilder-, Text- und Audio-Files.

4 z.B. die Kommunikation zwischen zwei laufenden Prozessen über die Steuerung der Prozessorlast oder der Schreib-/Lesekopfpositionen einzelner Laufwerke.

Der zweite, heute vor allem kommerziell genutzte Bereich, ist der des **Watermarkings**. Hierbei handelt es sich um das digitale Signieren von Inhalten. Dies können Bilder, Audio-Dateien und Texte sein, die mit einer Seriennummer versehen werden, um sie so vor illegalem Kopieren und Missbrauch zu schützen.

Es stellt sich natürlich die Frage wo sich Botschaft unbemerkt verstecken lassen. Wie eben schon angesprochen, werden heute die meisten Daten digital aufgezeichnet und übertragen. Entgegen viele Vorurteile sind digitale Verfahren weit davon entfernt perfekte Möglichkeiten zur Rauschfreien Speicherung von Daten zu sein, allerdings lassen sich digitale Daten beliebig oft kopieren und die Daten sind mit einer Fehlerkorrektur versehen, so dass sie auch einen gewissen Schutz gegenüber Übertragungsfehlern bieten. Eben dieses Rauschen ist der Ort wo sich Botschaften unbemerkt verbergen lassen.

Rauschen ist überall, es umgibt uns, es kommt in allen Lebensbereichen vor. Ob nun das Quantisierungsrauschen eines A/D-Wandlers, das statische Rauschen eines CCD-Chips einer Digitalkamera, das Rauschen eines Mikrophons oder das elektrostatische Übersprechen in Schaltkreisen, überall ist Rauschen und somit sind auch alle digitalen Daten (Audio, Video, Bild) mit Rauschen überlagert.
Auch wenn die moderne Computertechnik schon sehr weit entwickelt ist, birgt sie doch einige Ungenauigkeiten im System die mit Hilfe von mathematischen Mitteln umschifft werden. So gibt es auch in digitalen Inhalten noch eine gewisse Unsicherheit und Fehlertoleranz, die dafür sorgt, dass die Inhalte trotz minimaler Unterschiede im Datenmaterial noch richtig interpretiert werden können.

Nachrichten werden heute sehr oft in digitalen Bildern versteckt von denen es Millionen im Internet gibt. Wie dieses Verbergen prinzipiell abläuft und welche Unterschiede es zwischen unkomprimierten Formaten wie BMP und komprimierten wie GIF (CompuServe Graphics Interchange Format) oder JPEG (Joint Photographic Expert Group) gibt, werde ich im nächsten Abschnitt etwas vertiefen.

2.7.1 Digitale Steganographie

Eine unkomprimierte Bilddatei, die keinerlei Techniken zur Datenreduktion oder zur Rauschfilterung verwendet, besteht eigentlich nur aus einem Array in dem die verschiedenen Farb- und Helligkeitswerte der einzelnen Bildpunkte gespeichert sind.
Geht man von einem unkomprimierten Format mit 24 Bit Farbtiefe und einer Auflösung von 1024 x 768 aus, so liegen 8 Bit pro Farbkanal (R, G, B) vor. Es sind somit pro Pixel und pro Farbkanal 256 unterschiedliche Werte möglich. Insgesamt sind 16.777.216 Farben darstellbar.

Ein Bildpunkt mit der Folge

0100 1011 0011 0101 1001 1100 entspricht dem RGB-Farbwert (75, 53, 156).
R **G** **B**

Dieser Bildpunkt hätte einen lila Farbton. Wenn wir nun das letzte Bit des roten Farbkanals von '1' auf '0' ändern um darin eine Nachricht zu verbergen hätten wir eine gewisse Farbabweichung, der Farbwert würde sich von 75 auf 74 ändern.

Diese Änderung wäre sehr gering und würde im gesamten Bild einer Farbabweichung von ca. 1 % entsprechen. Stellen wir uns nun vor wir wollen eine Nachricht im Rotkanal eines Bildes mit einer Auflösung von 1024 x 768 unterbringen. Wenn wir nur das letzte Bit ändern, hätten wir 786.432 Bit zur Verfügung um darin z.B. einen geheimen Text zu verbergen. Da wir 3 Farbkanäle zur Verfügung haben, wären dies sogar 2.359.296 Bit dies entspricht 294.912 Byte, also ca. 300 KByte. Das unkomprimierte Bild hätte eine Größe von 6.291.456 Byte. Dieses Methode der Veränderung des niederwertigsten Bits sog. Least-Significant-Bit-Insert (LSB) wird nicht nur bei Bildern, sondern auch bei Audiodateien verwendet. Die Methode ist relativ leicht zu implementieren allerdings auch sehr anfällig gegenüber Angriffen, denn schon eine einfache Konvertierung des unkomprimierten Bildes (lossless compression) in ein Bild, welches mit verlustbehafteter Kompression (lossy compression) gespeichert wird, würde die Nachricht zerstören und unbrauchbar machen. Außerdem würde die Nachricht sollte sie einem Angreifer in die Hände fallen, sofort im Klartext vorliegen.
Allerdings ist es auch heute noch in Zeiten von DSL und viel Bandbreite eher verdächtig, wenn jemand riesige unkomprimierte Dateien versendet, außerdem ist es lästig. Deshalb wollen wir nun sehen, wie Inhalte in komprimierten Formaten wir GIF und JPEG gespeichert werden können.

2.7.1.1 GIF-Format (CompuServe Graphics Interchange Format)

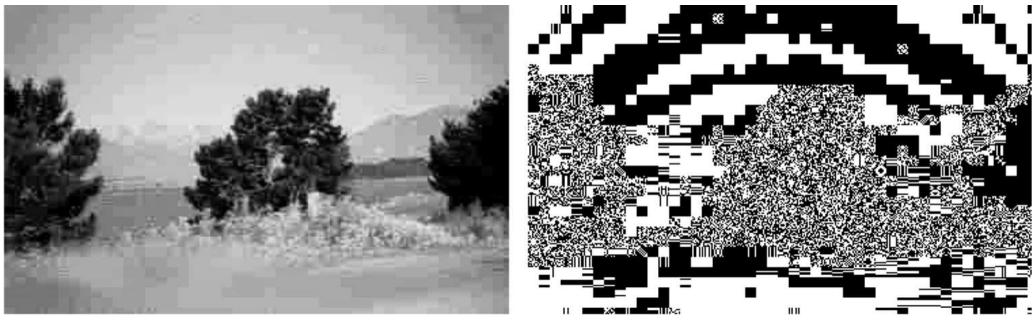
Ein Bild, dass im GIF-Format vorliegt ist prinzipiell anders aufgebaut als ein unkomprimiertes Bild. GIF hat nur 8 Bit um den Wert jedes einzelnen Pixels zu speichern, somit sind nicht mehr als 256 Farben möglich. Um die Farbmöglichkeiten bei GIF zu erweitern sind nicht alle Farben in der Palette eines Bildes enthalten, sondern diese wird aus den häufigsten 256 Farben gebildet.
Alle Pixel die einen von der Palette abweichenden Farbton haben werden auf einen ähnlichen Farbton beschränkt. Würde man die LSB-Methode bei einem Bild anwenden, welches im GIF-Format vorliegt würde sich die Farbe eines Pixels möglicherweise komplett ändern, denn der Wert würde auf einen anderen Eintrag der Palette zeigen. So könnte es sein, dass der Eintrag sich von 26 (dunkel blau) auf 27 (rot) ändert, die Änderungen im Bild wären unübersehbar.

Ein möglicher Lösungsansatz für dieses Problem wäre die Farbpalette eines Bildes von 256 auf nur 128 Farben zu beschränken und die Palette noch einmal mit den gleichen Farben zu füllen. Würde man jetzt den Wert eines Bildpunktes von 26 (dunkel blau) auf 27 ändern, würde dieser Wert ebenfalls dunkel blau entsprechen. Eine Änderung wäre somit im Bild nicht mehr auszumachen. Somit würde mit dieser Methode jeder Pixel ein Bit der Information tragen können. Führt man eine weitere Beschränkung der Palette auf nur 64, 32 oder sogar nur 16 Farben durch, kann jeder Pixel bis zu 4 Bit der Botschaft tragen. Ein Bild, dass nur 16 Farben hat ist allerdings sehr unansehnlich und könnte wieder Verdacht erwecken.

2.7.1.2 JPEG-Format (Joint Photographic Expert Group)

Das JPEG-Format birgt ein ganz anderes Problem, denn dieses Format verwendet eine verlustbehaftete Kompression (lossy compression). Ein Bild das mit dem JPEG-Algorithmus komprimiert wurde, entspricht nach seiner Dekomprimierung

nicht mehr dem Quellbild. Wie stark das Bild verändert wird, hängt vom Kompressionsgrad des Algorithmus ab. Würde man eine Nachricht mit der LSB-Methode in einem Bild verbergen, wäre diese nach der erneuten Dekomprimierung unbrauchbar und aus dem Bild entfernt.



Stark komprimierte JPEG-Datei, auf dem anderen Bild ist die Verteilung der Details zu sehen.[5]

Der JPEG-Algorithmus arbeitet so, dass er Teile des Bildes die viele Details enthalten mit mehr Frequenzen abtastet um diese optimaler anzunähern. Dazu wird das Bild zunächst in Blöcke von 8 x 8 Pixeln unterteilt. Diese werden jetzt mit Hilfe der diskreten Kosinustransformation (DKT) bearbeitet. Bereiche die viele Details enthalten werden dabei mit mehr Frequenzen abgetastet, als flächige, wenig detaillierte Bereiche.
Die Werte der Abtastung werden in einen Array geschrieben, wobei mit dem Gleichanteil des 8 x 8 Blocks begonnen wird, danach folgen die immer höheren Frequenzanteile, die bei wenig-detaillierten Stellen des Bildes meistens '0' sein können. In denen allerdings die Details des Bildes gespeichert sind. Eine Änderung dieser hohen Frequenzanteile, um dort eine Nachricht zu verbergen, fällt nicht weiter auf, da das Bild nur etwas mehr Rauschen erfährt, dieses bleibt bis zu einem gewissen Grad unbemerkbar. Eben dieser Grad beschränkt aber auch die Menge der versteckbaren Datenmenge.
Ein Verbergen ist auf eine ähnliche Art und Weise auch in MPEG-Filmen möglich.

2.7.2 Digitale Wasserzeichen

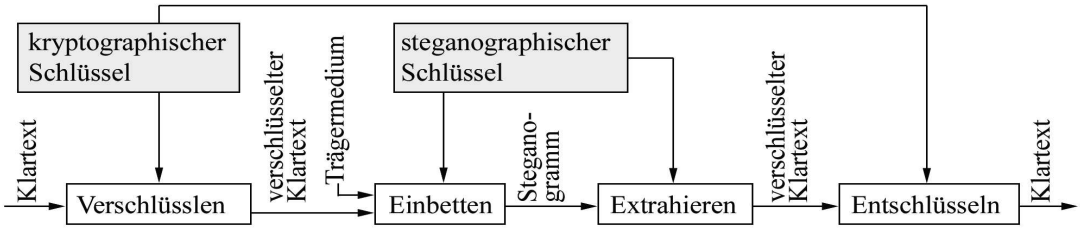
Seit der Herstellung des Papiers haben es sich Produzenten nicht nehmen lassen, ihre Produkte mit einem Wasserzeichen zu versehen, um sie unmissverständlich als ihr Werk zu kennzeichnen und die Echtheit nachzuweisen. Bei Künstlern ist es normal, dass ein Werk mit dem eigenen Namen oder Synonym verziert wird. Im digitalen Zeitalter wird diese Möglichkeit natürlich auch bei digitalen Inhalten verwendet, um z.B. den Urheber klar auszugeben.
Diese Watermarks sollen klar ausgeben wer die Rechte am vorliegenden Bild- oder Audio-Material hat und ein Kopieren eventuell nur eingeschränkt zu lassen. Diese meist sehr kleinen Datenmengen müssen stark mit dem zu signierenden Material verbunden sein und auch nach tief greifenden Veränderungen des Materials noch auffindbar sind.
Das Signieren von Daten kann auch eine Prüffunktion erfüllen. Hat sich eine eingebundene Nachricht verändert, handelt es sich eventuell nicht mehr um das Original material.

5 Bilder von http://www.fitug.de/bildung/kongress/stegano.html

2.7.3 Anwendung

Die Sicherheit eines steganographischen Systems hängst stark davon ab, wie die zu versteckenden Daten vorbereitet werden. Werden die Daten ohne eine vorherige Verschlüsslung ins Trägermedium eingebunden liegt die geheime Nachricht im Falle einer Extraktion sofort im Klartext vor. Deshalb sollten auch steganographische Systeme dem 'Kerckhoff Prinzip' folgen. Dieses Prinzip kommt vor allem in der Kryptographie zum tragen. Es geht davon aus, dass die Sicherheit eines kryptographischen Systems nicht von der Kenntnis der Verschlüsslungsmethode abhängen darf.

Um die Sicherheit zu erhöhen sollte die Menge der zu verbergenden Daten eine minimal wahrnehmbare Menge nicht überschreiten. Außerdem sollten die Daten vor der Einbringung ins Trägermaterial mit Hilfe eines assymetrischen Verschlüsslungsverfahrens gesichert werden (RSA/PGP). Durch diese Behandlung wird ein '*Weißes Rauschen*' erzeugt, so dass mögliche Muster verschwinden. Die Daten können so im Falle einer Entdeckung und Extraktion nicht entschlüsselt werden. Die Sicherheit eines Steganogramms kann weiter erhöht werden, wenn mehrere Chiffrier- und Verschlüsselungsverfahren nacheinander angewendet werden.



Der Ablauf einer steganografischen Verschlüsslung sollte wie im obigen Diagramm ablaufen. So sollte es vor jeder steganographischen Einbettung zu einer kryptographischen Verschlüsslung kommen. Die meisten Steganographie Programme bieten außerdem die Möglichkeit die Inhalte mit einem Passwort zu schützen.

3. Fazit

Beim Blick in die Vergangenheit fällt auf, dass ein Bedarf an sicherer Datenübermittlung schon immer bestand. Heute steht es auch dem gewöhnlichen Bürger offen von diversen Verschlüsslungsmaßnahmen Gebrauch zu machen, um sensible Daten vor den Augen Dritter zu schützen. Im Zeitalter der rechnergestützten Verschlüsslung und dem Verbergen tritt ein ganz neues Problem auf. Die Sicherheit hat ein Maß erreicht, dass es zum Teil auch großen Staaten wie den USA nicht mehr möglich ist die Daten ihrer Bürger abzuhören, aber auch die Daten von kommunizierenden Terroristen und Staatsfeinden. In Ländern wie China, Frankreich und den vereinigten Staaten ist der Einsatz von kryptographischen Maßnahmen nur eingeschränkt möglich.

So ist in den USA z.B. die Version 6.0 von PGP[6] im Umlauf die eine kürzere Schlüssellänge, eine Key-Revoke[7]-Funktion und keine RSA-Schlüsselerstellung unterstützt.
Werden allerdings die Möglichkeiten von Steganographie und Kryptographie vereint ist eine Strafverfolgung wegen des ungesetzlichen Gebrauchs verbotener Technologie nicht mehr möglich, denn der Gebrauch ist, wenn er ein Gewisses Maß nicht überschreitet und fortschrittliche Algorithmen verwendet, die eine Spreizung der Botschaft durchführen, nicht mehr nachweisbar.
Es bleibt festzuhalten, dass es eine 100%ige Sicherheit nicht gibt. Die Entwicklung wird auch bei der Steganographie weiter gehen, um eine immer tiefere Einbettung ins Trägermaterial zu ermöglichen. Bis heute ist es noch nicht gelungen eine Watermarking-Technologie zu entwickeln, die ein Medium sicher signieren konnte.
Allerdings ist es heute dem gewöhnlichen Menschen möglich so sicher wie nie eine Kommunikation vor den Augen und Ohren Dritter zu verbergen. Man muss sich allerdings auch die Frage stellen, ob man dieses Maß an Sicherheit für sich selbst in Anspruch nehmen muss.

4. Literaturhinweise/ Quellenangaben

- David Kahn, *The Codebreakers*, 1996 Simon & Schuster
- Fred B. Wrixon, *Codes, Chiffren & andere Geheimsprachen. Von den ägyptischen Hieroglyphen bis zur Computerkryptologie*, 2000 Könemann, S. 469ff.
- Simon Singh, *Geheime Botschaften: Die Kunst der Verschlüsslung von der Antike bis in die Zeiten des Internet*, 2001 dtv, S. 20-21
- Rudolf Kippenhahn, *Verschlüsselte Botschaften: Geheimschrift, Enigma und Chipkarte*, 1999 Rowohlt, S. 42
- Christian Thöing, *Steganographie*
  http://mitglied.lycos.de/cthoeing//stegano.htm
- Marit Köhntopp, *Steganographie als Verschlüsselungstechnik*
  http://123.koehntopp.de/marit/pub/steganographie/
- Andreas Westfeld, *Angriffe auf Steganographie*
  http://www.os.inf.tu-dresden.de/~westfeld/publikationen/vis99.pdf
- Alexandra Weickert, *Steganographie – ein Art der Verschlüsslung*
  http://www.fitug.de/bildung/kongress/stegano.html

6 PGP: Pretty Good Privacy, kryptographisches Verschlüsslungstool von Phil Zimmermann, in der Version 2.6.3, deren Verwendung in den USA untersagt ist, sind RSA-Keys mit einer Länge von 8192 Bits möglich.

7 Mit der Key-Revoke-Funktion läßt sich ein verlorener Schlüssel wieder herstellen, dies beeinträchtigt die Sicherheit beträchtlich, weil es Dritten möglich ist, auf den privaten Schlüssel zu zugreifen.

- Michael Seibold, *Top Secret*
  http://www.michael-seibold.de/topsecret/kryptologie-stegano.html

- Julius Robert Mayer, *Liste von unsichtbarer Tinte*
  http://www.wundersamessammelsurium.de/Chemisches/Tinte/

5. Links zu Steganographie-Software im Internet

(Stand 28.07.03)

- S-Tools v4.0 - Andrew Brown
  http://www.jjtc.com/stegoarchive/stego/s-tools4.html

- Hide and Seek v5.0 - Colin Maroney
  http://www.rugeley.demon.co.uk

- PGE v2.0 (Pretty Good Envelope) – Robert G. Durnal
  http://www.afn.org/~afn21533/pge20.zip

- MandelSteg v1.0 und GifExtract v1.0 – Henry Hastur
  ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/MandelSteg1.0.tar.z

- Steganosaurus – John Walker
  http://www.fourmilab.ch/stego/

- Steganos Internet Anonym v5.0 – Steganos GmbH
  http://www.steganos.com