



TECHNISCHE
UNIVERSITÄT
WIEN
VIENNA
UNIVERSITY OF
TECHNOLOGY

Steganographie

Gerald Haider¹, Alexander Fuchs²

¹ Matrikelnummer: 0125638, Studium: Wirtschaftsinformatik (033 526)
e0125638@student.tuwien.ac.at

² Matrikelnummer: 0106909, Studium: Software Engineering & Internet Computing (066 937)
e0106909@student.tuwien.ac.at

Inhaltsverzeichnis

1	Einführung in die Steganographie und die Kunst Informationen zu verstecken	4
1.1	Definition Steganographie	4
1.2	Geschichte der Steganographie.....	4
1.3	Wer sind die potentiellen Nutzer von Steganographie?.....	5
2	Kategorien von Steganographie	5
2.1	„Substitution system“ Technik – Verstecken durch Ersetzen.....	5
2.2	“Transform domain” Technik.....	6
2.2.1	Diskrete Kosinus Transformation (Discrete Cosine Transform (DCT)).....	6
2.3	Spread spectrum techniques.....	7
2.3.1	Direct Sequence	7
2.3.2	Frequency Hopping – Frequenzsprung Verfahren	7
2.4	Statistische Methoden.....	7
2.5	Verzerrungs- (Distortion) Technik	7
2.6	Trägergenerierungs- (Cover generation) Technik.....	7
3	Verschiedene Typen von Steganographie	8
3.1	Linguistische (sprachliche) Steganographie	8
3.2	Open Codes.....	8
3.2.1	Null Ciphers.....	8
3.2.2	Cues – Hinweise	8
3.2.3	Jargon Code	8
3.2.4	Grilles – Gitterfenster.....	8
3.3	Text Semagramme	8
3.3.1	Type Spacing and Offsetting.....	8
3.4	Technische Methoden der Steganographie	9
3.4.1	Unsichtbare Tinte.....	9
3.4.2	Verstecke	9
3.4.3	Microdots.....	9
4	Steganalysis – Finden von Steganographie – Attacken auf Steganographie	9
4.1	Arten von Angriffen auf Steganographie.....	9
4.1.1	„Stego-Only“ Angriff.....	9
4.1.2	„Known cover“ Angriff	9
4.1.3	„Known message“ Angriff.....	10
4.1.4	Bekanntes steganographisches Verfahren/Algorithmus.....	10
4.1.5	„Known stego“ Angriff.....	10

4.2	Finden von versteckter Information.....	10
4.2.1	Statistische Tests.....	10
5	Watermarking Techniken.....	11
5.1	Was ist Digital Watermarking?.....	11
5.1.1	Allgemeines.....	11
5.1.2	Anwendungen von Watermarks.....	11
5.1.3	Mögliche Methoden zur Einbettung in eines Wasserzeichens in eine Grafik.....	12
5.1.4	Hauptkriterien und Anforderungen von Watermarks.....	13
5.1.5	Digital Watermark und Steganographie.....	13
5.2	Einfügeprozess von Digital Watermarks.....	14
5.3	Klassifizierung von Watermarks anhand des Detektionsprozesses.....	14
5.3.1	Privates Watermarking.....	14
5.3.2	Semiprivates.....	15
5.3.3	Öffentliches.....	15
5.3.4	Assymetrisches.....	15
5.4	Klassifizierung von Watermarks im Bezug auf d. Raum.....	15
5.4.1	Einfügen im Ortsraum.....	15
5.4.2	Einfügen im transformierten Raum.....	15
5.5	Entfernen von Digital Watermarks.....	16
5.6	Attacken auf Watermarkingsystemen.....	16
5.6.1	Entfernungsattacken.....	16
5.6.2	Geometrische Attacken.....	17
5.6.3	Kryptographische Attacken.....	17
5.6.4	Orakel Attacken.....	17
5.6.5	Protokollatacken.....	17
6	Ausblick / Zusammenfassung.....	18
7	Referenzen.....	19
8	Abbildungen.....	19

Steganographie

Gerald Haider¹, Alexander Fuchs²

¹ Matrikelnummer: 0125638, Studium: Wirtschaftsinformatik (033 526)

e0125638@student.tuwien.ac.at

² Matrikelnummer: 0106909, Studium: Software Engineering & Internet Computing (066 937)

e0106909@student.tuwien.ac.at

Abstract: Allgemeine Abhandlung über die Verwendung und die Funktionsweise von Steganographie bzw. steganographischen Verfahren. Weiters werden Watermarking Techniken erläutert und eventuell mögliche Attacken auf eben diese dargestellt.

1 Einführung in die Steganographie und die Kunst Informationen zu verstecken

1.1 Definition Steganographie

„Die Steganographie ist die Kunst und Wissenschaft der verborgenen Übermittlung von Informationen.“

1.2 Geschichte der Steganographie

Die Geschichte der Steganographie geht zurück bis zu den alten Griechen. Dort wurde um aus der Gefangenschaft mit dem eigenen König zu kommunizieren, eine Botschaft auf die rasierte Kopfhaut eines Sklaven tätowiert, welche nach dem nachwachsen der Haare für die Gefängniswärter nicht mehr auffindbar war.

Die alten Römer nutzten bereits Techniken wie das Schreiben mit unsichtbarer Tinte (hergestellt aus Früchten oder Milch) zwischen den Zeilen eines offiziellen Dokuments. Diese „unsichtbaren“ Botschaften konnten meist durch Erhitzen zum Vorschein gebracht werden.

Im Jahre 1499 veröffentlichte Trithemius das Buch „Steganographia“, eines der ersten Bücher über Steganographie.

Im 2. Weltkrieg benutzten die Deutschen „Mikropunkte“ (extrem klein gedruckte Information die aussieht wie ein normaler Punkt) um große Mengen an Informationen in der Interpunktion von normalen Dokumenten zu verstecken.

1.3 Wer sind die potentiellen Nutzer von Steganographie?

Der potentielle Nutzerkreis von Steganographie geht von der durchaus erwünschten Nutzung in der sicheren Kommunikation zwischen Geschäftsleuten bis zur eher unerwünschten Verwendung durch Kriminelle/Terroristen. Wobei wahrscheinlich die Nutzung von steganographischen Protokollen durch unerwünschte Elemente unserer Gesellschaft anteilmäßig überwiegen wird.

2 Kategorien von Steganographie

2.1 „Substitution system“ Technik – Verstecken durch Ersetzen

Bei diesen Verfahren wird redundante oder unnötige Information im Träger durch die zu versteckenden Bits ersetzt. Viele derzeit verfügbaren Steganographie Tools nutzen dazu die Methode des letzten signifikanten Bits (Least-Significant-Bit) um die Nachricht in den Träger zu codieren.

Um das ganze an einem Beispiel zu demonstrieren nehmen wir an die folgende Bytesequenz stellt den Träger (z.B. ein Bild) dar:

```
10000100 10000110 10001001 10001101
01111001 01100101 01001010 00100110
```

Jedes Byte des Trägers wird durch 8 Bit dargestellt. Diese Bits stellen einen Farbwert dar, z.B.: wie viel rot/gelb der jeweilige Punkt enthält. Diese Bits die ein Byte codieren sind von der Wichtigkeit von links nach rechts angeordnet, sprich wenn das Bit außen links von 0 auf 1 gesetzt wird verändert sich das Bild viel stärker als wenn man das Bit auf der äußerst rechten Position von 0 auf 1 setzt. Darum wird das äußerst rechte Bit in diesem Fall auch das letzte signifikante Bit genannt (LSB), weil eine Änderung dieses Bits am wenigsten Auswirkung auf die den Farbwert (die Information) des Bytes hat.

Um nun zum Beispiel die Botschaft „42“ im obigen Träger zu verstecken, müsste man wie folgt vorgehen:

42 ist in binärer Darstellung 00101010

Nun wird diese Binärzahl mit Hilfe der LSB Methode in den Träger integriert:

```
10000100 -> 10000100
10000110 -> 10000110
10001001 -> 10001001
10001101 -> 10001100
01111001 -> 01111001
01100101 -> 01100100
01001010 -> 01001011
00100110 -> 00100110
```

Um unsere relativ kurze Botschaft zu verstecken wurden also insgesamt nur 3 Bit im originalen Träger verändert.

2.2 “Transform domain” Technik

Bei der Transform domain Technik wird die Nachricht im “transform space“ eines Signals gespeichert. Diese Technik wird zum Beispiel beim Einbetten in JPEG Bilder verwendet.

2.2.1 Diskrete Kosinus Transformation (Discrete Cosine Transform (DCT))

Die diskrete Kosinus Transformation dient dazu, unter Beachtung der visuellen Qualität, wichtige Teile eines Bilder von den unwichtigen Teil zu trennen. DCT nutzt zwei Techniken um die Daten die Notwendig sind ein Bild darzustellen zu reduzieren.

Quantisation des DCT Koeffizienten. Darunter versteht man den Prozess die Anzahl der möglichen Werte einer Größe zu reduzieren, um dadurch die Anzahl von Bits die zum Speichern dieser Größe benötigt wird zu verkleinern.

Entropie Kodierung der quantisierten Koeffizienten. Entropiecodierung ist eine Technik um die quantisierten Daten so kompakt als möglich darzustellen.

Ein einfaches Beispiel für Quantisierung ist das Runden von Realen Zahlen in ganze Zahlen.

Im JPEG Bildkomprimierungsstandard wird jeder Kosinustransformationskoeffizient quantisiert mit einer Gewichtung die auf den Frequenzen für diesen Koeffizienten basiert. Die Koeffizienten in jedem 8 x 8 Block werden dividiert durch den zugehörigen Wert einer 8 x 8 Quantisierungsmatrix und anschließend auf die nächste Ganzzahl gerundet.

Um DCT genauer zu verstehen, beschäftigen wir uns zuerst damit wie die JPEG Komprimierung im Detail funktioniert.

1. JPEG teilt das Bild in 8 x 8 Pixel Blöcke auf und berechnet für jeden Block den DCT
2. Der DCT hilft um das Bild in verschiedene Teile mit unterschiedlicher Wichtigkeit aufzuteilen.
3. Die DCT Koeffizienten werden aufgrund der Quantisierungsmatrix gerundet. Dabei muss darauf hingewiesen werden das die Bildqualität sehr stark vom Grad der Quantisierung abhängt, sprich eine große Änderung bei der Quantisierung kann zu unakzeptablen Bildstörungen führen. Da das menschliche Auge jedoch hohe Frequenzen weniger gut wahrnimmt, können diese stärker verändert werden ohne das dies vom Betrachter wahrgenommen wird. Eventuell mittels Steganographie einzubettende geheime Daten werden nach diesem Schritt in das Bild geladen. Wenn steganographische Daten integriert werden sollen, wird das niederwertigste Bit der DCT Koeffizienten aller Frequenzen die nicht null sind mit den Bits aus dem Geheimtext ersetzt. Die modifizierten Koeffizienten werden dann noch vom Huffman Kodierer behandelt, welcher die Farbfrequenzen in numerische Werte umwandelt.
4. Der nächste Schritt ist verantwortlich für den verlustbehafteten Output von JPEG.

5. Die JPEG Komprimierungstechnik nutzt variable Kodelängen und schreibt dann den komprimierten Datenfluss in die Ausgabedatei. Während der Dekompression werden bei JPEG die quantisierten DCT Koeffizienten aus der komprimierten Datei wiederhergestellt, das Ganze dann invertiert und anschließend dargestellt.

2.3 Spread spectrum techniques

2.3.1 Direct Sequence

Bei „Direct Sequence Spread Spectrum“ wird der Fluss der zu übertragenden Informationen in kleine Pakete zerteilt. Jedes dieser Pakete wird dann einer Frequenz des gesamten Spektrums zugeordnet. Das Daten-Signal wird zum Zeitpunkt der Übertragung kombiniert mit einem Signal mit höherer Datenrate, welches die Daten aufgrund der vorherbestimmten Aufteilungsrate teilt. Die zu übertragenden Daten werden teilweise redundant übertragen, um etwaige Übertragungsfehler ausgleichen zu können.

2.3.2 Frequency Hopping – Frequenzsprung Verfahren

Bei dieser Technik wird ein breites Frequenzband in mehrere kleinere zu verwendende Frequenzbänder aufgeteilt. Ein Gerät, das diese Technik nutzt, wechselt dann laufend zwischen diesen Bändern, und sendet somit niemals länger auf einer Frequenz.

2.4 Statistische Methoden

Statistische Methoden nutzen ein „1-bit“ Steganographie genanntes Verfahren. Dabei wird nur ein Bit an Information in einen Träger eingefügt und erzeugt dadurch eine statistisch messbare Änderung.

Eine statistische Änderung im Träger impliziert eine „1“, ein unveränderter Träger hingegen stellt eine „0“ dar. Dieses System geht davon aus, dass der Empfänger zwischen einem modifizierten und einem unmodifizierten Träger unterscheiden kann.

2.5 Verzerrungs- (Distortion) Technik

Diese Methode der Steganographie erzeugt eine Änderung im Träger, um Information zu verstecken. (z.B.: durch Verzerrung des Bildes). Die geheime Nachricht wird durch das Vergleichen des originalen Trägers mit der verzerrten Version wiederhergestellt.

2.6 Trägergenerierungs- (Cover generation) Technik

Bei der Trägergenerierungstechnik wird nicht wie bei den anderen Methoden ein Träger ausgesucht, in den Informationen eingebettet werden sollen. Stattdessen wird hier ein Träger generiert, nur um Informationen darin zu verstecken.

3 Verschiedene Typen von Steganographie

3.1 Linguistische (sprachliche) Steganographie

Linguistische Steganographie ist jegliche Form von Steganografie die Sprache als Trägermedium nutzt. Zu dieser Gruppe gehören sowohl „Open Codes“ als auch „Text Semagrams“.

3.2 Open Codes

Als „Open Codes“ bezeichnet man all jene Verfahren bei denen der Trägertext meist sehr genau nach einem gewissen Schema konstruiert wurde. So dass zum Beispiel gewisse Buchstaben immer an gewissen Positionen im Wort stehen oder Wörter diagonal oder vertikal im Text versteckt sind.

3.2.1 Null Ciphers

Bei „Null Ciphers“ kann der geheime Text aus dem Träger wiederhergestellt werden in dem zum Beispiel jeweils der erste oder zweite Buchstabe jedes Wortes genommen wird. Genauso gut kann der versteckte Text aber senkrecht, diagonal oder rückwärts im Text versteckt sein.

3.2.2 Cues – Hinweise

Dieses Verfahren beruht darauf einen gewissen Hinweis im Trägermedium unterzubringen. Ein Beispiel für dieses Verfahren wäre zum Beispiel ein Attentäter der erst dann zuschlägt wenn der Moderator einer gewissen Radiosendung zu einem vordefinierten Zeitpunkt ein gewisses Wort (den Hinweis) erwähnt. Das Problem bei diesem Verfahren ist die aufwendige Vorbereitung und der nur sehr beschränkte Informationsgehalt.

3.2.3 Jargon Code

Jargon Code ist nichts anderes als das simple Ersetzen von Wörtern durch andere Ausdrücke, und dadurch natürlich sehr leicht zu durchblicken. Ein Beispiel wäre wenn das Wort „Chef“ einfach durch das Wort „Drache“ ersetzt wird.

3.2.4 Grilles – Gitterfenster

Bei diesen Verfahren wird zum entschlüsseln ein Blatt Papier oder Karton mit Löchern verwendet. Diese Löcher verraten, wenn man das Blatt Papier korrekt über dem Trägermedium (z.B.: Zeitungstext) platziert den geheimen Text, somit ist die Botschaft nur für Personen mit dem korrekten Gitterfenster zu lesen.

3.3 Text Semagramme

3.3.1 Type Spacing and Offsetting

Bei diesen Verfahren wird nicht in den Text selbst die Information eingefügt, sondern stattdessen die grafische Darstellung des Textes modifiziert. So kann zum Beispiel durch einfügen von unnötigen Leerzeichen zwischen den Worten ein gewisses Maß an Informationen übermittelt werden. Selbiges kann durch teils nur geringfügige Verschiebungen von einzelnen Zeichen erreicht werden.

All diese Methoden sind im Zeitalter der digitalen Übermittlung von Information jedoch meist nur mehr schlecht anwendbar bzw. oft auch relativ einfach feststellbar.

3.4 Technische Methoden der Steganographie

3.4.1 Unsichtbare Tinte

Das Prinzip der Unsichtbaren Tinte soll hier nur am Rande erwähnt werden, da es wohl eines der bekanntesten Methoden von Steganographie ist.

Die verschiedenen Formen von unsichtbarer Tinte basieren alle darauf dass sie unter normalen Bedingungen fast unsichtbar sind und nur durch spezielle Verfahrensweisen (z.B.: durch erhitzen oder UV-Licht) wirklich gut sichtbar gemacht werden können.

3.4.2 Verstecke

Die klassische steganographische Methode wie sie in jedem besseren Agentenfilm dargestellt wird. Die geheime Nachricht wird einfach wo versteckt, ob dies die Absätze eines Schuhs sind oder der Benzintank eines Autos ist im Prinzip egal, alles in allem eine eher unsichere Methode.

3.4.3 Microdots

Microdots sind ein Verfahren ähnlich der Mikroverfilmung, welches es erlaubt mehrere Seiten Text auf eine von ½ Millimeter im Durchmesser zu drucken. Durch die extreme Dichte des Drucks ist solch ein Punkt kaum von einem normalen Interpunktionszeichen zu unterscheiden.

4 Steganalysis – Finden von Steganographie – Attacken auf Steganographie

4.1 Arten von Angriffen auf Steganographie

Ähnlich wie bei der Kryptoanalyse unterscheidet man bei der Analyse von Steganographie mehrere Arten von Attacken.

4.1.1 „Stego-Only“ Angriff

Es ist nur der Träger mit der vermutlich integrierten Information vorhanden, man besitzt aber keinen original Träger oder die versteckte Information.

4.1.2 „Known cover“ Angriff

Bei dieser Art von Angriff steht der modifizierte Träger als auch das Original des Trägers zur Verfügung.

4.1.3 „Known message“ Angriff

Dies liegt vor wenn der Angreifer in den Besitz der eingebetteten Information gelangt. Mit Hilfe des vorliegenden Trägerobjekts und dem Wissen um die eingebettete Information kann der Angreifer viele Schlüsse auf das verwendete steganographische Verfahren machen.

4.1.4 Bekanntes steganographisches Verfahren/Algorithmus

Liegt vor falls das verwendete steganographische Verfahren bekannt ist.

4.1.5 „Known stego“ Angriff

Falls der steganographische Algorithmus bekannt ist und außerdem das Original des Trägers und der Träger mit eingebetteter Nachricht vorliegen

4.2 Finden von versteckter Information

Das finden von versteckter Information kann relativ einfach sein im Fall von solch einfachen steganographischen Verfahren wie „Type Spacing“ oder „Offsetting“. Das auffinden von versteckter Information in ungenutzten Bereichen der Festplatte oder in TCP/IP Paketen ist, ebenfalls noch relativ einfach.

Werden jedoch Multimedia Daten als Träger verwendet wird das Auffinden von versteckten Daten zu einem relativ schwierigen Problem. Auf einige Methoden zum auffinden von versteckter Information in Bildern soll hier genauer eingegangen werden.

4.2.1 Statistische Tests

Mittels verschiedener Tests können Bilder auf „abnormale“ Parameter untersucht werden. So haben mit Steganographie versehene Bilder zum Beispiel meist eine höhere Entropie als solche ohne eingebettete Information.

Weitere statistische Test die zum Auffinden von Informationen in Bildern verwendet werden können sind:

- durchschnittliche Byteanzahl
- Variation der Bytes
- Lage (Skew)
- Kurtosis
- durchschnittliche Abweichung
- Differential Werte

5 Watermarking Techniken

5.1 Was ist Digital Watermarking?

5.1.1 Allgemeines

Unter Watermark versteht man ein durchsichtiges Merkmal auf einem Blatt Papier, das nur sichtbar ist, wenn man das Blatt gegen eine Lichtquelle hält. Dies dient dazu um die Authentizität des Blatt Papiers (und in weiterer Folge auch diesen Inhalt) sicherzustellen. Umgelegt auf die digitale Welt ist ein elektronisches Watermark ein Sicherheitsmerkmal, das in Daten beigemischt wird. Dieses Merkmal kann wiederum zur Prüfung der Authentizität der Datei, sodass niemand die Möglichkeit hat Fälschungen davon herzustellen. Dabei darf das Watermark nicht die Originaldatei massgeblich verändern, muss aber doch so signifikant sein, um sie validieren zu können. Im Gegensatz zur realen Welt soll eine digitale Watermark meist nur für den sichtbar sein, der weiß wie man nach ihr sucht, das entspricht dem Information Hiding und somit ist der Zusammenhang mit der Steganographie einleuchtend.

Viele Dateiformate sind dazu ausgelegt um eine gewisse Anzahl an Fehlern (z.B.: Bitfehler) zu tolerieren. Diesen Effekt macht sich das digitale Watermarking zu nutze. Es wird für eine gewisse Menge an spezifischen Hintergrundrauschen beigemischt, ohne dass dadurch die Qualität der Datei wesentlich leidet. Für jemanden der die Watermark nicht validieren kann und muß, soll diese somit nur als Hintergrundrauschen wahrnehmbar sein. Ein Problem hierbei sind komprimierte Dateiformate, sie sind dazu ausgelegt um möglichst wenig Redundanzen und somit auch Hintergrundrauschen aufzuweisen, somit bleibt sehr wenig bis gar kein Platz für Watermarks. Ein weiterer grundlegender Punkt ist die Verteilung der Watermark in einer Datei. Wird sie beispielsweise nur am unteren Ende eines Bildes angebracht, so ist es ein leichtes diesen Teil abzuschneiden und das restliche Bild zu verwenden.

5.1.2 Anwendungen von Watermarks

Dabei richtet sich das Hauptanwendungsgebiet von Watermarks auf Copyright Anwendungen im Bereich der Bilder, Audio und Videodateien. Immer mehr Daten sind in digitaler Form in einfacher Weise über das Internet abrufbar, was die Vermeidung von verbotener Vervielfältigung dieser Daten zum Problem macht. Wenn nun z.B.: ein Bild illegalerweise auf einer Webseite verwendet wurde, ohne dies mit dessen urheberrechtlichen Besitzer abzuklären, kann dieser sein Besitzrechte mit Hilfe einer Watermark geltend machen. Dies soll auch noch möglich sein, wenn der Fälscher kleine Veränderung an der Originaldatei vorgenommen hat (Robustheit einer Watermark). Dabei zu beachten ist jedoch, dass bei den meisten unsichtbaren Watermarks z.B.: einem Bild, der Schutz nur solange gegeben ist, solange sich die Datei in digitaler Form befindet. Wird sie z.B.: ausgedruckt und erneut eingescannt ist die Watermark entfernt.

Ein weiteres Anwendungsgebiet ist Wasserzeichen zum Nachweis von Veränderungen an einer Datei zu benutzen. Sobald jemand eine Datei die diese speziellen Art von Wasserzeichen enthält, verändert hat, wurde auch das Wasserzeichen dadurch verändert.

In weiter Folge wird am Häufigsten auf Watermarks in Bildern eingegangen, da sich dieses Szenario am Besten darstellen und verstehen lässt.

5.1.3 Mögliche Methoden zur Einbettung in eines Wasserzeichens in eine Grafik

Ein Beispiel für ein unsichtbares Watermark wäre die Veränderung der Farben einzelner Pixel. Das menschliche Auge ist nicht im Stande geringe Farbunterschiede konkret wahrzunehmen.

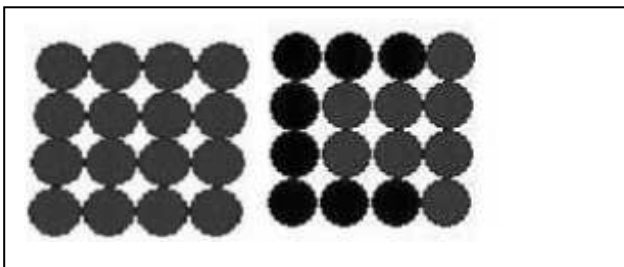


Abbildung 1 - Unterscheidung von Grautönen

Man könnte vermuten, die Pixel in dieser Grafik alle den selben Grauton haben. Wenn man es jedoch mit einem Grafikprogramm näher untersucht wird man feststellen, dass sie unterschiedlich Grauantteile haben. Eine digitales Watermark könnte nun eine spezifische Struktur von Pixel um einen geringfügigen Wert ändern, sodass sich dadurch ein unsichtbares Muster ergibt. Erst wenn man die Abweichungen größer macht, wird sie für das menschliche Auge sichtbar, wie man es anhand des zweiten Bildes sehen kann. Weiter mögliche Einbettungsmethoden sind:

Patchwork

Menge M von Bildpunktpaaren (a, b) werden jeweils zufällig ausgewählt und die Helligkeit von a z.B.: um 1 erhöht und die von b um 1 verringert. Wenn man nun „ n “ soche Pixel verändert hat erhält man eine Helligkeitsdifferenz von $2n$. Selbst wenn man nun das Bild hoch komprimiert ist es noch immer sehr wahrscheinlich, dass man bei guter und ausreichender Auswahl von den n bits, die eingebeteten Daten wieder extrahieren kann

Differenz von zwei Hälften

Ein Zufallsgenerator teilt das Bild in zwei Hälften. In einer der Teilmengen wird die Helligkeit um „s“ angehoben. „s“ definiert hierbei die Differenz von zwei zufälligen Stichproben in den beiden Hälften. Die Verifikation des Wasserzeichens kann dann insofern erfolgen, als dass man den mittleren Helligkeitswert der zwei Mengen errechnet. Ist dieser annähernd s so enthält es das Wasserzeichen. Ist hingegen „s“ gleich 0 dann ist dieses Wasserzeichen nicht vorhanden. Diese Methode ist jedoch nicht so resistent gegen Komprimierung wie die Patchworkmethode. Beide Methoden können jedoch miteinander kombiniert werden.

5.1.4 Hauptkriterien und Anforderungen von Watermarks

Keine Beeinträchtigung der Datei

Wahrnehmbarkeit

Eine Watermark sollte weder wahrgenommen werden können. Dies lässt sich jedoch nur gewährleisten wenn die statistische Verteilung mit der eingefügten Watermark und die statistische Verteilung der Daten ohne Watermark gleich sind

Robustheit

Die Watermark lässt sich nicht entfernen. Wenn sie entfernt wurde, sollte das Bild entweder nicht mehr verwendbar sein. Das bedeutet, dass sie immun gegen eine zielgerichtete Veränderung ist. Eine robuste Watermark bleibt stets im Bild vorhanden und übersteht jegliche Modifikation, solange bis die Qualität der Daten so schlecht wird, dass sie nicht mehr verwendbar sind. Robustheit lässt sich jedoch nicht testen. Wie bei der Softwareentwicklung kann man auch in diesem Fall nicht auf alle möglichen Fehler bzw. Modifikationen überprüfen. Man kann mit den Tests nur bestimmte Fälle abdecken und eine gewisse Wahrscheinlichkeit garantieren, dass die Anforderungen (=Robustheit) erfüllt ist. Eine Möglichkeit die Robustheit einer Watermark zu erhöhen ist, die Methode, dass eine Watermark öfters in der Datei eingebracht wird.

Kapazität

Watermark wird als eine kleine Menge an Informationen eingebracht. Je größer die Watermark ist, umso leichter kann sie auch entdeckt werden.

- Watermark sollte öfters in einer Datei vorkommen um ein Entfernen zu erschweren

Sicherheit

Bezieht sich auch auf die Robustheit gegenüber Modifikationen. Die Sicherheit einer Watermark sollte auf einem gewissen Schlüssel basieren und nicht auf der Geheimhaltung des Algorithmus für die Erzeugung der Watermark. Man vergleiche dazu das Prinzip von Kirckhoff. Oft wird die Sicherheit eines Watermarking Systems auch mit der Robustheit synonym verwendet.

5.1.5 Digital Watermark und Steganographie

Digitale Watermarks sind zwar eine Form von Steganographie, dennoch weisen sie eigene Charakteristiken auf. Beispielsweise ist bei der Steganographie das Ziel des Angreifers das Entdecken der Daten, jedoch bei dem Digitalen Watermark liegt das Anliegen des Angreifers beim Entfernen der Watermark. Außerdem wird reine Steganographie zum Verstecken von Informationen verwendet, sodass kein anderer sie finden kann. Dies ist zwar bei der Watermark ebenso ein Ziel, jedoch nur ein nebensächliches. Für eine Watermark ist das Hauptziel ihre Robustheit. Auch wenn sie entdeckt wird, ist nach wie vor das Problem vorhanden, dass sie noch entfernt werden muss. Digitales Watermarking kann als Steganographie mit aktivem Wächter angesehen werden. Ein aktiver Wächter transformiert absichtlich die Nachricht um geheime Nachrichten, die möglicherweise enthalten sind zu zerstören. Erst danach gibt sie der aktive Wächter weiter.

5.2 Einfügeprozess von Digital Watermarks

Dieser Prozess beschreibt das Einfügen der Watermark in die Daten. Dieses Einfügen einer Watermark bedeutet ein Einfügen eines zusätzlichen Informationsgehalt von (1 bit -> es ist eine Watermark vorhanden oder nicht). Dabei ist anzumerken das der eingefügte Informationsgehalt ungleich der eingefügten Datenmenge ist. Für den Informationsgehalt von einem Bit (Watermark ja/nein) muss man natürlich eine Watermark mit mehreren bit and Daten einfügen. Der Einfügeprozess ist im Grunde immer gleich. Gegeben sind ein Bild B ein Schlüssel S und eine Watermark W . Der Prozess ist definiert als $B_w = B \circ K \circ W$, wobei \circ die Verknüpfung symbolisiert. Dabei ist zu bemerken, dass meist die Watermark und der Schlüssel verknüpft sind. Die Watermark wird, meist in Abhängigkeit zu dem verwendeten Bild, durch den Schlüssel erzeugt

5.3 Klassifizierung von Watermarks anhand des Detektionsprozesses

Es lassen sich grundsätzlich vier Klassen unterscheiden, die definieren, wie ein Algorithmus eine Watermarking verifiziert bzw. findet. Diese Klassen unterscheiden sich in den Parametern die der Detektionsprozess zur Auffindung der Watermark benötigt.

5.3.1 Privates Watermarking

Diese Detektionsart benutzt das Originalbild B und den Schlüssel S um ein Bild B_w auf die Beinhaltung einer Watermark W zu prüfen. Dabei gibt es zwei Möglichkeiten wie der Detektionsmechanismus vorgeht

Extrahieren einer möglichen Watermark W

Hierzu wird mithilfe des Schlüssels S und dem Originalbild die Watermark extrahiert

$$B_w \circ S \circ B = W$$

Warheitswert ob Watermark vorhanden

Bei dieser Variante wird zusätzlich die Watermark für den Detektionsprozess benötigt

$$B_w \circ S \circ B \circ W = 0 \text{ oder } 1 \text{ (wobei } 1 \text{ die Beinhaltung von } W \text{ repräsentiert)}$$

5.3.2 Semiprivates

Es wird hier wie im privaten Watermarking die Watermark W verwendet, jedoch nicht das Originalbild B

Form des Detektionsprozesses

$$B_w \circ S \circ W = 0 \text{ oder } 1 \text{ (wobei } 1 \text{ die Beinhaltung von } W \text{ repräsentiert)}$$

5.3.3 Öffentliches

Diese Variante benötigt weder die Watermark W , noch das Originalbild B . Diese Variante wird zwar oft verwendet, ist jedoch im Vergleich zu den anderen Varianten nicht so robust

Form des Detektionsprozesses

$$B_w \circ S = W$$

5.3.4 Assymetrisches

Die Assymetrische Variante des Detektionsprozesses verwendet wie die assymetrische Signatur einen öffentlichen Schlüssel zum Verifizieren der Watermark und einen privaten Schlüssel zur Erzeugung. Dies bringt den Vorteil, dass für die Verifikation bzw. für die Suche, der private Schlüssel nicht benötigt wird. Durch den geheimen Schlüssel lässt sich die Watermark auch wieder aus der Datei entfernen.

Leider gibt es noch keine wirkliche Umsetzung von solchen assymetrischen Watermarking Systemen, jedoch wurde sich auf theoretischer Seite schon viel damit beschäftigt und auch Ansätze dafür erdacht.

5.4 Klassifizierung von Watermarks im Bezug auf d. Raum

Watermarks lassen sich nicht nur anhand ihres Detektionsprozesses klassifizieren, sondern auch anhand des Raums in dem der Einfügeprozess der Watermark geschieht. Dabei beziehen sich die folgenden Beispiele wiederum auf die Einbringung einer Watermark in eine Grafik

5.4.1 Einfügen im Ortsraum

Hierbei wird während des Einfügeprozesses ein Algorithmus verwendet, der die Pixel in Abhängigkeit vom Schlüssel und der Watermark direkt im Ortsraum verändert. Der Vorteil hierbei liegt in der Schnelligkeit des Vorgangs, da keine zusätzliche Transformation notwendig ist. Jedoch sind diese Arten von Watermarks nicht so robust.

5.4.2 Einfügen im transformierten Raum

Bei diesem Verfahren transformiert der Algorithmus zunächst das Originalbild in einen anderen Raum. Anschließend wird in diesem Raum die Watermark eingefügt und das Bild wiederum in den ursprünglichen Raum transformiert. Vorteil dieser Methode ist ihre relative Robustheit gegenüber der Ortsraummethode, jedoch geschieht dies auf Kosten der Geschwindigkeit

Beispiele für Transformierungsarten:

Diskrete Fourier Transformation

Ist eine der ersten eingesetzten Transformationsarten, wurde für die ersten Watermarks verwendet

Diskrete Wavelet Transformation

Diese Variante hat sehr gute Komprimierungsraten. Sie ist zwar sehr rechenintensiv im Gegensatz zu anderen Transformationen, jedoch ist dies aufgrund von modernen Prozessoren kein Problem. Ein prominenter Benutzer der Wavelet Transformation ist der JPEG 2000 Algorithmus. Deshalb sind auch jene Watermarks robuster gegenüber JPEG Komprimierungen (= Wavelet Transformation), da sie selbst in diesem Raum erzeugt wurden

Diskrete Kosinus Transformation

Diese Transformationsart wird auch vor allem in der Bildbearbeitung eingesetzt, da sie auch zur Komprimierung von Bildern gedacht ist. Diese Transformationsart macht jene Koeffizienten aus, die man weglassen kann, ohne dass es für das menschliche Auge sichtbar ist. Deshalb wird er auch im älteren JPEG Standard verwendet. Eine Watermark kann umso besser einer Kompression widerstehen, umso eher sie auf einem Koeffizienten angewendet wurde, der erst bei hoher Kompression vernachlässigt wird.

5.5 Entfernen von Digital Watermarks

Die Robustheit von Watermarks ist ein großes Problem. Beispielsweise ist bei digitalen Bildern fast jede Watermark durch folgenden Vorgang entfernt: Ein Bild in einem bestimmten Format in ein anderes Format konvertieren (womöglich eines mit guter Komprimierung wie jpeg) und das Ergebnis des Bildes wieder in das ursprüngliche Format zurück zu konvertieren

5.6 Attacken auf Watermarkingsystemen

Man kann die derzeit bekannten Attacken auf Dateien, die mit Watermarks versehen sind grundsätzlich in 4 verschiedene Klassen einteilen.

5.6.1 Entfernungsattacken

Diese Art des Angriffes setzt darauf eine Möglichkeit zu finden die Watermark vollständig aus der Datei zu entfernen. Es wird hierzu das theoretische Modell verwendet, dass eine Watermark ein zusätzliches Rauschen ist, das aber nicht zum Bild gehört. Dazu wird zunächst ein statistisches Modell vom Originalbild geschätzt und wenn gut geschätzt wurde, kann die Watermark natürlich entfernt werden. Dies ist jedoch nicht trivial da solche Schätzungen oft diverse Parameter benötigen. Oft reicht es jedoch nur große Teile der Watermark zu entfernen.

5.6.2 Geometrische Attacken

Diese Variante setzt nicht auf die Entfernung der Watermark sondern auf deren Unkenntlichmachung. Die Watermark muss dabei soweit verändert werden, so dass sie von einem Detektionsprozess nicht mehr als solche wahrgenommen wird. Möglichkeiten der Veränderungen des Bildes bestehen in der Transformation und in der Filterung von Hintergrundrauschen oder auch durch hinzufügen von neuem Hintergrundrauschen. Ein Beispiel für diese Attacke ist die Stirnmack Attacke, in der ein Bild durch zufällige Verzerrungen, Filterungen, Skalierungen und auch Rotationen verändert wird. Diese Transformationen sind jedoch so minimal, dass sie vom menschlichen Auge nicht wahrgenommen werden. Derzeit gibt es keine Watermark Anwendung, die gegenüber einer solchen Attacke robust ist

5.6.3 Kryptographische Attacken

Hierbei wird wie bei einem kryptografischen Angriff ein Brute Force Angriff getätigt. Da auch das Watermarking auf einem Schlüssel basiert, sollte auch dieser gut gewählt werden und durch ausreichende Länge sicher sein.

5.6.4 Orakel Attacken

Hierbei verfügt über das Wissen der Detektionsmethode für diese Watermark. Daher kann er solange versuchen die Datei zu verändern, bis sie von der Detektionsmethode nicht mehr mit dem Watermark in Verbindung gebracht wird.

Eine andere Methode kann angewendet werden wenn man über mehrere Duplikate von ein und der selbe Datei verfügt. Wobei jedoch jedes Duplikat mit einer unterschiedlichen Watermark versehen wurde (z.B.: wenn man für jeden Kunden eine eigene Watermark definiert). Hierbei sind dann zwei Angriffe möglich:

Durchschnittsmethode

Wenn man genug Bilder hat, kann man von jedem Pixel (von allen Dateien) einen Durchschnittswert errechnen und diesen in eine neue Variante der Datei überführen, wodurch auch sämtliche Watermarks entfernt werden.

Teilungsmethode

Hierbei werden alle Kopien in kleine Teile geteilt. Danach wird wieder ein ganzes Bild generiert, das jedoch aus den Teilen von unterschiedlichen Kopien geschaffen wurde.

5.6.5 Protokollatacken

Diese Attacken greifen nicht die Datei an, sondern versuchen die Watermark selbst zu verändern. Das führt zwar dazu, dass man eine Watermark noch in einer Datei finden kann, diese jedoch nicht mehr identifizieren kann.

6 Ausblick / Zusammenfassung

Wir wollen an dieser Stelle einen kleinen Ausblick in die Zukunft der Steganographie wagen. Jeder Versuch Dinge die noch nicht geschehen sind hervorzusagen ist zwar etwas gewagt, aber es gibt trotzdem schon Einzelheiten die sich jetzt schon abzeichnen.

Zukünftige Steganographie wird immer schwieriger zu entdecken bzw. zu entschlüsseln sein, was einerseits durch immer besser werdende steganographische Algorithmen erreicht wird, andererseits aber auch durch die immer größer werdende Menge an Daten (also potentiellen Trägern) um die Information zu verstecken. Diese größere Anzahl an Trägern für Steganographie wird aber großteils dadurch neutralisiert werden, das die zu versteckenden Daten auch immer umfangreicher sein werden.

Die Angriffsmöglichkeiten auf Steganographie werden sich natürlich auch weiter entwickeln, wobei insbesondere die von Quantenrechnern beobachtet werden muss, welche auf Steganographie eventuell eben so große Auswirkungen haben könnten wie auf die herkömmliche Kryptographie.

Der häufigste Einsatzzweck von Steganographie wird vermutlich der Einsatz als Watermarking Technik in den Digital Rights Management (DRM) Systemen der Zukunft sein. In größeren Konzernen wird es bei wirklich sensiblen Daten eventuell auch zu wirklich regelmäßigem Einsatz von Steganographie kommen. Die Nutzung von Steganographie für illegale Zwecke wird überproportional zunehmen, da es durch die immer besseren Überwachungsmöglichkeiten durch die Exekutive für Kriminelle immer wichtiger gar nicht erst aufzufallen.

Alles in allem kann nur gesagt werden das die Blütezeit der Steganographie noch bevorsteht und wir uns momentan sicher noch am Anfang der Entwicklung von steganographischen Techniken befinden.

7 Referenzen

- [1] Greg Kipper, *“Investigator’s Guide to Steganography”*, 2004, Auerbach Publications
- [2] Stefan Katzenbeisser, Fabien A. P. Petitcolas, *„Information Hiding Techniques for Steganography and Digital Watermarking”*, 2000, Artech House Inc.
- [3] Eric Cole, *“Hiding in Plain Sight: Steganography and the Art of Covert Communication”*, 2003, Wiley Publishing Inc.
- [4] Chun-Shien Lu, *“Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property”*, 2004, Idea Group Publishing

8 Abbildungen

Abbildung 1 - Unterscheidung von Grautönen	12
--	----