WIKIPEDIA

Steganographie

Die **Steganographie** (auch **Steganografie**) ist die Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container). Das Wort lässt sich auf die griechischen Bestandteile στεγανός *steganós* ‚bedeckt' und γράφειν *gráphein* ‚schreiben' zurückführen,[1] bedeutet also wörtlich „bedeckt schreiben" bzw. „geheimes Schreiben". Das modifizierte Medium wird als Steganogramm bezeichnet.

Inhaltsverzeichnis

Bild eines Baumes (88 kB), in das mit computergestützten steganographischen Methoden ein zusätzliches (nicht sichtbares) Bild einer Katze eingefügt ist

Bild der Katze (19 kB), das im obigen Bild in den beiden niederwertigsten Bits jedes Farbkanals jedes Bildpunkts versteckt ist

Ziele der Steganographie

Der Einsatz von Steganographie hat Geheimhaltung und Vertraulichkeit zum Ziel. Informationen werden so verborgen, dass ein Dritter bei Betrachtung des Trägermediums keinen Verdacht schöpft. Damit ist zugleich erreicht, dass die verborgenen Informationen nicht Dritten bekannt werden, d. h., die Geheimhaltung ist (wie bei der Kryptographie) gewährleistet.

Die Einordnung der Steganographie wird in der Regel auf zwei mögliche Weisen vorgenommen: Entweder wird sie als Unterkapitel der Kryptographie betrachtet oder als eigenständiger Wissenschaftsbereich. Für Letzteres spricht, dass die Zielsetzung der Kryptographie

(Geheimhaltung) nicht mit der Zielsetzung der Steganographie (vertrauliche Geheimhaltung durch Verbergen der Geheimhaltung) übereinstimmt. In der Praxis werden Kryptographie und Steganographie häufig kombiniert, da zum Beispiel Chiffretexte für die Steganographie interessante statistische Merkmale aufweisen.

Abgrenzungen

Das Funktionsprinzip der Steganographie beruht darauf, dass ein Außenstehender die Existenz der steganographierten Information nicht erkennt. Dadurch unterscheidet Steganographie sich von der Kryptographie, bei der ein Außenstehender zwar um die Existenz von Informationen weiß, aber aufgrund der Verschlüsselung nicht in der Lage ist, den Inhalt zu verstehen.

Beispiel

> Schickt Alice an Bob eine Nachricht, ersetzt aber vor dem Verschicken jeden Buchstaben durch den, der im Alphabet jeweils fünf Stellen weiter steht, so handelt es sich um Kryptographie (Cäsar-Chiffre). Walter, eine außenstehende Person (vielleicht ein Gefängniswärter), fängt die Nachricht beim Transport ab, kann sie aber ohne Kenntnis des Verschlüsselungsverfahrens nicht verstehen. Er sieht aber, dass eine Nachricht von Alice an Bob gesandt wurde. Wenn es in seiner Macht steht, ändert er die Nachricht oder stellt sie Bob nicht zu.
> Schickt Alice Bob dagegen eine Nachricht in Form eines (belanglosen) Gedichts, bei dem die Anfangsbuchstaben der Zeilen hintereinander gelesen die eigentliche Nachricht bilden, so kann der außenstehende Walter zwar sehen, dass Alice Bob eine Nachricht sendet, der Inhalt, den Walter wahrnimmt, entspricht aber nicht der relevanten Nachricht von Alice an Bob. Die Wahrscheinlichkeit, dass Walter die Nachricht verändert oder blockiert, ist mangels Interesse gering. Dies ist Steganographie.

In der Steganographie verwendet man als Szenario in der Regel den Nachrichtenversand von einem Sender zu einem Empfänger. Auch die Daten*speicherung* kann darauf abgebildet werden; in dem Fall handelt es sich um Kommunikation mit sich selbst (Sender = Empfänger). Dieser Spezialfall wird aber üblicherweise vernachlässigt.

Sehr ähnlich zur Steganographie sind nicht-wahrnehmbare digitale Wasserzeichen, deren Zielsetzung sich jedoch unterscheidet. Steganographie will Vertraulichkeit sichern, wohingegen digitale Wasserzeichen das Hauptaugenmerk auf Robustheit legen: Je nach Einsatzzweck wird die Robustheitseigenschaft eines Wasserzeichens so gewählt, dass es bereits durch kleine Änderungen zerstört wird (für den Nachweis von verletzter Integrität des Trägers) oder sehr starke Änderungen übersteht (für das Markieren des Trägers, bspw. mit wichtigen Informationen wie Besitzer, Urheber, Aufführungsort o. ä.). Zerstört man das Wasserzeichen im letzteren Fall, so ist der Träger dadurch so degradiert, dass er nicht mehr nutzbar ist. In Abhängigkeit vom Einsatzzweck kann die Robustheit zwischen den beschriebenen Polen variiert werden. Digitale Wasserzeichen verwenden steganographische Techniken und führen daher auch die übrigen Eigenschaften dieser Techniken wie z. B. Vertraulichkeit mit sich. Im Bedarfsfall werden diese übrigen Eigenschaften degradiert, um die Robustheit zu erhalten, genau wie bei Steganographie u. a. die Robustheit gelockert werden kann, um die Vertraulichkeit zu sichern.

Sicherheit

Ein steganographisches Verfahren gilt genau dann als sicher, wenn nach Anwendung des Verfahrens auf ein Medium dritte Personen keinerlei Rückschlüsse ziehen können, ob in einem vorliegenden Medium nichtoffensichtliche Informationen verborgen sind. Ein weiteres, aber nachrangiges Sicherheitsmerkmal ist, dass eingebettete Informationen selbst bei Kenntnis von

deren Existenz von Dritten nicht auslesbar sind. Mit dem Aufdecken steganographischer Inhalte und der Analyse steganographischer Verfahren beschäftigt sich die Steganalyse (analog der Kryptoanalyse bei der Kryptographie).

Verschlüsselt man ferner die Nachricht *vor* dem Einbetten, ist eine chiffrierte Nachricht normalerweise nicht von zufälligen Daten unterscheidbar. Damit ist sie für Uneingeweihte nicht von materiellen Irregularitäten von Bild- und Tonträgern zu unterscheiden (z. B. Textur des Trägergewebes, Hintergrundrauschen u. dergl.).

Kerckhoffs' Prinzip in der Steganographie

Kerckhoffs' Prinzip besagt, dass die Sicherheit eines Systems nicht von der Geheimhaltung der Algorithmen abhängen darf, sondern nur von der Geheimhaltung eines Schlüssels. Bei sicheren Verfahren ist also nur die Kenntnis des richtigen Schlüssels für die Erkennbarkeit von Bedeutung.

Die Berücksichtigung des kerckhoffsschen Prinzips in der Steganographie ist historisch betrachtet nur zweitrangig, da es zunächst darum ging, die Nichtdetektierbarkeit gegenüber menschlichen Sinnen herzustellen. Daher sind vor allem ältere Steganographiealgorithmen inhärent unsicher, sobald diese quelloffen zugänglich sind.[2]

In der Steganographie muss ein höherer Aufwand betrieben werden als in der Kryptographie, um Kerckhoffs' Prinzip zu erfüllen und gleichzeitig nicht das Hauptziel der Steganographie, die Erhaltung der Nichtwahrnehmbarkeit bzw. Nichtdetektierbarkeit, zu verfehlen.

Symmetrische Steganographie

Ähnlich der symmetrischen Kryptographie basiert die symmetrische Steganographie darauf, dass Sender und Empfänger einer Nachricht im Vorfeld der verdeckten Kommunikation einen geheimen Schlüssel ausgetauscht haben. Beide wissen, auf welche Art und Weise und an welcher Stelle eine Nachricht versteckt ist.[3]

Asymmetrische Steganographie

Die asymmetrische Steganographie (auch *Public-Key-Steganographie*) basiert – wie die asymmetrische Kryptographie – allein darauf, dass jeder potenzielle Empfänger einer verdeckten Nachricht einen (möglichst authentischen) öffentlichen Schlüssel zur Verfügung stellt, welcher zum Verstecken einer Nachricht benutzt wird. Mit diesem öffentlichen Schlüssel wird die Nachricht verschlüsselt und eingebettet. Ausgelesen werden kann die Nachricht nur vom Empfänger, der dafür eigens über einen privaten Schlüssel verfügt. Der Sender kann die Nachricht nicht wieder entschlüsseln. Richtet sich der verwendete Algorithmus nach Kerckhoffs' Prinzip, so ist er nicht einmal in der Lage herauszufinden, ob sich in einem Medium eine Nachricht verbirgt. Die einzige Ausnahme ist, dass er das Trägermedium direkt mit dem Steganogramm vergleicht.[4]

Arten der Steganographie

Historisches

Ein etwas zeitraubendes Verfahren ist aus der Antike bekannt: Dort wurde einem Sklaven der Kopf geschoren und eine Nachricht auf die Kopfhaut tätowiert. Sobald die Haare wieder nachgewachsen waren, wurde der Sklave zum Empfänger geschickt.[5]

Bekannte Beispiele sind auch Wachstafeln, die normalerweise in Wachs geritzte Botschaften enthalten. Im Gegensatz dazu wurden die geheimen Botschaften in das Holz darunter geritzt, das Wachs darüber gegossen und mit einer unverdächtigen Botschaft versehen.

Weitere historische Beispiele sind nicht oder schwer erkennbare Wasserzeichen in Papier oder Banknoten.

Friedrich L. Bauer beschreibt einen Soldaten im Krieg, der seinen Eltern in seinen Briefen nach Hause jeweils durch den ersten Buchstaben nach der Anrede einen Buchstaben seines Aufenthaltsortes *Tunis* mitteilt. Dabei beachtet er nicht die (zufällig verschiedenen) Laufzeiten der einzelnen Briefe. Als seine Eltern einige Zeit später nachfragen, wo denn *Nutsi* liege, fliegt das an sich unauffällige Verfahren auf.

Es gibt zahlreiche klassische Methoden der Steganographie, u. a.:

- die auf Papier „unsichtbare“ Geheimtinte (beispielsweise Zitronensaft)
- ein doppelter Boden in Paketen oder Briefumschlägen
- hohle Absätze von Schuhen und ähnliches
- der Mikropunkt
- geheimes Schreiben mit Licht: Stenographia
- das Einbetten einer Nachricht in einer anderen unterhalb der Wahrnehmungsschwelle.

Technische Steganographie

Siehe auch: Computergestützte Steganographie

Beispiele dazu sind:

- Der Einsatz von Mikrofilmen ist aus älteren Krimis bekannt, wobei teilweise eine A4-Seite auf der Größe eines Schreibmaschinenpunktes versteckt werden kann. Ein solcher Punkt (in der Fachterminologie „Mikrat“ oder Mikropunkt genannt) lässt sich leicht verstecken.
- Versteckte Tätowierung der Antike fällt unter diesen Begriff.
- Kennzeichnung von Kopien oder Ausdrucken durch Machine Identification Codes.

Linguistische Steganographie

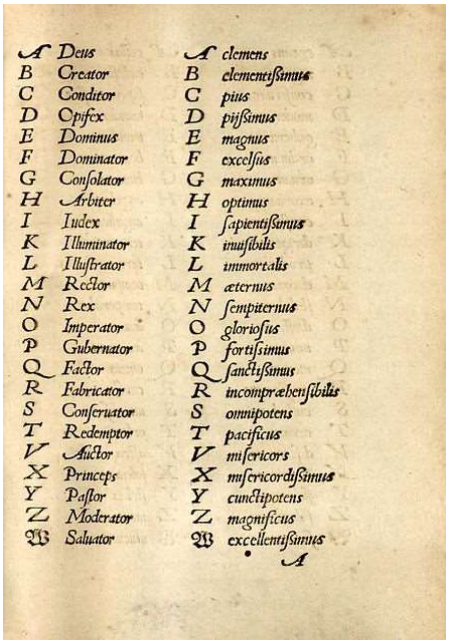
In Buch I und II von Johannes Trithemius’ *Steganographia* (1499/1500) werden die einzelnen Buchstaben des geheimzuhaltenden Textes, zuerst in nicht substituierter Form, dann mittels monoalphabetischer Substitution, in einem vorgegebenen Rhythmus, oft unter Einschluss von Leeren, zu neuen Wörtern gestreckt, und diese neuen Wörter syntaktisch und grammatikalisch korrekt zu einem thematisch stimmigen Text verbunden. In Buch I und II von Trithemius' *Polygraphia* (1508/1515) müssen die die Buchstaben des Klartexts ersetzenden Wörter vom Chiffrierer nicht länger selbst erfunden werden, sondern werden seitenlang und tabellarisch als syntaktisch und grammatisch aneinanderfügbare linguistische Fertigbauteile vorgegeben: in P I folgen auf 24 Substantive im Nominativ 24 entsprechende Adjektive, dann 24 Partizipien, dann 24 Akkusativobjekte, dann 24 Prädikate, dann 24 Dativobjekte usw. wobei die Worttabellen je einmal pro Buchstabe, von links nach rechts zu benutzen sind. So ergibt z. B. die Chiffrierung von *lieber* unmittelbar den Text „Illustrator sapientissimus gubernans celestia concedat requirentibus“. Der Satz „Salvator sapientissimus dirigens angelica deferat nobis charitas potentissimi creatoris“ ist eine Chiffrierung des Wortes *Wikipedia*.[7]

Spammimic[8] ist ein Programm, das eine kurze eingegebene Nachricht in harmlos aussehenden Text verschlüsselt, der Spam ähnelt.

Nicetext verwandelt eine Binärdatei in pseudo-natürlichen Text. Dazu benutzt das Programm kontextfreie Grammatiken. Das Programm enthält ein Wörterbuch und Schreibstile. Das Wörterbuch enthält englische Wörter, die in fünf grammatische Typen klassifiziert sind (Artikel, Substantiv, Verb, Adjektiv, Präposition). Der Stil bestimmt die syntaktischen Regeln für verschiedene Satztypen. Ein einfacher Satz hat z. B. den Aufbau ART-SUBST-VERB-ART-SUBST.

Für die Transformation wählt der Kodierer einen Stil. Die Input-Bits dienen als Pointer auf die Wörter in den verschiedenen Klassen des Wörterbuchs. Die Dekodierung beruht auf einfacher reverser Codebook-Suche.

Beispiel zum Prinzip: Angenommen das Wörterbuch enthält vier Wörter in der Klasse ART (mit den binären Indizes 00 bis 11) und 32 Wörter in SUBST (mit den binären Indizes 00000 bis 11111). Die Eingabe sei die Bitfolge 0101110. Die ersten zwei Bit der Eingabe (01) werden durch das zweite Wort in ART ersetzt. Das nächste Wort entspricht dem 15. Wort in SUBST.


A Deus — A clemens
B Creator — B clementiſſimus
C Conditor — C pius
D Opifex — D piiſſimus
E Dominus — E magnus
F Dominator — F excelſus
G Conſolator — G maximus
H Arbiter — H optimus
I Iudex — I ſapientiſſimus
K Illuminator — K inuiſibilis
L Illuſtrator — L immortalis
M Rector — M æternus
N Rex — N ſempiternus
O Imperator — O glorioſus
P Gubernator — P fortiſſimus
Q Factor — Q ſanctiſſimus
R Fabricator — R incomprehenſibilis
S Conſeruator — S omnipotens
T Redemptor — T pacificus
V Auctor — V miſericors
X Princeps — X miſericordiſſimus
Y Paſtor — Y cunctipotens
Z Moderator — Z magnificus
& Saluator — & excellentiſſimus

Buchstaben-Wort-Substitutionstabelle zu Beginn von Buch I der *Polygraphia* von Johannes Trithemius[6]

Semagramm

Eine Unterklasse der linguistischen Steganographie ist das Semagramm. Dabei werden durch kleine Details in einer an sich unverfänglichen Nachricht, einem Bild oder einer Zeichnung Informationen übertragen.

In einem Text können durch die Wahl unterschiedlicher Schriftarten die Zeichen einer geheimen Nachricht maskiert werden, wie beispielsweise die kodierten Zeichen in der ursprünglichen Form der Bacon-Chiffre. Allerdings sind diese kleinen Unterschiede auch für ein ungeübtes Auge deutlich sichtbar. Weniger auffällig sind beispielsweise die Verwendung von An- oder Abstrichen, kleinen Tintenpatzern, scheinbar hängenden Schreibmaschinen-Typen und Ähnliches.

Neben Textsemagrammen lassen sich in Bildern Nachrichten verstecken. So könnte die Länge von Grashalmen an einem Bachlauf ein Morsecode sein, die Zahl und Anordnung der Wolken in einer scheinbar von Kinderhand gezeichneten Landschaft für einen Buchstaben stehen. Der Versand einer Kiste mit Uhren kann ein Semagramm sein. Die Anordnung und Zeigerstellung könnten wichtige Informationen enthalten.[9]

Open Code

Aufwändiger ist es, eine eigene Geheimsprache zu entwickeln. Zum Beispiel werden Geheimzeichen nach einem bestimmten Muster eingestreut. Der Vorteil dieser Verfahren ist, dass sie, anders als ein Semagramm, nicht so einfach von Dritten als Geheimnachrichten identifiziert werden können.

Maskierte Geheimschrift, Jargon-Code

Eine maskierte Geheimschrift ist eine Art Geheimsprache. Bestimmten Floskeln, Wörtern oder Zeichen wird eine besondere Bedeutung zugewiesen, diese muss vorher zwischen den Partnern vereinbart werden. Einige Ausdrücke solcher Geheimsprachen haben als Jargon auch schon Einzug in die Alltagssprache gehalten, man denke an:

- „Kohle“, „Kies“ → Geld
- „Loch“, „Häfen“ → Gefängnis
- „Stoff“ → Drogen
- „Ratte“ → Verräter

Unlautere Kartenspieler können durch Handzeichen angeben, ob, mit wem und was sie spielen wollen. Auch möglich sind Hinweise durch Sätze oder Wörter, die mit „H“ beginnen, welche darauf hindeuten könnten, dass „Herz“ gespielt werden soll. Je individueller ein solcher Code ist, desto unauffälliger ist er. Allerdings kann der erstellte oder gesprochene Text leicht gekünstelt und aufgebläht wirken.

Maskierte Geheimschriften sind anfällig gegen Zensur: Ein Zensor, der Texte inhaltsgleich zum Beispiel durch Verwendung von Synonymen neu schreibt, kann den geheimen Inhalt unwissentlich zerstören.

Getarnte Geheimschriften

Geheime Nachrichten so in einem Text zu verstecken, dass sie den normalen Textfluss nicht stören, kann aufwändig sein. Die geheimen Zeichen stehen nach einem bestimmten Muster in dem an sich unauffälligen Text, so könnte beispielsweise jedes zweite Zeichen nach einem Komma ein Buchstabe eines Geheimwortes sein. Beim Westerlinck- oder „eins, eins, eins“-Code wird die Geheimnachricht durch die Anzahl der Silben der Textwörter codiert.

Schablonen, die über einen Text gelegt werden, deren Öffnungen nur noch die relevanten Geheimwörter durchscheinen lassen, heißen Cardan-Gitter. Da die Lücken dazwischen geometrisch passgenau mit Text auszufüllen sind, kommt es dadurch meist zu umständlichem Satzbau und eigenartiger Wortwahl.

Siehe auch: Bibelcode

Ähnliche Verfahren

- Spreu-und-Weizen-Algorithmus: Ein Verfahren, um geheime Nachrichten wie Nadeln in einem Heuhaufen aus irrelevanten, aber ähnlich aussehenden Daten zu verbergen.
- Verdeckter Kanal: Ein parasitärer Kommunikationskanal, welcher die Bandbreite eines legitimierten Kommunikationskanals benutzt, um Informationen zu übermitteln.

Siehe auch

- Molekularer Schlüssel

Literatur

- Friedrich L. Bauer: *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie.* 3., überarbeitete und erweiterte Auflage. Springer, Berlin u. a. 2000, ISBN 3-540-67931-6, (früherer Titel *Kryptologie*).
- Neil F. Johnson, Zoran Durić, Sushil Jajodia: *Information Hiding: Steganography and Watermarking – Attacks and Countermeasures.* Springer, Berlin u. a. 2001, ISBN 978-0-7923-7204-2.
- Fabien Petitcolas, Stefan Katzenbeisser: *Information Hiding Techniques for Steganography and Digital Watermarking.* Artech House, Boston, Mass. 2000, ISBN 978-1-58053-035-4.

Weblinks

Wiktionary: Steganographie – Bedeutungserklärungen, Wortherkunft, Synonyme, Übersetzungen

- Die „information hiding“-Homepage (http://www.cl.cam.ac.uk/~fapp2/steganography/) (englisch)
- Eine Sammlung ungewöhnlicher Methoden um das mancherorts illegale Programm DeCSS unbemerkt zu verteilen (http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/Stego/index.html) (englisch)

Einzelnachweise

1. Wilhelm Gemoll: *Griechisch-Deutsches Schul- und Handwörterbuch*. G. Freytag Verlag/Hölder-Pichler-Tempsky, München/Wien 1965.
2. Auguste Kerckhoffs: *La cryptographie militaire.* (http://www.petitcolas.net/fabien/kerckhoffs/) In: *Journal des sciences militaires.* Bd. 9, S. 5–38 (Jan. 1883), S. 161–191 (Feb. 1883).
3. Stephan Spitz, Michael Pramateftakis, Joachim Swoboda: *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*. Springer, 2011, ISBN 978-3-8348-8120-5, S. 15 (google.com (http://books.google.com/books?id=psAhBAAAQBAJ&pg=PA15)).
4. Günter Müller, Kai Rannenberg, Manfred Reitenspieß: *Verlässliche IT-Systeme: Zwischen Key Escrow und elektronischem Geld*. Vieweg+Teubner, 2013, ISBN 978-3-322-86842-8, S. 215 (google.com (http://books.google.com/books?id=8cyeBgAAQBAJ&pg=PA215)).
5. Fabien Petitcolas, Stefan Katzenbeisser: *Information Hiding Techniques for Steganography and Digital Watermarking.* Artech House, Boston, Mass. 2000, ISBN 978-1-58053-035-4.
6. Trithemius *POLYGRAPHIÆ LIBRI SEX*, Frankfurt 1550 (http://daten.digitale-sammlungen.de/~db/0002/bsb00026190/images/index.html?seite=71).
7. Richard Eier: *Kryptographie und Informationstheorie (http://digilib.happy-security.de/files/Steganographie.pdf).* PDF
8. Linguistische Steganographie mit Spammimic (http://www.spammimic.com/)
9. Eric Cole: *Hiding in Plain Sight. Steganography and the art of covert communication.* Wiley, New York 2003, ISBN 0-471-44449-9.