Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word *steganography* is of Greek origin and means "concealed writing" from the Greek words *steganos* (στεγανός) meaning "covered or protected", and *graphei* (γραφή) meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other *covertext* and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.[1] Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

History

The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples of steganography in his *Histories*.[2] Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand.

In his work "*Polygraphiae*" Johannes Trithemius developed his so-called "Ave-Maria-Cipher" with which one can hide information in a Latin praise of God. "*Auctor Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris*" for example contains the concealed word *VICIPEDIA*.[3]

Techniques

Physical

Steganography has been widely used, including in recent historical times and the present day. Possible permutations are endless and known examples include:

- Hidden messages within wax tablets — in ancient Greece, people wrote messages on the wood, then covered it with wax upon which an innocent covering message was written.
- Hidden messages on messenger's body — also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head again. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.
- During World War II, the French Resistance sent some messages written on the backs of couriers using invisible ink.
- Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages.
- Messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier.
- Messages written on envelopes in the area covered by postage stamps.

- During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute, approximately less than the size of the period produced by a typewriter. World War II microdots needed to be embedded in the paper and covered with an adhesive, such as collodion. This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.
- During World War II, a spy for Japan in New York City, Velvalee Dickinson, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed the quantity and type of doll to ship. The stegotext was the doll orders, while the concealed "plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.
- Cold War counter-propaganda. In 1968, crew members of the USS *Pueblo* intelligence ship held as prisoners by North Korea, communicated in sign language during staged photo opportunities, informing the United States they were not defectors, but rather were being held captive by the North Koreans. In other photos presented to the U.S., crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

Digital

Modern steganography entered the world in 1985 with the advent of the personal computer being applied to classical steganography problems.[4] Development following that was slow, but has since taken off, going by the number of "stego" programs available:

Image of a tree with a steganographically hidden image. The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization. The hidden image is shown below.

- Concealing messages within the lowest bits of noisy images or sound files.
- Concealing data within encrypted data or within random data. The data to be concealed is first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the one-time pad generates ciphertexts that look perfectly random if you do not have the private key).
- Chaffing and winnowing.
- Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a ciphertext-only attack.
- Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.
- Pictures embedded in video material (optionally played at slower or faster speed).
- Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in keypresses in some applications (telnet or remote desktop software) can mean a delay in packets, and the delays in the packets can be used to encode data.
- Changing the order of elements in a set.
- Content-Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a non-human adversary/warden.

- Blog-Steganography. Messages are fractionalized and the (encrypted) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole blogosphere.
- Modifying the echo of a sound file (Echo Steganography).[5]
- Secure Steganography for Audio Signals.[6]

Image of a cat extracted from the tree image above.

- Image bit-plane complexity segmentation steganography

Network

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. This nomenclature was originally introduced by Krzysztof Szczypiorski in 2003.[7] Contrary to the typical steganographic methods which utilize digital media (images, audio and video files) as a cover for hidden data, network steganography utilizes communication protocols' control elements and their basic intrinsic functionality. As a result, such methods are harder to detect and eliminate.[8]

Typical network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU (Protocol Data Unit),[9][10][11] to the time relations between the exchanged PDUs,[12] or both (hybrid methods).[13]

Moreover, it is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term inter-protocol steganography.[14]

Network steganography covers a broad spectrum of techniques, which include, among others:

- Steganophony - the concealment of messages in Voice-over-IP conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver (this method is called LACK - Lost Audio Packets Steganography), or, alternatively, hiding information in unused header fields.[15]
- WLAN Steganography – the utilization of methods that may be exercised to transmit steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks)[16]

Printed

Digital steganography output may be in the form of printed documents. A message, the *plaintext*, may be first encrypted by traditional means, producing a *ciphertext*. Then, an innocuous *covertext* is modified in some way so as to contain the ciphertext, resulting in the *stegotext*. For example, the letter size, spacing, typeface, or other characteristics of a covertext can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it. Francis Bacon developed Bacon's cipher as such a technique.

The ciphertext produced by most digital steganography methods, however, is not printable. Traditional digital methods rely on perturbing noise in the channel file to hide the message, as such, the channel file must be

transmitted to the recipient with no additional noise from the transmission. Printing introduces much noise in the ciphertext, generally rendering the message unrecoverable. There are techniques that address this limitation, one notable example is ASCII Art Steganography.[17]

Audio

In steganography, the message used to hide the secret message is called the host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as a stego message. In other words, a stego message is a combination of a host message and a secret message. Audio steganography requires a text or audio secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography and the stego message after steganography remains the same.[18]

Text

Steganography can be applied to different types of media including text, audio, image, video, etc. However, text steganography is considered to be the most difficult kind of steganography due to the lack of redundancy in text as compared to image or audio. However, it requires less memory and provides for simpler communication. One method that could be used for text steganography is data compression. Data compression encodes information in one representation, into another representation. The new representation of data is smaller in size. One of the possible schemes to achieve data compression is Huffman coding. Huffman coding assigns smaller length codewords to more frequently occurring source symbols and longer length codewords to less frequently occurring source symbols.

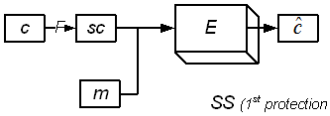
Unicode steganography uses lookalike characters of the usual ASCII set to look normal, while really carrying extra bits of information. If the text is displayed correctly, there should be no visual difference from ordinary text. Some systems, however, may display the fonts differently, and the extra information would be easily spotted.

Using Sudoku puzzles

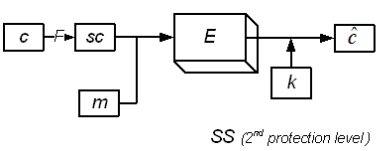
This is the art of concealing data in an image using Sudoku which is used like a key to hide the data within an image. Steganography using sudoku puzzles has as many keys as there are possible solutions of a Sudoku puzzle, which is 6.71×10^{21}. This is equivalent to around 70 bits, making it much stronger than the DES method which uses a 56 bit key.[19]

Data embedding security schemes

The choice of embedding algorithm in the most cases is driven by the results of the steganographic channel robustness analysis . One of the areas that improves steganographic robustness is usage of a key scheme for embedding messages.[20] Various key steganographic schemes have various levels of protection. Key scheme term means a procedure of how to use key steganographic system based on the extent of its use. However, when the steganographic robustness is increased a bandwidth of the whole embedding system is decreased. Therefore the task of a scheme selection for achieving the optimal values of the steganographic system is not trivial.



Steganographic System - The First Protection Level Scheme

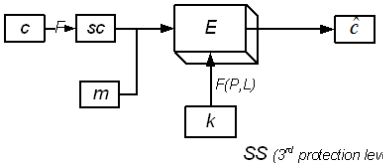


Steganographic System - The Second Protection Level Scheme

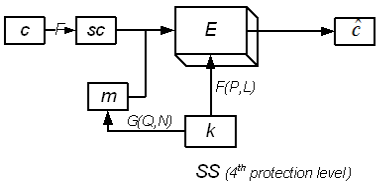
Embedding messages in steganographic system can be carried out without use of a key or with use of a key. To improve steganographic

robustness key can be used as a verification option. It can make an impact on the distribution of bits of a message within a container, as well as an impact on the procedure of forming a sequence of embedded bits of a message.

The first level of protection is determined only by the choice of embedding algorithm. This may be the least significant bits modification algorithm, or algorithms for modifying the frequency or spatial-temporal characteristics of the container. The first level of protection is presented in any steganographic channel. Steganographic system in this case can be represented as shown at *The First Protection Level Scheme* figure. There following notations are used: *c* - is a container file; *F* - steganographic channel space (frequency or/and amplitude container part, that is available for steganographic modification and message signal transmission); *SC* - steganographic system; *m* - message to be embedded; *E* - embedding method; $\hat{c}$ - modified container file.



Steganographic System - The Third Protection Level Scheme



Steganographic System - The Fourth Protection Level Scheme

The second protection level of the steganographic system, as well as all levels of protection of the higher orders, is characterized by the use of Key (password) via steganographic modification. An example of a simple key scheme, which provides a second level of protection, is to write the unmodified or modified password in the top or bottom of the message; or the distribution of the password sign on the entire length of the steganographic channel. Such key schemes do not affect the distribution of messages through the container and do not use a message preprocessing according to the defined key (see figure *The Second Protection Level Scheme*). This kind of steganographic systems are used in such tasks as, for instance, adding a digital signature for proof of copyright. Data embedding performance is not changed in comparison with the fastest approach of the first protection level usage.

Steganographic data channels that use key schemes based distribution of a message through the container and or preprocessing of an embedded message for data hiding are more secure. When the third protection level key scheme is used it affects the distribution of a message through the container (see figure *The Third Protection Level Scheme*, where *F(P, L)* − distribution function of a message within a container; *P* − minimum number of container samples that are needed to embed one message sample; *L* − step of a message distribution within a container). Accordingly, the performance of container processing will be lower than in the case of the first and the second key schemes. Taking into account that $P \geq L$, the simplest representation of the *F(P, L)* function could be as following:

$F(P, L) = cycle*L + step*P,$

where *cycle* is a number of the current *L* section and *step* is a number of the embedded message sample.

The difference between the fourth protection level scheme and the third one is that in steganographic system there are two distribution functions of a message within a container are used. The first is responsible for a message samples selection according to some function *G(Q, N)*, and the second function *F(P, L)* is responsible for position selection in a container for message sample hiding. Here *Q* − the size of message block to be inserted; *N* − the size (in bits) of one sample of the message file (see figure *The Fourth Protection Level Scheme*).

Based on the above discussion it is possible to define a classification table of key steganographic schemes:

Key Steganographic Schemes Classification

Steganographic system protection level	Steganographic algorithm usage	Key (password) usage	Key influence on a message signal bits distribution per container	Key influence on a message signal bits selection and distribution per container
1	+	-	-	-
2	+	+	-	-
3	+	+	+	-
4	+	+	+	+

Additional terminology

In general, terminology analogous to (and consistent with) more conventional radio and communications technology is used; however, a brief description of some terms which show up in software specifically, and are easily confused, is appropriate. These are most relevant to digital steganographic systems.

The *payload* is the data to be covertly communicated. The *carrier* is the signal, stream, or data file into which the payload is hidden; which differs from the "*channel*" (typically used to refer to the type of input, such as "a JPEG image"). The resulting signal, stream, or data file which has the payload encoded into it is sometimes referred to as the *package*, *stego file*, or *covert message*. The percentage of bytes, samples, or other signal elements which are modified to encode the payload is referred to as the *encoding density* and is typically expressed as a number between 0 and 1.

In a set of files, those files considered likely to contain a payload are called *suspects*. If the *suspect* was identified through some type of statistical analysis, it might be referred to as a *candidate*.

Countermeasures and detection

Detection of physical steganography requires careful physical examination, including the use of magnification, developer chemicals and ultraviolet light. It is a time-consuming process with obvious resource implications, even in countries where large numbers of people are employed to spy on their fellow nationals. However, it is feasible to screen mail of certain suspected individuals or institutions, such as prisons or prisoner-of-war (POW) camps. During World War II, a technology used to ease monitoring of POW mail was specially treated paper that would reveal invisible ink. An article in the June 24, 1948 issue of *Paper Trade Journal* by the Technical Director of the United States Government Printing Office, Morris S. Kantrowitz, describes in general terms the development of this paper, three prototypes of which were named *Sensicoat*, *Anilith*, and *Coatalith* paper. These were for the manufacture of post cards and stationery to be given to German prisoners of war in the US and Canada. If POWs tried to write a hidden message the special paper would render it visible. At least two US patents were granted related to this technology, one to Mr. Kantrowitz, No. 2,515,232, "Water-Detecting paper and Water-Detecting Coating Composition Therefor", patented July 18, 1950, and an earlier one, "Moisture-Sensitive Paper and the Manufacture Thereof", No. 2,445,586, patented July 20, 1948. A similar strategy is to issue prisoners with writing paper ruled with a water-soluble ink that "runs" when in contact with a water-based invisible ink.

In computing, detection of steganographically encoded packages is called steganalysis. The simplest method to detect modified files, however, is to compare them to known originals. For example, to detect information being moved through the graphics on a website, an analyst can maintain known-clean copies of these materials and compare them against the current contents of the site. The differences, assuming the carrier is the same, will compose the payload. In general, using extremely high compression rate makes steganography difficult, but not impossible. While compression errors provide a hiding place for data, high compression reduces the amount of data available to hide the payload in, raising the encoding density and facilitating easier detection (in the extreme case,

even by casual observation).

Applications

Usage in modern printers

Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.[21]

Example from modern practice

The larger the cover message is (in data content terms—number of bits) relative to the hidden message, the easier it is to hide the latter. For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media. It is not clear how commonly this is actually done. For example: a 24-bit bitmap will have 8 bits representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 2^8 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used (more or less undetectably) for something else other than color information. If we do it with the green and the red as well we can get one letter of ASCII text for every three pixels.

Stated somewhat more formally, the objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (the original signal) due to the injection of the payload (the signal to covertly embed) are visually (and ideally, statistically) negligible; that is to say, the changes are indistinguishable from the noise floor of the carrier. Any medium can be a carrier, but media with a large amount of redundant or compressible information are better suited.

From an information theoretical point of view, this means that the channel must have more capacity than the "surface" signal requires; that is, there must be redundancy. For a digital image, this may be noise from the imaging element; for digital audio, it may be noise from recording techniques or amplification equipment. In general, electronics that digitize an analog signal suffer from several noise sources such as thermal noise, flicker noise, and shot noise. This noise provides enough variation in the captured digital information that it can be exploited as a noise cover for hidden data. In addition, lossy compression schemes (such as JPEG) always introduce some error into the decompressed data; it is possible to exploit this for steganographic use as well.

Steganography can be used for digital watermarking, where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified (for example, Coded Anti-Piracy), or even just to identify an image (as in the EURion constellation).

Alleged use by terrorists

When one considers that messages could be encrypted steganographically in e-mail messages, particularly e-mail spam, the notion of junk e-mail takes on a whole new light. Coupled with the "chaffing and winnowing" technique, a sender could get messages out and cover their tracks all at once.

An example showing how terrorists may use forum avatars to send hidden messages. This avatar contains the message "Boss said that we should blow up the bridge at midnight." encrypted with mozaiq using "växjö" as password.

Rumors about terrorists using steganography started first in the daily newspaper *USA Today* on February 5, 2001 in two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption". In July the same year, an article was titled even more precisely: "Militants wire Web with links to jihad". A citation from the article: "*Lately, al-Qaeda operatives have been sending hundreds of encrypted messages that have been hidden in files on digital photographs on the auction site eBay.com*". Other media worldwide cited these rumors many times, especially after the terrorist attack of 9/11, without ever showing proof. The Italian newspaper *Corriere della Sera* reported that an Al Qaeda cell which had been captured at the Via Quaranta mosque in Milan had pornographic images on their computers, and that these images had been used to hide secret messages (although no other Italian paper ever covered the story). The *USA Today* articles were written by veteran foreign correspondent Jack Kelley, who in 2004 was fired after allegations emerged that he had fabricated stories and sources.

In October 2001, the *New York Times* published an article claiming that al-Qaeda had used steganography to encode messages into images, and then transported these via e-mail and possibly via USENET to prepare and execute the September 11, 2001 terrorist attack. The Federal Plan for Cyber Security and Information Assurance Research and Development,[22] published in April 2006 makes the following statements:

- "...immediate concerns also include the use of cyberspace for covert communications, particularly by terrorists but also by foreign intelligence services; espionage against sensitive but poorly defended data in government and industry systems; subversion by insiders, including vendors and contractors; criminal activity, primarily involving fraud and theft of financial or identity information, by hackers and organized crime groups..." (p. 9–10)
- "International interest in R&D for steganography technologies and their commercialization and application has exploded in recent years. These technologies pose a potential threat to national security. Because steganography secretly embeds additional, and nearly undetectable, information content in digital products, the potential for covert dissemination of malicious software, mobile code, or information is great." (p. 41–42)
- "The threat posed by steganography has been documented in numerous intelligence reports." (p. 42)

Moreover, an online "terrorist training manual", the "Technical Mujahid, a Training Manual for Jihadis" contained a section entitled "Covert Communications and Hiding Secrets Inside Images."[23]

By early 2002, a Cranfield University MSc thesis developed the first practical implementation of an online real-time Counter Terrorist Steganography Search Engine. This was designed to detect the most likely image steganography in transit and thereby provide UK Ministry of Defence Intelligence Staff a realistic approach to "narrowing the field", suggesting that interception capacity was never the difficulty but rather prioritising the target media.

Despite this, *there are no publicly reported instances of terrorists using computer steganography*. Al Qaeda's use of steganography is somewhat simpler: In 2008 a British man, Rangzieb Ahmed, was alleged to have a contact book with Al-Qaeda telephone numbers, written in invisible ink. He was convicted of terrorism.[24]

Alleged use by intelligence services

In 2010, the Federal Bureau of Investigation revealed that the Russian foreign intelligence service uses customized steganography software for embedding encrypted text messages inside image files for certain communications with "illegal agents" (agents under non-diplomatic cover) stationed abroad.[25]

Citations

[1] Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy" (http://web.archive.org/web/20070716093719/http://www.alternet.org/story/11986/). AlterNet. Archived from the original (http://www.alternet.org/story/11986/) on 2007-07-16. . Retrieved 2008-09-02.

[2] Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). "Information Hiding: A survey" (http://www.cl.cam.ac.uk/~fapp2/publications/ieee99-infohiding.pdf) (pdf). *Proceedings of the IEEE (special issue)* **87** (7): 1062–78. doi:10.1109/5.771065. . Retrieved 2008-09-02.

[3] Trimenius "Polygraphiae (cf. p. 71f)" (http://daten.digitale-sammlungen.de/~db/0002/bsb00026190/images/index.html?seite=71). Digitale Sammlungen. Trimenius. Retrieved 2012-02-21.

[4] The origin of Modern Steganography (http://www.mikebarney.net/stego.html)

[5] Echo Data Hiding (http://www.slidefinder.net/a/audio_steganography_echo_data_hiding/24367218)

[6] Secure Steganography for Audio Signals (http://beepdf.com/doc/92591/iscgav_01.html)

[7] Krzysztof Szczypiorski (4 November 2003). "Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System - HICCUPS" (http://www.tele.pw.edu.pl/~krzysiek/pdf/steg-seminar-2003.pdf). *Institute of Telecommunications Seminar*. . Retrieved 17 June 2010.

[8] Patrick Philippe Meier (5 June 2009). "Steganography 2.0: Digital Resistance against Repressive Regimes" (http://irevolution.wordpress.com/2009/06/05/steganography-2-0-digital-resistance-against-repressive-regimes/). *irevolution.wordpress.com*. . Retrieved 17 June 2010.

[9] Craig Rowland (May 1997). "Covert Channels in the TCP/IP Suite" (http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/issue/view/80). *First Monday Journal*. . Retrieved 16 June 2010.

[10] Steven J. Murdoch and Stephen Lewis (2005). "Embedding Covert Channels into TCP/IP" (http://www.cl.cam.ac.uk/~sjm217/papers/ih05coverttcp.pdf). *Information Hiding Workshop*. . Retrieved 16 June 2010.

[11] Kamran Ahsan and Deepa Kundur (December 2002). "Practical Data Hiding in TCP/IP" (http://wwwiti.cs.uni-magdeburg.de/iti_amsl/acm/acm02/ahsan_kundur.pdf). *ACM Wksp. Multimedia Security*. . Retrieved 16 June 2010.

[12] Kundur D. and Ahsan K. (April 2003). "Practical Internet Steganography: Data Hiding in IP" (http://www.ece.tamu.edu/~deepa/pub/KunAhsTXSecWrkshp03.pdf). *Texas Wksp. Security of Information Systems*. . Retrieved 16 June 2010.

[13] Wojciech Mazurczyk and Krzysztof Szczypiorski (November 2008). "Steganography of VoIP Streams" (http://home.elka.pw.edu.pl/~wmazurcz/moja/art/OTM_StegVoIP_2008.pdf). *Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Proc. of The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico*. . Retrieved 16 June 2010.

[14] Bartosz Jankowski, Wojciech Mazurczyk and Krzysztof Szczypiorski (11 May 2010). "Information Hiding Using Improper Frame Padding". arXiv:1005.1925 [cs.CR].

[15] Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski (February 2010). "Vice Over IP: The VoIP Steganography Threat" (http://spectrum.ieee.org/telecom/internet/vice-over-ip-the-voip-steganography-threat). *IEEE Spectrum*. . Retrieved 11 February 2010.

[16] Krzysztof Szczypiorski (October 2003). "HICCUPS: Hidden Communication System for Corrupted Networks" (http://krzysiek.tele.pw.edu.pl/pdf/acs2003-hiccups.pdf). *In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, pp. 31-40*. . Retrieved 11 February 2010.

[17] Vincent Chu. "ASCII Art Steganography" (http://pictureworthsthousandwords.appspot.com/). .

[18] Muhammad Asad, Junaid Gilani, Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 2011 International Conference on Computer Networks and Information Technology (ICCNIT), Date: 11–13 July 2011, Page(s): 143-147

[19] B.r., Roshan Shetty; J., Rohith; V., Mukund; Honwade, Rohan; Rangaswamy, Shanta (2009). *Steganography Using Sudoku Puzzle*. pp. 623–626. doi:10.1109/ARTCom.2009.116.

[20] Chvarkova, Iryna; Tsikhanenka, Siarhei; Sadau, Vasili (15 February 2008). "Steganographic Data Embedding Security Schemes Classification" (http://scientist.by/index.php?option=com_content&view=article&id=37:steganography-digital-data-embedding-techniques&catid=9&Itemid=27&limitstart=5). *Steganography: Digital Data Embedding Techniques*. Intelligent Systems Scientific Community, Belarus. . Retrieved 25 March 2011.

[21] "Secret Code in Color Printers Lets Government Track You; Tiny Dots Show Where and When You Made Your Print" (http://www.eff.org/press/archives/2005/10/16), *Electronic Frontier Foundation*, October 16th, 2005

[22] Federal Plan for Cyber Security and Information Assurance Research and Development (http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf) National Science and Technology Council, April 2006

[23] The Jamestown Foundation (http://www.jamestown.org/programs/gta/single/?tx_ttnews[tt_news]=1057&tx_ttnews[backPid]=182&no_cache=1)

[24] "British Muslim 'had Al Qaeda contacts book with terrorists' numbers written in invisible ink'" (http://www.dailymail.co.uk/news/article-1061190/British-Muslim-Al-Qaeda-contacts-book-terrorists-numbers-written-invisible-ink.html). *Daily Mail* (London). 24 September 2008. .

[25] "Criminal complaint by Special Agent Ricci against alleged Russian agents" (http://www.justice.gov/opa/documents/062810complaint2.pdf). United States Department of Justice. .

References

- Wayner, Peter (2002). *Disappearing cryptography: information hiding: steganography & watermarking* (http://www.wayner.org/node/6). Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 1-55860-769-2.
- Wayner, Peter (2009). *Disappearing cryptography 3rd Edition: information hiding: steganography & watermarking* (http://www.wayner.org/node/13). Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 978-0123744791.
- Petitcolas, Fabian A.P.; Katzenbeisser, Stefan (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House Publishers. ISBN 1-58053-035-4.
- Johnson, Neil; Duric, Zoran; Jajodia, Sushil (2001). *Information hiding: steganography and watermarking: attacks and countermeasures*. Springer. ISBN 978-0-7923-7204-2.

External links

- Steganography (http://www.dmoz.org/Computers/Security/Products_and_Tools/Cryptography/Steganography/) at the Open Directory Project
- Examples showing images hidden in other images (http://petitcolas.net/fabien/steganography/image_downgrading/index.html)
- Information Hiding: Steganography & Digital Watermarking. (http://www.jjtc.com/Steganography) Papers and information about steganography and steganalysis research from 1995 to the present. Includes Steganography Software Wiki list. Dr. Neil F. Johnson.
- Detecting Steganographic Content on the Internet. (http://niels.xtdnet.nl/papers/detecting.pdf) 2002 paper by Niels Provos and Peter Honeyman published in *Proceedings of the Network and Distributed System Security Symposium* (San Diego, CA, February 6–8, 2002). NDSS 2002. Internet Society, Washington, D.C.
- Covert Channels in the TCP/IP Suite (http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/528/449)—1996 paper by Craig Rowland detailing the hiding of data in TCP/IP packets.
- Network Steganography Centre Tutorials (http://stegano.net/tutorials.html). How-to articles on the subject of network steganography (Wireless LANs, VoIP - Steganophony, TCP/IP protocols and mechanisms, Steganographic Router, Inter-protocol steganography). By Krzysztof Szczypiorski and Wojciech Mazurczyk from Network Security Group.
- Invitation to BPCS-Steganography. (http://datahide.com/BPCSe/)
- Steganography by Michael T. Raggo, DefCon 12, Aug. 1, 2004. (http://www.spy-hunter.com/Steganography_V7.0_DefCon_V3_S.pdf)
- File Format Extension Through Steganography (http://ecommons.txstate.edu/cscitad/7) by Blake W. Ford and Khosrow Kaikhah

Article Sources and Contributors

Steganography *Source*: http://en.wikipedia.org/w/index.php?oldid=486941722 *Contributors*: 90 Auto, A. B., A930913, Aarktica, Aaron Kauppi, AceVentura, Adam Bishop, Ahoerstemeier, Aircorn, Akulkis, Alan McBeth, Alansohn, Alasdair, AlasdairBailey, Alexanderwdark, Andrewpmk, AndyKali, Andylindsay, Anikingos, Ann arbor street, Antandrus, Antipodean Contributor, Anwar saadat, Aphid360, Aristotle, ArnoldReinhold, Arthena, Arvindn, Authalic, Aydee, B jonas, Barek, Bartledan, Bdesham, Beanmaster758, Beltz, BenWillard, Benefros, Blackvisionit, Blues-harp, Boing! said Zebedee, Boonhead, Brandon5485, Breakpoint, Brianski, Bryan Derksen, ByScientist, Caliberoviv, Calieber, Camw, Cheddad, Cheeselog3000, Chinasaur, Chris Roy, Cndv, Cntras, Codyrank, Cogiati, Cojoco, Cometstyles, Conversion script, Cpl Syx, Crakkpot, Cralar, Cybercobra, Cynix, Cyp, DabMachine, Daeroni, DavidDouthitt, Davidmatt, Deflective, Deltabeignet, Deor, Dirkbike, Dlae, DocWatson42, Dogah, Donreed, Dougher, DougsTech, Drdefcom, Dycedarg, Dysprosia, DÂ,ugosz, Eaglemb, EbenVisher, Eclecticology, Ed g2s, Edggar, Edman274, Edub, Eeshsidhartha, Egg, El C, Elonka, EmreDuran, Erianna, Etienne.navarro, EvanProdromou, Evil Monkey, Evil saltine, Eyreland, Fama Clamosa, Fargoth, Fatrabbit, Felipe1982, Fergie4000, Flewis, Fonduelover, Furrykef, Futurevision, Fæ, Gappiah, Gerbrant, Ghettoblaster, Giftlite, Gilbertera, Gioto, Gjohnson9894, Gogo Dodo, Goldfishinapicklejar, Greenrd, GreyCat, Grubber, Gurch, Gut informiert, Guy M, H8gaR, Hadal, Haddock420, Haipa Doragon, Hairy Dude, Hans Dunkelberg, Hawaiirules, HeadOffice, Headbomb, Heron, HiddenMind, Hut 8.5, Hydrargyrum, INVERTED, Ilmari Karonen, Imnotminkus, Inter, Intgr, Intrigue, Inventm, Iobehmom, Iridescent, Ivangrimm, JMK, JackNapierX, Jancikotuc, Janke, Jeffz1, Jim.henderson, Jllopezpino, JoGusto, JoanneB, JoeDeRose, Joekasper, JohnsonL623, Jose Ramos, Joseph Solis in Australia, JoshuaZ, KDS4444, Kammerbulle, Katherine, Katt, Kelson, Kevinp, Kingpin13, Koyaanis Qatsi, Lazarus666, Lele giannoni, Lemojk7, LjL, Ljlego, Lkinkade, LokiClock, Lquilter, LukeFerry, Lunkwill, Lynda Finn, Madeleine Price Ball, Mandarax, MarioS, MarkHudson, Marudubshinki, Matt Crypto, Maximaximax, Maxt, Mclayto, Meggar, Mercan, Michael Hardy, Midnightcomm, Mike Rosoft, Minorbob, Mitsukai, Mmernex, Mohdavary, Moshe szweizer, Mpx, Mr0t1633, MrBlueSky, MrDarcy, MrFire, MrOllie, Muasad, MuthuKutty, Mysid, NEMT, NateEag, Newtown11, Nfj9800, Nick2253, Ninly, Nk, Novum, Nuwewsco, Octahedron80, Oli Filth, Omegatron, OpenToppedBus, Oseransky, Owain, Parhamr, PaulHanson, Peregrine981, PerryTachett, Peterhoneyman, Peterl, Petlif, Pgan002, PierreAbbat, Pillsmith, Pissas@acm.org, Pmetzger, Pne, Prodego, Pseudomonas, Psinu, Radon210, Raftermast, RainbowOfLight, RayAYang, Raymondwinn, Rbcafe, Refdoc, Repayne, Rfrohardt, Rhalah, Rich Farmbrough, Rjwilmsi, Robferrer, Rodzilla, Rohasnagpal, Roshanbrshetty, RossPatterson, Rschauer, Ruud Koot, SWAdair, Saforrest, Sannse, Saros136, Seared eyes, Securiger, Shadowjams, Shandris, Shonzilla, Shouta, Silvergriphon, Sinfocol, Singingwolfboy, Slash, Smack, SmackTacular, Smoore 500, Spacexplosion, Spihuntr, Spy message, Stefanomione, Steinsomers, Stewartadcock, Strait, Suffusion of Yellow, Surroundsound5000, Surv1v4l1st, Sverdrup, Syvaidya, Tabletop, Takaitra, TakuyaMurata, Talrias, TankMiche, Tbc, Teumteum, Thebarrin, Themindset, Theodore Kloba, Theresa knott, Thibbs, Thinking of England, Tkgd2007, Tkinkhorst, Tnolley, Tommstein, Tookiewana, Touisiau, TreasuryTag, Upholder, Valhalla, Van helsing, VernoWhitney, Vidiii, Vina, Vrenator, WLU, WPPWAH, WeißNix, Welshcorgi, WikiGonz, Wikiguy28272, Wikiklrsc, Wikistegano, Wingman4l7, WojPob, Ww, Wwoods, Wwwwolf, XDanielx, Xdpdc888, Yar Kramer, Yermiyahu, ZipoBibrok5x10^8, ترجمان05, 560 anonymous edits

Image Sources, Licenses and Contributors

Image:StenographyOriginal.png *Source*: http://en.wikipedia.org/w/index.php?title=File:StenographyOriginal.png *License*: GNU Free Documentation License *Contributors*: Original uploader was Cyp at en.wikipedia

Image:StenographyRecovered.png *Source*: http://en.wikipedia.org/w/index.php?title=File:StenographyRecovered.png *License*: GNU Free Documentation License *Contributors*: Original uploader was Cyp at en.wikipedia

File:Steganography Protection Level 01.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Steganography_Protection_Level_01.png *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: ByScientist

File:Steganography Protection Level 02.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Steganography_Protection_Level_02.png *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: ByScientist

File:Steganography Protection Level 03 00.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Steganography_Protection_Level_03_00.png *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: ByScientist

File:Steganography Protection Level 04 00.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Steganography_Protection_Level_04_00.png *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: ByScientist

Image:Avatar for terrorist.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Avatar_for_terrorist.png *License*: Free Art License *Contributors*: Own modification of source image.

License