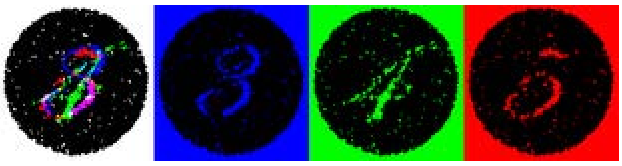
WIKIPEDIA
The Free Encyclopedia

Steganography



The same image viewed by white, blue, green, and red lights reveals different hidden numbers.

Steganography (/ˌstɛɡəˈnɒɡrəfi/ (🔊 listen) *STEG-ə-NOG-rə-fee*) is the practice of representing information within another message or physical object, in such a manner that the presence of the information is not evident to human inspection. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video. The word *steganography* comes from Greek *steganographia*, which combines the words *steganós* (στεγανός), meaning "covered or concealed", and *-graphia* (γραφή) meaning "writing".[1]

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, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle.[2]

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.[3]

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent and its contents.

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. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

History

The first recorded uses of steganography can be traced back to 440 BC in Greece, when Herodotus mentions two examples in his *Histories*.[4] Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, "marking" the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, "When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Additionally, 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" that 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*.[5]

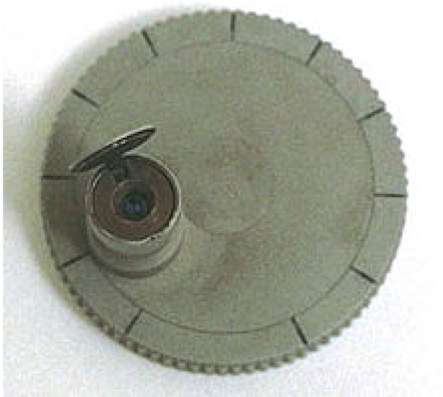
A chart from Johannes Trithemius's *Steganographia* copied by Dr John Dee in 1591

Techniques

Physical

Steganography has been widely used for centuries. Some examples include:[6]

Deciphering the code. *Steganographia*


A microdot camera

- Hidden messages on a paper written in secret inks.
- Hidden messages distributed, according to a certain rule or key, as smaller parts (e.g. words or letters) among other words of a less suspicious cover text. This particular form of steganography is called a null cipher.
- Messages written in Morse code on yarn and then knitted into a piece of clothing worn by a courier.
- Messages written on envelopes in the area covered by postage stamps.
- In the early days of the printing press, it was common to mix different typefaces on a printed page because the printer did not have enough copies of some letters in one typeface. Thus, a message could be hidden by using two or more different typefaces, such as normal or italic.
- During and after World War II, espionage agents used photographically-produced microdots to send information back and forth. Microdots were typically minute (less than the size of the period produced by a typewriter). World War II microdots were embedded in the paper and covered with an adhesive, such as collodion that was reflective and so was detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of postcards.
- During World War II, Velvalee Dickinson, a spy for Japan in New York City, 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, and 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.
- During World War II, photosensitive glass was declared secret, and used for transmitting information to Allied armies.
- Jeremiah Denton repeatedly blinked his eyes in Morse code during the 1966 televised press conference that he was forced into as an American prisoner-of-war by his North Vietnamese captors, spelling out "T-O-R-T-U-R-E". That confirmed for the first time to the US Naval Intelligence and other Americans that the North Vietnamese were torturing American prisoners-of-war.

- In 1968, crew members of the USS *Pueblo* intelligence ship, held as prisoners by North Korea, communicated in sign language during staged photo opportunities, to inform the United States that they were not defectors but captives of the North Koreans. In other photos presented to the US, crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.
- In 1985, a klezmer saxophonist smuggled secrets into and out of the Soviet Union by coding them as pitches of musical notes in sheet music.[7]

Digital messages

- Concealing messages within the lowest bits of noisy images or sound files. A survey and evaluation of relevant literature/techniques on the topic of digital image steganography can be found here.[8]
- Concealing data within encrypted data or within random data. The message to conceal is encrypted, then 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 without 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 a 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 nonhuman 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).[9]
- Steganography for audio signals.[10]
- Image bit-plane complexity segmentation steganography
- Including data in ignored sections of a file, such as after the logical end of the carrier file.[11]

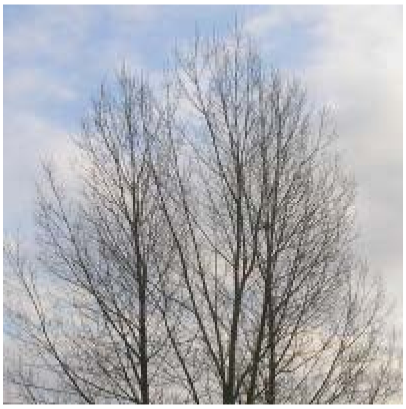


Image of a tree with a steganographically hidden image. The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization. The hidden image is shown below.

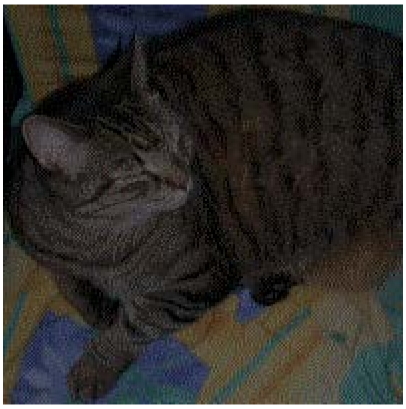


Image of a cat extracted from the tree image above.

- Adaptive steganography: Skin tone based steganography using a secret embedding angle.[12]
- Embedding data within the control-flow diagram of a program subjected to control flow analysis[13]

Digital text

- Using non-printing Unicode characters Zero-Width Joiner (ZWJ) and Zero-Width Non-Joiner (ZWNJ).[14][15] These characters are used for joining and disjoining letters in Arabic and Persian, but can be used in Roman alphabets for hiding information because they have no meaning in Roman alphabets: because they are "zero-width" they are not displayed. ZWJ and ZWNJ can represent "1" and "0". This may also be done with en space, figure space and whitespace characters.[16]
- Embedding a secret message in the pattern of deliberate errors and marked corrections in a word processing document, using the word processor's change tracking feature.[17]
- In 2020, Zhongliang Yang et al discovered that for text generative steganography, when the quality of the generated steganographic text is optimized to a certain extent, it may make the overall statistical distribution characteristics of the generated steganographic text more different from the normal text, making it easier to be recognized. They named this phenomenon Perceptual-Statistical Imperceptibility Conflict Effect (Psic Effect).[18]

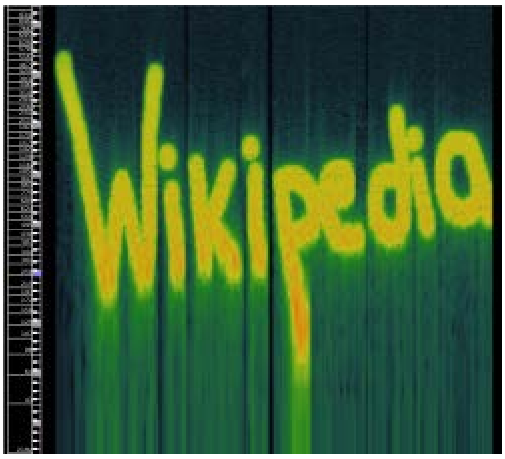
Hiding an image within a soundfile

An image or a text can be converted into a soundfile, which is then analysed with a spectrogram to reveal the image. Various artists have used this method to conceal hidden pictures in their songs, such as Aphex Twin in "Windowlicker" or Nine Inch Nails in their album *Year Zero*.[19]

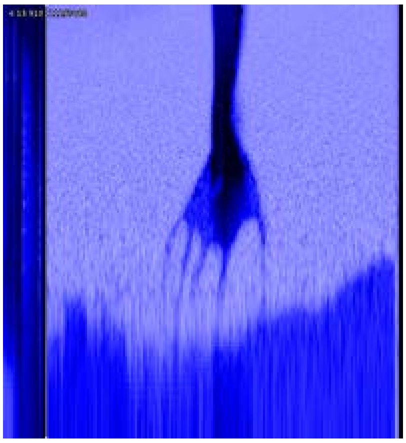
Images hidden in sound files

1. The word "Wikipedia" is drawn using computer software

2. The image is converted into an audio file



3. Finally, the audio is analysed through a spectrogram, revealing the initial image



Spectrogram of a hidden image encoded as sound in the song "My Violent Heart" by Nine Inch Nails from the *Year Zero* album (2007)

Social steganography

In communities with social or government taboos or censorship, people use cultural steganography—hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers.[20][21] Examples include:

- Hiding a message in the title and context of a shared video or image.
- Misspelling names or words that are popular in the media in a given week, to suggest an alternate meaning.
- Hiding a picture that can be traced by using Paint or any other drawing tool.

Steganography in streaming media

Since the era of evolving network applications, steganography research has shifted from image steganography to steganography in streaming media such as Voice over Internet Protocol (VoIP).

In 2003, Giannoula et al. developed a data hiding technique leading to compressed forms of source video signals on a frame-by-frame basis.[22]

In 2005, Dittmann et al. studied steganography and watermarking of multimedia contents such as VoIP.[23]

In 2008, Yongfeng Huang and Shanyu Tang presented a novel approach to information hiding in low bit-rate VoIP speech stream, and their published work on steganography is the first-ever effort to improve the codebook partition by using Graph theory along with Quantization Index Modulation in low bit-rate streaming media.[24]

In 2011 and 2012, Yongfeng Huang and Shanyu Tang devised new steganographic algorithms that use codec parameters as cover object to realise real-time covert VoIP steganography. Their findings were published in *IEEE Transactions on Information Forensics and Security*.[25][26][27]

Cyber-physical systems/Internet of Things

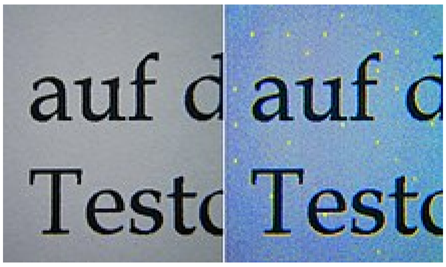
Academic work since 2012 demonstrated the feasibility of steganography for cyber-physical systems (CPS)/the Internet of Things (IoT). Some techniques of CPS/IoT steganography overlap with network steganography, i.e. hiding data in communication protocols used in CPS/the IoT. However, specific techniques hide data in CPS components. For instance, data can be stored in unused registers of IoT/CPS components and in the states of IoT/CPS actuators.[28][29]

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 *cover text* 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 cover text 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, and 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 being ASCII Art Steganography.[30]

Although not classic steganography, some types of modern color laser printers integrate the model, serial number, and timestamps on each printout for traceability reasons using a dot-matrix code made of small, yellow dots not recognizable to the naked eye—see printer steganography for details.



Yellow dots from a laser printer

Using puzzles

The art of concealing data in a puzzle can take advantage of the degrees of freedom in stating the puzzle, using the starting information to encode a key within the puzzle/puzzle image.

For instance, steganography using sudoku puzzles has as many keys as there are possible solutions of a Sudoku puzzle, which is 6.71×10^{21}.[31]

Network

In 1977, **Kent** concisely described the potential for covert channel signaling in general network communication protocols, even if the traffic is encrypted (in a footnote) in "Encryption-Based Protection for Interactive User/Computer Communication," Proceedings of the Fifth Data Communications Symposium, September 1977.

In 1987, **Girling** first studied covert channels on a local area network (LAN), identified and realised three obvious covert channels (two storage channels and one timing channel), and his research paper entitled "Covert channels in LAN's" published in *IEEE Transactions on Software Engineering*, vol. SE-13 of 2, in February 1987.[32]

In 1989, **Wolf** implemented covert channels in LAN protocols, e.g. using the reserved fields, pad fields, and undefined fields in the TCP/IP protocol.[33]

In 1997, **Rowland** used the IP identification field, the TCP initial sequence number and acknowledge sequence number fields in TCP/IP headers to build covert channels.[34]

In 2002, **Kamran Ahsan** made an excellent summary of research on network steganography.[35]

In 2005, Steven J. **Murdoch** and Stephen **Lewis** contributed a chapter entitled "Embedding Covert Channels into TCP/IP" in the "*Information Hiding*" book published by Springer.[36]

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.[37] Contrary to typical steganographic methods that use digital media (images, audio and video files) to hide data, network steganography uses communication protocols' control elements and their intrinsic functionality. As a result, such methods can be harder to detect and eliminate.[38]

Typical network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the protocol data unit (PDU),[39][40][41] to the time relations between the exchanged PDUs,[42] or both (hybrid methods).[43]

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.[44] Alternatively, multiple network protocols can be used simultaneously to transfer hidden information and so-called control protocols can be embedded into steganographic communications to extend their capabilities, e.g. to allow dynamic overlay routing or the switching of utilized hiding methods and network protocols.[45][46]

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.[47]
- WLAN Steganography – transmission of steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks)[48]

Terminology and Taxonomy

In 2015, a taxonomy of 109 network hiding methods was presented by Steffen Wendzel, Sebastian Zander et al. that summarized core concepts used in network steganography research.[49] The taxonomy was developed further in recent years by several publications and authors and adjusted to new domains, such as CPS steganography.[50][51][52]

Additional terminology

Discussions of steganography generally use terminology analogous to and consistent with conventional radio and communications technology. However, some terms appear specifically in software and are easily confused. These are the most relevant ones to digital steganographic systems:

The *payload* is the data covertly communicated. The *carrier* is the signal, stream, or data file that hides the payload, which differs from the *channel*, which typically means the type of input, such as a JPEG image. The resulting signal, stream, or data file with the encoded payload is sometimes called the *package*, *stego file*, or *covert message*. The proportion of bytes, samples, or other signal elements modified to encode the payload is called the *encoding density* and is typically expressed as a number between 0 and 1.

In a set of files, the files that are considered likely to contain a payload are *suspects*. A *suspect* identified through some type of statistical analysis can be referred to as a *candidate*.

Countermeasures and detection

Detecting physical steganography requires a 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 that employ many people 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, prisoner of war camps gave prisoners specially-treated paper that would reveal invisible ink. An article in the 24 June 1948 issue of *Paper Trade Journal* by the Technical Director of the United States Government Printing Office had Morris S. Kantrowitz describe in general terms the development of this paper. Three prototype papers (*Sensicoat*, *Anilith*, and *Coatalith*) were used to manufacture postcards and stationery provided to German prisoners of war in the US and Canada. If POWs tried to write a hidden message, the special paper rendered it visible. The US granted at least two patents related to the technology, one to Kantrowitz, U.S. Patent 2,515,232 (https://patents.google.com/patent/US2515232), "Water-Detecting paper and Water-Detecting Coating Composition Therefor," patented 18 July 1950, and an earlier one, "Moisture-Sensitive Paper and the Manufacture Thereof," U.S. Patent 2,445,586 (https://patents.google.com/patent/US2445586), patented 20 July 1948. A similar strategy issues prisoners with writing paper ruled with a water-soluble ink that runs in contact with water-based invisible ink.

In computing, steganographically encoded package detection 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 the materials and then compare them against the current contents of the site. The differences, if the carrier is the same, comprise the payload. In general, using extremely high compression rates makes steganography difficult but not impossible. Compression errors provide a hiding place for data, but high compression reduces the amount of data available to hold the payload, raising the encoding density, which facilitates easier detection (in extreme cases, even by casual observation).

There are a variety of basic tests that can be done to identify whether or not a secret message exists. This process is not concerned with the extraction of the message, which is a different process and a separate step. The most basic approaches of steganalysis are visual or aural attacks, structural attacks, and statistical attacks. These approaches attempt to detect the steganographic algorithms that were used.[53] These algorithms range from unsophisticated to very sophisticated, with early algorithms being much easier to detect due to statistical anomalies that were present. The size of the message that is being hidden is a factor in how difficult it is to detect. The overall size of the cover object also plays a factor as well. If the cover object is small and the message is large, this can distort the statistics and make it easier to detect. A larger cover object with a small message decreases the statistics and gives it a better chance of going unnoticed.

Steganalysis that targets a particular algorithm has much better success as it is able to key in on the anomalies that are left behind. This is because the analysis can perform a targeted search to discover known tendencies since it is aware of the behaviors that it commonly exhibits. When analyzing an image the least significant bits of many images are actually not random. The camera sensor, especially lower-end sensors are not the best quality and can introduce some random bits. This can also be affected by the file compression done on the image. Secret messages can be introduced into the least significant bits in an image and then hidden. A steganography tool can be used to camouflage the secret message in the least significant bits but it can introduce a random area that is too perfect. This area of perfect randomization stands out and can be detected by comparing the least significant bits to the next-to-least significant bits on an image that hasn't been compressed.[53]

Generally, though, there are many techniques known to be able to hide messages in data using steganographic techniques. None are, by definition, obvious when users employ standard applications, but some can be detected by specialist tools. Others, however, are resistant to detection—or rather it is not possible to reliably distinguish data containing a hidden message from data containing just noise—even when the most sophisticated analysis is performed. Steganography is being used to conceal and deliver more effective cyber attacks, referred to as *Stegware*. The term Stegware was first introduced in 2017[54] to describe any malicious operation involving steganography as a vehicle to conceal an attack. Detection of steganography is challenging, and because of that, not an adequate defence. Therefore, the only way of defeating the threat is to transform data in a way that destroys any hidden messages,[55] a process called Content Threat Removal.

Applications

Use in modern printers

Some modern computer printers use steganography, including Hewlett-Packard and Xerox brand color laser printers. The printers add tiny yellow dots to each page. The barely-visible dots contain encoded printer serial numbers and date and time stamps.[56]

Example from modern practice

The larger the cover message (in binary data, the number of bits) relative to the hidden message, the easier it is to hide the hidden message (as an analogy, the larger the "haystack", the easier it is to hide a "needle"). So digital pictures, which contain much data, are sometimes used to hide messages on the Internet and on other digital communication media. It is not clear how common this practice actually is.

For example, a 24-bit bitmap uses 8 bits to represent each of the three color values (red, green, and blue) of each pixel. The blue alone has 2^8 different levels of blue intensity. 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 that is repeated for the green and the red elements of each pixel as well, it is possible to encode 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) because of the injection of the payload (the signal to covertly embed) are visually (and ideally, statistically) negligible. The changes are indistinguishable from the noise floor of the carrier. All media can be a carrier, but media with a large amount of redundant or compressible information is better suited.

From an information theoretical point of view, that means that the channel must have more capacity than the "surface" signal requires. There must be redundancy. For a digital image, it 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. The 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 to the decompressed data, and it is possible to exploit that for steganographic use, as well.

Although steganography and digital watermarking seem similar, they are not. In steganography, the hidden message should remain intact until it reaches its destination. Steganography can be used for digital watermarking in which 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). In such a case, the technique of hiding the message (here, the watermark) must be robust to prevent tampering. However, digital watermarking sometimes requires a brittle watermark, which can be modified easily, to check whether the image has been tampered with. That is the key difference between steganography and digital watermarking.

Alleged use by intelligence services

In 2010, the Federal Bureau of Investigation alleged 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 without diplomatic cover) stationed abroad.[57]

On April 23, 2019 the U.S. Department of Justice unsealed an indictment charging Xiaoqing Zheng, a Chinese businessman and former Principal Engineer at General Electric, with 14 counts of conspiring to steal intellectual property and trade secrets from General Electric. Zheng had allegedly used steganography to exfiltrate 20,000 documents from General Electric to Tianyi Aviation Technology Co. in Nanjing, China, a company the FBI accused him of starting with backing from the Chinese government.[58]

Distributed steganography

There are distributed steganography methods,[59] including methodologies that distribute the payload through multiple carrier files in diverse locations to make detection more difficult. For example, U.S. Patent 8,527,779 (https://patents.google.com/patent/US8527779) by cryptographer William Easttom (Chuck Easttom).

Online challenge

The puzzles that are presented by Cicada 3301 incorporate steganography with cryptography and other solving techniques since 2012.[60] Puzzles involving steganography have also been featured in other alternate reality games.

The communications[61][62] of The May Day mystery incorporate steganography and other solving techniques since 1981.[63]

Computer malware

It is possible to steganographically hide computer malware into digital images, videos, audio and various other files in order to evade detection by antivirus software. This type of malware is called stegomalware. It can be activated by external code, which can be malicious or even non-malicious if some vulnerability in the software reading the file is exploited.[64]

Stegomalware can be removed from certain files without knowing whether they contain stegomalware or not. This is done through content disarm and reconstruction (CDR) software, and it involves reprocessing the entire file or removing parts from it.[65][66] Actually detecting stegomalware in a file can be difficult and may involve testing the file behaviour in virtual environments or deep learning analysis of the file.[64]

Stegoanalysis

Stegoanalytical algorithms

Stegoanalytical algorithms can be cataloged in different ways, highlighting: according to the available information and according to the purpose sought.

According to the information available

There is the possibility of cataloging these algorithms based on the information held by the stegoanalyst in terms of clear and encrypted messages. It is a technique similar to cryptography, however, they have several differences:

- Chosen stego attack: the stegoanalyst perceives the final target stego and the stenographic algorithm used.
- Known cover attack: the stegoanalyst comprises the initial conductive target and the final target stego.
- Known stego attack: the stegoanalyst knows the initial carrier target and the final target stego, in addition to the algorithm used.
- Stego only attack: the stegoanalyst perceives exclusively the stego target.
- Chosen message attack: the stegoanalyst, following a message selected by him, originates a stego target.
- Known message attack: the stegoanalyst owns the stego target and the hidden message, which is known to him.

According to the purpose sought

The principal purpose of steganography is to transfer information unnoticed, however, it is possible for an attacker to have two different pretensions:

- Passive stegoanalysis: does not alter the target stego, therefore, it examines the target stego in order to establish whether it carries hidden information and recovers the hidden message, the key used or both.
- Active stegoanalysis: changes the initial stego target, therefore, it seeks to suppress the transfer of information, if it exists.

See also

- Acrostic – Text formed from parts of another text
- BPCS-Steganography – computer message obfuscation technology
- Camera/Shy
- Canary trap – Method for exposing an information leak
- Warrant canary – Method of indirect notification of a subpoena
- Covert channel – Computer security attack
- Cryptography – Practice and study of secure communication techniques
- Deniable encryption – Encryption techniques where an adversary cannot prove that the plaintext data exists
- Digital watermarking – Marker covertly embedded in a signal
- Invisible ink – Substance used for writing which is invisible and can later be made visible
- Polybius square – Type of code
- Security engineering – Process of incorporating security controls into an information system
- Semiotics – Study of signs and sign processes
- Steganographic file system
- Steganography tools – Software for embedding hidden data inside a carrier file
- Audio watermark – Electronic identifier embedded in an audio signal
- Visual cryptography
- Security printing – Field of the printing industry for banknotes and other security products

References

1. "Definition of STEGANOGRAPHY" (https://www.merriam-webster.com/dictionary/steganography). *Merriam-webster.com*. Retrieved 14 December 2021.
2. Fridrich, Jessica; M. Goljan; D. Soukal (2004). Delp Iii, Edward J; Wong, Ping W (eds.). "Searching for the Stego Key" (http://www.ws.binghamton.edu/fridrich/Research/Keysearch_SPIE.pdf) (PDF). *Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI*. Security, Steganography, and Watermarking of Multimedia Contents VI. **5306**: 70–82. Bibcode:2004SPIE.5306...70F (https://ui.adsabs.harvard.edu/abs/2004SPIE.5306...70F). doi:10.1117/12.521353 (https://doi.org/10.1117%2F12.521353). S2CID 6773772 (https://api.semanticscholar.org/CorpusID:6773772). Retrieved 23 January 2014.
3. Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy" (https://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.
4. 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*. **87** (7): 1062–78. CiteSeerX 10.1.1.333.9397 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.333.9397). doi:10.1109/5.771065 (https://doi.org/10.1109%2F5.771065). Retrieved 2008-09-02.

5. "Polygraphiae (cf. p. 71f)" (http://daten.digitale-sammlungen.de/~db/0002/bsb00026190/images/index.html?seite=71) (in German). Digitale Sammlungen. Retrieved 2015-05-27.
6. "The Wartime Spies Who Used Knitting as an Espionage Tool – Atlas Obscura" (https://getpocket.com/explore/item/the-wartime-spies-who-used-knitting-as-an-espionage-tool). *Pocket*. Retrieved 2020-03-04.
7. Newman, Lily Hay. "How a Saxophonist Tricked the KGB by Encrypting Secrets in Music" (https://web.archive.org/web/20220608222058/https://www.wired.com/story/merryl-goldberg-music-encryption-ussr-phantom-orchestra/). *Wired*. ISSN 1059-1028 (https://www.worldcat.org/issn/1059-1028). Archived from the original (https://www.wired.com/story/merryl-goldberg-music-encryption-ussr-phantom-orchestra/) on 2022-06-08. Retrieved 2022-06-09.
8. Cheddad, Abbas; Condell, Joan; Curran, Kevin; Mc Kevitt, Paul (2010). "Digital image steganography: Survey and analysis of current methods". *Signal Processing*. **90** (3): 727–752. doi:10.1016/j.sigpro.2009.08.010 (https://doi.org/10.1016%2Fj.sigpro.2009.08.010).
9. "Archived copy" (https://web.archive.org/web/20181106222503/http://ww31.slidefinder.net/a/audio_steganography_echo_data_hiding/24367218). Archived from the original (http://ww31.slidefinder.net/a/audio_steganography_echo_data_hiding/24367218) on 2018-11-06. Retrieved 2019-09-17.
10. "Secure Steganography for Audio Signals" (http://www.wseas.us/e-library/conferences/2010/Taipei/ISCGAV/ISCGAV-01.pdf) (PDF). *Wseas.us*. Retrieved 14 December 2021.
11. Bender, W.; Gruhl, D.; Morimoto, N.; Lu, A. (1996). "Techniques for data hiding" (https://web.archive.org/web/20200611050549/https://pdfs.semanticscholar.org/8c82/c93dfc7d3672e58efd982a23791a8a419053.pdf) (PDF). *IBM Systems Journal*. IBM Corp. **35** (3.4): 313–336. doi:10.1147/sj.353.0313 (https://doi.org/10.1147%2Fsj.353.0313). ISSN 0018-8670 (https://www.worldcat.org/issn/0018-8670). S2CID 16672162 (https://api.semanticscholar.org/CorpusID:16672162). Archived from the original (https://pdfs.semanticscholar.org/8c82/c93dfc7d3672e58efd982a23791a8a419053.pdf) (PDF) on 2020-06-11.
12. Cheddad, Abbas; Condell, Joan; Curran, Kevin; Mc Kevitt, Paul (2009). "A skin tone detection algorithm for an adaptive approach to steganography". *Signal Processing*. **89** (12): 2465–2478. doi:10.1016/j.sigpro.2009.04.022 (https://doi.org/10.1016%2Fj.sigpro.2009.04.022).
13. El-Khalil, Rakan; Keromytis, Angelos D. (2004), "Hydan: Hiding Information in Program Binaries" (https://dx.doi.org/10.1007/978-3-540-30191-2_15), *Information and Communications Security*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 187–199, doi:10.1007/978-3-540-30191-2_15 (https://doi.org/10.1007%2F978-3-540-30191-2_15), ISBN 978-3-540-23563-7, retrieved 2020-10-04
14. Akbas E. Ali (2010). "A New Text Steganography Method By Using Non-Printing Unicode Characters" (http://www.uotechnology.edu.iq/tec_magaz/volume282010/No.1.2010/researches/Text%20%287%29.pdf) (PDF). *Eng. & Tech. Journal*. **28** (1).
15. Aysan, Zach (December 30, 2017). "Zero-Width Characters" (https://www.zachaysan.com/writing/2017-12-30-zero-width-characters). Retrieved January 2, 2018. "In early 2016 I realized that it was possible to use zero-width characters, like zero-width non-joiner or other zero-width characters like the zero-width space to fingerprint text. Even with just a single type of zero-width character the presence or non-presence of the non-visible character is enough bits to fingerprint even the shortest text."
16. Aysan, Zach (January 1, 2018). "Text Fingerprinting Update" (https://www.zachaysan.com/writing/2018-01-01-fingerprinting-update). Retrieved January 2, 2018.
17. T. Y. Liu and W. H. Tsai, "A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique," in IEEE Transactions on Information Forensics and Security, vol. 2, no. 1, pp. 24–30, March 2007. doi:10.1109/TIFS.2006.890310 (https://doi.org/10.1109%2FTIFS.2006.890310) [1] (http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4100626&isnumber=4100617)

18. Yang, Z., Zhang, S., Hu, Y., Hu, Z., & Huang, Y. (2020). VAE-Stega: Linguistic Steganography Based on Variational Auto-Encoder. IEEE Transactions on Information Forensics and Security.
19. Dachis, Adam (June 2011). "How to Hide Secret Messages and Codes in Audio Files" (https://lifehacker.com/how-to-hide-secret-messages-and-codes-in-audio-files-5807289). *Lifehacker*. Retrieved 2019-09-17.
20. Social Steganography: how teens smuggle meaning past the authority figures in their lives (https://boingboing.net/2013/05/22/social-steganography-how-teen.html), Boing Boing, May 22, 2013. Retrieved June 7, 2014.
21. Social Steganography (http://www.scenariomagazine.com/social-steganography/), Scenario Magazine, 2013.
22. Giannoula, A.; Hatzinakos, D. (2003). "Compressive data hiding for video signals". *Proceedings 2003 International Conference on Image Processing (Cat. No.03CH37429)*. IEEE. **1**: I–529–32. doi:10.1109/icip.2003.1247015 (https://doi.org/10.1109%2Ficip.2003.1247015). ISBN 0780377508. S2CID 361883 (https://api.semanticscholar.org/CorpusID:361883).
23. Dittmann, Jana; Hesse, Danny; Hillert, Reyk (2005-03-21). Delp Iii, Edward J; Wong, Ping W (eds.). "Steganography and steganalysis in voice-over IP scenarios: operational aspects and first experiences with a new steganalysis tool set". *Security, Steganography, and Watermarking of Multimedia Contents VII*. SPIE. **5681**: 607. Bibcode:2005SPIE.5681..607D (https://ui.adsabs.harvard.edu/abs/2005SPIE.5681..607D). doi:10.1117/12.586579 (https://doi.org/10.1117%2F12.586579). S2CID 206413447 (https://api.semanticscholar.org/CorpusID:206413447).
24. B. Xiao, Y. Huang, and S. Tang, "An Approach to Information Hiding in Low Bit-Rate Speech Stream", in *IEEE GLOBECOM 2008*, IEEE, pp. 371–375, 2008. ISBN 978-1-4244-2324-8.
25. Huang, Yong Feng; Tang, Shanyu; Yuan, Jian (June 2011). "Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec" (https://repository.uwl.ac.uk/id/eprint/3935/1/Steganography%20in%20inactive%20frames%20of%20VoIP%20streams%20encoded%20by%20source%20codec.pdf) (PDF). *IEEE Transactions on Information Forensics and Security*. **6** (2): 296–306. doi:10.1109/tifs.2011.2108649 (https://doi.org/10.1109%2Ftifs.2011.2108649). ISSN 1556-6013 (https://www.worldcat.org/issn/1556-6013). S2CID 15096702 (https://api.semanticscholar.org/CorpusID:15096702).
26. Huang, Yongfeng; Liu, Chenghao; Tang, Shanyu; Bai, Sen (December 2012). "Steganography Integration Into a Low-Bit Rate Speech Codec" (https://repository.uwl.ac.uk/id/eprint/3932/1/Steganography%20Integration%20into%20a%20low-bit%20rate%20speech%20codec.pdf) (PDF). *IEEE Transactions on Information Forensics and Security*. **7** (6): 1865–1875. doi:10.1109/tifs.2012.2218599 (https://doi.org/10.1109%2Ftifs.2012.2218599). ISSN 1556-6013 (https://www.worldcat.org/issn/1556-6013). S2CID 16539562 (https://api.semanticscholar.org/CorpusID:16539562).
27. Ghosal, Sudipta Kr; Mukhopadhyay, Souradeep; Hossain, Sabbir; Sarkar, Ram (2020). "Application of Lah transform for security and privacy of data through information hiding in telecommunication". *Transactions on Emerging Telecommunications Technologies*. **32** (2). doi:10.1002/ett.3984 (https://doi.org/10.1002%2Fett.3984). S2CID 225866797 (https://api.semanticscholar.org/CorpusID:225866797).
28. Wendzel, Steffen; Mazurczyk, Wojciech; Haas, Georg. "Don't You Touch My Nuts: Information Hiding In Cyber Physical Systems Using Smart Buildings". *Proceedings of the 2017 IEEE Security & Privacy Workshops*. IEEE.
29. Tuptuk, Nilufer; Hailes, Stephen. "Covert channel attacks in pervasive computing". *Proceedings 2015 IEEE International Conference on Pervasive Computing and Communications (PerCom)*.

30. Vincent Chu. "ASCII Art Steganography" (https://pictureworthsthousandwords.appspot.com/). *Pictureworthsthousandwords.appspot.com*.
31. B.r., Roshan Shetty; J., Rohith; V., Mukund; Honwade, Rohan; Rangaswamy, Shanta (2009). "Steganography Using Sudoku Puzzle". *2009 International Conference on Advances in Recent Technologies in Communication and Computing*. pp. 623–626. doi:10.1109/ARTCom.2009.116 (https://doi.org/10.1109%2FARTCom.2009.116). ISBN 978-1-4244-5104-3. S2CID 7850622 (https://api.semanticscholar.org/CorpusID:7850622).
32. Girling, C.G. (February 1987). "Covert Channels in LAN's". *IEEE Transactions on Software Engineering*. SE-13 (2): 292–296. doi:10.1109/tse.1987.233153 (https://doi.org/10.1109%2Ftse.1987.233153). ISSN 0098-5589 (https://www.worldcat.org/issn/0098-5589). S2CID 3042941 (https://api.semanticscholar.org/CorpusID:3042941).
33. M. Wolf, “Covert channels in LAN protocols,” in Proceedings of the Workshop on Local Area Network Security (LANSEC’89) (T.A. Berson and T. Beth, eds.), pp. 91–102, 1989.
34. Rowland, Craig H. (1997-05-05). "Covert channels in the TCP/IP protocol suite". *First Monday*. **2** (5). doi:10.5210/fm.v2i5.528 (https://doi.org/10.5210%2Ffm.v2i5.528). ISSN 1396-0466 (https://www.worldcat.org/issn/1396-0466).
35. Kamran Ahsan, “Covert Channel Analysis and Data Hiding in TCP/IP,” MSc Thesis, University of Toronto, 2002.
36. Murdoch, Steven J.; Lewis, Stephen (2005), "Embedding Covert Channels into TCP/IP", *Information Hiding*, Springer Berlin Heidelberg, pp. 247–261, doi:10.1007/11558859_19 (https://doi.org/10.1007%2F11558859_19), ISBN 9783540290391
37. 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) (PDF). *Institute of Telecommunications Seminar*. Retrieved 17 June 2010.
38. 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.
39. 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.
40. Steven J. Murdoch & Stephen Lewis (2005). "Embedding Covert Channels into TCP/IP" (http://www.cl.cam.ac.uk/~sjm217/papers/ih05coverttcp.pdf) (PDF). *Information Hiding Workshop*. Retrieved 16 June 2010.
41. Kamran Ahsan & Deepa Kundur (December 2002). "Practical Data Hiding in TCP/IP" (https://web.archive.org/web/20121029155725/http://wwwiti.cs.uni-magdeburg.de/iti_amsl/acm/acm02/ahsan_kundur.pdf) (PDF). *ACM Wksp. Multimedia Security*. Archived from the original (http://wwwiti.cs.uni-magdeburg.de/iti_amsl/acm/acm02/ahsan_kundur.pdf) (PDF) on 29 October 2012. Retrieved 16 June 2010.
42. Kundur D. & Ahsan K. (April 2003). "Practical Internet Steganography: Data Hiding in IP" (https://web.archive.org/web/20121029155725/http://www.ece.tamu.edu/~deepa/pub/KunAhsTXSecWrkshp03.pdf) (PDF). *Texas Wksp. Security of Information Systems*. Archived from the original (http://www.ece.tamu.edu/~deepa/pub/KunAhsTXSecWrkshp03.pdf) (PDF) on 29 October 2012. Retrieved 16 June 2010.
43. Wojciech Mazurczyk & Krzysztof Szczypiorski (November 2008). "Steganography of VoIP Streams" (http://home.elka.pw.edu.pl/~wmazurcz/moja/art/OTM_StegVoIP_2008.pdf) (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.

44. Bartosz Jankowski; Wojciech Mazurczyk & Krzysztof Szczypiorski (11 May 2010). "Information Hiding Using Improper Frame Padding". arXiv:1005.1925 (https://arxiv.org/abs/1005.1925) [cs.CR (https://arxiv.org/archive/cs.CR)].

45. Wendzel, Steffen; Keller, Joerg (20 October 2011). *Low-Attention Forwarding for Mobile Network Covert Channels* (https://www.researchgate.net/publication/215661202). *12th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS)*. Lecture Notes in Computer Science. Vol. 7025. pp. 122–133. doi:10.1007/978-3-642-24712-5_10 (https://doi.org/10.1007%2F978-3-642-24712-5_10). ISBN 978-3-642-24711-8. Retrieved 4 September 2016.

46. Mazurczyk, Wojciech; Wendzel, Steffen; Zander, Sebastian; Houmansadr, Amir; Szczypiorski, Krzysztof (2016). *Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications* (http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1118861698.html) (1 ed.). Wiley-IEEE. ISBN 978-1-118-86169-1.

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

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

49. Wendzel, Steffen; Zander, Sebastian; Fechner, Bernhard; Herdin, Christian (2015-04-16). "Pattern-Based Survey and Categorization of Network Covert Channel Techniques" (https://www.researchgate.net/publication/263048788). *ACM Computing Surveys*. **47** (3): 1–26. doi:10.1145/2684195 (https://doi.org/10.1145%2F2684195). S2CID 14654993 (https://api.semanticscholar.org/CorpusID:14654993).

50. Mazurczyk, Wojciech; Wendzel, Steffen; Cabaj, Krzysztof (2018-08-27). "Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach". *Proceedings of the 13th International Conference on Availability, Reliability and Security*: 1–10. doi:10.1145/3230833.3233261 (https://doi.org/10.1145%2F3230833.3233261). ISBN 9781450364485. S2CID 51976841 (https://api.semanticscholar.org/CorpusID:51976841).

51. Hildebrandt, Mario; Altschaffel, Robert; Lamshöft, Kevin; Lange, Matthias; Szemkus, Martin; Neubert, Tom; Vielhauer, Claus; Ding, Yongjian; Dittmann, Jana (2020). "Threat Analysis of Steganographic and Covert Communication in Nuclear I&C Systems". *International Conference on Nuclear Security: Sustaining and Strengthening Efforts*.

52. Mileva, Aleksandra; Velinov, Aleksandar; Hartmann, Laura; Wendzel, Steffen; Mazurczyk, Wojciech (May 2021). "Comprehensive analysis of MQTT 5.0 susceptibility to network covert channels". *Computers & Security*. **104**: 102207. doi:10.1016/j.cose.2021.102207 (https://doi.org/10.1016%2Fj.cose.2021.102207). S2CID 232342523 (https://api.semanticscholar.org/CorpusID:232342523).

53. Wayner, Peter (2009). *Disappearing Cryptography: Information Hiding: Steganography & Watermarking*, Morgan Kaufmann Publishers, Amsterdam; Boston

54. Lancioni, German (2017-10-16). "What's Hidden in That Picture Online? Seeing Through "Stegware" " (https://www.mcafee.com/blogs/enterprise/seeing-through-stegware/). McAfee.

55. Wiseman, Simon (2017). "Defenders Guide to Steganography" (https://www.researchgate.net/publication/319943090). doi:10.13140/RG.2.2.21608.98561 (https://doi.org/10.13140%2FRG.2.2.21608.98561).

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

57. "Criminal complaint by Special Agent Ricci against alleged Russian agents" (https://www.justice.gov/opa/documents/062810complaint2.pdf) (PDF). United States Department of Justice.
58. "GE Engineer Charged in Elaborate Theft of Trade Secrets" (https://blog.twinstate.com/news/ge-trade-secrets-theft). Twinstate Technologies.
59. Liao, Xin; Wen, Qiao-yan; Shi, Sha (2011). "Distributed Steganography". *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE. pp. 153–156. doi:10.1109/IIHMSP.2011.20 (https://doi.org/10.1109%2FIIHMSP.2011.20). ISBN 978-1-4577-1397-2. S2CID 17769131 (https://api.semanticscholar.org/CorpusID:17769131).
60. Jane Wakefield (9 January 2014). "Cicada 3301: The darknet treasure trail reopens" (https://www.bbc.co.uk/news/technology-25667292). *BBC News*. Retrieved 11 January 2014.
61. "The texts" (http://www.maydaymystery.org/mayday/texts/index.html). *Maydaymystery.org*. Retrieved 2017-11-23.
62. "Recent things" (http://www.maydaymystery.org/mayday/recent.html). *Maydaymystery.org*. Retrieved 2017-11-23.
63. "The Mystery" (http://www.maydaymystery.org/mayday/mystery.html). *Maydaymystery.org*. Retrieved 2017-11-23.
64. Chaganti, Raj; R, Vinayakumar; Alazab, Mamoun; Pham, Tuan (2021-10-12). "Stegomalware: A Systematic Survey of Malware Hiding and Detection in Images, Machine Learning Models and Research Challenges" (https://www.techrxiv.org/articles/preprint/Stegomalware_A_Systematic_Survey_of_Malware_Hiding_and_Detection_in_Images_Machine_Learning_Models_and_Research_Challenges/16755457/1). doi:10.36227/techrxiv.16755457.v1 (https://doi.org/10.36227%2Ftechrxiv.16755457.v1).
65. Votiro (2021-11-30). "Finding a Content Disarm & Reconstruction (CDR) Vendor" (https://votiro.com/blog/what-to-look-for-in-cdr-file-sanitization-vendors/). *Votiro*. Retrieved 2023-01-11.
66. "Content Disarm and Reconstruct – SecureIQLab" (https://secureiqlab.com/content-disarm-and-reconstruct/). Retrieved 2023-01-11.

Sources

- Wayner, Peter (2002). *Disappearing cryptography: information hiding: steganography & watermarking* (http://www.wayner.org/node/6). Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 978-1-558-60769-9.
- Wayner, Peter (2009). *Disappearing cryptography 3rd Edition: information hiding: steganography & watermarking* (http://www.wayner.org/node/13). Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 978-0-123-74479-1.
- Petitcolas, Fabien A.P.; Katzenbeisser, Stefan (2000). *Information Hiding Techniques for Steganography and Digital Watermarking* (http://petitcolas.net/fabien/publications/book99-ih/). Artech House Publishers. ISBN 978-1-580-53035-4.
- Johnson, Neil; Duric, Zoran; Jajodia, Sushil (2001). *Information hiding: steganography and watermarking: attacks and countermeasures*. Springer. ISBN 978-0-792-37204-2.
- Petitcolas, Fabien A.P.; Katzenbeisser, Stefan (2016). *Information Hiding* (http://petitcolas.net/book15-ih/). Artech House Publishers. ISBN 978-1608079285.

External links

- An overview of digital steganography, particularly within images, for the computationally curious (https://www.youtube.com/watch?v=-7FBPgQDX5o) by Chris League, Long Island University, 2015

- Steganography (https://curlie.org/Computers/Security/Products_and_Tools/Cryptography/Steganography) at Curlie
- 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.org/BPCSe/)
- Steganography by Michael T. Raggo (http://www.spy-hunter.com/Steganography_V7.0_DefCon_V3_S.pdf), DefCon 12 (1 August 2004)
- File Format Extension Through Steganography (http://ecommons.txstate.edu/cscitad/7) by Blake W. Ford and Khosrow Kaikhah
- Computer steganography. Theory and practice with Mathcad (Rus) (https://web.archive.org/web/20140221205846/http://er.nau.edu.ua/bitstream/NAU/8049/1/CompSteganoRU.pdf) 2006 paper by Konakhovich G. F., Puzyrenko A. Yu. published in *MK-Press* Kyiv, Ukraine
- stegano (https://bztsrc.gitlab.io/stegano) a Free and Open Source steganography web service.