Https://searchsecurity.techtarget.com/definition/steganography

1. Steganography

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

The word steganography is derived from the greek words steganos (meaning hidden or covered) and the greek root graph (meaning to write).

Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content.

The content to be concealed through steganography -- called hidden text -- is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream.

If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

Steganography is practiced by those wishing to convey a secret message or code.

While there are many legitimate uses for steganography, malware developers have also been found to use steganography to obscure the transmission of malicious code.

Forms of steganography have been used for centuries and include almost any technique for hiding a secret message in an otherwise harmless container.

For example, using invisible ink to hide secret messages in otherwise inoffensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information.

2. Steganography techniques

In modern digital steganography, data is first encrypted or obfuscated in some other way and then inserted, using a special algorithm, into data that is part of a particular file format such as a jpeg image, audio or video file.

The secret message can be embedded into ordinary data files in many different ways.

One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file.

By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data.

The practice of adding a watermark -- a trademark or other identifying data hidden in multimedia or other content files -- is one common use of steganography.

Watermarking is a technique often used by online publishers to identify the source of media files that have been found being shared without permission.

While there are many different uses of steganography, including embedding sensitive information into file types, one of the most common techniques is to embed a text file into an image file.

When this is done, anyone viewing the image file should not be able to see a difference between the original image file and the encrypted file; this is accomplished by storing the message with less significant bites in the data file.

This process can be completed manually or with the use of a steganography tool.

3. Advantages over cryptography

Steganography is distinct from cryptography, but using both together can help improve the security of the protected information and prevent detection of the secret communication.

If steganographically-hidden data is also encrypted, the data may still be safe from detection -- though the channel will no longer be safe from detection.

There are advantages to using steganography combined with encryption over encryption-only communication.

The primary advantage of using steganography to hide data over encryption is that it helps obscure the fact that there is sensitive data hidden in the file or other content carrying the hidden text.

Whereas an encrypted file, message or network packet payload is clearly marked and identifiable as such, using steganographic techniques helps to obscure the presence of the secure channel.

4. Steganography software

Steganography software is used to perform a variety of functions in order to hide data, including encoding the data in order to prepare it to be hidden inside another file, keeping track of which bits of the cover text file contain hidden data, encrypting the data to be hidden and extracting hidden data by its intended recipient.

There are proprietary as well as open source and other free-to-use programs available for doing steganography.

Openstego is an open source steganography program; other programs can be characterized by the types of data that can be hidden as well as what types of files that data can be hidden inside.

Some online steganography software tools include xiao steganography, used to hide secret files in bmp images or wav files; image steganography, a javascript tool that hides images inside other image files; and crypture, a command line tool that is used to perform steganography.

The art and science of hiding information by embedding messages within other, seemingly harmless messages.

Steganography works by replacing bits of useless or unused [data](https://www.webopedia.com/TERM/D/data.html) in regular computer [files](https://www.webopedia.com/TERM/F/file.html) (such as graphics, sound, text, [HTML](https://www.webopedia.com/TERM/H/HTML.html), or even [floppy disks](https://www.webopedia.com/TERM/F/floppy_disk.html) ) with bits of different, invisible information.

This hidden information can be [plain text](https://www.webopedia.com/TERM/P/plain_text.html), [cipher text](https://www.webopedia.com/TERM/C/cipher_text.html), or even images.

Steganography sometimes is used when encryption is not permitted.

Or, more commonly, steganography is used to supplement encryption.

An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

Special software is needed for steganography, and there are freeware versions available at any good download site.

Steganography (literally meaning covered writing) dates back to ancient Greece, where common practices consisted of etching messages in wooden tablets and covering them with wax, and tattooing a shaved messenger's head, letting his hair grow back, then shaving it again when he arrived at his contact point.