

# Steganography Revealed

*Kristy Westphal* 2003-04-09

Over the past couple of years, steganography has been the source of a lot of discussion, particularly as it was suspected that terrorists connected with the September 11 attacks might have used it for covert communications. While no such connection has been proven, the concern points out the effectiveness of steganography as a means of obscuring data. Indeed, along with encryption, steganography is one of the fundamental ways by which data can be kept confidential. This article will offer a brief introductory discussion of steganography: what it is, how it can be used, and the true implications it can have on information security.

## What is Steganography?

While we are discussing it in terms of computer security, steganography is really nothing new, as it has been around since the times of ancient Rome. For example, in ancient Rome and Greece, text was traditionally written on wax that was poured on top of stone tablets. If the sender of the information wanted to obscure the message - for purposes of military intelligence, for instance - they would use steganography: the wax would be scraped off and the message would be inscribed or written directly on the tablet, wax would then be poured on top of the message, thereby obscuring not just its meaning but its very existence[1].

According to [Dictionary.com](http://www.dictionary.com), steganography (also known as "steg" or "stego") is "the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key; cryptography" [2]. In computer terms, steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message[3]. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file (like a .wav or mp3) or even a video file.

## What is Steganography Used for?

Like many security tools, steganography can be used for a variety of reasons, some good, some not so good. Legitimate purposes can include things like watermarking images for reasons such as copyright protection. Digital watermarks (also known as fingerprinting, significant especially in copyrighting material) are similar to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person.

Steganography can also be used as a way to make a substitute for a one-way [hash](#) value (where you take a variable length input and create a static length output string to verify that no changes have been made to the original variable length input)[\[4\]](#). Further, steganography can be used to tag notes to online images (like post-it notes attached to paper files). Finally, steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing[\[5\]](#).

Unfortunately, steganography can also be used for illegitimate reasons. For instance, if someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer. Furthermore, a person with a hobby of saving pornography, or worse, to their hard drive, may choose to hide the evidence through the use of steganography. And, as was pointed out in the concern for terroristic purposes, it can be used as a means of covert communication. Of course, this can be both a legitimate and an illegitimate application.

## Steganography Tools

There are a vast number of tools that are available for steganography. An important distinction that should be made among the tools available today is the difference between tools that do steganography, and tools that do steganalysis, which is the method of detecting steganography and destroying the original message. Steganalysis focuses on this aspect, as opposed to simply discovering and decrypting the message, because this can be difficult to do unless the encryption keys are known.

A comprehensive discussion of steganography tools is beyond the scope of this article. However, there are many good places to find steganography tools on the Net. One good place to start your search for stego tools is on Neil Johnson's [Steganography and Digital Watermarking](#) Web site. The site includes an extensive list of steganography tools. Another comprehensive tools site is located at the [StegoArchive.com](#).

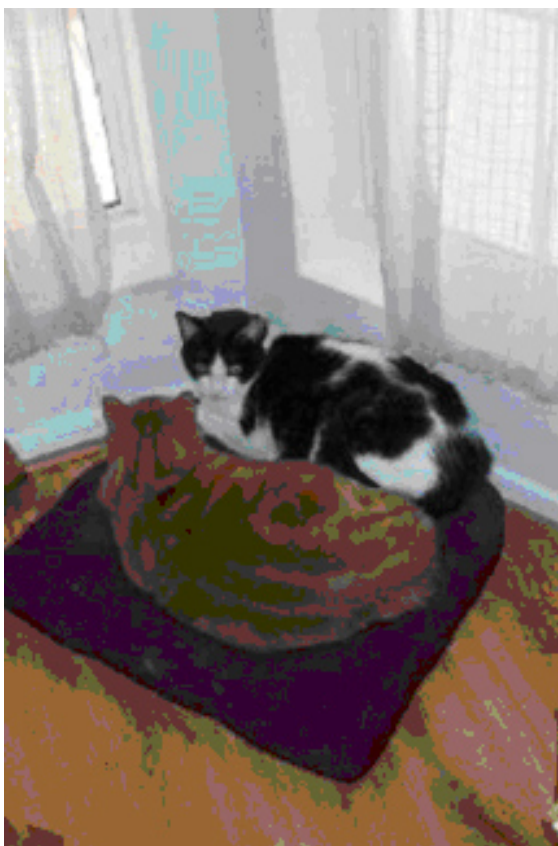
For steganalysis tools, a good site to start with is Neil Johnson's [Steganalysis site](#). Niels Provos's [site](#), is also a great reference site, but is currently being relocated, so keep checking back on its progress.

The plethora of tools available also tends to span the spectrum of operating systems. Windows, DOS, Linux, Mac, Unix: you name it, and you can probably find it.

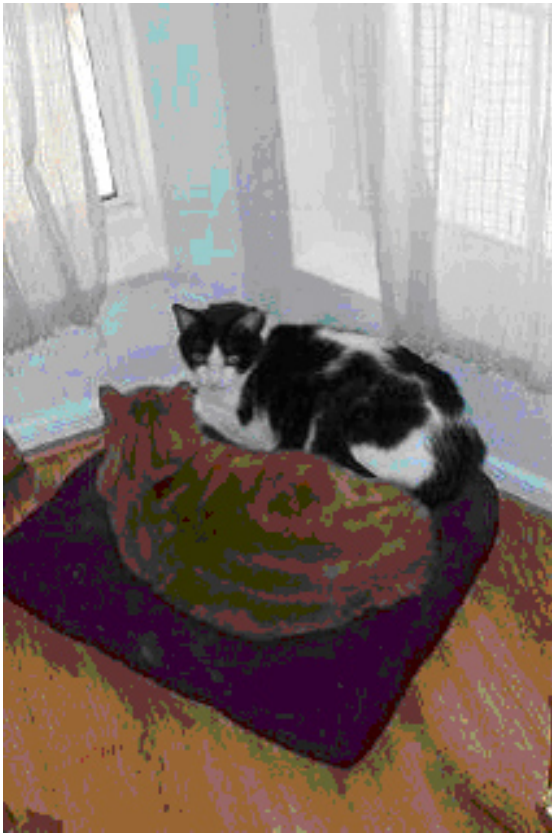
## How Do Steganography Tools Work?

To show how easy steganography is, I started out by downloading one of the more popular freeware tools out now: [F5](#), then moved to a tool called [SecurEngine](#), which hides text files within larger text files, and lastly a tool that hides files in MP3s called [MP3Stego](#). I also tested one commercial steganography product, [Steganos Suite](#).

F5 was developed by Andreas Westfield, and runs as a DOS client. A couple of GUIs were later developed: one named "Frontend", developed by Christian Wohne and the other, named "Stegano", by Thomas Biel. I tried F5, beta version 12. I found it very easy to encode a message into a JPEG file, even if the buttons in the GUI are written in German! Users can simply do this by following the buttons, inputting the JPEG file path, then the location of the data that is being hidden (in my case, I used a simple text file created in Notepad), at which point the program prompts the user for a pass phrase. As you can see by the before and after pictures below, it is very hard to tell them apart, embedded message or not.



**Figure 1: JPEG file without embedded text**



**Figure 2: JPEG file with embedded text**

Granted, the file that I embedded here was very small (it included one line of text: "This is a test. This is only a test."), so not that many pixels had to be replaced to hide my message. But what if I tried to hide a larger file? F5 only hides text files. I tried to hide a larger word document and although it did hide the file, when I tried to decrypt it, it came out as garbage. However, larger text files seemed to hide in the picture just as well as my small, one-line message.

SecurEngine doesn't seem to be as foolproof as the tools that hide text within pictures. When I hid my small text file in a bigger text file, I found an odd character at the bottom of the encoded file ("ÿ"). This character was not in the original file. SecurEngine gives users the option of just hiding the image, hiding the image as well as encrypting it, or both. The test message was encrypted and decrypted without issue. SecurEngine also has a feature that helps to "wipe" files (to delete them more securely).

MP3Stego, a tool that hides data in MP3 files worked very well. How the process works is like this: you encode a file, a text file for example, with a .WAV file, in order for it to be compressed into MP3 format. One problem that I ran into was that in order to hide data of any size, I had to find a file that was proportional in size. So, for instance, my small text message from the

previous exercise was too big to hide in a .WAV file (the one that I originally tried was 121KB, and the text file was around 36 bytes). In order to ultimately hide a file that was 5 bytes (only bearing the message "test."), I found a .WAV file that was 627 KB. The ultimate MP3 file size was 57KB.

Steganos Suite is a commercial software package of numerous stego tools all rolled into one. In addition to a nifty Internet trace destructor function and a computer file shredder, it has a function called the File Manager. This allows users to encrypt and hide files on their hard drive. The user selects a file or folder to hide, and then selects a "carrier" file, which is defined as a graphic or sound file. It will also create one for you if you prefer, if you have a scanner or microphone available. If you don't have a file handy or if you want to create one, the File Manager will search your hard drive for an appropriate carrier. This tool looks for a wider variety of file types than the majority of the freeware tools that I perused (such as .DLL and .DIB files), so if you intend to do quite a bit of file hiding, you might want to invest in a commercial package.

## Steganography and Security

As mentioned previously, steganography is an effective means of hiding data, thereby protecting the data from unauthorized or unwanted viewing. But stego is simply one of many ways to protect the confidentiality of data. It is probably best used in conjunction with another data-hiding method. When used in combination, these methods can all be a part of a layered security approach. Some good complementary methods include:

- **Encryption** - [Encryption](#) is the process of passing data or plaintext through a series of mathematical operations that generate an alternate form of the original data known as ciphertext. The encrypted data can only be read by parties who have been given the necessary key to decrypt the ciphertext back into its original plaintext form. Encryption doesn't hide data, but it does make it hard to read!
- **Hidden directories (Windows)** - Windows offers this feature, which allows users to hide files. Using this feature is as easy as changing the properties of a directory to "hidden", and hoping that no one displays all types of files in their explorer.
- **Hiding directories (Unix)** - in existing directories that have a lot of files, such as in the /dev directory on a Unix implementation, or making a directory that starts with three dots (...) versus the normal single or double dot.
- **Covert channels** - Some tools can be used to transmit valuable data in seemingly

normal network traffic. One such tool is Loki. Loki is a tool that hides data in ICMP traffic (like ping).

## Protecting Against Malicious Steganography

Unfortunately, all of the methods mentioned above can also be used to hide illicit, unauthorized or unwanted activity. What can you do to prevent or detect issues with stego? There is no easy answer. If someone has decided to hide their data, they will probably be able to do so fairly easily. The only way to detect steganography is to be actively looking for in specific files, or to get very lucky. Sometimes an actively enforced security policy can provide the answer: this would require the implementation of company-wide acceptable use policies that restrict the installation of unauthorized programs on company computers.

Using the tools that you already have to detect movement and behavior of traffic on your network may also be helpful. Network intrusion detection systems can help administrators to gain an understanding of normal traffic in and around your network and can thus assist in detecting any type of anomaly, especially with any changes in the behavior of increased movement of large images around your network. If the administrator is aware of this sort of anomalous activity, it may warrant further investigation. Host-based intrusion detection systems deployed on computers may also help to identify anomalous storage of image and/or video files.

A research paper by [Stefan Hetzel](#) cites two methods of attacking steganography, which really are also methods of detecting it. They are the visual attack (actually seeing the differences in the files that are encoded) and the statistical attack: "The idea of the statistical attack is to compare the frequency distribution of the colors of a potential stego file with the theoretically expected frequency distribution for a stego file." It might not be the quickest method of protection, but if you suspect this type of activity, it might be the most effective. For JPEG files specifically, a tool called [Stegdetect](#), which looks for signs of steganography in JPEG files, can be employed. Stegbreak, a companion tool to Stegdetect, works to decrypt possible messages encoded in a suspected steganographic file, should that be the path you wish to take once the stego has been detected.

## Conclusions

Steganography is a fascinating and effective method of hiding data that has been used

throughout history. Methods that can be employed to uncover such devious tactics, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game.

## Resources:

[1] Steganography, by Neil F. Johnson, George Mason University,  
<http://www.jjtc.com/stegdoc/sec202.html>

[2] <http://dictionary.reference.com/search?q=steganography>

[3] The Free On-line Dictionary of Computing, © 1993-2001 Denis Howe  
<http://www.nightflight.com/foldoc/index.html>

[4] Applied Cryptography, Bruce Schneier, John Wiley and Sons Inc., 1996

[5] Steganography: Hidden Data, by Deborah Radcliff, June 10, 2002,  
<http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html>

*Kristy Westphal, CISSP, is a versatile IT professional, skilled in information security, troubleshooting and process analysis. Her experience in the Information Technology field has allowed her to become knowledgeable in several flavors of UNIX and Windows, as well as various aspects of intrusion detection and disaster recovery planning. She is currently employed by Pegasus Solutions Companies as Information Security Officer.*

## Relevant Links

[Steganography Press Information](#)

*Neils Provo*

[Steganalysis](#)

*Stefan Hetzl*

[Privacy Statement](#)

Copyright 2006, SecurityFocus