



# Steganography

2nd Lt. James Caldwell  
U.S. Air Force

*Steganography is the ancient art of embedding a secret message into a seemingly harmless message. This art, in contrast to cryptography, does not use ciphers or codes to scramble a message, and therefore is not obvious. U.S. and foreign officials suspect that Osama bin Laden is using steganography to pass embedded maps and photographs of terrorist targets through chat rooms and pornographic Web sites.*

The text below contains a message sent by a German spy in World War II.

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects for pretext embargo on by-products, ejecting suets and vegetable oils.

Decoding the message by extracting the second character of every word reveals the following text: "Pershing sails for NY June 1."

This type of ciphering is known as steganography, the ancient art of hiding messages so that they are not detectable [1]. No substitution or permutation was used. The hidden message is plain, but unsuspecting to the reader. Although a cousin to cryptography, steganography is not inherently obvious. Whereas cryptography is easily detectable as secret code, steganography, as its Greek root implies, is *covered writing*. It uses a physical cover message to camouflage its secrecy.

## History

Steganography is widely employed today, but its origins trace back millennia ago. Before the computers and e-mail of today, messengers had two options for delivering messages: memorize the message or hide it on the messenger.

Several techniques of steganography are etched in history. One account speaks of the Greek ruler Histaeus who shaved the head of one of his slaves, tattooed the message onto his scalp, and sent him along to deliver the message *after his hair had grown back*. The recipient would shave the slave's head to uncover the message and find an untainted scalp on which to reply.

Other accounts in Greek history tell of Demeratus who wrote a message to the Spartans warning of an eminent invasion from Xerxes. The message was carved on a wood backing of a wax tablet, and then covered in a fresh layer of wax.

The *seemingly* blank tablet was then delivered successfully.

Invisible ink was also used commonly throughout history, but not through stamps or specially equipped markers. Instead, onion juice, alum, ammonia salts and several other materials were used and would glow dark when held over a flame.

Wartime especially involved steganography. During the American Revolution, the British and Americans used invisible inks extensively. During World War II, for instance, the Germans used microdots. The microdot was essentially a secret message photographed and reduced to the size of a period. When the Americans realized the volume of microdots contained within communications and transactions intercepted, they quickly realized as FBI director J. Edgar Hoover did, "the enemy's masterpiece of espionage" [2].

The advent of computers further advanced disguising messages. For instance, laser printers could be used to offset lines and character spaces by as little as 1/300th of an inch. A binary message could be sent easily using a normal space to represent 0s, and by offsetting characters 1/300th of an inch to represent 1s.

These early approaches were based on the principle that secret messages were hidden inside the physical object containing them. Ostensibly, the cover message holds the intrinsic meaning of the communication, but in reality, nothing could be further from the truth. However, despite the myriad of approaches to steganography aforementioned, this approach is unquestionably powerless in digital communications. Only pure information can be sent. There is no hot wax or hair regeneration to camouflage the secret transmission. Even so, a technique was found.

This article will address uses of steganography today and discuss several approaches to steganography. This knowledge will then be applied to understanding how the network has proliferat-

ed the accessibility and employability of steganography, and the benefits and perils associated with it.

## Secret Channels

Digital technology offers new ways to apply steganography techniques, including the ability to hide information inside digital images<sup>1</sup>. A digital image is "an array of numbers that represent light intensities at various points" [3]. Combined, these light intensities or pixels form the image's raster data. Images with 640 x 480 pixels and 256 colors can contain up to 300 kilobits of data. But it is more typical to see digital images in sizes of eight-bit or 24-bit files. This provides an excellent opportunity for hiding information, especially in image sizes of 24-bits.

Each pixel on a computer monitor selects from three primary color variations: red, blue, and green. Each color is represented by a single storage byte. With 24-bit images, three bytes are allocated for each primary color (hence eight bits per byte multiplied by three bytes).

Represented in binary values, for instance, a white background is 11111111, 11111111, 11111111. Pixel representation makes up a file's size. Thus a 24-bit image displayed in high resolution (1,024 x 768) has more than 2 million pixels, producing a file over 2MB in size. The larger the file, the greater opportunity there is to apply steganography techniques. The downside to this of course is that large file sizes might induce unwanted suspicions.

To deal with this, file compression is used. There are two kinds available today: lossy and lossless. Both methods compress files to save storage space, but do so differently. This is important because certain compression applications can interfere with hidden messages. Lossy compression is the most efficient space saver, but does not retain the original image's exactness. JPEG (Joint Photographic Experts Group) is an example of such compression. A lossless approach, in contrast, retains the integrity of the original

image. Images saved as GIF (Graphic Interchange Format) or BMP (bitmap file) apply lossless compression.

### Inserting Hidden Data

Two files are required for steganography to work. The first file is an innocuous cover image that will host the second file containing hidden information. The hidden message can be anything that is embeddable into a *bit stream* such as plain text or cipher text. There are several methods to hide information in digital images, from taking advantage of *noisy* areas that draw less attention in an image, to scattering the message randomly throughout the image. A brief discussion on each of these approaches is in order before continuing.

### Least Significant Bit

In her book "Information Warfare and Security" [4], Dorothy Denning addresses the least significant bit and its vulnerability to modifications without careful detection. A color byte contains eight bits, each of which varies in terms of impact on the resulting color. The least significant bit (or the final bit in a stream) affects the smallest change of the eight bits. On the other hand, the first bit of the stream has the largest influence on color selection. For instance, as Denning illustrates, the least and most significant bit are similar to the hour and second hand on a clock. While a change in the second hand alters time very slightly, a change in the hour hand is extreme.

If the least significant bit of every bit stream were to be allocated for a hidden message, the resulting image file would appear unaltered. Moreover, the larger the bit size, the more subtle the change. For example, using the least significant bit in a 24-bit image size, the original raster data for three pixels is:

```
00101100 10101100 10101000
00101011 01101000 00101011
00101010 00111001 00101010
```

Inserting the binary value for A (1000001) would result in<sup>2</sup>:

```
00101101 10101100 10101000
00101010 01101000 00101010
00101010 00111001 00101011
```

Several software tools for implementing least-significant bit insertion are available and easy to use. S-Tools, for example, executes by dragging the document you wish to hide over the cover image. The user is asked for a password to recover the

message.

The least significant bit approach is simple to understand and use, but it is largely vulnerable to changes in data due to file compression. Since JPEG compression is so efficient in reducing file sizes, most image traffic over the Internet utilizes it. However, as stated previously, the lossy compression technique JPEG employs may alter the least significant bit.

### Steganography Uses

The use of steganography undeniably connotes dishonest activity, but there is a peaceful aspect to consider. Steganography is used in map making, where cartographers add a nonexistent street or lake in order to detect copyright offenders. Or similarly, fictional names are added to mailing lists to catch unauthorized resellers. Modern techniques use steganography as a watermark to inject encrypted copyright marks and serial numbers into electronic mediums such as books, audio, and video. For instance, DVD recorders detect copy protection on DVDs that contain embedded authorizations.

Potential uses of steganography are undoubtedly vast. Companies could advertise public Web pages containing private, hidden text that only internal members could intercept. An attempt to decipher the hidden text would be unwarranted since no encryption (or code) was used. Steganography could also be used to hide the existence of sensitive files on storage media. This would entail a cover folder and an embedded hidden folder.

### Protection Against Steganography

The proliferation of networks has added intensity to both noble and ignoble purposes of steganography. Network security analysts face an insidious foe for sure. But how is steganography detected, and why should network security analysts be alarmed and cautious?

Nearly all steganography programs in use leave behind traces or fingerprints that indicate something is not right. Based on research conducted over the years, organized crime, terrorists, and various other groups operating worldwide commonly use steganography to operate via public forums, Web sites, etc.

Software programs that detect steganography do exist, and enhanced iterations are under development. Neil Johnson, a graduate student at George Mason University, is developing a *stego detector*. The program, he describes, is

designed to search hard drives for electronic fingerprints that typically result from steganography applications. Similar to a virus scanner, this stego detector identifies signatures. As Johnson explains:

Different authors have different ways to hide information to make it less perceptible. The author may come up with ideas that nobody else is using. That tool may have a special signature. Once that signature is detected, it can be tied to a tool. [3]

Johnson and other law enforcement agencies use software to locate signatures by studying the native structure of files including image, voice, text, and video files, and known software tools that implement steganography.

The Pentagon is also interested in uncovering ignoble practices of steganography and annually funds the Naval Research Laboratory. Their interest spawns, in part, from news reports that link terrorist Osama bin Laden to steganography communications. The concern is that data messages are being embedded in chat room messaging or bulletins unnoticed, while intelligence agencies are *off in another world* monitoring communications traffic (e.g., e-mail).

Cyber forensics at WetStone Technologies have successfully developed several tools to detect steganography. The ultimate device will uncover steganography regardless of its implementation methods. So far, steganography has turned up primarily on hacker Web sites. But steganography was also found on frequently visited sites such as Amazon.com and eBay. The forms of steganography vary, but unsurprisingly, *innocuous* spam messages are turning up more often containing embedded text.

WetStone Technologies considered steganography a technological threat worthy enough to caution the U.S. Air Force, beginning in 1998, to guard against it. But the National Security Agency took it a step further and cautioned all government agencies and private employers, warning that internal employees could send embedded, sensitive information via e-mail that would pass through firewalls and security unsuspected. Without a doubt, the ubiquity of steganography merits closer observation by network security analysts.

### Conclusion

Steganography is an instrument of security, but not exclusively secure. There are tradeoffs with steganography of which

the security community is becoming aware: There is a tradeoff between reliability and message size and there is a tradeoff between message size and detectability. The approach steganography offers reduces the chance of a message being detected by its *inadvertent* layer of cover. However, if the hidden message is discovered, it is easily readable. For this reason, combining encryption algorithms with steganography offers a much stronger encryption routine.

Although this article discusses some applications of steganography, there are many more uses in voice, media applications (such as communication channels), audio, and text, to name a few.

This article unveils potential exploits of steganography regarding network security. Although awareness of steganography applications today is limited, progress is unfolding to expose the hidden art. Unfortunately, in the information age, the old adage “what you don’t know can’t hurt you” is not always accurate. ♦

## References

1. Clair, Bryan. “Steganography: How to Send a Secret Message.” 8 Nov. 2001 <[www.strangehorizons.com/2001/200111008/steganography.shtml](http://www.strangehorizons.com/2001/200111008/steganography.shtml)>.
2. Kahn, D. *The Codebreakers*. New York: MacMillan, 1967.
3. Johnson, Neil F., and Sushil Jajodia. “Exploring Steganography: Seeing the Unseen.” *IEEE Computer* Feb. 1998: 26-34.
4. Denning, Dorothy E. *Information Warfare and Security*. Boston, MA: ACM Press, 1999: 310-313.

## Notes

1. Note that steganography can be used to embed hidden files into text documents, audio, video, or images. The scope of this will include an image-based approach primarily, with some mention of other media applications.
2. Least significant bit insertion in this example is possible only by discarding the 9th byte in the data stream.

## About the Author



**2nd Lt. James Caldwell** was commissioned into the United States Air Force through the Air Force Reserve Officer Training Corps and was assigned to Tinker Air Force Base, Okla. Caldwell has a bachelor’s degree in management information systems and is pursuing a master’s degree in computer resources and information systems at Webster University. He is currently assigned to the 552 Computer Systems Squadron as a Project Manager in the Software Services Flight.

552 Computer Systems Squadron  
Bldg. 284 Rm. 209  
Tinker AFB, OK 73145  
Phone: (405) 734-3394  
E-mail: [james.caldwell@tinker.af.mil](mailto:james.caldwell@tinker.af.mil)

## FEELING A LITTLE TIED UP? Why not get some *free* help?

### ONE FREE CONSULTANT

#### Get Some Help With Software Process Improvement

Good for assistance with configuration management, appraisals, personal and team software process, systems engineering, requirements, project management, software acquisition, Capability Maturity Model®, software quality and test, and process improvement.



### ONE HOUR

That’s right—one free consultant. If you are a manager, a practitioner, or a software engineering process group member who is committed to improving your software process, we can help you.

Software Technology Support Center (STSC) software process improvement (SPI) veterans can help answer questions and research your problems for up to an hour without charge to Department of Defense organizations. We can answer questions about starting SPI, key process areas, training, best practices, return on investment, and appraisals. And if our veterans can’t produce an immediate solution, we will get you headed in the right direction.

Call the SPI Hotline at 801-777-7214, DSN 777-7214, or e-mail [larry.smith4@hill.af.mil](mailto:larry.smith4@hill.af.mil) and mention this offer. And let us help you get untied.

