Global Information Assurance Certification Paper

Steganography: A Privacy Protector or Just a Computer Security Trick?
By Patricia V. Cristobal

In a world where privacy is a right, many people try to find a way to hide information especially when it comes to sensitive documents and files. A person would like to send an email or file with no fear that a person aside from the recipient will read the message. Also, with all information that is on the Internet, owners of such information must protect themselves from unwanted spying, copying, theft and false representation. One technique of information hiding is steganography.

What is steganography?

Steganography is the art and science of communicating which hides the existence of the communication. The purpose of steganography is to convey a message to a receiver in such a way that the very presence of the message is undetectable by a third party. In the computer world, steganography means hiding secret messages in graphics, pictures, movie, or sound.

When did it start?

Steganography comes from the Greek word *steganos*, which means 'covered', and *-graphy*, which means 'writing'. Covered writing has been manifested way back during the ancient Greek times around 440 B.C. Herodotus wrote in his text, Histories, that Histiaeus shaved the head of his slave and tattooed it with a message. After the hair grew back, the message would be undetected until the head was shaved again.

More recently during World War I, the Germans used the concept of microdots. A message would be photographed and reduced to a size of a period or the dot of the letter 'i'. These microdots would then be placed in innocuous materials such as books or magazines. Spies can than carry around the secret message to places securely.

The 'invisible ink' that children play around with nowadays can also be a form of steganography. But this method was first used by the ancient Romans where they would use invisible ink based on organic substances such as fruit juices, urine or milk and write between lines and developed with heat.

How does it work?

A graphic image is used as a host or "container". Computer images are composed of pixels. One way to represent a pixel is to have a numerical value range from 0 to 255. An 8-bit (1 byte) base two number represents a value to the computer; i.e., byte 00000000 equals 0. Information will be sorted in the rightmost bit or least significant bit (LSB)

because the seven bits to the LSB's left contain enough information to establish the correct pixel color. Changing the LSB's value will have no effect on the pixel's appearance to the eye. Even if the "container" image is viewed side-by-side with the original, a person will see no difference. Thus, the message's bits will be inserted into the LSB for each byte of graphic image. Think of a bag of red jellybeans. If you replace one red jellybean with a pink jellybean, at a distance, the overall appearance of the bag will still be of the red jellybeans. The same technique is used for audio and text files.

A 640 X 480 image that utilizes 256 colors could hold a nearly 300 KB message or image. With a 24-bit image 1024 X 768 three bytes determine each pixel's value, so each pixel contains three bits of the message resulting in a 2 MB file. Thus, steganographic images have large capacities in which to hide messages.

Steganography vs. Cryptography

Cryptography is the science of converting plaintext into ciphertext, which protects the contents of messages. Steganography is about concealing their very existence. Some researchers prefer hiding over ciphering because it arouses less suspicion. An example of obvious implication is when a known convict sends an encrypted email message to somebody not yet under suspicion.

Below is a table that compares steganography and cryptography.

Steganography	Cryptography
Hides messages in the message; looks like a plain graphic image or sound file	The message is encrypted; looks like a meaningless jumble of random characters
A collection of graphic images on a disk may not look suspicious	A collection of random characters on a disk may look suspicious
A smart eavesdropper can detect something suspicious from a sudden change of message format (i.e., text to graphic images)	A smart eavesdropper can detect a secret communication from a message that has been cryptographically encoded
Caution with reusing pictures	Caution with reusing keys
No Laws associated with steganography	The are certain Laws that ban cryptography

Steganography can protect data by hiding it but by using it alone may not guarantee the total protection. This is the same for plain encryption. However, if you use both methods, this will lead to 'security in depth'. The message should first be encoded using a strong encryption algorithm like triples DES, Twofish or RSA and then embedded into a container. Even if the steganographic layer gets compromise, the crypt layer of protection remains.

Steganography Tools

The are a number of steganography software proliferating on the Internet. These software range from commercial/shareware to freeware and they run different OS platforms like Windows, DOS, Unix, and Mac. Some tools hide information in BMP, JPG, GIF, TGA, TIF, PNG, MIDI, WAV, AVI, and MPEG formats. Others offer the protection of both steganography and cryptography.

Here is a list of some good steganography tools:

Steganos II Security Suite

> Steganos has been completely rewritten and is now a suite of Win 95/98/NT applications designed to keep data safe. Steganos II uses strong encryption and steganographic techniques to hide data in graphic, sound, text, and HTML files, but now it includes new features like: 'InKA' (Invisible Key Agreement) an implementation of public key steganography, disk encryption, advanced password management tools, a "Zero-Emission-Pad" text editor to combat tempest attacks, a data shredder, and the "SysLock" function that effectively locks access to your PC when you are away.

S-Mail

> S-Mail is a program that runs under all versions of Windows and DOS that uses strong encryption and compression to hide files in EXE and DLL files. It takes measures to ensure that pattern or ID string scanners do not detect its hiding scheme.

Stealth

> Stealth is a simple filter for PGP, which strips off all identifying header information to leave only the encrypted data in a format suitable for steganographic use. That is, the data can be hidden in images, audio files, text files, CAD files, and/or any other file type that may contain random data, and then sent to another person who can retrieve the data from the file, attach headers, and PGP decrypt it.

Invisible Secrets Pro

> Invisible Secrets Pro encrypts and hides files in JPEG, PNG, BMP, HTML and WAV. It also provides strong encryption (Blowfish, Twofish, RC4, Cast128, and GOST), a shredder, and a password manager and generator.

Conclusion

There is still a lot of debate whether or not steganography is a privacy protector or just a security trick. People argue that steganography on top of cryptography will be an added layer of protection however there are still other points to be taken into consideration.

Let's say Alice needs to send a top-secret document to Bob. In order for Alice to hide her document, she needs a steganography program that her "enemy" can easily get a hold of. If that person has a copy, the "enemy" will be on the lookout for steganographic messages. If Alice uses the sample image that came with the program she downloaded, her eavesdropper will quickly distinguish it. Other than that, if Alice uses images of bears to hide her document, she should also have a very good detailed story why she keeps sending pictures of bears to Bob. An eavesdropper will get suspicious if Alice's communication patterns suddenly changed from all text to all images of bears. Alice should not also use images known to the public or images on the Internet because differences in those images can easily be detected using sufficient careful analysis.

Another point to consider is when Alice wants to hide all her sensitive documents in her hard drive. So she uses a steganography program to embed all her documents to pictures. For example the police comes in, arrest Alice and scans through her hard drive. All they will see are image files but when they see that she also has a steganographic program, they will get suspicious.

These are just trivial examples but the key to secrecy is to select a proper mechanism. Right now steganography may not be the best choice but it can be one of the options to take.

Bibliography

Mendel, Ronald. "Steganography – Electronic Spycraft." Security Portal 18 October 1999. URL: http://securityportal.com/cover/coverstory19991018.html (20 January 2000)

Milbrandt, Eric. "StegoArchive.Com" URL: http://steganography.tripod.com/stego.html (20 January 2000)

Mr. Byte. "Steganography" URL: http://www.tamos.com/privacy/steganoen.htm (20 January 2000)

Schneier, Bruce. "Steganography." Crypto-Gram. 15 October 1998. URL: http://www.counterpane.com/crypto-gram.html (20 January 2000)

Wayner, Peter. "More on Steganography." Crypto-Gram. 15 November 1998. URL: http://www.counterpane.com/crypto-gram-9811.html (20 January 2000)

Johnson, Neil "Steganography" URL: http://isse.gmu.edu/~njohnson/stegdoc/
(20 January 2000)

Schneier, Bruce. "Secret & Lies: Digital Security in a Networked World." 2000. Wiley Computer Publishing.