Global Information Assurance Certification Paper

Information Hiding – The Art of Steganography

GSEC Practical (v.1.4b)

By Asha A. Patel

Summary

Steganography is the art of passing information in a manner that the very existence of the message is unknown. Originally used to hide secret messages to avoid detection, steganography also serves as a method of protecting copyrights for digital works. Stego, as it is often referred to, differs from it's close relative, cryptography, in that with crypto, messages are garbled up so they are unreadable and make no coherent sense. However, the fact that a message was sent is known, whereas with the use of steganography, the sender is concealing the existence of a message. Steganography has been given a boost in the internet age as governments attempt to regulate or prohibit the use of cryptography for personal privacy purposes. In this paper, we discuss what steganography is, detailing its goal and providing a brief background, in addition to some advantages and disadvantages for using it as well as a comparison of it to cryptography. We move on to methods of its utilization and provide a list of software available for deployment. Finally, we conclude with how to safeguard your network from it.

It is important to note that all the research for this paper was conducted through the internet, a popular medium for research among network security professionals, and one heavily relied upon for fast, up-to-date information.

Definition

Steganography, originating from the Greek word "steganos" which means "covered" and "graphy" which means "writing or drawing", is the art and science of hiding the existence of communication. The techniques used in steganography make it difficult to detect that there is a hidden message inside an innocent file. This way you not only hide the message itself, but also the fact that you are sending the message. This characteristic makes steganography the ideal science for hiding messages on the web, which is widely seen as a mass communication outlet.

Goal of Steganography

The primary goal of steganography is to hide a message inside another message in a way that avoids drawing suspicion to the transmission of the hidden message. If suspicion is raised, then the goal is defeated. Furthermore, actual detection of an embedded message renders the primary goal of steganography useless.

Steganalysis is the science of detecting hidden messages and rendering useless such covert messages. This is frequently accomplished by looking at variances between bit patterns and unusually large file sizes. Many tools are also available to aid in this purpose. Steganalysis is a field that is increasingly becoming popular as steganography gains more exposure. It is also an area that is becoming more and more important in the role of forensic science and law enforcement as well as an area of interest for intelligence agencies.

Background

Dating back to the ancient Greeks, early forms of steganography included hiding secret messages on wax covered tablets and tattooing messages on a messenger's scalp only later to be replaced by invisible inks, the German invention of the microdot and null cipher messages.

It was not until the twentieth century that steganography started to finally blossom. The German invention of the microdot (photographs the size of a printed period allowing the transmission of large amounts of data) was a breakthrough invention. Invisible inks were also heavily used during WWII. In addition, null ciphers (unencrypted messages that often appear to be innocent messages about ordinary occurrences), were used to hide secret messages. Since they would not alert suspicion, they were difficult to intercept. Modern steganography has evolved into hiding data within many formats, such as images, text, email and IP headers, etc. A key attribute has been that throughout history, steganography has been pivotal in information warfare.

Steganography continued to be seen as another aspect of the internet until the September 11th terrorist attacks against the United States when media outlets reported the speculation that terrorists might be using steganography software for encoding secret messages into publicly available pornographic image files, chat rooms, bulletin boards and websites. However, there has been no such proof to substantiate this, and the issue has been kept a close eye on. Many fear a cyber attack that could have worldwide implications. As such, internet civil libertarians worry that politicians will put further restrictions on steganography & encryption.

Steganography in the Information Age

With the advent of the computer age, steganography has been given an incredible push into realms of other uses for hiding data. Its rapid growth can be attributed to two reasons:

(1) the publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products as a means for protecting digital works from piracy.

(2) people have been motivated to study steganography as a result of various governments attempt to restrict the availability of encryption services.

In essence, steganography serves a number of purposes, such as transmitting hidden messages, safeguarding business secrets, watermarking copyright protected data and is used for personal privacy.

Copyright Marking

Watermarking is the process of hiding copyright messages. Authors of images, music, and software can place a hidden "trademark" in their product, allowing them to keep a check on piracy. It can also be used to authenticate the integrity of an image. Most importantly, it is used to prove ownership and/or prosecute copyright violators.

Fingerprinting is the process of hiding serial numbers or a set of characteristics that distinguish an object from other similar objects. It enables the intellectual property owner to identify customers who break their license agreement by supplying the assets to third parties. Most noticeably, it is used to detect copyright violators.

The difference between classical steganography and copyright marking is that in classical steganography, a successful attack consists of a third party observing that a given message is marked. In copyright marking, all parties may be aware that marks are in use and as a result, some properties of the marks may be observable. In this case, successful attacks don't mean detecting a mark but rendering it useless.

The vulnerability in using watermarking and fingerprinting lies within the fact that it is made known that a watermark or fingerprint is being used. Making that information public knowledge hinders its goal. Perhaps if vendors not publically advertise this fact, watermarking would be a more effective strategy to combat against piracy.

Digital watermarking and fingerprinting will continue to grow as more stronger and effective techniques are developed and implemented.

Advantages

Why use steganography? The primary advantage is that it can be used to secretly transmit messages without the fact of the transmission being discovered. You can conceal any file(s) over any communication line in a format, which leaves the hidden data undetectable and unreadable. This has enormous implications, both good and bad, in today's world. Individuals could use steganography for private communications. A company can take steps to protect copyrighted property. Employees could pass confidential, secret business plans. Governments could use steganography in information warfare, and if in the wrong hands, it could be used for malicious intent. So as you can see, steganography is a powerful tool in the present age of information.

Disadvantages

However, there are also a few disadvantages to point out. One of steganography's disadvantages lies in the fact that there is considerable overhead to hide very small amounts of information. Hiding short text messages within extensive text is limited by the overall size of the lengthy text. Text files simply aren't big enough to hide more complex data like images or audio files. The answer to this dilemma is found in over 200 steganography software packages available over the internet.

Another key concern is that once a steganographic system is discovered, it is rendered useless. The greatest risk for steganography is the conflict between an original image without the hidden message and the steganated image with the hidden message. In addition, you could cause severe degradation of an image in attempting to analyze it.

Perhaps one can argue that the primary advantage of being able to secretly communicate is well worth the many disadvantages involved. Once again, it is notable to point out the importance of weighing the risk involved in using such a science, the risk of being discovered and its potential consequences.

Cryptography vs. Steganography

Although cryptography and steganography are closing related, often referred to as "cousins", they differ in approach.

Cryptography is the science of encrypting messages in such a way that if another party were listening, the message would not make sense. With cryptography, an unauthorized party cannot read the message because it has been encrypted, or garbled. However, it is easily apparent that there is in fact a message and that the message has been encoded. That by itself raises suspicion and curiosity.

With steganography, the message itself is concealed and thus undetectable to an unauthorized party and as such there is no suspicion that a secret message is being sent. Steganography works by embedding a hidden message within an "open" message. The open message is referred to as the host and can be files such as text or images, IP packets, data streams, etc. The hidden message can be embedded in certain parts of the host or can cause a new file to be generated. Virtually anything that can carry a data stream can hold a hidden message. One is only limited by imagination and creativity.

Steganography Methods

Several methods exist for hiding information in text, images, sound, signals, and more. Generally, there are three methods used in steganography and are covered in the

SANS Security Essentials curriculm. These include injection, substitution or generating a new file.

Injection

Because there is hidden data within another file, a method known as injection, the file size will be increased and thus easy to detect. With injection, certain data is "hidden" and thus ignored. Some examples include the use of comments or the use of hidden columns or rows or hiding messages within file properties.

Substitution

Another method, referred to as substitution, works by replacing, or substituting, certain information in a file without increasing the file size. With substitution, insignificant data in a host file can be substituted with hidden text. For example, one could insert hidden data inside the pixels of an image by replacing the color. To the unknown eye, it would appear harmless.

Generate a New File

A much newer technique involves using the embedded hidden message to generate a new file. A host file is not needed to generate a new file. For example, one could fill out and submit a form online and generate a document "on the fly". This method poses a greater security risk because there is no host file involved.

Techniques Used

Many techniques are available for use in the art of steganography. To reiterate, one is only bound by the boundaries of his or her own imagination. Such a field leaves room for much imagination and creativity but is ultimately hindered by the crosshairs of what will work and what you can get away with (in terms of the ability to hide secret messages).

Below is a table summarizing common stego techniques as discussed by Duncan Sellars in his article "An Introduction to Steganography." Please see the Glossary portion of this paper for precise definitions.

media	***techniques used***
text	Line Shift, Word Shift, or Feature Coding
images	Least Significant Bit, Masking & Filtering, or Algorithms & Transformations
audio	Least Significant Bit, Phase Coding, Spread Spectrum Coding or Echo Hiding

(summarized from Duncan Sellars, "An Introduction to Steganography")

Stego Tools

There are many freeware and shareware steganography tools available for use. Many are readily available over the internet. Please see the Appendix portion of this paper for a compiled list. Please note, that the use of steganography tools should be used with caution and at your own risk. It is not the author's intention to promote any malicious or illegal use of any software. Measures should be taken to secure legal ownership and ensure proper use of all software.

Steganography and Network Security

There is no sure fire way to defend against steganography – and no way to detect it. So how do you defend your network against it? As always, it's a good idea to practice defense in depth and incorporate a strategy for safeguarding your network against the malicious use of steganography. This includes within your network, from employees using steganography software to send proprietary information out and externally, from an unknown attacker. A key aspect and a first step to this approach is to "know your network." Knowing that a treat exists is the first step in developing and implementing a plan to safeguard your network.

One method of detecting the use of steganography is to "look for obvious and repetitive patterns which may point to the identification or signature of a steganography tool or hidden message." (Johnson, Neil and Jaodia, Sushil) For the most part, if it's visible to the human eye, it will be easy to detect. As steganography is increasingly receiving more attention, tools for use in the area of steganalysis will be widespread.

There are some general guidelines involved in detecting the use of steganography tools. Some basic things to look for include overly large files, uneven bit mapping, or whether a bitmap image has a large number of duplicate colors. This would indicate that data has been embedded in the image. Also, looking at the file size and file properties will tell you a lot. Anything unusual should raise immediate suspicion. Lastly, if you are lucky enough to know what tool was used, you can obtain the same tool to compare the files. Or, rarely, if you have the original source file, you can do a comparison analysis.

Remember that the art of steganography will be used where companies and/or governments will not allow one to encrypt communications.

To combat the uses of steganography software in the corporate workplace or within your network, it is necessary and integral to make it part of written information security policy that employees are not allowed to use steganographic programs on the company network. If you choose to allow any exceptions, then stipulate them in your written policy. Your security policy should also address the posting, emailing or receiving of text files, images, graphics or sound files especially on PCs that handle sensitive data. You may want to stipulate that these contain trusted digital watermarks, as watermarks

will improve security and overwrite any previous messages. Also, your security policy needs to address how you wish to handle the use of chat rooms, forums and group lists on user workstations. Lastly, you want to address the issue of firewalls. Firewalls need filters to limit the importation of pornography into the company, as it is a popular medium of carrying hidden messages. As a consideration you may want to set up policies and procedures to monitor employees' email, attachments, web access, etc. and address your stance in your written security policy.

A New World – How 9/11 Changed Everything

Until the September 11th terrorist attacks against the United States, steganography was just seen as a mechanism to provide a way of hiding information, whether that be for protecting business plans, for personal privacy or for protecting copyrighted materials in an effort to combat piracy. What has now become a cliché – September 11th changed many realms of how we live – and most noticeable, how governments, particularly the United States, views its national security policy.

Immediately thereafter, the United States declared war against terrorism and the world was forever changed. News reports began circulating, claiming that terrorist mastermind Osama Bin Laden and his ruthless al-Qaeda network were perhaps using steganography to communicate and plan attacks. These reports came unsubstantiated and claims that the group was indeed "sophisticated" in using steganography were abandoned – abandoned in the public eye. Without a doubt, the government is and will be keeping a close eye on steganography – its use, its defenses and its countermeasures in communications.

As our national security focus continues to evolve around a new definition of homeland security, we will see how government regulations come into play in the realm of communications. As we have seen with cryptography, steganography, too, will be tightened down with restrictions.

A first step towards that approach began when President Bush signed into law unprecedented anti-terrorism legislation known as the USA-Patriot Act of 2001. Included among the historic legislation, the role of authorities was expanded "to tap email accounts, access personal data and monitor electronic voice mail." (Carvin, Andy)

Although no provisions were set forth addressing steganography, it is only a matter of time. Future legislation will be forced to address the issue as ruthless groups and governments that support them invest more time, money and resources to develop newer and more improved communication methods and techniques to conceal secret messages and carry out their plans.

An ever-increasing concern is that of terrorist organizations using a global approach in their attacks by targeting the internet's infrastructure. Since so much of our global economy is entwined within the internet, it is a viable and credible threat. Measures

should be taken to safeguard any attack, including and not limited to the many avenues of penetration such as email systems, corporate networks, or e-commerce.

Conclusion

Although steganography and cryptography are similar in the sense that both are used as a measure of network defense, they vary fundamentally in their goals. Cryptography is used to protect the contents of a message. In essence, it provides confidentiality but not secrecy. This is where steganography comes to play. Steganography hides the fact that the message actually exists. However, both can be used together to further practice "defense in depth." With our rapidly changing world, stego is continuously improving and being utilized. With increasing attention being given to its many uses, steganography poses a valid security threat. Malicious intent of its utilization can be detrimental to network security. Proper measures should be considered in advance and be placed within the corporate network security plan.

The internet is providing a new outlet for hiding messages. Development in the area of covert communications and steganography is predicted to continue to grow through the coming years. We will continue to see governments addressing the area of steganography in its fight against terrorism as well as incorporating its growth in the area of forensic science. Federal intelligence agencies will enhance their measures to further the use of steganography tools. With it, "the ease in use and availability of steganography tools has law enforcement concerned in trafficking of illicit material via web page images, audio and other files transmitted through the internet." (Johnson, Neil and Jajodia, Sushil) It will be interesting to see if stricter guidelines will be placed by governments in attempts to regulate the use of steganography. For now, very little is being done, which leaves it wide open for its use, leaving room for lethal intent as well.

GLOSSARY

(As defined by Duncan Sellars, “An Introduction to Steganography”)

Line Shift Coding: text lines are vertically shifted to encode a document

Word Shift Coding: codewords are coded into a document by shifting the horizontal locations of words within text lines, while maintaining a natural spacing appearance

Feature Coding: certain text features are altered (or not) depending on the codeword

Least Significant Bit insertion: embedding information in a graphical image file, is the most well-known image steganography method.

Masking & Filtering: techniques hide information by marking an image in a manner similar to paper watermarks

LSB (Audio): Binary data can be stored in the least-significant bit of audio files

Phase Recording: works by substituting the phase of an initial audio segment with a reference phase that represents the data

Spread Spectrum: Most communication channels try to concentrate audio data in as narrow a region of the frequency spectrum as possible in order to conserve bandwidth and power. When using a spread spectrum technique, however, the encoded data is spread across as much of the frequency spectrum as possible

Echo Data Hiding: embeds data into a host signal by introducing an echo

APPENDIX: Steganography Software Tools

Below is a list of software tools, on various platforms, available for download through the internet:

(**Disclaimer**: Use these software programs at your own risk!)

Windows

Blindside *Freeware*
an application of steganography that allows one to conceal a file, or set of files within a standard computer image. The new image looks identical to the human eye, but can contain up to 50k or so of secret data. The hidden files can also be password encrypted, to prevent unauthorized access to their data. Also available are Linux, HP, Solaris, and AIX versions

BMP Secrets *Freeware*
a stego product for Windows with a very large hiding capacity. Includes built-in encryption and ability to hide data within specific sub-areas of the image

Courier v1.0a *Freeware*
Simple program that hides messages in BMPs.

Camouflage *Freeware*
a Windows-based program that allows you to hide files by scrambling them and then attaching them to the end of the file of your choice; can hide data in any kind of file, pictures, Word documents, Excel document, etc.

Contraband Hell Edition *Freeware*
a BMP-based stego program with strong encryption built in.

Contraband *Freeware*
Windows-based program, which embeds and extracts any thinkable file into 24-bit BMP's.

Data Stash *Shareware*
Hides files in BMP or database files. Comes w/ password protection.

Digital Picture Envelope
a program you can make your secret data imperceptible to any human eyes

D.P.T. (Data Privacy Tools) *Freeware*
Strong encryption with optional BMP steganography.

East-Tec Eraser
Allows you to encrypt and hide files in other files (carriers), which are not suspect of encryption.

Encrypt Pic *Shareware*
hide data in 24 bit BMP images. It has the added benefit of offering data encryption via the BlowFish algorithm.

Gif-It-Up v1.0 *Freeware*
a Win95-based stego program that hides data in GIF files. It replaces color indexes of the gif color table with indexes of matching colors

Gifshuffle *Freeware*
a command-line-only program for windows which conceals messages in GIF images by shuffling the colourmap. The picture remains visibly intact, only the

order of color within the palette is changed. It works with all GIF images, including those with transparency and animation, and in addition provides compression and encryption of the concealed message.

Hide4PGP
: a freeware program distributed as source code in ANSI C and precompiled executables for DOS), OS/2 (Warp and up), and the Win32 console (9x and NT). It's purpose is to hide any data in a way that the viewer or listener does not recognize any difference.

Hide and Seek
: a stego program that hide any data into GIF images. It flips the LSB of pseudo-randomly chosen pixels. The data is first encrypted using the blowfish algorithm.

Hide and Seek for Win95 *Shareware*
: a BMP-based steganography program

Hide In Picture 2.0 *Freeware*
: a Win9x or DOS stego program with blowfish encryption that hides data in BMP images.

Hide4PGP v2.0 *Freeware*
: a command-line steganographic program for Windows, DOS, OS/2, and Linux that hides data within BMP, WAV, and VOC files. It is designed to be used with both PGP and Stealth, but also works well as a stand-alone program.

ImageHide *Freeware*
: Windows-based program which hide files in a number of different formats without increasing file size.

In Plain View *Freeware*
: BMP steganography with password protection.

In The Picture *Shareware*
: Encrypt files & messages into redundant space in Windows Bitmap (BMP) image files.

InfoStego *Freeware*
: Windows-based program which hide files in a BMP with compression and encryption.

Invisible Secrets 2002 *Shareware*
: 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.

JPHIDE and JPSEEK *Freeware*
: a Win95/98/NT stego program with a GUI that hides data in the JPG image format. It uses Blowfish encryption. DOS and Linux version also available.

JPEG-JSTEG
: hides data inside a JPEG file. (source code available)

JPegX *Freeware*
: an encryption program that hides your important information inside standard JPEG image files. The image is left visually unchanged and messages are encrypted and password protected. To decrypt the message, you need to open the JPEG file that holds it and enter the password if prompted.

JSteg Shell v2.0 *Freeware*

a Win95/98/NT (not Win2000) interface to run JSteg DOS, which hides data in the JPG image format. Includes 40 bit RC4 encryption, determination of the amount of data a JPG can hide beforehand, and user-selectable JPG options (ie. degree of compression).

MandelSteg and GIFExtract
: hide data in fractal GIF images. MandelSteg will create a Mandelbrot image (though it could be modified to produce other fractals), storing your data in the specified bit of the image pixels, after which GIFExtract can be used by the recipient to extract that bit-plane of the image. (source code available)

MP3Stego *Freeware*
: has both GUI and command-line versions that hide information in MP3 files, which are wav file sound tracks that are compressed using the MPEG Audio Layer III format. They offer near-CD quality sound at a compression ratio of 11 to 1 (128 kilobits per second). Available as Windows 95/98/NT executables and Linux/Unix source code (found in the zip file).

NICETEXT
: transforms cipher-text into innocuous text which can be transformed back into the original cipher-text.

OutGuess
: a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources.

PGPn123 *Freeware*
: a pgp "windows clipboard" shell program that makes using pgp for Eudora, Agent, or Pegasus Mail very easy. The algorithm is based on the Texto program, making encrypted text files look like something between mad libs and bad poetry.

PGP encryption
: Even though the file is hidden inside something else, it may still be possible to recover it from that file by someone else. In such a case, you should encrypt the data first. This makes it a lot harder for this other person to determine whether he has really extracted the file you put in the image.

Pretty Good Envelope
: hides data in almost any file. It embeds a binary message in a larger binary file by appending the message to the covert file as well as a 4-byte pointer to the start of the message. To retrieve the message, the last 4 bytes of the file are read, the file pointer is set to that value, and the file read from that point.

S-Mail *Shareware v1.3*
: a stego program that runs under all versions of Windows and DOS that uses strong encryption and compression to hide files in EXE and DLL files.

S-Tools4 *Freeware*
: a Win 95/NT based steganography tool that hides files in BMP, GIF, and WAV files.

S-Tools3 *Freeware/Shareware*
: a Windows based steganography tool. Hides files in BMP, GIF, WAV, and unused space on floppies.

Sam's Big Play Maker *Freeware*

a Windows-based program that converts arbitrary text to an amusing play. Only practical for small messages.

Scytale

A Windows PGP interface that includes an option to hide data in .PCX files.

Security: File wiping

A normal "delete" does not actually erase files. The data itself remains on the disk, it's just not part of a file anymore. By using a wiper, the data is replaced with random junk first. This prevents people with undelete utilities to get your erased files back.

Snow

is used to conceal messages in ASCII text by appending white spaces to the end of lines.

Spam Mimic

encodes your message into what looks like your typical, quickly deleted spam mail.

Stash-It v1.1 *Freeware*

a simple Win95/98/NT-based stego program that will allow you to hide and extract any data file inside a perfectly normal BMP, GIF, TIFF, PNG or PCX file.

Steganos

A steganography tool that uses a wizard interface to hide data in BMP, DIB, VOC, WAV, ASCII, and HTML files.

Steganos for Windows 95

a wizard-style Windows 95 application that can hide and/or encrypt files. It can hide files inside BMP, DIB, VOC, WAV, ASCII, and HTML files.

Steganos Security Suite 4 *Shareware/Commercialware*

a complete, easy to use security suite that uses strong encyption and steganographic techniques to hide data in graphic and sound files. Also include is The Safe (drive encryption up to 1 GB in < 1 second), Internet Trace Destructor, file shredder, e-mail encryption, password manager and computer locking.

Stegdetect (XSteg) (2.3 mb) *Freeware*

an automated tool for detecting steganographic content in images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images. Currently, the detectable schemes are jsteg, jphide (unix and windows), invisible secrets, outguess 01.3b, F5, appendX, and camouflage.

Steghide 0.4.6.b *Freeware*

a command-line application that features hiding data in bmp, wav and au files, blowfish encryption, 128 bit MD5 hashing of passphrases to blowfish keys and pseudo-random distribution of hidden bits in the container data.

Steghide

embeds message in .bmp, .wav and .au files

Stealthencrypt *Commercialware*

features BMPand TIF steganography and uses triple DES and Blowfish encryption. Stego program that hides data in .BMP files.

StirMark and UnZign *Freeware*

command-line programs that remove copyright and stego'd information from files.

Scramdisk
: a program that allows the creation and use of virtual encrypted drives.

Snow
: used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers.

SpamMimic.com
: allows users to encode and decode secret text messages in what appears to be rambling spam messages.

Stash-It
: allow you to hide (and extract, of course) any data file inside a perfectly normal BMP, TIFF, PNG or PCX file.

SteganoGifPaletteOrder
: Hiding data into the palette of a GIF file.

Stego
: Hide and recover encrypted data in your GIF files

TextHide *Free Demo/Commercialware*
: a program that subtly changes text features, such as narration tense, perspective, and single word synonym replacements to hide data within any text file.

The Third Eye *Freeware*
: Hides files in BMP, GIF, and PCX files. Includes encryption and nice user interface.

wbStego
: allows you hide data in bitmaps, text files and also HTML files. The data is encrypted before embedding. Two different user interfaces are proposed: 'the wizard' guides the user step by step and the 'pro' mode gives him full control

wbStego4.2 *Shareware*
: BMP, TXT, HTML/XML, and PDF steganography for Windows. Includes a handy Wizard interface, a new (faster) engine, passphrase support to 2 GB, built-in encryption, and key generation.

WeavWav *Freeware*
: Software that can hide secret data in .wav files. Very basic interface.

wbStego
: a tool that hides any type of file in bitmap images, text files, HTML files or Adobe PDF files.

Wnstorm
: Wnstorm (White Noise Storm) is a cryptography and steganography software package which you can use to encrypt and hide files within PCX images.

DOS

FFEncode

a DOS program that "hides" a file in a text file by using a "morse code" of NULL chararcters.

GZSteg
: hides data in GZip compressed files.

Hide and Seek v5.0
: Data hiding/seeking using GIF image files. These DOS programs take data, usually text, including encrypted text, and hide it in a GIF file.

JSteg
: a DOS program available for hiding data within the popular JPG format.

Pretty Good Envelope
: a DOS based program that hides a message in another file by the very simple method of appending the message to the file, and then appending a 4 byte little endian number which points to the start of the message.

Stealth
: 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.

Steganos v1.4
: a DOS program that hides data inside BMP, VOC, WAV and even ASCII files.

Stegodos
: This DOS based picture encoder consists of a group of programs designed to let you capture a picture, encode a message in it, and display it so that it may be captured again into another format with a third-party program, then recapture it and decode the message previously placed inside it.

Snow
: a text-based stego program that conceals messages in text files by appending tabs and spaces on the end of lines. Tabs and spaces are invisible to most text viewers, hence the steganographic nature of this encoding scheme. Snow includes a compression function to allow you to stego more information into a given file and has some basic crypto functions via the ICE algorithm.

Unix

Hide and Seek
: unix based stego program

MandelSteg
: for a gif-based stego program

SNOW
: unix based stego program

Stegonosaurus
: a Unix program that will convert any binary file into nonsense text, but which statistically resembles text in the language of the dictionary supplied

Texto
: text-based stego program

White Noise Storm

unix based stego program

Java

EZStego Java

a Java based steganographic software which modifies the LSB of still pictures (supports only GIF and PICT formats) and rearrange the color palette.

Snow

a text-based stego program that conceals messages in text files by appending tabs and spaces on the end of lines. Tabs and spaces are invisible to most text viewers, hence the steganographic nature of this encoding scheme. Snow includes a compression function to allow you to stego more information into a given file and has some basic crypto functions via the ICE algorithm.

Macintosh

FatMacPGP 2.6.3

has a stealth option which strips off all identifying header information to leave only the encrypted data in a format suitable for steganographic use.

Stego

a steganography tool that enables you to embed data in Macintosh PICT format files, without changing the appearance or size of the PICT file.

References

Sellars, Duncan. "An Introduction to Steganogrpahy."
URL: http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html

Anderson, Ross A. and Petitcolas, Fabien A.P. "On the Limits of Steganography."
URL: http://www.cl.cam.ac.uk/~fapp2/publications/index.html

Johnson, Neil. "Steganalysis."
URL: http://www.jjtc.com/Steganalysis

Radcliff, Deborah. "Steganography: Hidden Data."
URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html

Petitcolas, Fabien A.P. "The Information Hiding Homepage Digital Watermarking & Steganography."
URL: http://www.cl.cam.ac.uk/~fapp2/steganography

Johnson, Neil F. and Jaodia, Sushil. "Steganalysis of Images Created Using Current Steganography Software."
URL: http://www.jjtc.com/ihws98/jjgmu.html

McCullagh, Declan. "Bin Laden: Steganography Master?"
URL: http://www.wired.com/news/politics/0,1283,41658,00.html

Schneier, Bruce. "Steganography: Truths and Fictions."
URL: http://www.counterpane.com/crypto-gram-9810.html

Carvin, Andy. "When a Picture is Worth a Thousand Secrets: The Debate Over Online Steganography."
URL: http://www.benton.org/DigitalBeat/db103101.html

NetSecurity.com. "Hacking and Cracking Take on New Implications."
URL: http://www.netsecurity.about.com/library/weekly/aa111801a.htm

Berg, Erik C. "Legal ramifications of Digital Imaging in law Enforcement."
URL: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm

Appendix References

Cotse.com. "Steganography Tools."
URL: http://www.cotse.com/tools/stega.htm

StegoArchive.com. "What is Steganography?"
URL: http://steganography.tripod.com/stego.html

NetSecurity.com. "Stegano Software – Win 95/98."
URL: http://www.netsecurity.about.com/cs/steganoappswin

StegoArchive.com. "Steganography Software."
URL: http://steganography.tripod.com/stego/software.html

Flynn, Jean. "Reverser's Steganography (Starting Page)."
URL: http://www.woodmann.com/fravia/stego.htm

Engelfriet, Arnoud. "Privacy:Steganography."
URL: http://www.stack.nl/~galactus/remailers/index-stego.html

Last Updated: July 23rd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor