GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Steganography: Why it Matters in a "Post 911" World

Abstract

Prior to the tragedy of Sept 11, 2001 steganography was barely known outside of academic and security circles. Now, it has become a much-reported element in one of the most significant events in the early 21st century. The ability to hide a text message inside a picture on a PC has gone from an interesting bit of trivia to a communications method possibly used by al-Qaeda as a means to covertly transmit their plans to various terrorist cells. On the global economic front, the use of robust digital watermarks using similar technology is a critical success factor in the multi-billion dollar digital works distribution industry.

Cryptography attempts to conceal messages by various translation methods that create new, unrecognizable messages. Even though this new, encoded message may be unintelligible to an observer it still remains in plain view. By contrast, the main purpose of steganography or "stego" as it is often called is to hide *even the occurrence of messages*. While the underlying concepts of steganography have been around for thousands of years, it wasn't until the mid 90s that the concepts evolved into software capable of being run on standard PCs. Trying to keep up with developments in steganography is steganalysis, the science of discovering hidden messages. Today, messages can be hidden in a variety of audio and video files using increasingly sophisticated tools that incorporate both steganography and cryptography. The aptly named "OutGuess", a modern stego tool available from the Internet already makes the claim to be able to defeat steganalytical tools that use statistical analysis, one of the more common discovery techniques.

In its current form, steganography is barely 5 years old. Given the global nature of some of the related issues and the pace of technology, it is difficult to say exactly where stego will be in another 5 years. Nevertheless it is reasonable to assume that steganography will become more sophisticated and a bigger part of our lives, both as individuals and as security professionals.

© SANS Institute 2000 - 2005 Author retains full rights.

History of Steganography

Steganography has been with us in many forms since the time of the Greek empire. Even the word steganography comes from the Greek *steganos*, hidden or covered, plus *graphein,* to write. Herodotus, the Greek historian recorded the story of a slave used as the medium to transmit the hidden message. The slave's head was shaved and the message tattooed on the bare skull after which the hair was allowed to re-grow. The slave was sent to the message recipient who shaved the slave's head to reveal the message. Hopefully the message was not time-dependent! Lord Robert Baden-Powell, as scout for the British during the Boer War marked the positions of Boer artillery bases by embedding maps into drawings of butterflies. Appearing innocent to a casual observer, certain markings on the wings were actually the positions of the enemy military installations. Later, Axis and Allied spies used invisible inks containing fruit juice or urine to transmit messages that would reveal themselves when heated or when in the presence of ultraviolet light.

In the mid-90s a number of the older techniques of hiding messages inside other messages and even images became more popular with the advent of modern software and powerful computers.

Regardless of the technique used, the key similarity in all cases was that messages were *hidden in plain view.*

Steganography vs. Cryptography

There is an important distinction between these two complementary but different technologies. The intent of steganography is to conceal even the occurrence of a message. Cryptography, by contrast, reveals itself by scrambling a message that cannot be readily understood. The following is a piece of a message encrypted with the encryption tool, "Steganos Security Suite" reviewed later in this article.

> ®VÉW½+Ôpf ¬X÷£ê‰ ÉtÏÆV «á-s¼x– É Óý JÉl8½Â\=«quü"üÜ¹š€µû
> "4åb§åÜÝáAéUðÑVV œÌ¤kÒÌ]1Ì«À ÀYõ«bîÂ[ )

An individual viewing such a message may suspect that an encryption process had occurred. That same person observing the following picture of a family pet would have no reason to think that the stego tool S-Tools4 was used to hide a message in the picture. To view the message you will need to open this document in Word, right click on the image, open it as a BMP file, save it to the desktop and then drag the file to S-Tools4 using the password "kitty" to reveal the message.

Figure 1 Picture of Family Cat Containing An Encoded Message

© SANS Institute 2000 - 2005 Author retains full rights.



Today, it is not uncommon to use a combination of the two technologies with messages being both encrypted and inserted into an image.

Steganography techniques

Stego techniques can be grouped into 3 broad categories: injection, substitution and the generation of new files.

Injection

Injection refers to the insertion of a message into an existing medium. The simplest example is the use of the hidden attribute in Microsoft Word, which allows for hiding text with a special, hidden font. This very simple technique was used to store notes and references during the creation of this document. A casual observer can view the report and not be aware of rough notes that are easily revealed by going to Word's tools/options and clicking on "hidden text". The HTML language allows for the hidden attribute that works in a similar fashion by hiding text from a web browser. Moving up the technology scale and into the security arena it could be argued that the Unicode vulnerability, a technique that has corrupted many web servers by hiding commands in unprintable pieces of web addresses is also a form of stego.

Somewhere between injection and substitution are techniques that modify text features in documents. "Line shift coding" moves every nth line up or down a tiny fraction, typically 1/300 of an inch. A variation, "word-shift encoding" adjusts the horizontal spaces between words. Any of these minor variations becomes the underlying method to encode messages.

More advanced techniques make use of various combinations of syntactic methods that utilize subtle changes in punctuation and contractions to encode a message. Semantic methods utilize characteristics of words. The following example, a combination of

© SANS Institute 2000 - 2005 Author retains full rights.

cryptography and steganography, uses semantics by assigning 0 through 9 to the colours red, orange, yellow, green, blue, violet, black, white, and pink to encode the current year.

> *The yellow flowers at the side of the racetrack took on a red hue as the sun set. At the same time, the clouds transformed themselves into giant, red balls of fire as the lead car, a yellow Corvette came screeching around the final turn.*

Creating messages that look like ordinary text is quite difficult and the amount of information that can be encoded must be kept low in order to preserve the appearance and understandability of non-encoded text.

The childhood memory aid for remembering the planets is yet another simple example: "Mary's violet eyes make John sit up nights, period" with the first letter representing the first letter of each planet in order. While this last example is hardly a threat to world order it does demonstrate the technique of hiding one message within another.

Substitution

This technique replaces data in the original file with a coded representation of the original message. The colours of "pixels", tiny elements of digital images are often represented by the value of a number contained in an eight-bit byte of data. For example, three increasingly redder shades of red might be represented as follows:

"00001100" or decimal 12 might represent basic red in a particular 8-bit colour palette

Each of the following numbers would then represent a minor increase in the redness.

"00001101" or decimal 13
"00001110" or decimal 14

The likelihood of a casual observer noticing the difference in the shades in the middle of a picture is very slight. The result is that steganographers are able to use the 2 least significant bits to encode messages and while the image does degrade slightly, it is not apparent to the naked eye.

The following two figures show a picture of a family pet. Figure 2 was taken with a digital camera at a 320 X 240 resolution. Figure 3 shows the result of using S-Tools4 to insert a small text file in to the image using the least significant bit (LSB) technique.

© SANS Institute 2000 - 2005 Author retains full rights.

Figure 2 Original Picture



Figure 3 Picture With Hidden Message



Even a side-by-side comparison of the above pictures shows no visual cues to the existence of a message.

24-bit "True Colour" images have a finer colour definition than images created by 8-bit coding. In essence the change of a single bit of a 24-bit based colour palette will have less of an impact than the change of a single bit in an 8-bit palette and the change is therefore easier to hide. Even more preferable is an image based on a 256-colour gray scale palette as the colours change more gradually between gray scale palette entries than colour palettes

The complexity of the techniques goes well beyond manipulation of least significant bits and extends to sophisticated processes such as manipulating the discrete cosine transformation process used to create JPEG files. Other techniques, such as those used in digital watermarking manipulate other image properties such as luminance. Luminance is often chosen as the Human Visual System (HVS) has a lower sensitivity to changes in luminance than other image characteristics.

The use of technology is only one element in the successful use of steganography to hide messages. One lesson probably learned very early was not to use well-known pictures, such as the "Mona Lisa" as people may notice a colour differences. Various analytical tools could also be used to compare to the original. When inserting a message in a picture, the steganographer will almost certainly be more successful using a picture of the family pet than well-known images! Trying to hide a message in a picture also requires a certain amount of contextual awareness in the sense that the person should only be receiving images that are typical and reasonable for his or her context. Anything else might trigger alarms.

The technique of embedding messages in digital pictures has caught the eye of both Hollywood and the mainstream press. In the 2001 movie, "Along Came a Spider", two children used stego to transmit secret messages under the noses of unsuspecting adults.

© SANS Institute 2000 - 2005 Author retains full rights.

On a more tragic note, there have been many articles, particularly in the American press that suggest that the al-Qaeda network used stego technology to transmit hidden messages in images on eBay.

Variations of the image based stego techniques are also used to encode messages in audio files and video formats. The Human Auditory System (HAS) has different perception capabilities than the HVS. HAS, for example, is particularly sensitive to random noise. The goal of the steganographer is to exploit the particular weaknesses of the HAS while avoiding its strengths. In addition to the LSB techniques used in the image-based stego there are methods such as phase shift encoding and echo data hiding that are unique to the audio world.

Generation of a new file

Both insertion and substitution require a host file, sometimes called a container, in reference to images, and a host signal in reference to audio signals. Host files, like the pictures above, contain embedded message but may also exhibit characteristics that reveal a pattern that can be used by steganalysis tools to detect the presence of the message.

To eliminate this potential weakness, a coded message can be generated as part of an original computer generated text, audio or image file. One example of an authoring program demonstrating stego techniques is called "Spam Mimic" found at http://www.spammimic.com/index.shtml. This web site allows the viewer to encode a message in a message that looks like spam email. As if regular spam wasn't bad enough, now we have stego spam!

The first few sentences of the spam mail created by the message "Mary had a little lamb" are as follows:

> Dear Friend, This letter was specially selected to be sent to you! We will comply with all removal requests! This mail is being sent in compliance with Senate bill 1618; Title 6; Section 302! THIS IS NOT MULTI-LEVEL MARKETING! Why work for somebody else when you can become rich in 38 days! Have you ever noticed how long the line-ups are at bank machines and more people than ever are surfing the web.

The message, truncated for the sake of brevity, nevertheless demonstrates what can be done. Of special note is that Spam Mimic was one of several tools and techniques mentioned in connection with Bin Laden in an article by Wired magazine.

Steganography tools

There are a wide variety of tools available on the Internet. Two such sources for software

© SANS Institute 2000 - 2005 Author retains full rights.

are:
http://www.cl.cam.ac.uk/~fapp2/steganography/stego_soft.html and
http://www.members.tripod.com/steganography/stego/software.html

The research for this paper was restricted to three of these tools: "S-Tools4", a freeware program from the second link above and "The Steganos Suite", a retail product available online at http://www.steganos.com and OutGuess available from http://www.outguess.org.

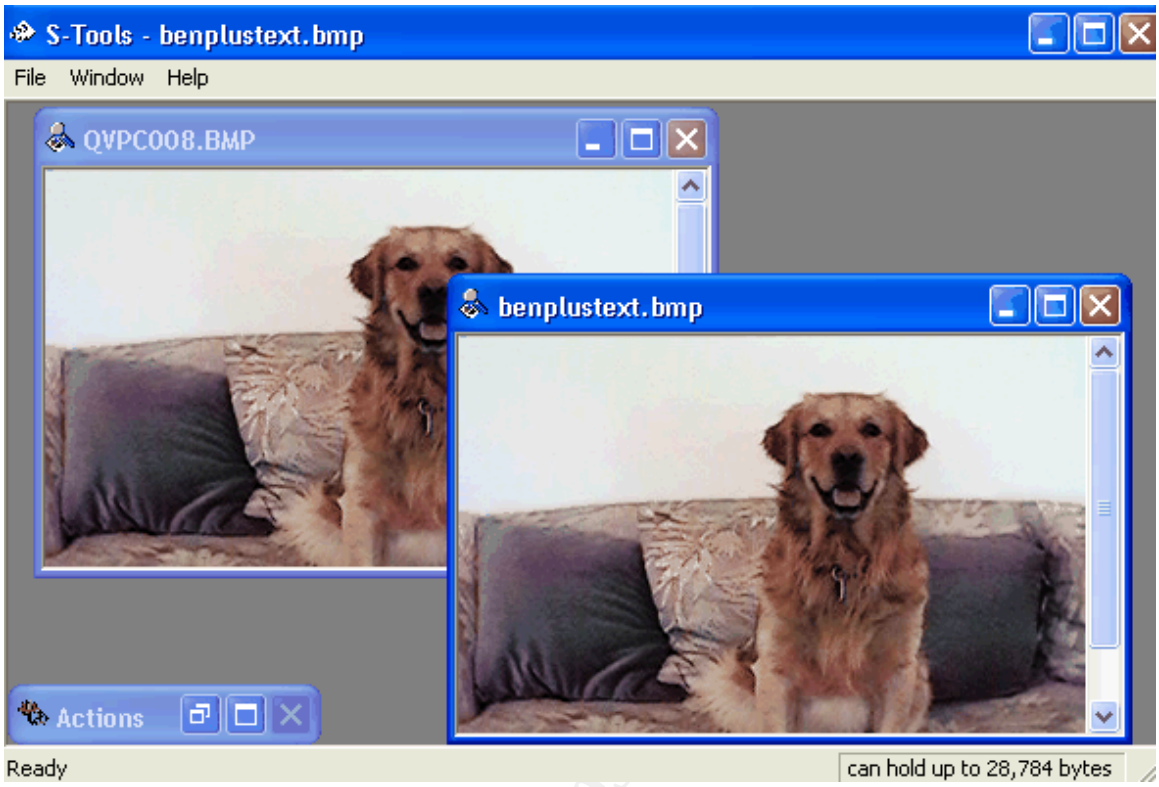
S-Tools4

S-Tools4 is extremely easy to use with a graphical interface and simple model that involves dragging the host file to the S-Tools window and then dragging the file to be embedded on top of the host file. It can embed single or multiple messages in images and in audio files, although it only supports .WAV files at this time. It employs a pass phrase along with cryptography techniques to further hide the message. The "help" is clear and describes not only how to use the software but also the underlying theory.

The following figure shows two BMP images, "QVPC008.BMP" the original picture and the final picture, "benplustext.bmp" created from the original after a 20k Word file was dragged onto it. The software reported that the original image could have held a hidden message approximately 29K in size. Image statistics from the properties of each image show the same numbers for pixel size, resolution, colour depth and size.

Figure 4 S-Tools Main Window

© SANS Institute 2000 - 2005 Author retains full rights.



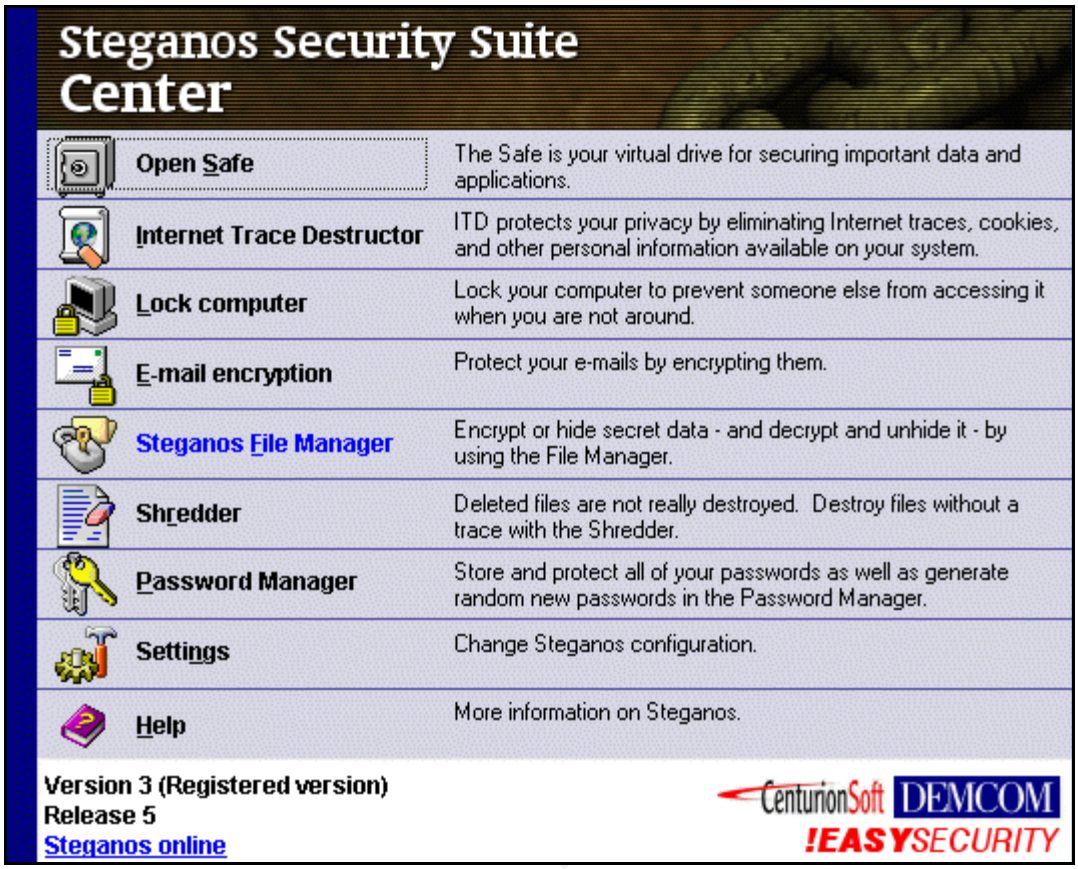
Steganos

The Steganos Security Suite is a retail product with a range of desktop cryptography and steganography functions including: email encryption, password management, file shredding, and file encryption. Hiding a message or multiple messages is a matter of selecting the files and then selecting an existing audio or image file as the carrier file. The software will even search your hard drive for potential candidates. Like S-Tools4, this program uses cryptography as well as the LSB stego technique to conceal messages. Once the message has been embedded the program assists by suggesting that you "irrevocably destroy the original"!

The following picture illustrates the wide range of functions of this tool.

Figure 4 Steganos Security Suite

© SANS Institute 2000 - 2005 Author retains full rights.



The simplicity of S-Tools4 easily demonstrated the power of embedding files within files while the Steganos Suite is a comprehensive desktop business crypto and stego tool intended for business use.

OutGuess

Illustrative of the direction of stego tools is "OutGuess" which can be obtained from: http://www.outguess.org

OutGuess is an example of the increasingly sophisticated nature of these tools. Information from the web site indicates that it preserves the statistical properties of the cover medium thereby defeating steganalysis tools that use statistical discrepancies as a method of discovering hidden messages in images.

Steganalysis

Steganalysis is the science of detecting hidden messages created by tools such as those mentioned above. Steganalysis is made possible by the fact that some stego processes can leave fingerprints in the form of information patterns indicating the presence of a

© SANS Institute 2000 - 2005 Author retains full rights.

hidden message.

Analysis can determine the statistical nature of the colours in various types of normal pictures. Some tools, such as S-Tools4 change the statistical makeup by increasing the number of duplicate colours revealing a deviation from an equivalent normal picture. Other tools may increase the amount of background noise. Steganalytical programs such as "stegdetect" found at http://www.outguess.org look for specific signatures by well-known stego programs such as "jsteg", "jphide" and earlier versions of OutGuess.

In all cases, knowing that there is a hidden message and having the original image or audio file makes the process considerably easier!

Steganography, by its very nature of being hidden writing is a powerful method for hiding messages. Until recently it was considered impractical to scan large numbers of images in the hope that something would be found. Largely driven by events of September 11, this supposedly near impossible task has already been done. In October, two computer scientists at the University of Michigan's Center for Information Technology Integration, using multiple workstations downloaded and interrogated over two million images from eBay auctions. No hidden messages were found. Of course, the paranoid observer would just say that this doesn't mean they weren't there!

Steganography, Digital Watermarking and Digital Copyright

Steganographic techniques are critical to the success of the burgeoning multi-billion dollar digital media distribution industry.

Two problems continue to plague the industry and both are seen as significant impediments to its development. The first problem comes from the lack of a technology that guarantees that copyrighted digital items are not illegally copied. The second involves the development and acceptance of technologies typically called digital watermarking that prove the ownership of a digital product.

While not strictly a steganography issue, the most recent example of the entertainment industry's inability to stop the illegal copying of digital media was the furor created last year over the release of DeCSS on the Internet. This program, while ostensibly developed to play DVDs on Linux systems, also allowed the copying of DVDs. As recently as November 2001, a California Appeals Court released a decision that eliminated prosecution for possession and distribution of this software. This has dealt a blow to the movie industry as it struggles with protection of copyrighted works.

By contrast, digital watermarking is clearly a business issue that involves stego-related techniques and tools although with decidedly different objectives. How can a copyrighted image get stolen from the web? It is as easy as right clicking on the image on a web site and doing a "save as". Digital watermarking, which started in the early 90s, stamps digital products such as audio files or images with an electronic signature. It is

© SANS Institute 2000 - 2005 Author retains full rights.

critical that the process does not materially degrade the quality or the product but yet still provide irrefutable proof of the ownership of that product. Much work has been done on watermark visibility vs. watermark robustness with strengths in one area adversely affecting the other. Digital watermarks must be seen to be robust and in particular, tamper proof, if they are to be of use as a general purpose, economically viable business tool.

The business of digital rights protection is also generating business opportunities with companies such as Digimarc at http://www.digimarc.com, one of the leading developers of digital watermarking technologies. They offer a number of tools including a small mouse-like device that can scan an image and determine whether the image is original or a copy. The sample picture in Figure 5 below shows authentication information embedded in a picture as revealed by a special watermark viewer from Digimarc. Installation of the Digimarc viewer also adds capabilities to Internet Explorer by automatically revealing the presence of watermarked images on web sites. Visiting the web site at http://www.cl.cam.ac.uk/users/fapp2/watermarking/stirmark/samples.html immediately generated the "watermarks detected" message in the browser.

Figure 5 Picture with watermark



Distributor: Corbis, 15395 SE 30th Place, Suite 300, Bellevue, WA 98007 USA Telephone (425) 649-4552, Fax (425) 957-9253.

CreatorID: 84324, ImageID: 2001004, Copyright: 2001 Corbis

In addition, there are tools such as Epson's "Image Authentication System"(IAS) that provide image authentication directly from the point of capture in a standard JPEG file using commercially available digital cameras. While IAS doesn't prevent copying, it does provide a means to detect tampering and authentication of the original owner. For the technically inclined, protecting web based images can be done with Java script from Java Script Planet. Typically, moving the cursor over the protected image produces a copyright protected or equivalent image. Other programs such as SecurityPlus by Softbyte labs and Cryptapix by Briggs Software support fast encryption and decryption of images. The encryption limits access to those who have been given the rights to view the images.

The related issues of copyright and digital watermarking are of sufficient scope to stir national governments into action. The Canadian government recently announced a white paper requesting input for a major overhaul of Canadian copyright legislation. Statements from the government web site at http://strategis.ic.gc.ca/SSG/rp01099e.html reveal their concern as follows:

> Several of the copyright sectors or "industries" have suggested that their

© SANS Institute 2000 - 2005 Author retains full rights.

> willingness to embrace the Internet as a channel for disseminating their works or making them available ultimately depends on their ability to prevent or discourage unauthorized copying and distribution activities which are easily carried out in the digitally networked environment.

Of more concern to businesses involved in this technology sector should be the following comments.

> Legislative measures are needed to deter the circumvention of technological measures that are used by rights holders to protect their rights
>
> Legislative measures are needed to deter tampering with rights management information

They clearly suggest the government is concerned and is considering taking action that will have a direct bearing on the strength of digital watermarking. They also indicate what might be done to deter tampering with these watermarks.

The Future

Given the nascent nature of this technology, the scope of the business issues that are affected and the continuing impact of Moore's law on the power of computing it is difficult to predict with any certainty where we will be in 5 years. Nevertheless, the following predictions are presented as a reasonable set of possibilities.

- Steganographic techniques will become more common and increasingly sophisticated.
- Steganalysis tools will also become more complex but will typically be behind their steganographic counterparts.
- A stego process will be developed to embed Trojans, worms and viruses in media such as images or audio files and have them become active by viewing or listening to the files. In 2001, the Nimda worm demonstrated that it was possible to get a virus just by visiting an infected web site. In January of 2002, viruses were being delivered by Macromedia flash images. One day, merely viewing a bitmap image might cause a virus attack on your PC.
- Intrusion Detection Systems (IDS) will include images as part of their attack signatures.
- Anti-virus software will be developed with steganalytical capabilities to detect viruses in audio and image files
- A strong tamper-resistant, economically viable digital watermark will be developed.

The person who develops the last item will undoubtedly become very rich. There is probably no better motivating factor for learning about steganography!

© SANS Institute 2000 - 2005 Author retains full rights.

References

Quinion, Michael. "Weird Words Section. Steganography", 23 Oct 1999
http://www.quinion.com/words/weirdwords/ww-ste1.htm (12 Jan 2002)

Ross, Brian. "A Secret Language, Hijackers May Have Used Secret Internet Messaging Technique". 04 Oct 2001
http://abcnews.go.com/sections/primetime/DailyNews/PRIMETIME_011004_steganography.html (12 Jan 2002)

Eng, Paul. "Watching The Web For Wicked Messages. Experts Say Spotting Terrorist Messages OnLine is Mission Impossible". 11 Oct 2001
http://abcnews.go.com/sections/scitech/DailyNews/webwatch011011.html (12 Jan 2002)

Kelly, Jack. "Terror Groups Hide Behind Web Encryption". 06 June 2001
http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm (12 Jan 2002)

McCullagh, Declan. "Bin Laden: Steganography Master?" 07 Feb 2001
http://www.wired.com/news/politics/0,1283,41658,00.html (12 Jan 2002)

McGrath, Peter. "Coded Communications. Did the hijackers their messages in harmless-looking messages on the Internet?" 21 Sept 2001
http://www.msnbc.com/news/632358.asp (12 Jan 2002)

Sellars, Duncan. "An Introduction to Steganography" 1999
http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars

Honeyman, Peter. "Detecting Steganographic Content On The Internet". 31 Aug 2001
http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf (12 Jan 2002)

Provos, Neils. "Defeating Statistical Analysis"
http://www.citi.umich.edu/u/provos/stego/ (12 Jan, 2002)

Jajodia, Sushil; Johnson, Neil. "Steganalysis of Images Created Using Current Steganography Software" 15 April 1998
http://www.jjtc.com/ihws98/jjgmu.html (12 Jan 2002)

Kutter, M., Petitcolas, F. A. P. "A fair benchmark for image watermarking systems"
http://www.cl.cam.ac.uk/users/fapp2/publications/ei99-benchmark.pdf (12 Jan 2002)

Petitcolas, F. A. P. "Prepare yourself for the next generation of Stirmark"
http://www.cl.cam.ac.uk/users/fapp2/watermarking/stirmark/index.html (12 Jan 2002)

Petitcolas, F. A. P. "The information hiding homepage, digital copyright and

© SANS Institute 2000 - 2005, Author retains full rights.

steganography"
http://www.cl.cam.ac.uk/~fapp2/steganography/ (12 Jan 2002)
Borland, John. "Movie industry dealt DVD-cracking blow" 01 Nov 2001
http://news.cnet.com/news/0-1005-200-7751876.html (12 Jan 2002)

Levy, Trudy. "Guarding Your Assets" 20 Feb 2000
http://www.dig-mar.com/Commentaries/Guard_Asset.html (12 Jan 2000)

"Epson Image Authentication System"
http://www.epson.co.uk/options/imaging/ias.htm (12 Jan 2002)

Stromberg, Michael. "Secure Content Protection: An overview of the proposed security mechanisms in digital cinema". 20 Oct 2001
http://www.amt.kth.se/dokument/Digital%20Cinema%20Security.pdf (12 Jan 2002)

Brown, Andrew. "S-ToolsV4"
http://members.tripod.com/steganography/stego/s-tools4.html (12 Jan 2002)

Steganos Security Suite home page
http://www.steganos.com/en/index.htm (12 Jan 2002)

Provos, Neils. "OutGuess home page"
http://www.OutGuess.org (12 Jan 2002)

Briggs, Kent. "Briggs Softworks Home Page"
http://www.briggsoft.com/ (12 Jan 2002)

"Softbyte Labs Home Page"
http://softbytelabs.com/index.htm (12 Jan 2002)

Brannan, Andrew. "Unicode Vulnerability – How and Why". 07 Aug 2001
http://rr.sans.org/threats/unicode.php (12 Jan 2002)

© SANS Institute 2000 - 2005 Author retains full rights.