Global Information Assurance Certification Paper

Steganography

Jeremy Krinn

The historic use of steganography was the concealing of communications. This has been accomplished in a number of ways ranging from microdot printing and invisible inks to spread spectrum communications. This differs from cryptography in that cryptosystems assume that the enemy can access and modify the communication if possible. Steganography can augment cryptography by obscuring communication and prevent the enemy from knowing a communication is even being sent. However it should not be considered a replacement for cryptography. (1,2). Using computers to hide information on a hard drive is easily done with free tools or comprehensive security packages.

The world of computing has developed some interesting applications for steganography that instead of hiding information seeks to fingerprint or watermarking. These techniques can be used to protect distributed intellectual property such as films, audio recordings, books, and multimedia products by embedding copyright information. Some applications for steganography presented by Anderson and Petitcolas are for embedding signatures in advertising and monitor them for contractual adherence; embedding comments in video-mail; or embedding patient information into medical images. (3)

Information Hiding Tools

Steganos II (4)

I started my exploration of steganography with a package from Demcom called Steganos II for Windows. The software is a security suite that includes a ray diffusing notepad, a password management utility, a "shredder" to permanently delete files to DOD standards and steganography tools. I used the US version, which uses a RC-4 compatible encryption algorithm with a 128-bit key. There is a charge for the full version of the suite of software.

Launching the program runs a desktop for utilizing the Steganos Suite. A split pane window allows for easy browsing. Steganos allows you to use either encrypt a file or encrypt and hide a file. A drag and drop concept works between the two panes to select the files to hide. Steganos also integrates with Windows to give an option to hide data from an explorer view by right clicking on the file and choosing the Hide… feature. Demcom makes a "reader" program for people who do not have the full suite but may want to read embedded data. The additional features and the suite of programs included with this software package make it worth the initial cost.

I think everyone is familiar with the default Microsoft Startup WAV. I have used Steganos to embed this paper you are reading (without pictures or sounds). 

Here is the original for comparison. 

S-Tools (5)

S-tools seemed to be the most popular tool cited in many papers as well as by number of downloads from Zdnet. S-Tools fits on a floppy, after it's been decompressed from download. This is a big plus if you are like me and visit many machines during any given day. The interface is simple to use just drag a picture into the frame of the running program. The lower left part of the picture will indicate the how a large a file your carrier will hold. Then you can simply drag the file you want to hide into the image. A dialog box then asks for a passphrase and encryption algorithm that you want to use. A simple right click allows you to save the carrier/hidden file to your hard drive.

To unhide the information, drag the picture into the frame, right click, select reveal the type in your passphrase. You still need to drag the revealed file from the program window to the hard disk. The size of the program makes it easy to transport or send via email. However the small size means you sacrifice some features. S-tools will only allow gif, bmp or wav carrier files. This is a limiting factor if you wish to send or store information in other file formats.

Here is a picture of a spider web downloaded from Imagebank.com. The size of this gif is 186 KB. Below it is the same picture using S-Tools to embed the Samples.XLS workbook that comes with Microsoft Office. The original size of the embedded file is 215 KB. This is about the limit that S-Tools recommended for the maximum file size. Close observation of the two images shows a definite change in pixilation in places. I purposely embedded a larger file to show some differences in the two images. The second image is only 272 KB. Comparing this to the original would show an obvious difference. However a small image in a large file would not be as obvious. A large image could hold a great deal of data, especially if compressed. This could even be made more difficult to detect by embedding the data in the original and not having copies to compare it.

There are programs available for most popular operating systems. I have reviewed two for Windows for comparison. Please reference the table at the end of this paper for a guide to some of the tools available.

Before discussing digital watermarking I would like to mention Craig Rowland describes another method of data hiding that in a paper. Craig describes techniques to leverage weaknesses in the TCP/IP protocol suite that would allow covert channel communications. The areas encoded in the packet can be: 1) the IP packet identification field 2) the TCP initial sequence number field and 3) the TCP acknowledged sequence number field. The fields are replaced with numerical ASCII representation of the character to be encoded. Each subsequent packet contains the next letter in the code. This could provide a means to "smuggle" data between networks. There is source code available for Linux at the end of Craig's paper for TCP header manipulation. (7)

Digital Watermarking

The use of hidden copyright or fingerprinting can be used to identify electronic media or carry data about the media. This could ensure ownership and identify illicit copying of digital media. (4). This has become an issue recently with the emergence of mp3 and the recent charges against Napster. A great deal of research has been done on techniques for watermarking and fingerprinting. Rather then discuss the techniques I am going to profile a company that provides commercial watermarking products. I will provide links to research papers at the end of the document.

Recently an e-column from Red Herring (8) magazine profile companies that are linking old-world media like catalogs and magazines to online content by using watermark image embedded in advertising that can be read by digi-cams. Digimarc (http://www.digimarc.com) is a company that is offering commercial steganography tools. They have patented processes to protect movies, photographs, as well as financial records. The technology involves both digital images that can have embedded images on them. These images can be tracked by searching for meta data embedded in the images.(9)

The second technology allows embedding of information into identification cards such as a drivers license or credit card. This helps prevent counterfeiting by using high quality reproductions. The embedded data would be undetectable except by computers with digital cameras. The watermarks can survive printing and laminating. The documents can then be personalized to an individual.

There are tools available to test the robustness of watermarking and these are available unZign (available at http://www.altern.org/watermark) and Stirmark (available at http://www.cl.cam.ac.uk/~fapp2/steganography/image_watermarking/stirmark/)

Bibliography

1) Johnson, Neil. "Steganography". URL: http://www.jjtc.com/stegdoc/
2) Unknown , "Hidden in Plain Sight-Steganography" Counterintelligence New and Developments June 1998 Vol. 2 URL: http://www.nacic.gov/cind/jun98.htm#rtoc4
3) Anderson, Ross J. and Petitcolas, Fabien A.P.. "On the Limits of Steganography". IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998. URL: http://www.cl.cam.ac.uk/~fapp2/papers/jsac98-limsteg/
4) Demcom. http://www.demcom.com/english/steganos/index.html
5) StegArchive http://members.tripod.com/steganography/stego.html
6) Johnson, Neil. "Steganography & Digital Watermarking". http://www.jitc.com/Steganography
7) Rowland, Craig. " Covert Channels in the TCP/IP Protocol Suite." URL: http://www.psionic.com/papers/covert/
8) Needleman, Rafe. "Stripes and Blobs." Red Herring.com July 21, 2000. URL : http://www.redherring.com/cod/2000/0621.html
9) Johnson, Neil. "In Search of the Right Image: Recognition and Tracking of Images in Image Databases, Collections and The Internet." URL: http://www.isse.gmu.edu/~njohnson/pub/csis_tr_99_05_nfj
10) Digimarc. "Digimarc Watermark Guide" URL: http://www.digimarc.com/support/cswater.shtml
11) Fridrich, Jiri and Goljan, Miroslav " Comparing robustness of watermarking techniques"

Other Links(not used directly in this article but can provide more information):

Petitcolas, Fabien A.P. "Annotated Bibliography on Information Hiding" URL: http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/

Ed. Katzenbeisser, Stefan and Petitcolas, Fabien. Information Hiding Techniques For Steganography and Digital Watermarking. Publisher : Artech House
Available at Amazon: Steganography and Watermarking .

Below is a table listing various tools for comparison. The original version of this table appears at http://www.jtc.com/Steganography/toolsmatrix.htm. (6)

Tool	Vendor -Author	Operating System	Coexisting Requirement	Technology	Image Formats	Comments
Argent	Commercial, Digital Information Commodities Exchange (DICE) http://digital-watermark.com/				Images are not yet supported.	Embeds copyright or license information as watermark.
Copyright	Commercial, Intellectual Protocols2 (IP2) http://www.ip2.com/	Web based and requires a Java compliant browser.			JPEG and GIF	Only phase 3 involves digital watermarking.
EZStego, Stego Online, Stego	Shareware, Romana Machado romana@stego.com http://www.stego.com/	1) EZStego - Java 2) Stego Online - Web 3) Stego - Mac	EzStego requires Java Virtual Machine. Stego Online requires HTML 3.2 compliant web browser. Stego requires Mac.	LSB. Sorts palette to similar colors - palette shifts. All three tools use the same approach to information hiding.	EzStego - GIF StegoOnline - GIF Stego - PICT	Only supports GIF images. Stego supports PICT images only.
Giovanni	Commercial Blue Spike, Inc. 800 381 8344 E-Mail: info@bluespike.com http://www.bluespike.com/	Win, MAC		Fast Fourier Transform (FFT)	Digital Media: Image and audio	More information is available at the Giovanni web page. All the information resides in the watermarked copy and does not require a web site lookup, as do other commercial products. As long as one has the Giovanni software, the encoding keys, and the copy, the watermark can be extracted. Also see questions and answers about Giovanni for both image and audio watermarking.
Hide and Seek	Shareware, Colin Maroney cjm@cypher.net http://www.cypher.net/	Win, DOS		LSB	V5.0 - GIF Win95 - 8-bit BMP	Hide and Seek 1.0 for Win95 http://www.cypher.net/products/ Hide and Seek 5.0 for DOS http://www.rugeley.demon.co.uk/security/hdsk50.zip
IBM Digital Library System	Commercial, IBM Howard Sachar sachar@watson.ibm.com Manager, image applications IBM T. J. Watson Research Center P.O. Box 218 Yorktown Heights, NY 10598-0218 (914) 945-1432 Fax: (914) 945-4003		IBM's Digital Library System.	Discrete Cosine Transformation (DCT).		Watermark is an internal function to the library system. http://www.research.ibm.com/image_apps/ http://www.research.ibm.com/image_apps/commerce.html (commercial use)

JK_PGS (Pretty Good Signature)	Evaluation, PhD Students Mr. Martin Kutter (Switzerland - kutter@ltssg3.epfl.ch) and Mr. Frederic Jordan (France) at Signal Processing Laboratory at Swiss Federal Institute of Technology (EPFL).	UNIX (Sun, SGI, LINUX) (Win95/NT version is under development)	PPM image format only.			Working on development for Photo Shop and Paint Shop plug-ins. http://ltswww.epfl.ch/~kutter/watermarking/JK_PGS.html
Jsteg	Freeware, Derek Upham	UNIX, DOS, Win (source code is available)		Combination within the JPEG algorithm at compression?	Input: PPM (PBMPLUS color format), PGM (PBMPLUS gray-scale format), GIF, Targa, and RLE (Utah Raster Toolkit format). Output: JFIF format JPEG	When extracting the hidden message, a "decoded" image must be created.
Mandelsteg	Freeware, Henry Hastur	C source code.			Generates a Mandelbrot fractal GIF image.	Insecure. Signature: 128 unique colors. Each color used two palette entries. Software is available worldwide at many sites.
PictureMarc and BatchMarc	Commercial, Digimarc Corporation http://www.digimarc.com/		Photoshop Compatible image processing software. Requires MarcCenter to verify the watermark "code."	Pattern block encoding.	The mark may be embedded into any image readable by Adobe Photo Shop and can be processed with filters (24-bit or grayscale).	Subtle changes to "flat" areas may be detected when compared with the original
PixelTag	MIT Media Lab Joshua Smith and Barrett Comiskey pixeltag@media.mit.edu			Pattern block encoding.		Patent Pending http://www.media.mit.edu/pixeltag
Steganos	Shareware, Deus Ex Machina Communications http://www.steganography.com/ Fabian Hansmann (may be going commercial) Internet: steganos-support@demcom.com WWW: http://www.demcom.com/english/steganos/ Mail: Deus Ex Machina Communications, Sophienstr. 28, 60487, Frankfurt, Germany	Win, DOS		LSB	V1.4 (DOS) BMP Win95: BMP, DIB	Noticeable noise in 8-bit images. V1.4 also hides data in VOC, WAV, or ASCII files. Win95 also processes VOC, WAV, TXT, HTML V1.4 hangs when processing a 1byte message.
Stegodos, Black Wolf's Picture Encoder	Public Domain, Black Wolf	DOS	Requires third party screen capturing	LSB. The encoded image is displayed and must be	Multiple images formats since it use screen	Software is available through various web sources. Noticeable noise in most images.

			software to save the encoded image.	"captured" in a paint program before saving.	captures. Only supports 320x200 images with 256 colors.	
S-Tools	Shareware, Andy Brown a.brown@nexor.co.uk 28 Ashburn Drive Wetherby West Yorkshire LS22 5RD United Kingdom	Win		LSB. Color reduction then insert additional colors as necessary to cover LSBs without adversely impacting the image quality.	V4.0: GIF, BMP	Software is available through various web sources. V4.0 also supports S-tools has trouble recovering small messages (1-2 bytes). 3 byte+ messages are more reliable.
SureSign	Commercial, Signum Technologies http://www.signumtech.com/ signum@signumtech.com Signum Technologies Ltd. 2-6 St George's Business Park Alstone Lane Cheltenham Glos. GL51 8HF UK	Win, MAC	Photoshop Compatible image processing software. Works with Paint Shop Pro (shareware)	Pattern block encoding.	Any image that can be displayed in Paint Shop Pro, Photo Shop or compatible image processing programs and can be manipulated with image filters.	Watermark follows the image pattern. Signum SureSign's watermark logo is visible on the image.
SysCoP	Commercial, Fraunhofer Center for Research in Computer Graphics (CRCG) a non-profit computer graphics research group, Jian Zhao http://syscop.igd.fhg.de/ and http://www.crcg.edu/syscop/ Send email to syscop@igd.fhg.de if you have any question.	Sun Solaris, HP-UX, SGI IRIX, Win95/NT (Mac and Netscape plug-in are under development)			PPM, PGM, PBM, and with a conversion toolkit supports JPEG, GIF, and TIFF.	For still images, it reads PPM (PGM, PBM) formats, and uses a conversion toolkit to support JPEG, GIF, and TIFF formats. For motion data, Motion JPEG and MPEG-1 are supported. In 8-bit images, SysCop has a signature pattern, especially with images of lower unique colors, of like colors grouped in a range.
TigerMark (NEC) and Informix Datablade	Commercial, NEC		Requires use of Informix DBMS as core.	Discrete Cosine Transformation (DCT) or fast fourier transformation (FFT) with "secure spread spectrum."		TigerMark is NEC's watermarking tool which has been integrated with Informix Databalde technology. There is a software development kit (SDK) which provides access to the watermark capability without the requirement for Informix (under development?).
Visual Cryptography	Freeware, Jouko Holopainen	DOS		Generates postscript files of the first two input images. The hidden image is spread across the two carriers so if the carriers are overlapped, then the hidden image will be seen.	Severe degradation of container images.	"Visual cryptography", Moni Naor and Adi Shamir; Advances in Cryptology - EUROCRYPT '94, Lecture notes in Computer Science 950; Springer 1995

White Noise Storm (WNS)	Shareware, Ray Arachelian	DOS		Spread Spectrum, LSB	PCX	Degrades 8-bit images and may cause complete color shifts in 24-bit.

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
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
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
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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event