A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator

Pedram Hayati[1], Vidyasagar Potdar[2], and Elizabeth Chang[2]
1 Institute for Advanced Studies in Basic Science of Zanjan, Iran
WWW home page: http:// http://www.iasbs.ac.ir/students/pedram
2 Digital Ecosystems and Business Intelligence Institute, Curtin Business School, Curtin University of Technology, Perth, Australia
{Vidyasagar.Potdar, Elizabeth.Chang}@cbs.curtin.edu.au,
WWW home page: http://www.fit.cbs.curtin.edu.au/~potdarv

Abstract. In this paper we survey 111 different steganographic and steganalytic tools available in the market as freeware or shareware or for commercial sale. The main motivation for conducting this survey was to identify what steganographic tools are available on the Internet and which of those could be used by terrorist organization around the world. The following different categories of steganographic tools were studied – image steganography, audio and video steganography, text and database steganography, file system and hard disk steganography, executable files, and network steganography. This study has been conducted from a forensic investigators perspective to guide them with first hand information on available steganographic and steganalytic tools. The results from this initial study are presented in this paper, however we are now testing all these tools and the results from these tests would be published in the future.

1 Introduction

With the recent advances in Internet computing and its intrusion in our day to day life, the need for private and personal communication has increased. Privacy in digital communication is desired when confidential information is being shared between two entities via the computer communication. Existing technologies like cryptography offer a solution by scrambling the confidential information such that it cannot be read by anyone else except the intended recipient. However the issue with encryption is that the significance of the communication is highlighted because cryptographic data lacks the required logical sense and can be easily recognized.

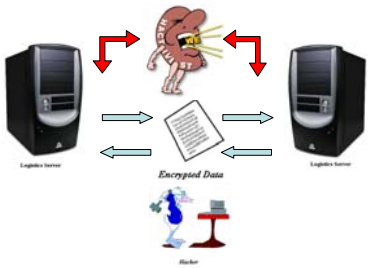

Figure 1a. Cryptography **Figure 1b.** Steganography

Such illegible data can attract undue attention from eavesdropper, which is a threat for private and confidential communication. Thus privacy and confidentially is lost by the nature of cryptographic solutions. This has caused concerns for those people who desire private and confidential communication.

In an attempt to address above security issue, information hiding techniques like *steganography* have shows some promising solutions. Steganographic communication is difficult to trace and hence it makes the job of the hacker difficult because the hacker now has to track all network communication rather than just encrypted communication. This steganographic feature increases the level of privacy and security by making the confidential communication invisible.

Steganography is a term derived from the Greek word *steganos*, which means "*covered writing*". It is an art and science of communicating information in a covert manner such that the existence of this communication is not detectable.

Figure 1a shows the limitations of conventional connection oriented security protocols for the problem of privacy in confidential communication. Two entities exchange secret information using encryption. This information can be eavesdropped, hence privacy and confidentiality is lost. Figure 1b shows the advantages of using Digital Steganography which can be used to address the issue raised in Figure 1a. Steganographic communication increases the level of privacy and confidentiality in digital communication by transmitting information in an invisible manner.

1.1 Steganographic Applications

Steganographic technique finds its main application in the field of *secret communication*. It can be used by intelligence agencies across the world to exchange highly confidential data in a covert manner e.g. a secret agent can hide a map of a terrorist camp in a photograph using image steganographic software and post it on a public discussion board or forum. An officer from the head office could download the photograph from the forum and easily recover the hidden map.

Apart from secret communication steganographic techniques can also be used for *secure* and *invisible storage* of confidential information. Confidential information like patents or trade secrets can be securely stored in steganographic hard disk partitions. Such partitions are invisible and can only be accessed by its owner. Even

the existence of such partition is not known to others. Without a proper file name and associated password no one can access the partition and the confidential information stored in it.

Steganographic techniques can also prevent a legitimate entity against *coercion* e.g. if trade secrets are encrypted and stored on hard disks they can be easily visible and a malicious user may coerce the legitimate user to disclose the same. However if a legitimate user relies on steganographic techniques, coercion can be avoided because the user may let the malicious entity to get hold of the machine to find the confidential information, since the information is invisible the malicious entity might end up loosing the battle.

1.2 Key Issues with Steganographic use

Steganographic applications are neutral; however if it is used in an inappropriate manner it can be a major concern e.g. if terrorists organizations use steganographic tools for secret communication, it would makes the job of the intelligence agencies very difficult to track down such communication. In an attempt to address this issue steganalysis techniques can be used.

Steganalysis is the art and science of detecting messages hidden using steganography. Once the presence of steganographic content is detected in a media e.g. images, audio, video, network packets etc. the infected media can be quarantined for further analysis or the steganographic content can be destroyed by tampering the infected media. These tools are very important for a forensic investigator because it gives them the power to analyze, detect and even destroy secret communication.

In this paper, we survey more than 100 different steganographic and steganalytic tools which can be used to hide (detect or destroy) secret information embedded in a number of digital media like image, audio, video, text, database, file system, hard disk, executable files and network packets. This survey has been conducted to help the digital forensic investigators in their analysis. The paper is structured in the following manner –

1. Section 2 outlines image steganographic tools.
2. Section 3 outlines audio steganographic tools.
3. Section 4 outlines video steganographic tools.
4. Section 5 outlines text steganographic tools.
5. Section 6 outlines file system steganographic tools.
6. Section 7 outlines hard disk steganographic tools.
7. Section 8 outlines other miscellaneous steganographic tools.
8. Section 9 concludes the paper with some future research directions.

2 Image Steganography Tools

In this category of steganographic tools we surveyed 14 different products open source products and 34 commercial products. These are shown in Table 1. For the open source products JPEG and BMP is the favorite choice as a cover medium as 9 products offer the functionality to embed in these image formats. The next popular

format is GIF, where F5, GifShuffle and Mandlesteg are useful. Wnstorm and dc-Steganograph embed information with PCX files whereas OutGuess and PGMStealth use PNG and PGM formats respectively. From all the 14 tools most of them embed information in spatial domain i.e. by replacing or changing pixel values, whereas dc-Steganograph, F5 and OutGuess embed in the Transform Domain i.e. by manipulating the transform domain coefficients. All these three tools modify the Discrete Cosine Transform (DCT) coefficients to embed the secret data.

Table 1. Image Steganographic Tools with Open Source Code

Image Steganographic Tools	JPEG	BMP	Others	Embedding Approach	Production
Blindside		Yes		SDS	Yes
Camera Shy	Yes			SDS	Yes
dc-Steganograph			PCX	TDS	
F5	Yes	Yes	GIF	TDS	Yes
Gif Shuffle			GIF	Change the order of the color map	Yes
Hide4PGP		Yes		SDS	Yes
JP Hide and Seek	Yes			SDS	Yes
Jsteg Jpeg	Yes			SDS	Yes
Mandelsteg			GIF	SDS	Yes
OutGuess	Yes		PNG	TDS	Yes
PGM Stealth			PGM		Yes
Steghide		Yes		SDS	Yes
wbStego		Yes		SDS	Yes
WnStorm			PCX		Yes

TDS - Transform Domain Steganography
SDS - Spatial Domain Steganography (LSB Replacement and LSB Matching)

In the freeware or shareware products the most popular cover image is BMP followed by JPEG, GIF, PNG, TGA, TIF, PPM, PCX and DIB. A total of 20 tools can embed in BMP images followed by 10 in JPEG and 9 in GIF. From the 34 tools 17 of them are in production i.e. the website was accessible and the latest version of the tool was available. This include Contraband Hell, Contraband, Crypto123, Dound, Gif it Up, Camouflage, Hide and Seek, InThePicture, Hermetic Stego, IBM DLS, Invisible Secrets, S-Tools, Jpegx, Info Stego, Syscop, StegMark, Steganos. Of this StegMark is of particular interest as it can embed in BMP, JPEG, GIF, PNG, TGA and TIF formats. From the 34 tools 8 are shareware, 10 are freeware and the remaining tools are either not in production or their license information was not available at the time of the survey.

Table 2. Image Steganographic Tools where Source Code is not available. Tools sorted according the license – shareware and freeware

Image Steganographic Tools	BMP	JPEG	GIF	PNG	TGA	Other	Production	License
Crypto123	Yes	Yes					Yes	S
Hermetic Stego	Yes						Yes	S
IBM DLS	Yes	Yes	Yes	Yes			Yes	S
Invisible Secrets	Yes	Yes		Yes			Yes	S
Info Stego	Yes	Yes	Yes				Yes	S
Syscop		Yes					Yes	S
StegMark	Yes	Yes	Yes	Yes	Yes	TIF	Yes	S
Cloak	Yes							S
Contraband Hell	Yes						Yes	F
Contraband	Yes						Yes	F
Dound	Yes						Yes	F
Gif it Up			Yes				Yes	F
Camouflage				Yes	Yes		Yes	F
Hide and Seek	Yes		Yes				Yes	F
InThePicture	Yes						Yes	F
S-Tools	Yes						Yes	F
Jpegx		Yes					Yes	F
Steganos	Yes					DIB	Yes	F
BMP Secrets	Yes							
DCT-Steg		Yes						
Digital Picture Envelope	Yes							
EikonAmark		Yes						
Empty Pic			Yes					
Encrypt Pic	Yes							
EzStego			Yes					
BMP Embed	Yes							
BMPTable	Yes							
StegoTif					Yes	TIF		
Hide Unhide						TIF		
In Plain View	Yes							
Invisible Encryption			Yes					
JK-PGS						PPM		
Scytale						PCX		
appendX		Yes	Yes	Yes				
Total	20	10	9	5	3	6	17	

S – Shareware License
F – Freeware License

3 Audio Steganography Tools

In this category of steganographic tools we surveyed 11 different products. These are shown in Table 3. There are 5 open source products which can be used for free while others are commercial or shareware programs with time limited functionality. Majority of the products hide data in WAV file format while three of those hide in MP3 format. Products like Hide4PGP and Steganos provide steganographic capability for other file formats like VOC where as StegMark and StegHide embed secret data in MIDI and AU format respectively.

Table 3. Audio Steganographic Tools sorted according the License – Shareware, Open Source and Commercial

Audio Steganographic Tools	MP3	WAV	Others	Production	License
Info Stego	Yes			Yes	Shareware
ScramDisk		Yes		Yes	Shareware
MP3Stego	Yes			Yes	Open Source
StegoWav		Yes		Yes	Open Source
Hide4PGP	Yes		VOC	Yes	Open Source
Steghide		Yes	AU	Yes	Open Source
S-Tool		Yes		Yes	Open Source
Invisible Secrets		Yes		Yes	Commercial
Paranoid			Yes	Yes	Commercial
Steganos		Yes	VOC	Yes	Commercial

Invisible Secrets is a commercial grade product which can embed in several different cover mediums like images, audio and text. All the 10 tools are in production and the latest version was available during the survey.

4 Text Steganography Tools

Within the text steganographic area we survey a total of 15 tools, which included freeware, shareware, open source and commercial license products; these are shown in Table 4.

Majority of these products embedded secret information within plain text however with a few exceptions like wbStego, Steganos, Invisible Secrets which embedded in HTML pages. The robustness of these tools needs to tested further; it is not sure at this moment if they can sustain HTML formatting done by HTML editors like Dreamweaver etc. wbStego also embed messages in PDF document and by far is the only one product that can offer steganographic capability in PDF format. There are many other tools that embed visible watermark in PDF but not steganographic content. Most of the text steganographic tools are freeware or open source except Steganos, Invisible Secrets and PGPn123.

Table 4. Text Steganographic Tools sorted according to License – Shareware, Freeware, Open Source and Commercial

Text Steganographic Tools	Plain Text	Other	Source Code	License	Production
PGPn123		Yes		Shareware	Yes
Nicetext	Yes		Yes	Open Source	Yes
Snow	Yes		Yes	Open Source	Yes
Texto	Yes		Yes	Open Source	Yes
Sam's Big Play Maker	Yes		Yes	Open Source	Yes
Steganosaurus	Yes		Yes	Open Source	Yes
FFEncode	Yes			Open Source	Yes
Mimic	Yes			Open Source	Yes
wbStego	Yes	HTML, PDF	Yes	Open Source	Yes
Spam Mimic	Yes			Not Specified	Yes
Secret Space	Yes			Not Specified	Yes
WitnesSoft	Yes	Yes		No longer in production	
MergeStreams		Hides excel file in word		Freeware	Yes
Steganos	Yes	HTML		Commercial	Yes
Invisible Secrets		HTML		Commercial	Yes

5 File System & Hard Disk Steganography Tools

Within the file system and hard disk steganographic area we survey a total of 19 tools, which included freeware, shareware and open source products. We did not find any commercial grade license products. All these tools are listed in Table 5.

Majority of these products embedded secret information in the *File System* and *Windows Registry*. Products like Magic Folders, Dark Files, bProtected 2000, BuryBury, StegFS, Folder Guard Jr, Dmagic, BackYard use the file system for embedding whereas Disk Hide and Drive Hider relied on the Windows registry. Easy File & Folder Protector and Anahtar are quite unique as the former embeds in the VXD driver, Windows Kernel whereas the latter uses 3.5-inch diskette. Anahtar is not in production any more since floppies are out of date now, but it would be interesting to see if USB thumb drives could be used instead. None of the products provide any source code as all of then are either freeware or shareware but not open source. Snow disk is also a good program which embeds secret information in the disk space although no longer in production any more.

Table 5. File System Steganographic Tools according to License – Shareware, Freeware and Open Source

File System Steganographic Tools	Location of Embedding	Source Code	License	Production
Disk Hide	Windows Registry	No		No
Drive Hider	Windows Registry	No		No
Easy File & Folder Protector	VXD driver, Windows Kernel	No	Shareware	Yes
Invisible Files 2000	Hard Disk	No	Shareware	Yes
Magic Folders	File System	No	Shareware	Yes
Dark Files	File system	No	Shareware	Yes
bProtected 2000	File system	No	Shareware	Yes
BuryBury	File system	No	Shareware	Yes
StegFS	File system	Yes	Open Source	Yes
Folder Guard Jr	File System	No	Freeware	Yes
Dmagic	File System	No	Freeware	Yes
BackYard	File System	No		No
Snowdisk	Disk space			No
Masker	Any file (Image, Text, Audio, Video)	No	Shareware	Yes
Anahtar	3.5-inch diskette	No		No
Hide Folders		No	Shareware	Yes
Hidden		No		No
Paranoid		No		No
Diskhide		No		No

6 Other Miscellaneous Steganography Tools

We categorized the following tools in the miscellaneous categories because they were very unique steganographic tools. gzSteg embedded secret information within the gz files. S-Mail and Hydan embedded information within executables and Dynamic link libraries (dll files). Hydan specifically embedded in the program binaries. Hiderman, StegMark, InfoSteg embedded in image, audio, video files. Finally KPK File was quite unique as it embedded information within Word files as well as BMP files.

Table 6. Miscellaneous Steganographic Tools

Miscellaneous Steganographic Tools	Cover Media	Source Code	License
GZSteg	.gz files	Yes	
InfoStego	Image, audio, video		Shareware
KPK File	Word, BMP		Shareware
S-Mail	.exe and .dll files		
Hiderman	Many different media		Shareware
StegMark	Image, audio, video		
Steghide	JPEG, BMP, WAV, AU	Yes	
S-Tools	BMP, GIF, WAV	Not sure	
Hydan	Program Binaries	Yes	Open Source
Covert.tcp	TCP/IP Packets	Yes	Open Source

7 Steganalytic Tools

In this section we discuss some of the steganalytic tools that we surveyed as shown in Table 7.

Table 7. List of Steganalytic Tools

Hard Disk Steganographic Tools	Tools Analyzed	Detection Approach	Extraction Approach	Destruction Approach
2Mosaic	Removes stego content from any images			Break Apart
StirMark Benchmark	Removes stego content from any images			Resample
Phototile	Removes stego content from any images			Break Apart
Steganography Analyzer Real-Time Scanner	Analyzes Network Packets	Signature		
StegBreak	Jsteg-shell, JPhide, and Outguess 0.13b		Dictionary	
StegDetect	Jsteg, JPhide, Invisible Secrets, Outguess 01.3b, F5, appendX, Camouflage	Statistical		
StegSpy	Hiderman, JPHIde and Seek, Masker, JPegX, Invisible Secrets			
Stego-Suite	Detects Stego Image and Audio file		Dictionary	

A total of 8 steganalytic tools were studied. 2Mosaic, StirMark Benchmark and PhotoTitle are the three steganalytic tools that can remove steganographic content from any image. This is achieved by destroying secret message by two techniques – break apart and resample. StegDetect, StegBreak, StegSpy identify information embedded via the following tools - Jsteg-shell, JPhide, and Outguess 0.13b, Invisible Secrets, F5, appendX, Camouflage, Hiderman, JPHIde and Seek, Masker, JPegX, Steganography Analyzer Real-Time Scanner is the best available steganalysis software in the market at the moment, which can analyze all the network traffic to look for traces of steganographic communication.

11 Discussion & Conclusion

In this paper we surveyed 111 different steganographic and steganalytic tools, which were available in the market. Although this is not a very comprehensive survey it does provide some insights on the tools that can be easily accessed on the Internet. Of the 111 tools surveyed, only 8 were steganalytic tools and that too do not detect all the steganographic signatures. A total of 30 open source, 27 freeware, 22 shareware, and 8 commercial products are available in the market. The remaining products did not have enough information to decide the category of user license. This survey can be very valuable for forensic investigators as well as security agencies across the world that is constantly analyzing network traffic to detect steganographic communication. In the future we would test all these tools to develop robust real time steganalytic software that can be used as a steganographic firewall to prevent confidential information from entering and exiting a secure network.

12 Reference

1. Investigator's Guide to Steganography by Greg Kipper, ISBN:0849324335, Auerbach Publications © 2004
2. Chen Ming Zhang Ru Niu Xinxin Yang Yixian, “Analysis of Current Steganography Tools: Classifications & Features”, in International Conference on Intelligent Information Hiding and Multimedia pp. 384-387, 2006
3. BlindSide http://www.cs.bath.ac.uk/~jpc/blindside
4. Camera Shy http://hacktivismo.com/projects/index.php
5. dc-Steganograph http://members.tripod.com/~Nikola_Injac/stegano/
6. F5 http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html
7. Gif Shuffle http://www.darkside.com.au/gifshuffle
8. Hide4PGP http://www.heinz-repp.onlinehome.de/Hide4PGP.htm
9. JP Hide and Seek http://linux01.gwdg.de/~alatham/stego.html
10. Jsteg Jpeg http://www.nic.funet.fi/pub/crypt/steganography/
11. Mandelsteg ftp://ftp.funet.fi/pub/crypt/steganography/
12. OutGuess http://www.outguess.org/download.php
13. PGM Stealth ftp://ftp.funet.fi/pub/crypt/steganography/
14. Steghide http://steghide.sourceforge.net/

15. wbStego http://members.xoom.com/wbailer/wbstego/index.htm
16. WnStorm http://ftp.univie.ac.at/security/crypt/steganography
17. Crypto123 http://www.kellysoftware.com/software/Crypto123.asp
18. Hermetic Stego http://www.hermetic.ch/hst/hst.htm
19. IBM DLS http://www.research.ibm.com/image_apps/commerce.html
20. Invisible Secrets http://www.neo-bytesolutions.com/
21. Info Stego http://www.antiy.net/infostego/
22. Syscop http://www.mediasec.com/html/en/products_services/syscop.htm
23. StegMark http://www.datamark-tech.com/index.htm
24. Cloak http://www.softslist.com/download-9-5-16609.html
25. Contraband Hell http://jthz.com/puter/
26. Contraband http://come.to/us
27. Dound http://evidence-eliminators.co.uk/dound.htm
28. Gif it Up http://digitalforensics.champlain.edu/download/Gif-it-up.exe
29. Camouflage http://camouflage.unfiction.com/
30. Hide and Seek ftp://ftp.funet.fi/pub/crypt/steganography/hdsk41.zip
31. InThePicture http://www.guillermito2.net/stegano/inthepicture/index.html
32. S-Tools ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/
33. Jpegx http://www.leetupload.com/dbindex2/index.php?dir=Win32/
34. Steganos http://www.steganography.com/
35. BMP Secrets http://www.pworlds.com/products/bmp-secrets.phtml
36. StegoTif http://www.geocities.com/SiliconValley/9210
37. ScramDisk http://www.scramdisk.clara.net/
38. MP3Stego http://www.petitcolas.net/fabien/steganography/mp3stego/index.html
39. StegoWav http://www.geocities.com/SiliconValley/9210/
40. Hide4PGP http://www.heinz-repp.onlinehome.de/Hide4PGP.htm
41. Paranoid ftp://ftp.hacktic.nl/pub/crypto/macintosh/
42. PGPn123 http://www.securityfocus.com/tools/1435
43. Nicetext http://www.nicetext.com/
44. Snow http://www.darkside.com.au/snow/
45. Texto ftp://ftp.funet.fi/pub/crypt/steganography
46. Sam's Big Play Maker http://www.scramdisk.clara.net/play/playmaker.html
47. Steganosaurus http://www.fourmilab.ch/stego/
48. FFEncode http://www.burks.de/stegano/ffencode.html
49. Mimic http://www.nic.funet.fi/pub/crypt/old/mimic/Mimic-Manual.txt
50. wbStego http://members.xoom.com/wbailer/wbstego/index.htm
51. Spam Mimic http://www.spammimic.com/
52. Secret Space http://www.soft14.com/Utilities_and_Hardware/Security_and_Encryption/SecretSpace_1388_Review.html
53. MergeStreams http://www.ntkernel.com/w&p.php?id=23
54. Easy File & Folder Protector http://www.softstack.com/fileprotpro.html
55. Invisible Files 2000 http://www.downloadstock.info/Invisible-Files-2000-Pro-60_de10671.html
56. Magic Folders http://www.pc-magic.com/
57. Dark Files http://www.redsofts.com/soft/494/36867/Dark_Files.html

58. bProtected 2000 http://www.clasys.com/b_protected.html
59. BuryBury http://www.winsite.com/bin/Info?1000000034624
60. StegFS http://www.mcdonald.org.uk/StegFS/
61. Folder Guard Jr http://www.winability.com/folderguard/
62. Dmagic ftp://ftp.elf.stuba.sk/pub/pc/security
63. Masker http://www.softpuls.com/masker/
64. Hide Folders http://www.fspro.net/
65. Paranoid(File System Steganography) http://sac-ftp.externet.hu/security10.html
66. GZSteg http://www.funet.fi/pub/crypt/steganography/
67. KPK File http://www.kpkfile.com/
68. Hiderman http://www.alnini.com/Hiderman/dt-8782.html
69. Hydan http://www.crazyboy.com/hydan/
70. Covert.tcp http://www.firstmonday.org/issues/issue2_5/rowland/
71. 2Mosaic http://www.petitcolas.net/fabien/watermarking/2mosaic/index.html
72. StirMark Benchmark http://www.petitcolas.net/fabien/watermarking/stirmark/index.html
73. Phototile http://www.pcadvisor.co.uk/downloads/index.cfm?categoryID=1490&itemID=7895
74. Steganography Analyzer Real-Time Scanner http://www.sarc-wv.com/stegalyzerrts.aspx
75. StegBreak http://www.outguess.org/download.php
76. StegDetect http://www.outguess.org/detection.php
77. StegSpy http://www.spy-hunter.com/
78. Stego-Suite http://www.000.shoppingcartsplus.com/catalog/item/4170630/4050552.htm
79. http://www.infosec-technologies.com/StegToolandWatermarkingTable.pdf