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

James C. Judge
GSEC Version 1.2f
Steganography: Past, Present, Future

Abstract
Steganography (a rough Greek translation of the term Steganography is secret writing) has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. This paper will explore steganography from its earliest instances through potential future application.

Past
Johannes Trithemius (1462-1516) was a German Abbot. His writing, "Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa" is ostensibly a work describing methods to communicate with spirits(1). A very rough translation (with apologies to my Latin instructors) of this Latin title is: "Steganography: the art through which writing is hidden requiring recovery by the minds of men." Published as a trilogy in Latin, the first two parts of his works are apparently some of the first books on cryptology describing methods to hide messages in writing. The third part of the trilogy is outwardly a book on occult astrology. The third book contains a number of tables containing numbers.

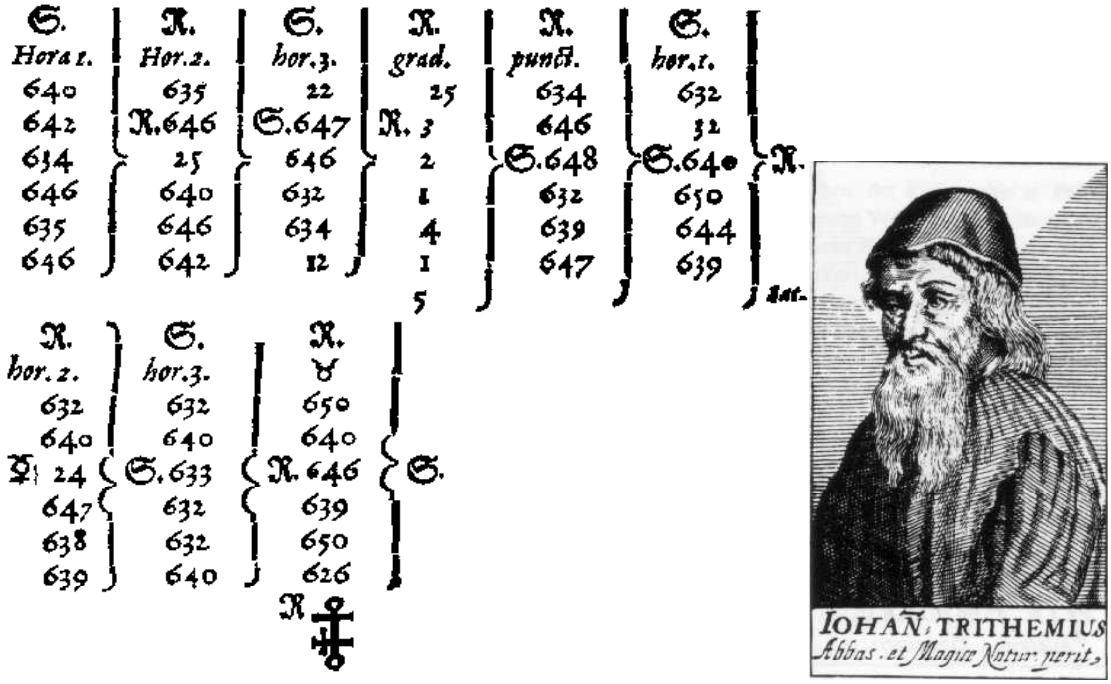


Figure 1 (left). Example of table included in Book 3 of "Steganographia" (1)

Figure 2: (right) Johannes Trithemius

Two researchers, Dr. Thomas Ernst and Dr Jim Reeds (2) were convinced that the third tome

© SANS Institute 2000 - 2005 Author retains full rights.

contained hidden code. Dr Ernst, while a graduate student at the University of Pittsburgh published a 200 page paper, but it was written in German, published in 1996 in a Dutch Journal, *Daphnis*, and attracted little attention. Dr. Reeds, a mathematician at AT&T Labs independently began delving into this tome. As he searched for information on Trithemius' works, he discovered Dr. Ernst paper.

These two researchers discovered in relatively short order, that there were hidden messages contained in the third book. The messages contained in the tables were of minor interest. One message contained the Latin equivalent of "The quick brown fox jumps over the lazy dog." A second message was "The bearer of this letter is a rogue and a thief. Guard yourself against him. He wants to do something to you." And, the third message was the beginning of the 23rd Psalm.

Although "Steganographia" is the work that we derive the term steganography from, it is certainly not the first example of hidden writing. There are examples from history that serve to illustrate the desire to hide messages or some type of intelligence from others. Mary Queen of Scots (3, 4) used a combination of cryptography and steganography to hide letters. Her letters were hidden in the bunghole of a beer barrel, which freely passed in and out of her prison.

Other uses of steganography weren't limited to normal writing materials. One may consider the huge geoglyphs of the Nazca in Peru to be a form of steganography. The geoglyphs are obviously open to view, yet many of the images were not detected until viewed from the air. Human vectors include the efforts of Histaiacus in the 5th century BC. Histaiacus shaved the head of a messenger, wrote a note encouraging Aristagoras of Miletus to revolt against the king of Persia. After the messenger's hair grew back, the messenger was dispatched with the message. Obviously, this message wasn't especially time constrained. Another human vector example includes writing messages on silk, which would then be compressed into a ball and covered with wax. The messenger would swallow the wax ball. The method of retrieval was not described in my source.

In 480 BC a Greek by the name of Demaratus sent a message to the Spartans warning of a pending invasion by Xerxes. Heroclotus described the method used by Demaratus (4):

> *"As the danger of discovery was great, there was only one way in which he could contrive to get the message through: this was by scraping the wax off a pair of wooden folding tables, writing on the wood underneath what Xerxes intended to do, and then covering the message over with the wax again. In this way the tablets, being apparently blank, would cause no trouble with the guards along the road…."*

References to other early works on steganography and cryptology may be found at a web page posted by Fabien A. P. Petitcolas (5).

In more recent history, several stenographic methods were used during World War II (6). Microdots developed by the Nazis are essentially microfilm chips created at high magnification (usually over 200X). These microfilm chips are the size of periods on a standard typewriter. These dots could contain pages of information, drawings, etc. The Nazis also employed invisible inks and null ciphers. One of the most noted null cipher messages sent by a Nazi spy follows:

© SANS Institute 2000 - 2005 Author retains full rights.

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Using the second letter from each word, the following message appears:

Pershing sails from NY June I

Other suspected methods of passing secret messages ranged from the arrangement of dials on wristwatches to chess games being played via the mail.

One steganographic method employed by the United States Marines during WW II, was the use of Navajo "codetalkers." While the codetalkers employed a simplistic cryptographic technique, the messages were sent in clear text.

Another example of steganography involves the use of the Cardano grill (7). This device, named after its inventor Girolama Cardano, can be as simple as a piece of paper with holes cut in it. When the grill is laid over printed text, the intended message can be retrieved. In techniques related to the Cardano grill, classical steganography techniques include pin punctures in text (e.g. newspapers), and overwriting printed text with pencil.

There is evidence that prior to the Civil War, there was a method of providing secret messages to slaves to aid in their escape (8). By using various patterns in quilts, which were commonly hung from windowsills to dry, messages were passed to slaves guiding them in their quest for freedom. An example of one such quit pattern is the Bear Paw symbol.



Figure 3: The Bear Paw quilt symbol. Advice to follow the bear tracks over the mountain (8).

More recent uses of stenographic techniques involved a photograph of the captured crew of the U.S.S. Pueblo where the crewmembers spelled the word "snowjob" using various hand positions.

Finally, during the Viet Nam era, there were instances where captured members of the U.S. Armed Forces would use various hand gestures during photo ops, often only to have these gestures airbrushed out by the media (9). Other techniques employed were using the eyelids to blink words in Morse code (such as torture). Prisoners of the infamous Hanoi Hilton used a "tap code" to communicate with each other. The code was based on a five by five matrix with each letter being assigned a tap sequence based on this matrix. Spaces (pauses) between characters were twice as long as the spaces in that letters code.

© SANS Institute 2000 - 2005 Author retains full rights.

	1	2	3	4	5
1	**A . .**	**B . ..**	**C, K . …**	**D . ….**	**E . …..**
2	**F .. .**	**G .. ..**	**H .. …**	**I .. ….**	**J .. …..**
3	**L … .**	**M … ..**	**N … …**	**O … ….**	**P … …..**
4	**Q … .**	**R …. ..**	**S …. …**	**T …. ….**	**U …. …..**
5	**V ….. .**	**W ….. ..**	**X ….. …**	**Y ….. ….**	**Z ….. …..**

Figure 4: The 5x5 tap code used by Armed Forces prisoners in Viet Nam

Present

Currently, the emphasis has been on various forms of digital steganography. Commonly there are a number of digital technologies that the community is concerned with, namely text files, still images, movie images, and audio. It is beyond the scope of this paper to go into the details of steganographic methods, suffice it to say that there are two primary groups. "Image Domain tools encompass bit-wise methods that apply least significant bit (LSB) insertion and noise manipulation… The transform domain group of tools include those that involve manipulation of algorithms and image transforms such as discrete cosine transformation (DCT) [CKSL96], [KRZ94] and wavelet transformation [XBA97]."(10) There is a good website one can visit to access a large variety of steganography tools, www.stegoarchive.com. This website offers tools for DOS, Windows, Java, Macintosh, OS/2, Unix/OpenBSD/Linux, and Amiga. In addition, the website offers a CD which includes over 80 steganography tools at a reasonable price.

After the events of September 11, 2001, there was immediate concern voiced regarding the possible use of steganography by the al Queda network. Initially, there were reports that hidden messages might be located in images located on XXX rated sex web sites. Following up on this, a group at the University of Michigan (11) began scanning images located on various sites such as eBay auctions. After scanning over two millions images, the researchers reported back that they had not found any suspect images. The article in USA Today didn't indicate if the researchers actually scanned any images located on XXX web sites.

Beyond the concerns of hidden messages in images, there has been additional concern voiced regarding the television broadcast of bin Laden. Remembering that steganography is hardly the sole property of digital technology, there is the possibility that there could have been hidden messages in the audio portion of the broadcasts, or even in the background of the televised images.

Are terrorist organizations hiding information using steganographic technology? At this point, there doesn't seem to be any conclusive evidence, at least available to the general public.

Are ANY organizations hiding information using stenographic technology? Yes, there are many organizations using stenographic technology to hide information. In seeking to determine an answer to this question while doing searches on the web, a web site posting belonging to the

© SANS Institute 2000 - 2005 Author retains full rights.

Ulster Loyalist Volunteer Force (www.ulisnet.com). was found. This web site posted information on steganography. To quote from the first paragraph:

> *"In an ideal world we would all be able to openly send encrypted mail or files to each other with no fear of reprisals. However there are often cases when this is not possible, either because you are working for a company that does not allow encrypted mail or perhaps the local government does not approve of encrypted communication (a reality in some parts of the world). This is where steganography can come into play."* (12)

The majority of other organizations using steganographic techniques involve individuals or corporations interested in protecting intellectual property. Software piracy is only one aspect of this concern, according to the Business Software Alliance:

> *"A study published in June 1998, by the Business Software Alliance, another industry trade group, estimated that the software industryloses more than $11.4 billion a year worldwide to piracy. Although the group estimates that over 25 percent of all software applications inthe U.S. are pirated, the problem is far worse in developing areas of he world such as Southeast Asia and Eastern Europe, where piracyrates are said to hover as high as 95 percent or more of all applications in use."* (13)

Other interests who are making use of steganographic techniques are involved in the application of digital watermarks. Using a variety of techniques, images, music, movies can be imprinted with digital watermarks. Watermarks are available in several configurations: fragile vs. robust, visible vs. invisible, and private vs. public. Fragile watermarks are those that are easily destroyed by image manipulation, and find utilization in image authentication systems (14) There are a number of commercial software applications and services from firms such as: Alpha-Tec, Cognicity, Giovanni, Digmarc, , Signum Technologies, SysCoP, , and Verance Digital (15) to name a few. On the testing side, StirMark(16) and unZign (17) are freeware programs for testing the robustness of watermarks.

Digital watermarking is not limited to use in what we typically think of as digital media. Xerox has developed a digital watermark system for printed images (18) This technique involves generating a half tone screen with a key image. When this screen is positioned such that it is superimposed over the original image, with a slight offset, the key image will appear. This technique appears to be hardened to the point that only degrading the image significantly will result in a loss of the key image.

Stochastic screens are analogous to the half-tone screens normally used in printing processes, but the dots that make up the stochastic screen are not regularly spaced, and are generally much smaller (on the order of 21 microns typically) (19). One could liken the stochastic screen to the algorithms used on digital images, with the exception that the screen would be considered firmware, thus the robustness of this technique.

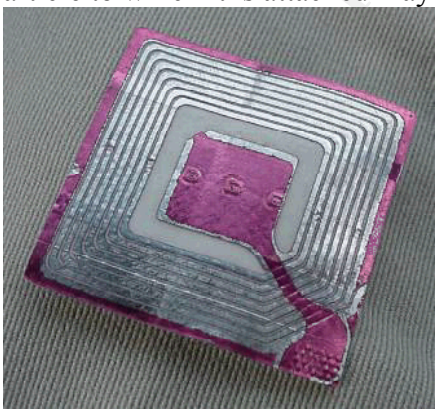
© SANS Institute 2000 - 2005 Author retains full rights.


Figure 5: Original image (left), image overlaid with stochastic screen to reveal watermark (right) (18).

As one would expect, as the science of digital watermarking progresses, there is equal progress in the sophistication of attack methods. Generally stated, attacks can be categorized as (20): Additive Noise, Filtering, Cropping, Compression, Rotation and Scaling, Statistical Averaging, Multiple Watermarking, and Attacks at Other Levels.

Although we are currently more interested in digital steganography, other forms of steganography are currently in use today, primarily in physical security measures. The venerable microdots pioneered by the Nazis are currently being marketed as a simple technique that can be used to mark equipment. Equipment marked with microdots aids in identification in the case of theft. There are a number of firms producing microdots for this purpose.

The author would contend that the Electronic Article Surveillance (EAS) tags, so prevalent on merchandise today are a form of steganography. The tag is obvious, and unless the message contained in the tag is deleted, it gives a clear message when anyone tries to take an article past the storefront scanning mechanism. To paraphrase, "this article has not been deactivated and the article to which it is attached may be stolen."


Figure 6: The invisible message side of a Swept RF EAS tag (21). The front likely has a message such as "Thanks for Shopping with us."

© SANS Institute 2000 - 2005 Author retains full rights.

While in the search for steganographic examples, a few other items deserve at least a cursory glance. For example, hidden messages on phonograph records. There have been any number of reports, that various phonograph records, when played backwards may contain messages (usually satanic messages) (22). While many of these claims have been proven erroneous, there is that possibility that today's technology could produce messages using this simple technique.

Another steganographic technique involves the use of subliminal suggestion. While in the 1950's, the American public was obsessed with subliminal messages being show on theater screens (e.g. "go to the snackbar), there was significant research being done by the Central Intelligence Agency (CIA) (23). Subliminal suggestions may range from advertisements (either blatant suggestions, to images/messages perceived by various groups as having a particular meaning) to modern subliminal suggestion programs such as those available from InnerTalk (24).

While not classified as a steganographic technique, the potential for hiding information in PhotoTiled pictures is a possibility. There is an excellent web site hosted by William Leigh Hunt, wherein a program is presented that will create images from other pictures (25).

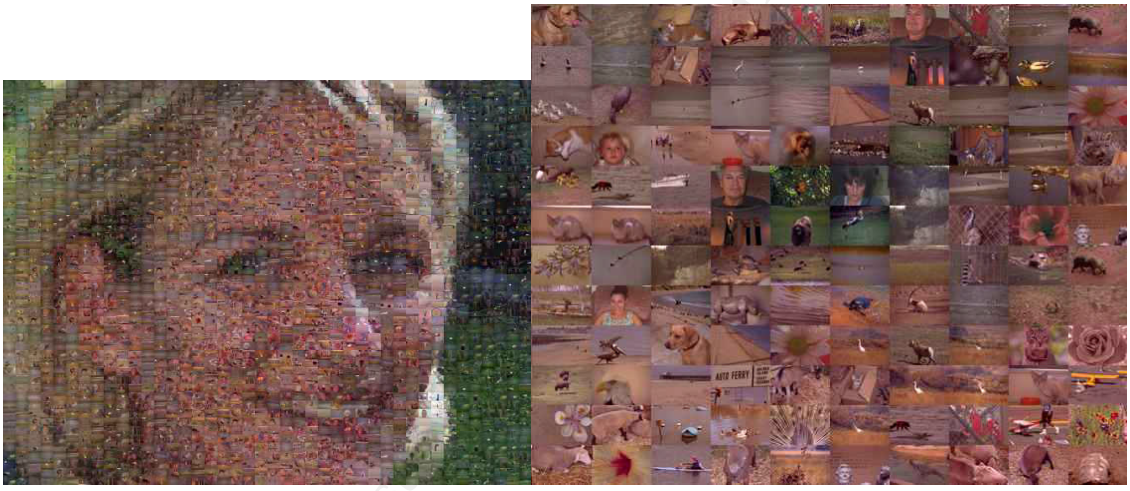


Figure 7: (left) PhotoTiled image, (right) expanded view of left eye (25).

While this application provides some striking examples of manipulation of collections of photographs to create an entirely new picture, one could always argue that there is the possibility that hidden information could be contained in the output. The application itself, PhotoTile, is a highly rated shareware program available at:
http://www.prismaticsoftware.com/Phototile/PhotoTile.html

A short history of PhotoTiled pictures is available at:
http://home.earthlink.net/~wlhunt/History/History.html

© SANS Institute 2000 - 2005 Author retains full rights.

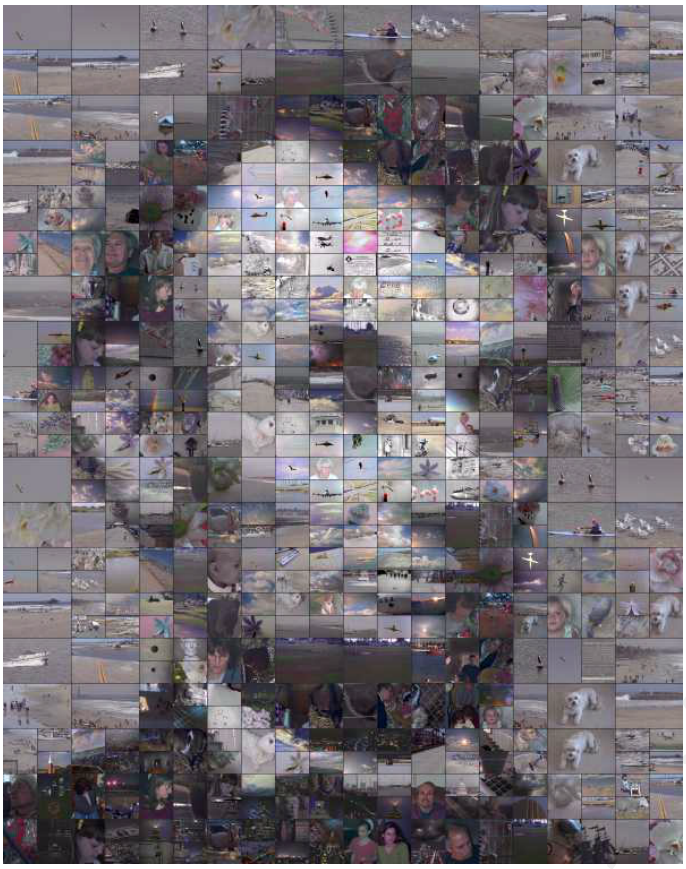


Figure 8. A PhotoTiled image of Lincoln (25).

Taking a slightly different direction, applications that convert image files to "ASCII art" should also be considered as potential steganography applications. An example of a conversion from a full color image to an ASCII text image follows:



Figure 9: An ascii text file generated from a full color image (original image from Mad Magazine, DC Comics) (26)

© SANS Institute 2000 - 2005 Author retains full rights.

On viewing the ASCII text file (converted to .jpg here for convenience), it is apparent that while the text file itself might not have a hidden file, an industrious individual could arrange certain letters in the visible text file itself to have certain meanings.

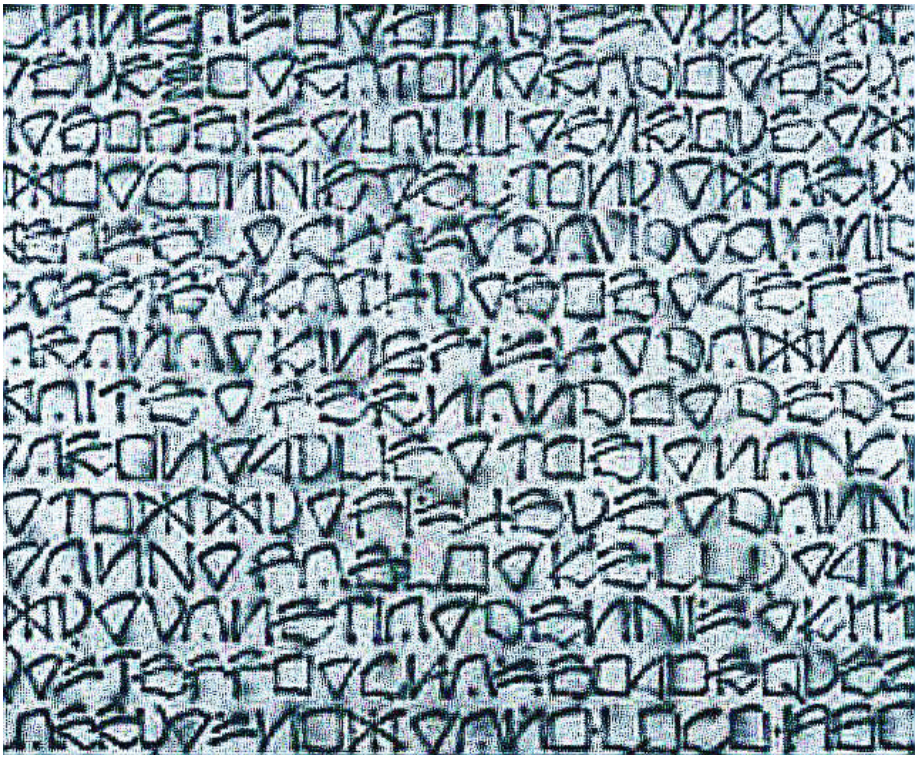
Another digital format that may escape notice is the venerable animated GIF format. Normal steganalysis of GIF formats wouldn't necessarily indicate any hidden messages while it would be trivial to hide a message using this format.

Without going into detail, other areas that could conceivably be employed to hide messages are:

- Holography technology
- Infrared (e.g. programmable IR hand controls for computers (27)
- Pagers
- Colored glasses that filter all but intended wavelengths to make hidden messages visible
- Ink, magnetic, thermochromic, photochromic
- DNA message hiding (28)
- Jargon speak
- "Blank" areas on hard drives, floppies, etc.
- HTML code

This list should not be considered exhaustive, there are numerous other possibilities.

One last bit of steganotrivia before we return to "serious steganography." If one viewed the following image at an art gallery, it might not be obvious that this is another work of steganography.



© SANS Institute 2000 - 2005 Author retains full rights.

Figure 10. Charles "Chaz" Bojorquez, *Placa, Rollcall*.(29)
The figure above (Figure 10.) actually contains a list of the author's (Chaz Bojorquez) friends. The author used a modified alphabet, and created his own punctuation. (29)

What is the point of this endless listing of possible steganographic carriers. The point is that steganographic content can easily exist in more than .jpg or .gif images located on the internet. In fact, the Center for Innovative Computer Applications at Indiana University (30) lists 141 common image file formats. Now we can proceed with the more common steganographic techniques that are available in the present.

Textual steganography.
"British Prime Minister Margaret Thatcher became so irritated at press leaks of cabinet documents that she had the word processors programmed to encode their identity in the word spacing of documents, so that disloyal ministers could be traced." (31) This type of steganography is available due to the precision with which text can be printed on modern printers (from 300 to 1600dpi and up) . In addition, there are a number of techniques that can be employed in textual steganography (32).

- Open space methods
  - Line shift coding
  - Word shifting coding
- Syntactic methods
- Semantic methods
- Feature coding

There are several applications/services that will encode messages into plaintext that do not rely on line or word shifting, however they may produce results that would invite investigation. A demonstration of textual steganography is available at http://ip-service.com/cgi-bin/stego.pl This demo illustrates the use of an application called Texto.
In this demo application, the original message was:
"Place your message here.
This is my message y'all."

The encoded message was:
"The raindrop stupidly kicks to the silly cafe. I close usable shoes near the plastic goofy bathroom. Sometimes, sandwichs vend behind closed signs, unless they're blue. Never dream dully while you're opening through a powerful tag. We bimonthly place around solid cold fields. While dogs surprisingly lean, the dryers often roll on the red smogs. Other new quiet bushs will type eerily with dogs. Going below a planet with a tag is often tall. Have a idle envelope. The wierd cloud rarely kicks. Tell the wooden exit it's quietly kicking against a coffee. Many cold closed elbows will slide surprisingly to games. To be usable or red will cause plastic dogs to twist. Will you think the solid bright cases? Let's kick near the sly forests, but don't grasp."

Yet another on-line application is provided by Spam Mimic (http://www.spammimic.com)

© SANS Institute 2000 - 2005 Author retains full rights.

Using the following text as the message to be hidden:
"The dog howls at noon"

The resulting output text was:
Dear Friend ; Thank-you for your interest in our publication . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club ! This mail is being sent in compliance with Senate bill 1627 ; Title 6 , Section 303 ! This is NOT unsolicited bulk mail . Why work for somebody else when you can become rich inside 44 DAYS . Have you ever noticed how long the line-ups are at bank machines and people are much more likely to BUY with a credit card than cash ! Well, now is your chance to capitalize on this . We will help you use credit cards on your website and use credit cards on your website ! You are guaranteed to succeed because we take all the risk ! But don't believe us . Mrs Simpson of Arkansas tried us and says "I've been poor and I've been rich - rich is better" ! We are licensed to operate in all states ! For God's sake, order now . Sign up a friend and your friend will be rich too ! Warmest regards . Dear Salaryman , This letter was specially selected to be sent to you ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1624 , Title 3 , Section 304 ! This is not a get rich scheme . Why work for somebody else when you can become rich as few as 53 weeks ! Have you ever noticed people will do almost anything to avoid mailing their bills plus people love convenience ! Well, now is your chance to capitalize on this ! WE will help YOU use credit cards on your website & deliver goods right to the customer's doorstep ! You are guaranteed to succeed because we take all the risk . But don't believe us ! Prof Ames who resides in North Dakota tried us and says "Now I'm rich many more things are possible" . We assure you that we operate within all applicable laws ! We beseech you - act now ! Sign up a friend and you'll get a discount of 20%! Cheers

The resultant output does appear as a standard spam message, and would likely raise less suspicion than the previous example. The problem is that we have gone from five words to 395 words to hide the message.

In examining the WBStego application (33) the text portion of the application was tested, with poor results. The following screen dumps illustrate the original text, the text after hiding a message, and the text as it would appear after printing. The text feature of WBStego relies on the individual to keep the text in ascii .txt format. When the ascii file is loaded into Microsoft Word, the special characters inserted in the ascii file become readily apparent.

© SANS Institute 2000 - 2005 Author retains full rights.

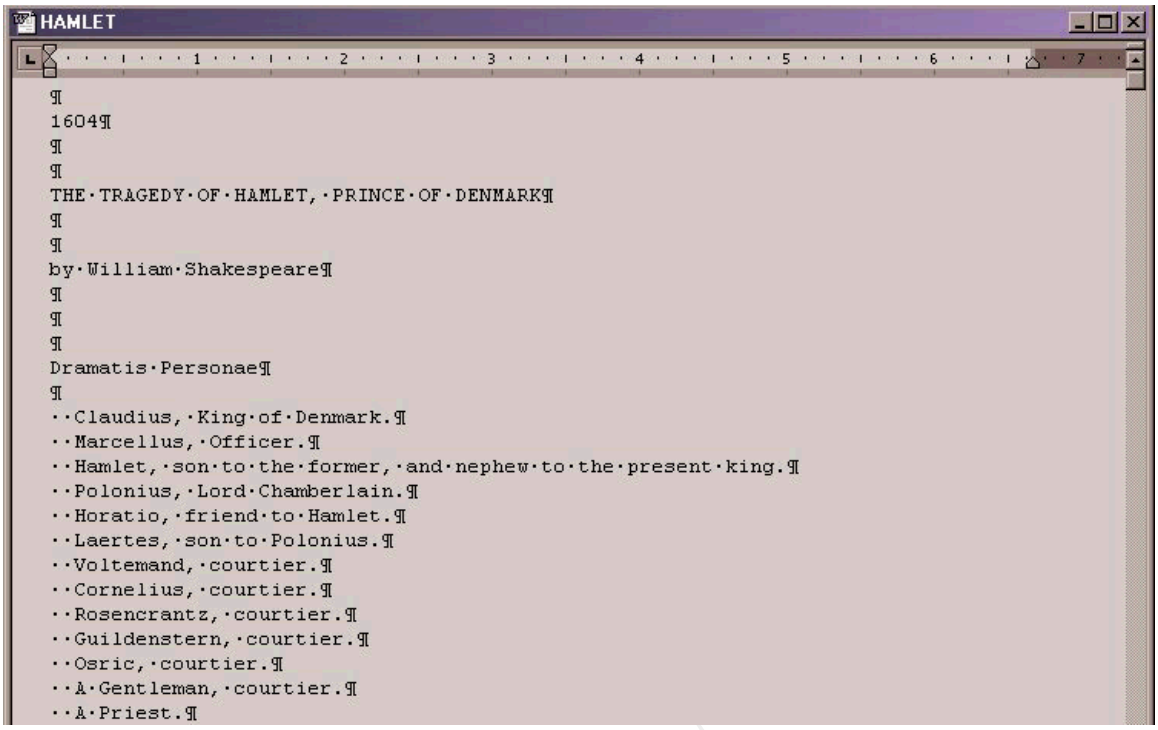


Figure 11: Hamlet.txt in MS Word showing special characters.

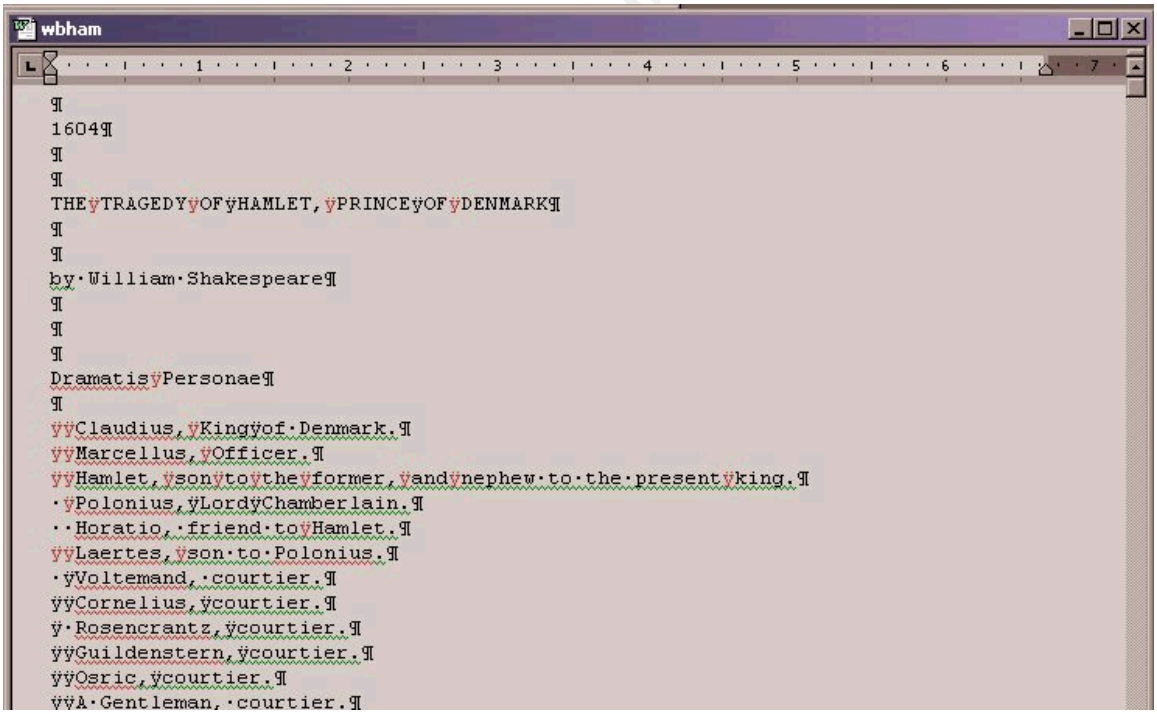


Figure 12: Wbham.txt in MS Word showing special characters – note changes from the previous figure.

© SANS Institute 2000 - 2005 Author retains full rights.

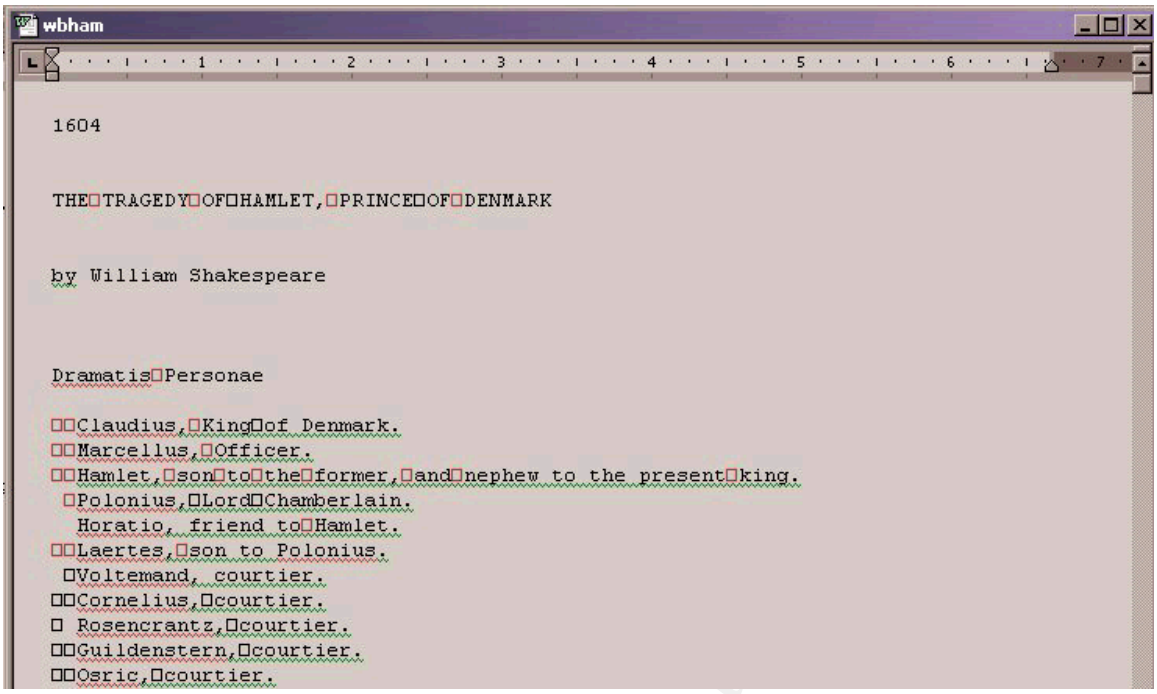


Figure 13: Wbham.txt when printed displays boxes for unprintable characters.

There are a number of other textual steganography applications. Just to mention a few of them:

- TextHide – a commercial application which relies on rephrasing original text, includes RSA encryption, Twofish encryption, long key lengths. For more information see: www.compris.com/TextHide/en/Overview.html
- Snow whitespace steganogaphy. Freeware for personal use, relies on trailing whitespace in text, and uses the ICE encryption algorithm. For more information see:
- Lexical Steganography – An excellent paper and "Tyrannosaurux Lex", an implementation of lexical steganography are available at: www.imsa.edu/~keithw/tlex
- NICETEXT – a demo package of this application, which converts files into "pseudo-natural-language text" is available at: www.ctgi.net/nicetext/

Sound/Movie File Steganography

For those interested in hiding files in .mp3 files, there appears to be a paucity of software available. The only .mp3 software that was found readily available on the web was an application called mp3stego. The author notes that "The hiding process takes place at the heart of the Layer III encoding process name in the *inner_loop*." (34) The web site indicated in the references offers access to the full C code and binaries.

There are a number of applications that offer information hiding in various formats such as .wav, .avi, .au, and .mpeg formats. The applications range from those that actually hide data, often encrypted, within the file, to those that simply attach hidden information to the end of a file such as Camouflage (35).

Still Image Steganography

There are a relatively large number of applications for still image steganography. Andrew S.

© SANS Institute 2000 - 2005 Author retains full rights.

Tanenbaum (the author of the Minix operating system) has posted one interesting and impressive demo. The demo provides a copy of S-Tools v4 (available at www.stegoarchive.com) by Andy Brown (, and two bitmap (.bmp) images at 1024x768 pixels (original photography by Andrew S. Tannenbaum). (36)



Figure 14: Bitmap (.bmp)files from Tanenbaum demo. The left images is the original, the right image contains hidden text (36)

From a visual perspective, both of the images appear to be identical, and the file sizes are only two bytes different, 2,359,352 for the original and 2,359,350 for the file with hidden text. While hex dumps of the images were quite different, histograms of both files were remarkably similar. There is an obvious change on the far right portion of the histograms, and a less obvious change if one overlays the two involving the larger of the peaks on both pictures.

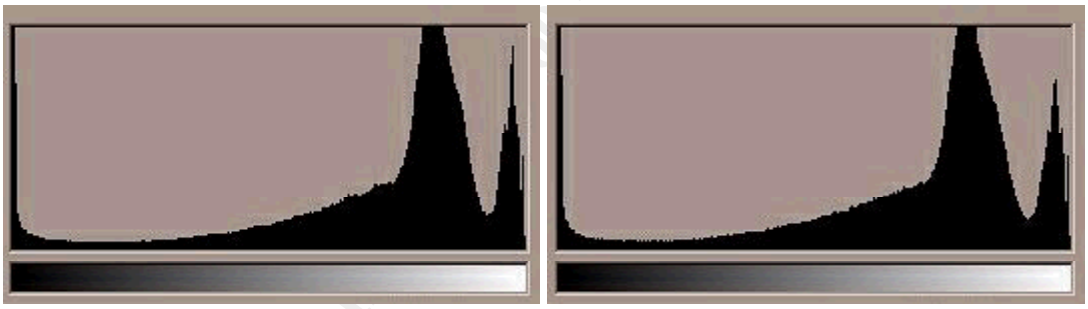


Figure 15: Histograms of the "zebra" images. Histogram on the left from the original, histogram on the right from the image containing hidden text.

The image that contains the hidden text reveals that the contents are the entire e-texts of:

- Hamlet 201,788 bytes
- Julius_Caesar 115,805 bytes
- King_Lear 176,952 bytes
- Macbeth 103,609 bytes
- Merchant 120,927 bytes
- Notice 15,810 bytes

For a grand total of 734,891 bytes hidden in the original bitmap.

Returning to WBStego after the textual steganography test, a pure white image was created (1024

© SANS Institute 2000 - 2005 Author retains full rights.

x 768 pixels) as a test bed. In addition, a bitmap image from the web was tested. The pure white image was created with the idea that if there were any artifacts created by embedding text, they might be visible on a white image. This proved not to be the case. After embedding a short message of 114 words, there were no discernable artifacts in either of the images, nor were the files sizes changed. The only tip off that there was any amiss in the images took a hex dump of the images.

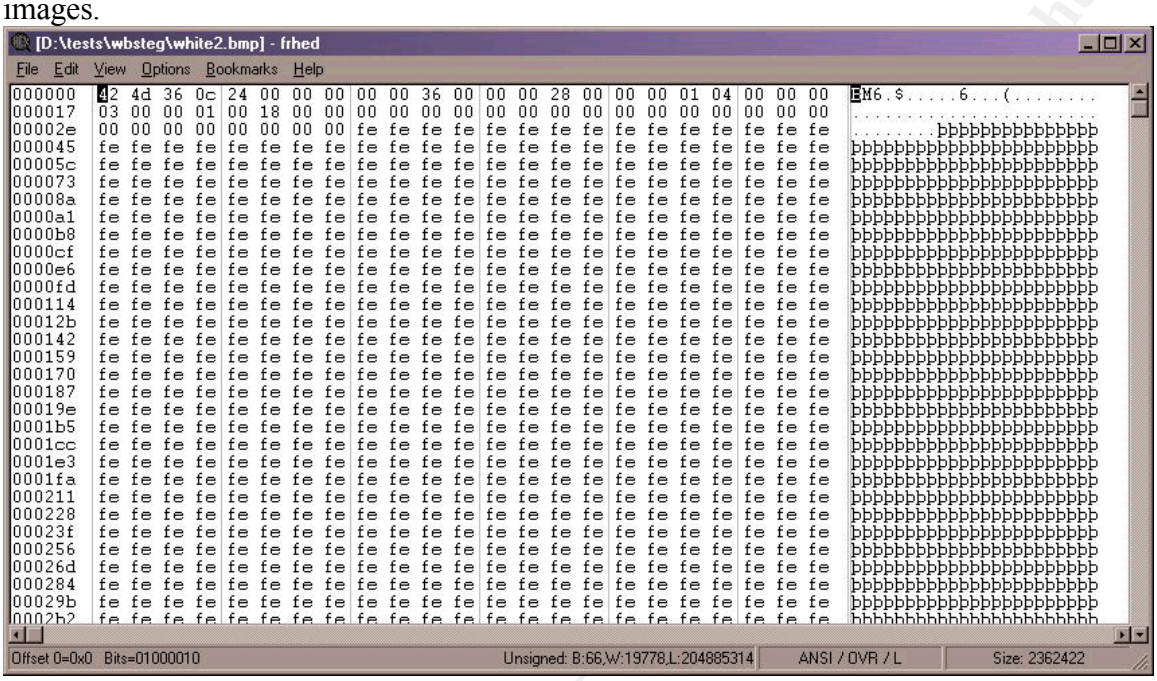


Figure 16: Hex dump of pure white bitmap image.

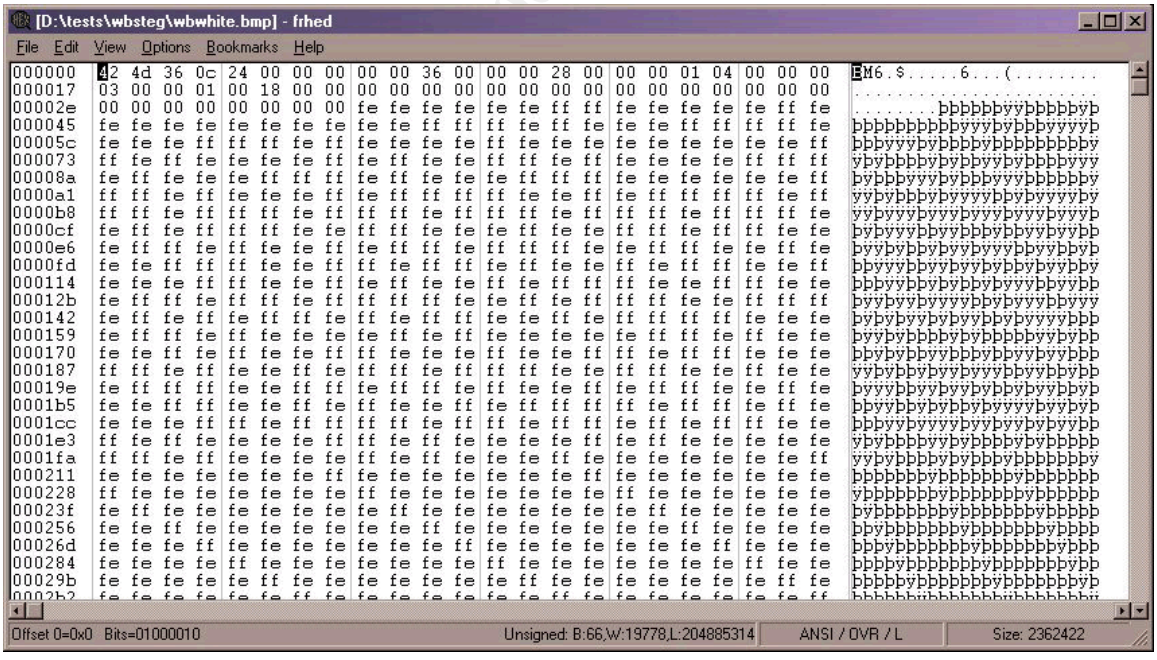


Figure 17: Hex dump of white image with text embedded

The hex tool used in comparing these images was "frhed, the free hex editor" available from http://homepages.tu-darmstadt.de/~rkibria/

© SANS Institute 2000 - 2005 Author retains full rights.

Similar testing was done on the white bitmap image after converting it to a JPEG image. The tool used in this example was "JSteg Shell Version 2.0" available at: http://www.tiac.net/users/korejwa/jsteg.htm A short message of 187 bytes was again inserted into the white .jpg image. In this test there were no artifacts discernable on the image, however there were other clues that this image had changed. The file size with the embedded image increased by 244 bytes, and examination of the image indicated that it now consisted of two colors (the original indicated one color). In addition, there was a change in the histogram.



Figure 18: Histogram of pure white image with text embedded. Note the two peaks at the far right side of the histogram indicating two colors.

Finally, to complete the set of simple experiments, an application called "Gifshuffle," available at: http://www.darkside.com.au/gifshuffle/ was used on a .gif image. Again the original pure white bitmap image was converted to a .gif image. After embedding a short message of 187 bytes, the file sizes did not change (2,402 bytes). In checking the number of colors, both images indicated that there was one color in the image. The only indication that the image had changed was using the hex dump tool (frhed) mentioned earlier.

While these tests didn't break any new ground, it did serve to illustrate that there are some very good steganography applications available, and some that are less trustworthy. In terms of commercial software, there is an application called "Invisible Secrets 3" available from www.neobytesolutions.com/invsecr that offers a tool to hide documents in JPEG, .png, .bmp, HTML, and .wav files. This application includes "strong cryptography" and a "shredder" to destroy files completely.

Other forms of Steganography

What are the possibilities of hiding data in other media? If one takes the time to analyze different approaches, one may observe that the possible applications are nearly limitless. For example, consider the TCP carrier itself. The forward of a paper presented by Rowland (37) states:

> "The TCP/IP protocol suite has a number of weaknesses that allow an attacker to leverage techniques in the form of covert channels to surreptitiously pass data in otherwise benign packets. This paper attempts to illustrate these weaknesses in both theoretical and practical examples. "

In an article (38) "TV sounds can hide machine instructions" it is reported that a firm (Scientific

© SANS Institute 2000 - 2005 Author retains full rights.

Generics, Harston near Cambridge UK) is patenting a technique which they call "intrasonics." The firm has developed a technique of hiding control signals in television broadcast sound. The technique will be used to control toys to help maintain children's interest in television shows. Aside from this author's personal feelings about creating another generation of TV kids, there obviously exists the opportunity for other types of signals to be hidden in various types of broadcast.

Hiding information in ISDN transmissions is another area that presents possible information hiding. The potential of using the Global System for Mobile communications (GSM) channel during ISDN video conferencing has been discussed (39). In addition, there is a paper describing a steganography program called "DigiStilz" which hides data in the LSB of ISDN telephone conversations (40).

The information above is certainly not exhaustive. The more one looks for areas where messages could be hidden, the more one realizes that the possibilities are nearly limitless whether the medium be digital, analog or crayon on paper.

Steganalysis (Detection of Steganography)

"Researchers: No secret bin Laden messages on sites" was a headline from Reuters recently (41). The article describes the scouring of over 2 million images on popular web sites for signs of steganography with a search of USENET currently underway. Those interested in the progress of the USENET scans might check at: http://www.citi.umich.edu/u/provos/stego/usenet.php and at http://www.citi.umich.edu/u/provos/stego/faq.html
for information on the entire project.

The discovery of digital files that may contain secret messages may be broadly divided into two types, images and textual. In the matter of images, one method is "creating a statistical profile of compressed data files that make up natural, or undisturbed images, then checking a given image against the profile." (42) Another method is to use a tool such as "Stegdetect." Developed by Niels Provos (43) This application scans JPEG images for four different schemes. Detection of real time steganography (e.g. ISDN or TCP/IP steganographic techniques) will require either real time steganalysis, or capture of packets for later analysis. When one considered the number of transactions that are completed, just on an hourly basis worldwide, one can easily become overwhelmed.

In the instance of detecting secret messages in textual material, Kevin Q Brown (44) developed a set of measures that should be considered in 1993:

- Letter Frequency
- Word Frequency
- Compressibility
- Grammar, style, and readability
- Semantic continuity and logic
- Message context

© SANS Institute 2000 - 2005 Author retains full rights.

- Obvious
- Other measures

Considering the variety of methods by which textual steganography could be delivered (post, telegraph, fax, etc.) textual steganography again appears to be an extremely broad category that could easily overwhelm steganalysis efforts.

Steganalysis, or attacks on steganographic "carriers" can also be broadly split into two categories: discovery of the message, or destruction of the message. While discovery of a message may be the most desirable outcome, it is also the most difficult. Many of the steganographic techniques yield rather fragile "carriers" which are susceptible to destruction with trivial effort.

In reviewing the literature on steganalysis, it becomes quickly apparent that it bears a striking parallel to the general category of computer security and efforts to exploit vulnerabilities. As one camp develops a technique that is relatively secure, the opposite camp immediately develops opposing techniques, sort of an intellectual ping-pong match.

Future Steganography

Why steganography? Who needs steganography? What are the uses for steganography? Where can one use steganography?

According to Richard E. Smith (a data security expert), he doesn't "see many practical uses for steganography because it only works as long as nobody expects you to use it." (45) The author respectfully takes exception to this statement. Initially after reading this statement, the myth that Charles H. Duell, Commissioner of Patents in 1899 had declared that the Patent Office should be closed because everything that could possibly be invented had already been invented came to mind. Perhaps the computer security community should give up on endless patches, security applications, etc because they only work if nobody expects that they are in use. To quote Dale Carnegie, "Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all."

There are ongoing studies to harden steganographic images from steganalysis (46). In his paper, "Defending Against Statistical Steganalysis," Provos presents new methods which would allow one to select a file in which a message might be safely hidden and resistant to standard statistical analysis.

Legitimate Use

Steganographic techniques have obvious uses, some legitimate, some less so, and some are likely illegal. The business case for protection of property, real and intellectual is strong. The watermarking of digital media is constantly improving, primarily in an attempt to provide hardened watermarks or proof of ownership.

Individuals or organizations may decide to place personal/private/sensitive information in

© SANS Institute 2000 - 2005 Author retains full rights.

steganographic carriers. Admittedly, there are usually better ways to manage this task. One can liken these applications to the use of a deadbolt lock on a door. The deadbolt will keep honest people honest, but those determined to break and enter can simply break a window and gain entry. With advances in steganography, it is possible that this medium could serve as a relatively secure storage/transmission method.

Illegal Use

Other uses for steganography range from the trivial to the abhorrent. There are claims (47) that child pornography may be lurking inside innocent image or sound files. While this is entirely possible, a search on the internet for confirmation of this claim was unsuccessful.

An annual report on High Technology crime (48) lists nine common types of computer crime:

- Criminal communications
- Fraud
- Hacking
- Electronic payments
- Gambling and pornography
- Harassment
- Intellectual property offenses
- Viruses
- Pedophilia

In examining this list, one can identify several of these areas where steganography could be used, especially considering the broad term "criminal communications." If one includes steganographic techniques other than computer related, the potential grows even more.

In terms of computer security, there are some areas to be aware of. One area that has potential far ranging implications is "A protocol that uses steganography to circumvent network level censorship." (49) The author, Bennet Haselton, the coordinator of Peacefire.org (an organization that "opposes censorship that targets Internet users under 18…") describes a protocol that is "undetectable to censors."

Finally, computer warfare should be addressed. In his Masters Thesis, Jordan T. Cochran, Captain, USAF investigates steganographic virus attacks (50). He finds that "The results indicate that steganography tools are not conducive to be sole attack weapons. However, the tools combined with other applications could be used to automatically extract the hidden information with minimal user intervention."

In another Masters Thesis, Dale A. Lathrop, Captain, USAF also investigates the possibility of virus attacks using steganographic techniques (51). He finds that "The results of this research indicate that the use of a separate engine followed by an HTML-based electronic mail message containing a photographic image with a steganographically embedded virus or other payload is a vulnerable attack if implemented without the proper environment variables in place." He further finds that "it still requires human intervention to initiate the virus attack."

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

For those who find themselves as first responders in electronic crimes, the "Electronic Crime Scene Investigation, A Guide for First Responders" written in July 2001 (52) is freely available on the internet. This publication offers basic, sound advice in the preservation and investigation of electronic crime scenes, and does give mention to steganography.

Conclusion

Steganography, in its multitude of forms, has been in use literally for thousands of years. It appears to have been utilized primarily and most effectively in time of war or civil strife. It would appear that based on the variety of forms that steganographic messages can take that there could be steganographic content on the internet. Location of some forms of steganographic content would require techniques other than statistical profiling not the least of which could be visual examination (refer to Figure 10) notwithstanding the ability to encrypt.

While practical uses of steganography, with the exception of watermarking, seems to be relatively limited with the abundance of other techniques freely available, it will likely fill a niche for some activities. Consider that hiding an object in plain sight, recall Edgar Allen Poe's "The Purloined Letter", can on occasion be the best option.

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

References:

(1)Trithemius, Johannes, "Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa" URL: www.esotericarchives.com/tritheim/stegano.htm

(2) Kolata, Gina, "A Mystery Unraveled, Twice" URL: cryptome.unicast.org/cryptome022401/tri.crack.htm

(3) "The Science of Secrecy, Steganography" URL: www.channel4.com/plus/secrecy/page1b.html

(4) Singh, Simon, "The Cipher of Mary Queen of Scots" URL: www.arch.columbia.edu/DDL/cad/A4513/S2001/r9/

(5) Petitcolas, Fabien A. P., "History of Steganography" URL: www.cl.cam.ac.uk/~fapp2/steganography/history.html

(6) Counterintelligence News and Developments, Volume 2, June 1998 "Hidden in Plain Sight-Steganography" URL:www.nacic.gov/pubs/news/1998/jun98.htm

(7)"Classical Steganography, Cardano Grille" URL: http://library.thinkquest.org/27993/crypto/steg/classic1.shtml

(8) Home and Garden Television, "Clues in the Quilts" URL: http://www.hgtv.com/HGTV/project/0,1158,CRHO_project_7305,00.html

(9) The Pink, Blue, and White Pages "What the Returning POWs Said About Missing Men" URL: www.miafacts.org/pages.htm

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

(11) USA Today, 11/03/2001 "Researchers: No secret bin Laden messages on sites" URL: http://www.usatoday.com/life/cyber/tech/2001/10/17/bin-laden-site.htm

(12) Ulster Loyalist Information Services "Steganography" URL: www.ulisnet.com/cfs_steno.htm

(13) Young, Brad, "Digital Piracy: Theft in the Modern Age" URL: http://biz.howstuffworks.com/by-digital-piracy.htm?printable=1

(14) Lin, Eugene T. and Delp, Edward J. "A Review of Fragile Watermarks" URL: http://citeseer.nj.nec.com/cache/papers/cs/14065/ftp:zSzzSzskynet.ecn.purdue.eduzSzpubzSzdistzSzdelpzSzacm99zSzpaper.pdf/lin99review.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

(15) WebRef, "Watermarks" URL:
http://www.webreference.com/multimedia/watermarks.html

(16) Petitcolas, Fabien A. P. "Stirmark 3.1" URL:
http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/

(17) Stegoarchive.com "Steganography Software" URL: http://www.StegoArchive.com/

(18) XRCE TeXnology Showroom "Digital watermarking in printed images: Stochastic halftone screen design" Fact Sheet, URL:
http://www.xrce.xerox.com/showroom/fs/stochas.pdf

(19) Ostrofsky, Steven, "What Dot to Plot" URL:
http://www.naa.org/technews/tn951112/p12dot.html

(20) Gonzalez, Fernando Perez, and Hernandez, Juan R. "A Tutorial On Digital Watermarking" URL:
http://www.gts.tsc.uvigo.es/~wmark/carnahan99.pdf

(21) Howstuffworks.com "How Anti-shoplifting Devices Work" URL:
http://www.howstuffworks.com/anti-shoplifting-device.htm/printable

(22) Oates, David and Albrecht, Greg "Backward Satanic Messages in Rock 'n Roll" URL:
http://www.reversespeech.com/btv3n4.shtml

(23) Gafford, Richard, "The Operational Potential of Subliminal Perception" URL:
http://www.parascope.com/ds/articles/ciasubliminaldoc.htm

(24) InnerTalk®: Technology "Advancing Your Mind Power" URL:
http://www.innertalk.com/

(25) Hunt, William Leigh "PhotoTiled Pictures Homepage" URL:
http://home.earthlink.net/~wlhunt/

(26) Mathews, Jonathan "AscGen, Beta 1.2, Copyright1999-2001" URL:
http://go.to.ascgen

(27) Keyspan "Digital Media Remote" URL:
http://www.keyspan.com/products/usb/remote/

(28) Petersen, Ivars "Data in Hiding" URL:
http://home.att.net/~mathtrek/muse0101.htm

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

© SANS Institute 2000 - 2005 Author retains full rights.

(29) Smithsonian American Art Museum ""Hidden" Letters" URL:
http://nmaa-ryder.si.edu/education/kids/cappy/14cactivity2.html

(30) Center for Innovative Computer Applications, "Image File Formats List" URL:
http://www.cica.indiana.edu/graphics/image.formats.html

(31) Anderson, Ross "Stretching the Limits of Steganography" URL:
www.cl.cam.ac.uk/ftp/users/rja14/stegan.ps.gz

(32) Braynov Svet, "Secure Sockets Level, Steganography" URL:
www.cs.buffalo.edu/~sbraynov/lectures/lecture6_pdf.pdf

(33) Bailer, Werner "wbStego Steganography Tool Website" URL:
http://wbstego.wbailer.com/

(34) Petitcolas, Fabien A. P. "mp3stego" URL:
www.cl.cam.ac.uk/~fapp2/steganography/mp3stego

(35) CamouflageSoftware.com "Camouflage" URL:
http://www.camouflagesoftware.com/

(36) Tannenbaum, Andrew S. "Steganography Demo for Modern Operating Systems", 2nd ed.
URL: www.cs.vu.nl/~ast/books/mos2/zebras.html

(37) Rowland, Craig H. "Covert Channels in the TCP/IP Suite" URL:
http://www.firstmonday.dk/issues/issue2_5/rowland/

(38) Fox, Barry, NewScientist.com, "TV sounds can hide machine instructions" URL:
http://www.futuretalk.org/01/quarter3/09021348.html

(39) Petricek, Vaclav "Information Hiding and covert channels" URL:
http://www.kolej.mff.cuni.cz/~vpet4339/work/covertalk/doc/ih-wds.pdf

(40) Johnson and Johnson Technology Consultants, LLC "Information Hiding – An Annotated Bibliography" URL:http://www.jjtc.com/Security/sbib01.htm

(41) USA Today, San Francisco, Reuters "Researchers: No secret bin Laden messages on sites"
URL: www.usatoday.com/life/cyber/tech/2001/10/17/bin-laden-site.htm

(42) Patch, Kimberly "Statistics sniff out secrets" URL:
www.cs.dartmouth.edu/~farid/press/trn01/trn01.html

(43) Provos, Neils "Steganography Detection with Stegdetect" URL:
www.outguess.org/detection.php

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

© SANS Institute 2000 - 2005 Author retains full rights.

(44) Brown, Kevin Q. "Steganography and Steganalysis"
http://cypherpunks.venona.com/date/1993/05/msg00420.html

(45) Gupta, Milon, EURESCOM "Steganography is more than a tool for spies" URL:
http://www.eurescom.de/message/messageSep2001/stegano.asp

(46) Provos, Niels, "Defending Against Statistical Steganalysis" URL:
www.citi.umich.edu/u/provos/stego

(47) Astrowsky, Brad H., "Steganography: Hidden Images, A New Challenge in the Fight Against Child Porn" URL http://www.antichildporn.org/steganog.html

(48) The High Technology Crime Advisory Committee "High Technology Crime in California" URL: http://www.ocjp.ca.gov/publications/pub_htk1.pdf

(49) Haselton, Bennett, "A Protocol that uses steganography to circumvent network level censorship" URL: www.defcon.org/html/defcon-8-post.html

(50) Cochtan, Jordan T. Captain, USAF, "Steganographic Computer Warfare" URL:
http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2000/afit-gcs-eng-00m-03.htm

(51) Lathrop, Dale A. Captain, USAF, "Viral Computer Warfare Via Activation Engine Employing Steganography" URL:
:http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2000/afit-gcs-eng-00m-14.htm

(52) , U.S. Department of Justice , "Electronic Crime Scene Investigation, A Guide for First Responders" URL:
http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Additional Reading

In addition to the works cited in this paper, there are a number of excellent papers available on the internet for those interested in the study of Steganography. A short list follows:

Steganography and Digital Watermarking: a global view.
Matteo Fortini
www-lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/ fortini/project.pdf

Steganography and Steganalysis
http://cypherpunks.venona.com/date/1993/05/msg00420.html

Recovering Watermarks from Images
Zoran Duric, Neil F. Johnson, Sushil Jajodia
http://ise.gmu.edu/techrep/1999/99_04_jajodia.pdf

An Introduction to Watermark Recovery from Images
Neil F. Johnson
http://www.jjtc.com/pub/nfjidr99.pdf

Electronic Marking and Identification Techniques to Discourage Document Copying, J.Brassil, S. Low, N. Maxemchuk, L. O'Gorman
http://citeseer.nj.nec.com/cache/papers2/cs/1079/ftp:zSzzSzftp.research.att.comzSzdistzSzbrassilzSzinfocom94.pdf/brassil94electronic.pdf

A New Paradigm Hidden in Steganography
Ira S. Moskowitz, Garth E. Longdon, LiWu Chang
http://chacs.nrl.navy.mil/publications/CHACS/2000/2000moskowitz-stego.pdf

One-Time Hash Steganography
Natori Shin
http://naomi.is.s.u-tokyo.ac.jp/~natori/papers/ihw99.html

Digital Steganography for Information Security
Anthony T.S. Ho, Sui-Chung Tam, Siong-Chai Tan, Lian-Tek Yap, Kok-Beng Neo, Sim-Peng Thia
http://www.datamark-tech.com/publications/steganography.pdf

Lexical Steganography Through Adaptive Modulation of the Word Choice Hash
Keith Winstein
http://www.imsa.edu/~keithw/tlex/

Steganography for a Low Bit-Rate Wavelet Based Image Coder
S. Areepongsa, Y F. Syed, N. Kaewkammenerd, K. R. Rao
http://www-ee.uta.edu/dip/paper/icip_2000.pdf

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

© SANS Institute 2000 - 2005 Author retains full rights.

Wavelet-based digital image watermarking
Houng-Jyh Mike Wang, Po-Chyi Su, C. C. Jao Kuo
http://epubs.osa.org/oearchive/pdf/7081.pdf

A Review of Data Hiding in Digital Images
Eugene T. Lin, Edward J. Delp
http://citeseer.nj.nec.com/cache/papers/cs/1313/ftp:zSzzSzskynet.ecn.purdue.eduzSzpubzSzdistzSzdelpzSzpics99-stegozSzpaper.pdf/lin99review.pdf

Surmounting the Effects of Lossy Compression on Steganography
Daniel L. Currie, III, Cynthia E. Irvine
http://citeseer.nj.nec.com/cache/papers/cs/346/ftp:zSzzSztaurus.cs.nps.navy.milzSzpubzSzirvinezSznissc96.pdf/currie96surmounting.pdf

On The Limits of Steganography
Ross J. Anderson, Fabien A. P. Petitcolas
http://www.cl.cam.ac.uk/~fapp2/publications/jsac98-limsteg.pdf

Steganography – a Cryptographic Layer
Vlad Rabinovich
http://www.rit.edu/~vxr8205/crypto2/cryptopaper.html

A Secure Robust Image Steganographic Model
Yeuan-Kuen Lee, Ling-Hwei Chen
http://debut.cis.nctu.edu.tw/~yklee/Personal/ISC2000.pdf

Applications of Data Hiding in Digital Images
Jiri Fridrich
http://citeseer.nj.nec.com/cache/papers/cs/500/http:zSzzSzssie.binghamton.eduzSz~jirifzSzResearchzSzispacs98.pdf/fridrich98application.pdf

Spread Spectrum Image Steganography
Lisa M. Marvel, Charles G. Broncelet, Jr., Charles T. Retter
http://citeseer.nj.nec.com/cache/papers/cs/19508/http:zSzzSzdebut.cis.nctu.edu.twzSz~ykleezSzResearchzSzDataHidingzSzREFzSzSSIS.pdf/marvel99spread.pdf

A High Capcity Image Steganographic Model
Yeuan-Kuen Lee, Ling-Hwei Chen
http://citeseer.nj.nec.com/cache/papers/cs/17792/http:zSzzSzdebut.cis.nctu.edu.twzSz~ykleezSzPersonalzSzHCISM-IEE2000.pdf/lee00high.pdf

Steganalysis of Images Created Using Current Steganography Software
Neil F. Johnson, Sushil Jajodia

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

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.jjtc.com/ihws98/jjgmu.html

Detecting Steganographic Content on the Internet
Neils Provos, Peter Honeyman
http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

Secure and Invisible Data Hiding in 2-Color Images
Yu-Chee Tseng, Hsiang-Kuang Pan
http://www.ieee-infocom.org/2001/paper/20.pdf

Hidden in Plain Sight-Steganography
Counterintelligence News & Developments
http://www.nacic.gov/pubs/news/1998/jun98.htm

and finally, an excellent annotated bibliography:

Information Hiding – An Annotated bibiography
Ross J. Anderson, Fabien A. P Petitcolas
http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/Annotated_Bibliography.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.