

Steganography

Neil F. Johnson

Introduction

Steganography conceals the fact that a message is being sent. It is a method akin to covert channels, spread spectrum communication and invisible inks which adds another step in security. A message in ciphertext may arouse suspicion while an invisible message will not.

This paper introduces steganography by explaining what it is, providing a brief history with illustrations of some methods for implementing steganography, and comparing available software providing steganographic services. Though the forms are many, the focus of the software evaluation in this paper is on the use of images in steganography. Section 2 will define steganography, provide a brief history, and explain various methods of steganography. Section 3 will review several software applications that provide steganographic services and mention the approaches taken. Section 4 will conclude with a brief discussion of the implications of steganographic technology. Section 5 will list the resources used in researching this topic and additional readings for those interested in more in-depth understanding of steganography.

Steganography

The word steganography literally means covered writing as derived from Greek. It includes a vast array of methods of secret communications that conceal the very existence of the message. Among these methods are invisible inks, microdots, character arrangement (other than the cryptographic methods of permutation and substitution), digital signatures, covert channels and spread-spectrum communications.

Steganography is the art of concealing the existence of information within seemingly innocuous carriers. Steganography can be viewed as akin to cryptography. Both have been used throughout recorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not [JDJ01].

David Kahn places steganography and cryptography in a table to differentiate against the types and counter methods used. Here security is defined as methods of "protecting" information where intelligence is defined as methods of "retrieving" information [Kahn67]:

Signal Security	Signal Intelligence
Communication Security	Communication Intelligence
Steganography (invisible inks, open codes, messages in hollow heels) and Transmission Security (spurt radio and spread spectrum systems)	Interception and direction-finding
Cryptography(codes and ciphers)	Cryptanalysis
Traffic security(call-sign changes, dummy messages, radio silence)	Traffic analysis (direction-finding, message-flow studies, radio finger printing)
Electronic Security	Electronic Intelligence
Emission Security (shifting of radar frequencies, spread spectrum)	Electronic Reconnaissance (eaves-dropping on radar emissions)
Counter-Countermeasures "looking through" (jammed radar)	Countermeasures (jamming radar and false radar echoes)

Table 1: Kahn's Security Table

Steganography

Neil F. Johnson

Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection).

History and Steganography

Throughout history, a multitude of methods and variations have been used to hide information. David Kahn's *The Codebreakers* provides an excellent accounting of this history [Kahn67]. Bruce Norman recounts numerous tales of cryptography and steganography during times of war in *Secret Warfare*:

The Battle of Codes and Ciphers

One of the first documents describing steganography is from the *Histories* of Herodotus. In ancient Greece, text was written on wax covered tablets. In one story Demeratus wanted to notify Sparta that Xerxes intended to invade Greece. To avoid capture, he scraped the wax off of the tablets and wrote a message on the underlying wood. He then covered the tablets with wax again. The tablets appeared to be blank and unused so they passed inspection by sentries without question.

Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messengers head. After allowing his hair to grow, the message would be undetected until the head was shaved again.

Another common form of invisible writing is through the use of Invisible inks. Such inks were used with much success as recently as WWII. An innocent letter may contain a very different message written between the lines [Zim48]. Early in WWII steganographic technology consisted almost exclusively of invisible inks [Kahn67]. Common sources for invisible inks are milk, vinegar, fruit juices and urine. All of these darken when heated.

With the improvement of technology and the ease as to the decoding of these invisible inks, more sophisticated inks were developed which react to various chemicals. Some messages had to be "developed" much as photographs are developed with a number of chemicals in processing labs.

Null ciphers (unencrypted messages) were also used. The real message is "camouflaged" in an innocent sounding message. Due to the "sound" of many open coded messages, the suspect communications were detected by mail filters. However "innocent" messages were allowed to flow through. An example of a message containing such a null cipher is:

Fishing freshwater bends and saltwater
coasts rewards anyone feeling stressed.
Resourceful anglers usually find masterful
leapers fun and admit swordfish rank
overwhelming anyday.

By taking the third letter in each word, the following message emerges [Zevon]:

Send Lawyers, Guns, and Money.

The following message was actually sent by a German Spy in WWII [Kahn67]:

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.

Steganography

Neil F. Johnson

Taking the second letter in each word the following message emerges:

Pershing sails from NY June 1.

As message detection improved, new technologies were developed which could pass more information and be even less conspicuous. The Germans developed microdot technology which FBI Director J. Edgar Hoover referred to as "the enemy's masterpiece of espionage." Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941. The message was not hidden, nor encrypted. It was just so small as to not draw attention to itself (for a while). Besides being so small, microdots permitted the transmission of large amounts of data including drawings and photographs [Kahn67].

With many methods being discovered and intercepted, the Office of Censorship took extreme actions such as banning flower deliveries which contained delivery dates, crossword puzzles and even report cards as they can all contain secret messages. Censors even went as far as rewording letters and replacing stamps on envelopes.

With every discovery of a message hidden using an existing application, a new steganographic application is being devised. There are even new twists to old methods. Drawings have often been used to conceal or reveal information. It is simple to encode a message by varying lines, colors or other elements in pictures. Computers take such a method to new dimensions as we will see later.

Even the layout of a document can provide information about that document. Brassil et al authored a series of publications dealing with document identification and marking by modulating the position of lines and words [Brassil-Infocom94, Brassil- Infocom94, Brassil-CISS95]. Similar techniques can also be used to provide some other "covert" information just as 0 and 1 are informational bits for a computer. As in one of their examples, word-shifting can be used to help identify an original document [Brassil-CISS95]. Though not applied as discussed in the series by Brassil et al, a similar method can be applied to display an entirely different message. Take the following sentence (S0):

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

and apply some word shifting algorithm (this is sentence S1).

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

By overlapping S0 and S1, the following sentence is the result:

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

This is achieved by expanding the space before explore, the, wide, and web by one point and condensing the space after explore, world, wide and web by one point in sentence S1. Independently,

Steganography

Neil F. Johnson

the sentences containing the shifted words appear harmless, but combining this with the original sentence produces a different message: explore the world wide web.

PC Software that Provide Steganographic Services

Background³

Steganographic software is new and very effective. Such software enables information to be hidden in graphic, sound and apparently "blank" media. Charles Kurak and John McHugh discuss the implications of downgrading an image (security downgrading) when it may contain some other information [Kurak92]. Though not explicitly stated the author(s) of StegoDos mention embedding viruses in images [StegoDos].

In the computer, an image is an array of numbers that represent light intensities at various points (pixels¹) in the image. A common image size is 640 by 480 and 256 colors (or 8 bits per pixel). Such an image could contain about 300 kilobits of data.

There are usually two type of files used when embedding data into an image. The innocent looking image which will hold the hidden information is a "container." A "message" is the information to be hidden. A message may be plain-text, ciphertext, other images or any thing that can be embedded in the least significant bits (LSB) of an image.

For example:

Suppose we have a 24-bit image 1024 x 768 (this is a common resolution for satellite images, electronic astral photographs and other high resolution graphics). This may produce a file over 2 megabytes in size ($1024 \times 768 \times 24 / 8 = 2,359,296$ bytes). All color variations are derived from three primary colors, Red, Green and Blue. Each primary color is represented by 1 byte (8 bits). 24-bit images use 3 bytes per pixel. If information is stored in the least significant bit (LSB) of each byte, 3 bits can be a stored in each pixel. The "container" image will look identical to the human eye, even if viewing the picture side by side with the original. Unfortunately, 24-bit images are uncommon (with exception of the formats mentioned earlier) and quite large. They would draw attention to themselves when being transmitted across a network. Compression would be beneficial if not necessary to transmit such a file. But file compression may interfere with the storage of information.

Kurak and McHugh identify two kinds of compression, lossless and lossy [Kurak92]. Both methods save storage space but may present different results when the information is uncompressed.

- Lossless compression is preferred when there is a requirement that the original information remain intact (as with steganographic images). The original message can be reconstructed exactly. This type of compression is typical in GIF² and BMP³ images.
- Lossy compression, while also saving space, may not maintain the integrity of the original image. This method is typical in JPG⁴ images and yields very good compression.

To illustrate the advantage of lossy compression, Renoir's Le Moulin de la Galette was retrieved as a 175,808 byte JPG image 1073 x 790 pixels with 16 million possible colors. The colors were maintained when converting it to a 24-bit BMP file but the file size became 2,649,019 bytes! Converting again to a GIF file, the colors were reduced to 256 colors (8-bit) and the new file is 775,252 bytes. The 256 color image is a very good approximation of Renoir's painting.

³ A pixel is an instance of color, a point in a picture.

Steganography

Neil F. Johnson

Most steganographic software available does not support, nor recommends, using JPG files (an exception is note4d later in the paper). The next best alternative to 24-bit images, is to use 256 color (or gray-scale) images. These are the most common images found on the Internet in the form of GIF files. Each pixel is represented as a byte (8-bits). Many authors of the steganography software and articles stress the use of gray-scale images (those with 256 shades of gray or better) [Arachelian, Aura95, Kurak92, Maroney]. The importance is not whether the image is gray-scale or not, the importance is the degree to which the colors change between bit values.

Gray-scale images are very good because the shades gradually change from byte to byte. The following is a palette containing 256 shades of gray.

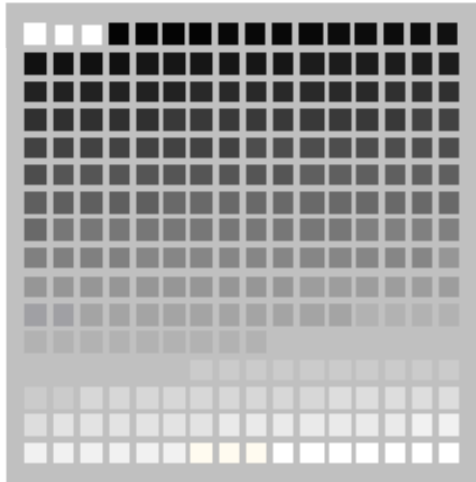



Figure 1: Gray-Scale Palette

A similar image with 16 shades of gray (four-bit color) may look very close to one with 256 shades of gray  but the palette has less variations with which to work. The subtleties permit data to be stored without the human eye catching the changes. Many argue that gray-scale images render the "best" results for steganography. However, using gray-scale or color is not as important as the subtleties in color variation. Consider the following two 256 color palettes.

² Graphic Interchange Format developed by CompuServe to be a device-independent method of storing images.

³ Windows and OS/2 bitmap picture file.

⁴ Joint Photography experts Group (JPG/JPEG) is a device-independent method for storing images which supports 24-bit images.

Steganography

Neil F. Johnson

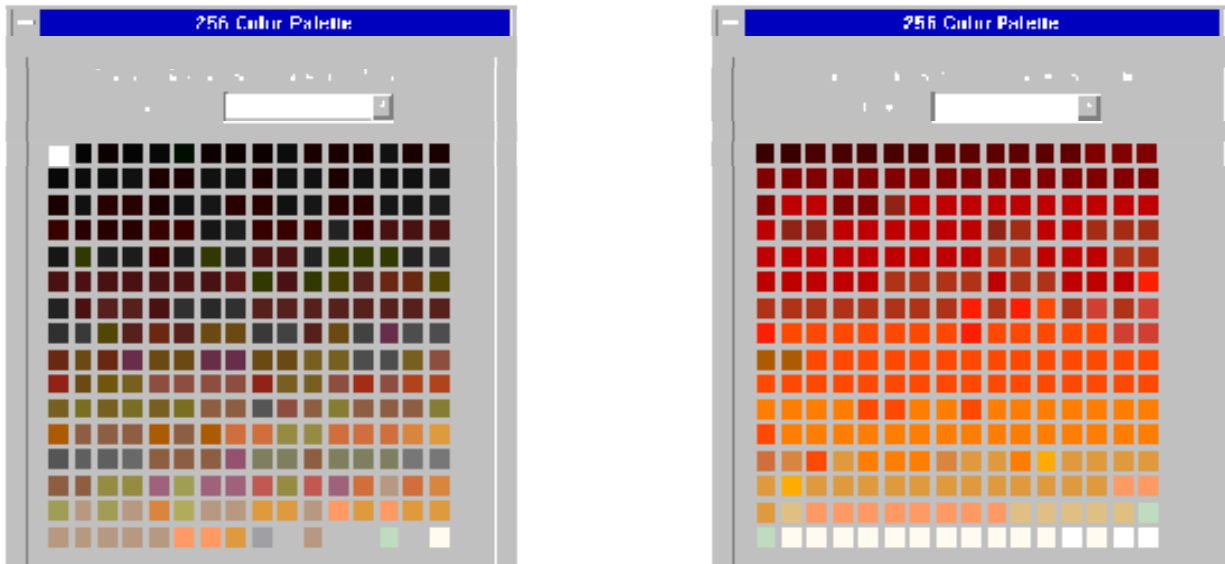


Figure 3 illustrates subtle changes in color variations. It is difficult to differentiate between many of the colors in this palette. Is this palette in Figure 2 "good" for steganography? Well, it depends. Subtle color changes can be seen in Figure 2, but other color variances seem to be rather drastic. However, one must consider the image in addition to the palette. Obviously, an image with large areas of solid colors is a poor choice as variances created from the embedded message will be noticeable in the solid areas (a palette as in Figure 3 would offset this). Figure 2 is the palette from a 256 color version of Renoir's *Le Moulin de la Galette*. Based on embedding this image with text and graphic messages, it is a very good container for holding data.

Evaluation Method

Various steganographic software packages were explored. The evaluation process was to determine limitations and flexibility of the software readily available to the public.

Message and container files were selected before testing. This proved to be a problem with some packages due to limitations of the software. The images selected had to be altered to fit into the constraints of the software and other containers were used. In all, a total of 25 files were used as containers (much more than I have room to discuss).

The files used for evaluation included two "message" files and two "container" files. The "message" files are those to be hidden in the innocent looking "container" files.

The message files:

Message 1 contains the following plain-text and will be referred to as M1:

Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present [Markus Kuhn 1995-07-03].

Steganography

Neil F. Johnson

Message 2 is a satellite image which will be referred to as M2:

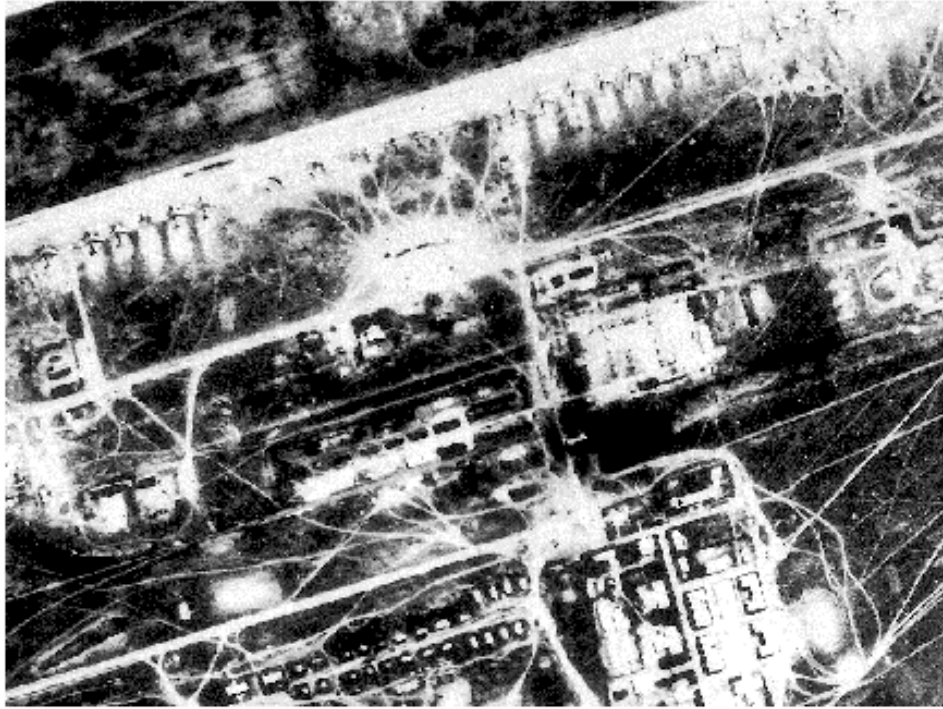


Figure 4: Long-Range Aviation Airfield⁵

The Container Files:

Figure 5: Renoir's *Le Moulin de la Galette* - Container C1⁶



Steganography

Neil F. Johnson

Figure 6: Droeshout engraving of William Shakespeare - Container C2⁷



The image of Shakespeare is too small to contain M2, but M1 could be embedded without any degradation of the image. For the most part, all the software teste5d could handle the 518 byte plain-text message, however, only two could handle the image labeled M2. Of the two, only one software package could reliably handle 24-bit images and other formats consistently: S-Tools by Andy Brown.

Next, an attempt was made to embed messages M1 and M2 using each software package. If the software could not handle processing these containers (C1 and C2), other containers were tried. All the software could embed M1 into some container. These files were reviewed before and after applying steganographic methods.

Software Evaluation

The following software packages were reviewed with respect to steganographic manipulation of images: Hide and Seek v4.1, StegoDos v0.90a, White Noise Storm, and S-Tools for Windows v3.00. Nearly all the authors encourage encrypting messages before embedding them in images as an added layer of protection and reviewing the images after embedding data. Even with the most reliable software tested, there may be some unexpected results.

Hide and Seek v 4.1

Hide and Seek versions 4.1 and 5.0 by Colin Maroney have similar limitations with minimum image sizes (320 x 480). In version 4.1 if the image is smaller than the minimum, then the stego-image is padded with black space. If the cover image is larger, the stego-image is cropped to fit. In version 5.0 the same is true with minimum image sizes. If any image exceeds 1024 x 768, an error message is returned. The Hide and Seek 1.0 for Windows 95 version seems to have these issues resolved and is

⁵ *Le Moulin de la Galette* by Pierre-Auguste Renoir is available via the WebMuseum, Paris and accessible through <http://www.cnam.fr/wm/paint/auth/renoir>.

⁶ A JPG version of Droeshout engraving of William Shakespeare is available at <http://www.cultureware.com/cultureware/shakespeare/Droeshout.jpg>.

Steganography

Neil F. Johnson

a much improved steganography tool. Version 4.1 is evaluated here to illustrate limitations of some steganography tools.

Hide and Seek 4.1 is free software which contains a series of DOS programs that embed data in GIF files and comes with the source code. Hide and Seek uses the Least Significant Bit of each pixel to encode characters, 8 pixels per character and spreads the data throughout the GIF in a somewhat random fashion. The larger the message the more likely the resulting image will be degraded. Since the data is dispersed "randomly" and the message file header is encrypted, there is no telling what is in an embedded file.

Unfortunately the hidden file can be no longer than 19,000 bytes because the maximum display used is 320 x 480 pixels. Each character takes 8 pixels to hide ($(320 \times 480) / 8 = 19200$).

C2 (Shakespeare) was used to embed M1. The original image of Shakespeare is 222 x 282 pixels and 256 shades of gray. The resulting image was forced to 320 x 480 pixels. Instead of "stretching" the image to fit, large black areas were added to the image making it 320 x 480. The image on the left is the original C2 and the image on the right is embedded with M1.

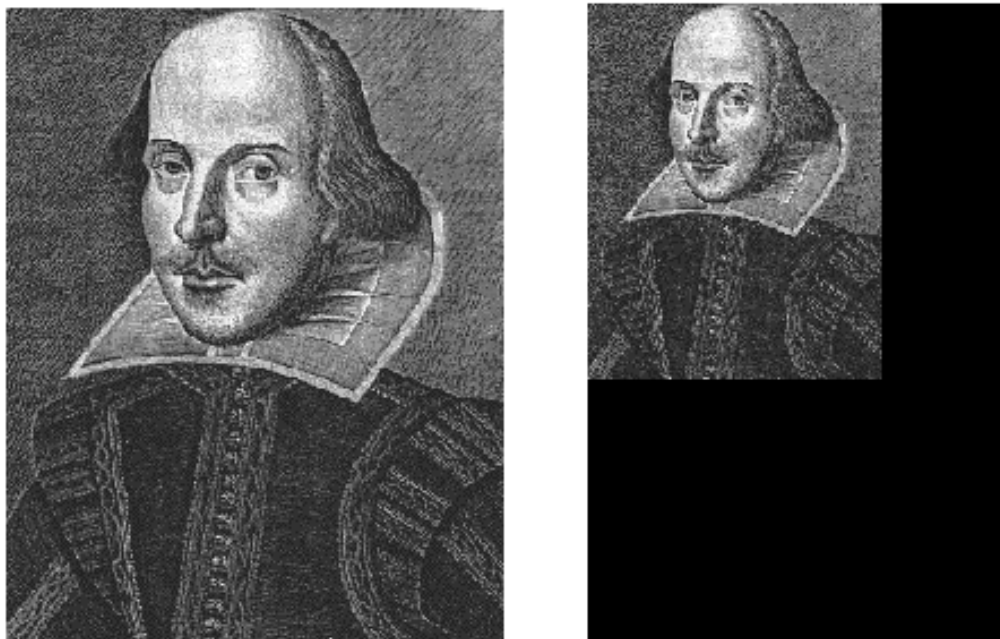


Figure 7: Result of using Hide and Seek for embedding M1 into C2.

StegoDos

StegoDos is also known as Black Wolf's Picture Encoder version 0.90a. This is Public Domain software written by Black Wolf (anonymous). This is a series of DOS programs that require far too much effort for the results. It will only work with 320x200 images with 256 colors. To encode a message, one must:

1. Run GETSCR. This starts a TSR which will perform a screen capture when PRINTSCREEN is pressed.
2. View the image with a third-party image viewing software (not included with StegoDos) and press PRINTSCREEN to save the image in MESSAGE.SCR.

Steganography

Neil F. Johnson

3. Save your message to be embedded in the image as MESSAGE.DAT.
4. Run ENCODE. This will merge MESSAGE.DAT with MESSAGE.SCR.
5. Use a third party screen capturing program (not included with StegoDos) to capture the new image from the screen.
6. Run PUTSCR and capture the image displayed on the screen.

Decoding the message is not as involved but still requires a third party program to view the image. To decode a message, one must:

1. Run GETSCR. This starts a TSR which will perform a screen capture when PRINTSCREEN is pressed.
2. View the image containing a message with a third-party image viewing software (not included with StegoDos) and press PRINTSCREEN to save the image in MESSAGE.SCR.
3. Run DECODE. This will extract the stored message from MESSAGE.SCR.

Due to the size restrictions, M2 and C1 could not be used. C2 (Shakespeare) and a number of other containers were tested (both color and gray-scale) with M1. Every one of them were obviously distorted. There was little distortion within the C2 image, but it was cropped and fitted into a 320 x 200 pixel image. The image on the left is the original C2 file. The image on the right contains the M1 message:



Figure 8: Result of embedding M1 in C2 with StegoDos.

This application uses the Least Significant Bit method with less success than the others. It also appends an EOF (end of file) character to the end of the message. Even with the EOF character, the message retrieved from the altered imaged most likely contained garbage at the end. The following is

Steganography

Neil F. Johnson

the original message (M1) and a portion of the message extracted from the image created with StegoDos:

Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present [Markus Kuhn 1995-07-03].

The original file is 518 bytes. The extracted file is around 8 kilobytes:

Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present [Markus Kuhn 1995-07-03].eC'' @ hee_E_Ae._C&jP-hT,eAT_A eq.Pe_. _A@#*,-h6~?]\`V(UY3A/X?Uok iRO_+Yu?DU)>YOTc*\:Mu',...

White Noise Storm

White Noise Storm by Ray (Arsen) Arachelian is a very versatile steganography application for DOS. Embedding M1 in the containers C1 and C2 was rather trivial and no degradation could be detected. White Noise Storm was the first software tested that could embed M2 into C1 - notice the "noise" interfering with the image integrity.

The image on the left is the original C2. The image on the right contains message M1:

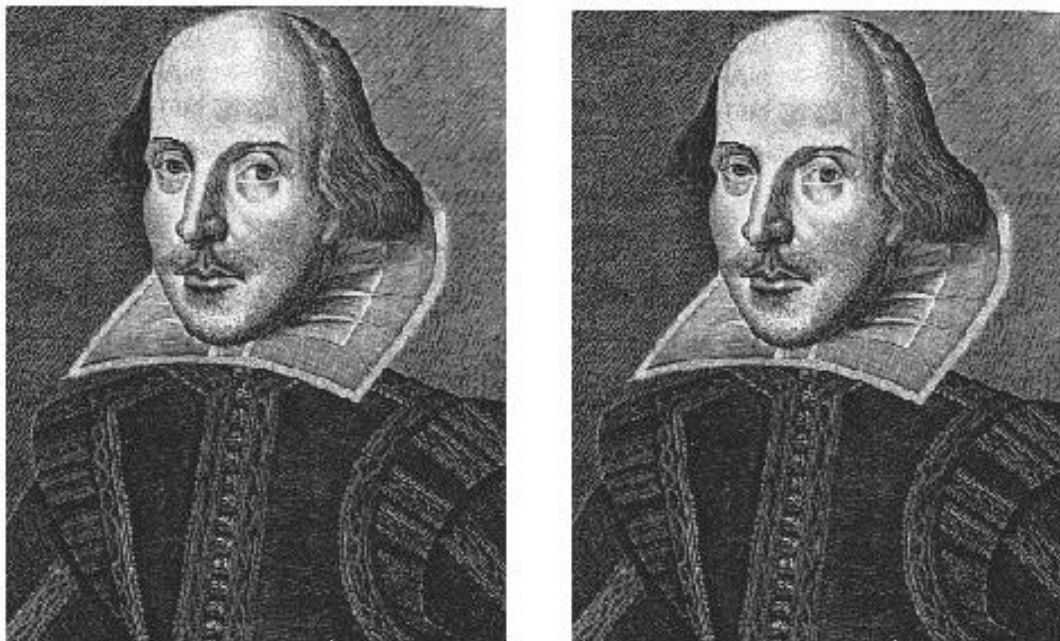


Figure 9: Result of embedding M1 in C2 using White Noise Storm.

Steganography

Neil F. Johnson



Steganography

Neil F. Johnson

Arachelian encourages encrypting the message before embedding it into an image. White Noise Storm (WNS) also includes an encryption routine to "randomize" the bits within an image. His use of encryption with steganography is well integrated, but is beyond the scope of this paper.

WNS was designed based on the idea of spread spectrum technology and frequency hopping. "Instead of having X channels of communication which are changed with a fixed formula and passkey.

Eight channels are spread within a number of 8-bits*W byte channels. W represents a random sized window of W bytes. Each of these eight channels represents one single bit, so each window holds one byte of information and a lot of unused bits. These channels rotate among themselves, for instance bit 1 might be swapped with bit 7, or all the bits may rotate positions at once. These bits change location within the window on the byte level. The rules for this swapping are dictated not only by the passphrase but also by the previous window's random data (similar to DES block encryption)" [Arachelian, RE: Steganography].

WNS also used the Least Significant Bit (LSB) application of steganography and applies this method to PCX⁸ files. The software extracts the LSBs from the container image and stores them in a file. The message is encrypted and applied to these bits to create a "new" set of LSBs. These are then "injected" into the container image to create a new image. The documentation that accompanies White Noise Storm is well organized and explains some of the theory behind the implementation of encryption and ⁶steganography.

The main disadvantage of applying the WNS encryption method to steganography is the loss of many bits that can be used to hold information. Relatively large files must be used to hold the same amount of information other methods provide.

S-Tools

Steganography Tools (S-Tools) for Windows 3.00 by Andy Brown is the most versatile steganography tools of any applications tested. It includes several programs that process GIF and BMP images (ST-BMP.EXE), audio WAV files (ST-WAV.EXE) and will even hide information in the "unused" areas on floppy diskettes (ST-FDD.EXE). In addition to supporting 24-bit images, S-Tools also includes a barrage of encryption routines (Idea, MPJ2, DES, 3DES and NSEA) with many options.

S-Tools applies the LSB methods discussed before to both images and audio files. Due to the lack of resources, only images were tested. Brown developed a very nice interface with prompts and well developed on-line documentation. The only apparent limitations were the resources available. There were times large 24-bit images would bring the Windows to a halt. A very useful feature is a status line that displays the largest message size that can be stored in an open container file. This saved the time of attempting to store a message that is too large for a container. After hiding the message, the "new" image will be displayed and let you toggle between the new and original images. At times the new image looked to be grossly distorted, but after saving the new image looked nearly identical to the original. This may be due to memory limitations. On occasion a saved image was actually corrupted and could not be read. A saved image should always be reviewed before sending it out.

S-Tools provided the most impressive results. Unlike the obvious distortions in "A Cautionary Note on Image Downgrading" [Kurak92], S-Tools maintained remarkable image integrity. The following figure illustrates the text message M1 embedded in container C2.

⁶ IBM PC Paintbrush picture file.

Steganography

Neil F. Johnson

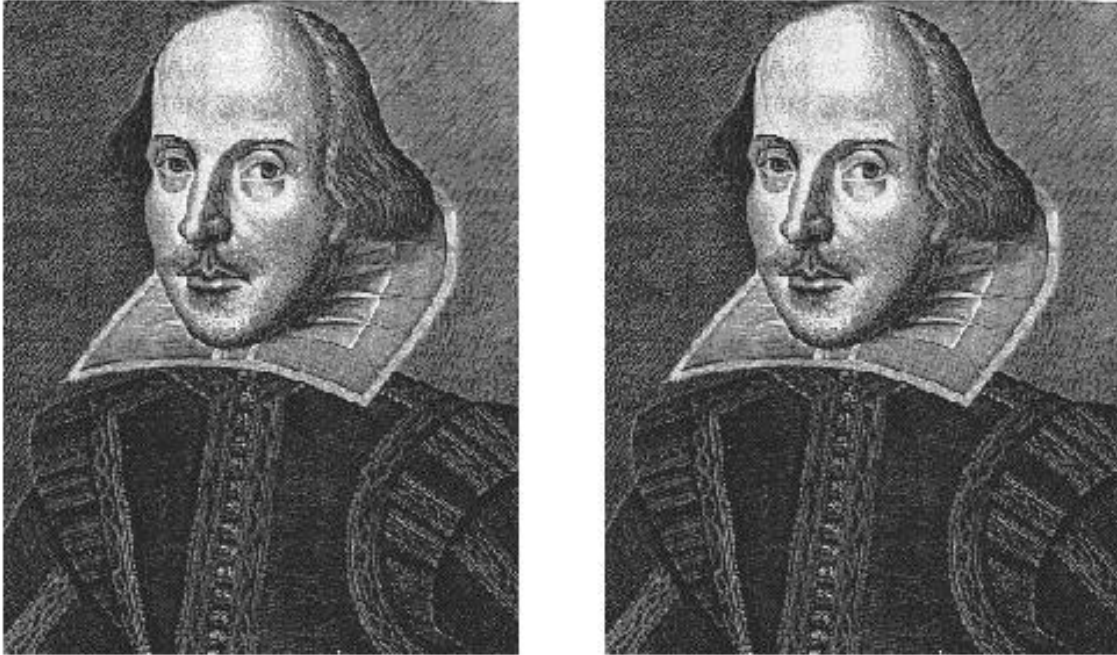
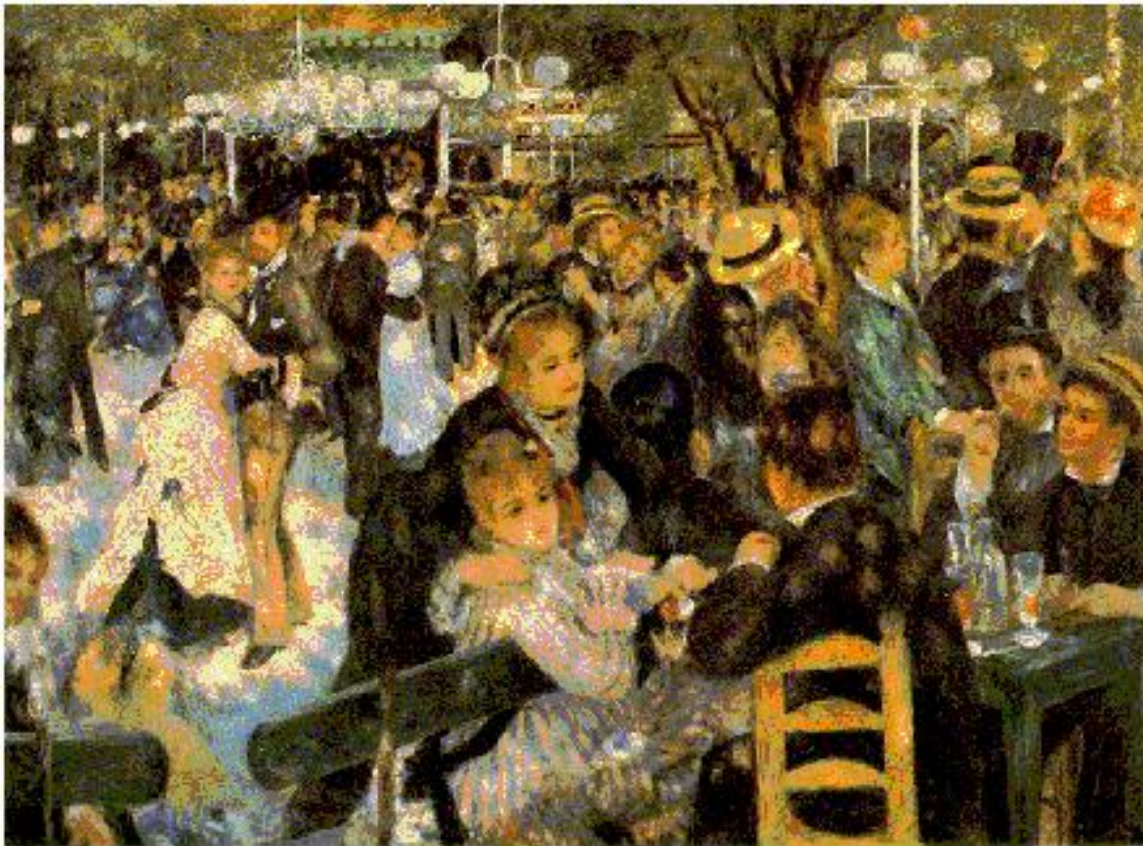


Figure 11: Left is the original C2. Right is C2 with M1 embedded with S-Tools.

The following is the original C1 (top) and C1 embedded with M2 (airfield):



Steganography

Neil F. Johnson



The following is derived from S-Tools BMP - How it is done by Andy Brown:

"S-Tools works by 'spreading' the bit-pattern of the message file to be hidden across the least-significant bits of the color levels in the image. S-Tools tries to reduce the number of image colors in a manner that preserves as much of the image detail as possible. It is difficult to tell the difference between a 256 color image and one reduced to 32."

"S-Tools adds some extra information on to the front of the message file before hiding. 32 bits of time-dependent random garbage is added first. This step means that two identical hidden files that are encrypted in CBC or PCBC mode will never encipher to the same ciphertext. The 32 bit length of the hidden file is then included. This is required for S-Tools to be able to extract the hidden file. Encryption will conceal this value."

"To further conceal the presence of a file, S-Tools picks its bits from the image based on the output of a random number generator. This is designed to defeat an attacker who might apply a statistical randomness test to the lower bits of the image to determine whether encrypted data is hidden there (well-encrypted data shows up as pure white noise). The random number generator used by S-Tools is based on the output of the MD5 message digest algorithm, and is not easily (if at all) defeatable" [S-Tools Documentation by Andy Brown].

Software not tested but worth noting

The following software packages were reviewed but not tested: Jpeg-Jsteg v4 and Stealth v1.1.

Steganography

Neil F. Johnson

Jpeg-Jsteg v4

Cryptography and steganography rely on retrieving a message in its original form without losing any information. Such is the idea behind lossless compression. Since JPG images use lossy encoding to compress its data, it is generally thought that steganography would be infeasible with such images. "This version of the Independent JPEG Group's JPEG Software has been modified for 1-bit steganography in JFIF output files" [Independent JPEG Group]. The Jpeg-Jsteg software comes with source code and instructions for compiling the code on various platforms.

According to the Independent JPEG Group (IJPG), the JFIF format is composed of lossy and non-lossy stages. Information can be inserted between these stages without corrupting the image.

As discussed earlier with Renoir's Le Moulin de la Galette compression is a great advantage JPG images have over other formats. JPEG images are becoming more abundant on the Internet because large images with unlimited colors can be stored in relatively small files (a 1073 x 790 pixel image with 16 million colors can be stored in a 170 Kilobyte file. The same image is over 2 Megabytes if converted to a BMP).

Stealth v1.1

Stealth by Henry Hastur in and of itself is not a steganographic program or method. It is usually found with steganographic software on the Internet and is used to complement the steganographic methods. Stealth is a filter that strips off the PGP header that is on a PGP encrypted file. This leaves only the encrypted data. Why is this important? Applying steganography to an encrypted message is more secure than a "plain text" message. However, many encryption applications add header information to the encrypted message. This header information identifies the method used to encrypt the data. For example, if a cracker has identified hidden data in an image and has successfully extracted the encrypted message, a header for the encryption method would point the cracker in the right direction for additional cryptanalysis. But, if the header is removed, the cracker cannot determine the method for encryption. Some steganography software (White Noise Storm and S-Tools) provide this step in security, but others do not.

Conclusion and Comments

Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection).

There are an infinite number of steganography applications. This paper explores a tiny fraction of the art of steganography. It goes well beyond simply embedding text in an image. Steganography does not only pertain to digital images but also to other media (files such as voice, other text and binaries; other media such as communication channels, the list can go on and on). Consider the following example:

A person has a cassette tape of Pink Floyd's "The Wall." The plans of a Top Secret project (e.g., device, aircraft, covert operation) are embedded, using some steganographic method, on that tape. Since the alterations of the "expected contents" cannot be detected, (especially by human ears and probably not easily so by digital means) these plans can cross borders and trade hands undetected. How do you detect which recording has the message?

This is a trivial (and incomplete) example, but it goes far beyond simple image encoding in an image with homogeneous regions. Part of secrecy is selecting the proper mechanisms. Consider encoding using an Mandelbrot image [Hastur].

Steganography

Neil F. Johnson

In and of itself, steganography is not a good solution to secrecy, but neither is simple substitution and short block permutation for encryption. But if these methods are combined, you have much stronger encryption routines (methods).

For example (again over simplified): If a message is encrypted using substitution (substituting one alphabet with another), permute the message (shuffle the text) and apply a substitution again, then the encrypted ciphertext is more secure than using only substitution or only permutation. NOW, if the ciphertext is embedded in an [image, video, voice, etc.] it is even more secure. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message. With steganography, the interceptor may not know the object contains a message.

References and Resources

Note: Many of the references and resources listed include Internet references (URL), and are also available via my Security and Privacy Issues Web Page. Also see my Steganography page which includes information specific to steganography and has been developed to consolidate research topics for this paper.

Publications

[Aura95] Tuomas Aura, "Invisible Communication," EET 1995,
http://deadlock.hut.fi/ste/ste_html.html, <ftp://saturn.hut.fi/pub/aaura/ste1195.ps>

[Brassil-Infocom95] J. Brassil, S. Low, N. Maxemchuk, L. O'Goram,
"Document Marking and Identification using Both Line and Word Shifting," Infocom95, <ftp://ftp.research.att.com/dist/brassil/1995/infocom95.ps.Z>

[Brassil-Infocom94] J. Brassil, S. Low, N. Maxemchuk, L. O'Goram,
"Electronic Marking and Identification Techniques to Discourage Document Copying," Infocom94,
<ftp://ftp.research.att.com/dist/brassil/1994/infocom94a.ps.Z>.

[Brassil-CISS95] J. Brassil, S. Low, N. Maxemchuk, L. O'Goram,
"Hiding Information in Document Images," CISS95, <ftp://ftp.research.att.com/dist/brassil/1995/ciss95.ps.Z>.

[JDJ01] Neil F. Johnson, Zoran Duric, Sushil Jajodia, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures
Kluwer Academic Press, Norwrl, MA, New York, The Hague, London, 2000.

[Kahn67] David Kahn, The Codebreakers,
The Macmillan Company. New York, NY 1967.

[Kurak92] C. Kurak, J. McHugh,
"A Cautionary Note On Image Downgrading," IEEE Eighth Annual Computer Security Applications Conference, 1992. pp. 153-159.

[Norman73] Bruce Norman, Secret Warfare,
Acropolis Books Ltd. Washington, DC 1973.

[Zevon] Warren Zevon, Lawyers, Guns, and Money.
Music track released in the albums Excitable Boy, 1978; Stand in the Fire, 1981; A Quiet Normal Life, 1986; Learning to Flinch, 1993.

[Zim48] Herbert S. Zim, Codes and Secret Writing,
William Marrow and Company. New York, NY, 1948.

Steganography

Neil F. Johnson

Software References

There are many other software applications available that provide steganographic results. This is just a sample of software available for the PC platform. Every effort is being made to credit the authors of the software reviewed in this paper. However, some authors wish to remain anonymous. Only links to software outside the United States are made below.

[Arachelian] Ray Arachelian, White Noise Storm, Shareware 1992, 1993, 1994. <ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/wns210.zip>.

[Brown] Andy Brown, S-Tools for Windows, Shareware 1994. s-tools3.zip (version 3.0) s-tools4.zip (version 4.0 - not yet reviewed).

[Hastur] Henry Hastur, Stealth for PGP v1.1, <ftp://ftp.netcom.com>. MandelSteg v1.0 and GIFExtract v1.0, <ftp://ftp.dsi.unimi.it/pub/security/crypt/code>.

[Maroney] Colin Maroney, Hide and Seek v4.1, Freeware. <ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/hdsk41b.zip>.

[JSteg] Independent JPEG Group, Jpeg-Jsteg v 4. <ftp://ftp.funet.fi/pub/crypt/steganography>.

[StegoDos] Author alias: Black Wolf, StegoDos - Black Wolf's Picture Encoder v0.90B, Public Domain. <ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/stegodos.zip>.

WEB Page Resources

AT&T Bell Laboratories Research Web Page, <http://www.research.att.com>.
Carl Landwehr (ed), Cipher -

Electronic Newsletter of the IEEE Computer Society's TC on Security and Privacy, <http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/> (see also <http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-links.html> for an excellent listing of links to organizations and publications related to security).

Codex Links to Law Enforcement, Security, Intelligence, Investigative and Other sites, http://www.trcone.com/t_links.html.

Cypherpunks, <ftp://ftp.csua.berkeley.edu/pub/cypherpunks/index.html>.

Digimarc® Corporation Web Site, <http://www.teleport.com/~digimarc>.

Electronic Privacy Information Center (EPIC), <http://www.epic.org>.

National Security Institute Library, <http://nsi.org/Library/Library.html>.
Security and Privacy Issues by Neil Johnson, <http://www.jjtc.com/Security>.

Steganography News Mailing List maintained by Markus Kuhn. Information about the list can be found at [../sec/steglist.htm](http://sec/steglist.htm).