**DEFINITION OF STEGANOGRAPHY**

Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. The word steganography combines the [Ancient Greek](http://en.wikipedia.org/wiki/Ancient_Greek) words steganos (στεγανός), meaning "covered, concealed, or protected",and graphei (γραφή) meaning "writing". The first recorded use of the term was in 1499 by [Johannes Trithemius](http://en.wikipedia.org/wiki/Johannes_Trithemius) in his [Steganographia](http://en.wikipedia.org/wiki/Johannes_Trithemius#Steganographia), a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in [invisible ink](http://en.wikipedia.org/wiki/Invisible_ink) between the visible lines of a private letter. Some implementations of steganography which lack a [shared secret](http://en.wikipedia.org/wiki/Shared_secret) are forms of [security through obscurity](http://en.wikipedia.org/wiki/Security_through_obscurity), where as key dependent steganographic schemes adhere to [Kerckhoffs's principle](http://en.wikipedia.org/wiki/Kerckhoffs%27s_principle).

The advantage of steganography over [cryptography](http://en.wikipedia.org/wiki/Cryptography) alone is that the intended secret message does not attract attention to it self as an object of secrutiny. Plainly visible encrypted messages no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where [encryption](http://en.wikipedia.org/wiki/Encryption) is illegal. Thus, where as cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

**HISTORY OF STEGANOGRAPHY**

The first recorded uses of steganography can be traced back to 440 BC when [Herodotus](http://en.wikipedia.org/wiki/Herodotus) mentions two examples in his Histories. [Demaratus](http://en.wikipedia.org/wiki/Demaratus) sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. [Wax tablets](http://en.wikipedia.org/wiki/Wax_tablet" \o "Wax tablet) were in common use then as reusable writing surfaces, sometimes used for shorthand.

In his work Polygraphiae [Johannes Trithemius](http://en.wikipedia.org/wiki/Johannes_Trithemius) developed his so called "[Ave Maria Cipher](http://en.wikipedia.org/w/index.php?title=Ave_Maria_Cipher&action=edit&redlink=1" \o "Ave Maria Cipher (page does not exist))" with which one can hide information in a Latin praise of God. " Auctor Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris " for example contains the concealed word VICIPEDIA.

**SOME TECHNIQUE OF STEGANOGRAPHY**

Physic

Steganography has been widely used, including in recent historical times and the present day. Known examples include:

1. Hidden messages within [wax tablets](http://en.wikipedia.org/wiki/Wax_tablet) in ancient [Greece](http://en.wikipedia.org/wiki/Greece), people wrote messages on the wood, then covered it with [wax](http://en.wikipedia.org/wiki/Wax) upon which an innocent covering message was written.
2. Hidden messages on messenger's body also used in ancient Greece. [Herodotus](http://en.wikipedia.org/wiki/Herodotus" \o "Herodotus) tells the story of a message tattooed on the shaved head of a slave of [Histiaeus](http://en.wikipedia.org/wiki/Histiaeus), hidden by the hair that afterwards grew over it, and exposed by shaving the head again. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.
3. In the early days of the printing press, it was common to mix different type faces on a printed page due to the printer not having enough copies of some letters otherwise. Because of this, a message could be hidden using 2 (or more) different typefaces, such as normal or italic.
4. During [World War II](http://en.wikipedia.org/wiki/World_War_II), the French Resistance sent some messages written on the backs of couriers using invisible ink.
5. Hidden messages on paper written in [secret inks](http://en.wikipedia.org/wiki/Invisible_ink), under other messages or on the blank parts of other messages.
6. Messages written in [Morse code](http://en.wikipedia.org/wiki/Morse_code) on knitting [yarn](http://en.wikipedia.org/wiki/Yarn) and then knitted into a piece of clothing worn by a courier.
7. [Jeremiah Denton](http://en.wikipedia.org/wiki/Jeremiah_Denton) repeatedly blinked his eyes in Morse Code during the 1966 televised press conference that he was forced into as an American [POW](http://en.wikipedia.org/wiki/POW) by his North Vietnamese captors, spelling out the word, "T-O-R-T-U-R-E". This confirmed for the first time to the U.S. Military (naval intelligence) and Americans that American. POWs were being tortured in North Vietnam.
8. Messages written on envelopes in the area covered by [postage stamps](http://en.wikipedia.org/wiki/Postage_stamp).
9. During and after World War II, [espionage](http://en.wikipedia.org/wiki/Espionage) agents used photographically produced [microdots](http://en.wikipedia.org/wiki/Microdot) to send information back and forth. Microdots were typically minute, approximately less than the size of the [period](http://en.wikipedia.org/wiki/Full_stop) produced by a [typewriter](http://en.wikipedia.org/wiki/Typewriter). World War II microdots needed to be embedded in the paper and covered with an adhesive, such as [collodion](http://en.wikipedia.org/wiki/Collodion). This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.
10. During WWII, [Velvalee Dickinson](http://en.wikipedia.org/wiki/Velvalee_Dickinson), a spy for [Japan](http://en.wikipedia.org/wiki/Japan) in [New York City](http://en.wikipedia.org/wiki/New_York_City), sent information to accommodation addresses in neutral [South America](http://en.wikipedia.org/wiki/South_America). She was a dealer in [dolls](http://en.wikipedia.org/wiki/Doll), and her letters discussed the quantity and type of doll to ship. The stegotext was the doll orders, while the concealed " plaintext " was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.
11. Cold War counter-propaganda. In 1968, crew members of the [USS Pueblo](http://en.wikipedia.org/wiki/USS_Pueblo_(AGER-2)) intelligence ship held as prisoners by [North Korea](http://en.wikipedia.org/wiki/North_Korea), communicated in sign language during staged photo opportunities, informing the [United States](http://en.wikipedia.org/wiki/United_States) they were not defectors, but were captives of the North Korean. In other photos presented to the US, crew members gave " [the finger](http://en.wikipedia.org/wiki/The_finger) " to the unsuspecting North Korean, in an attempt to discredit photos that showed them smiling and comfortable.

DIGITAL

Modern steganography entered the world in 1985 with the advent of the personal computers being applied to classical steganography problems. Development following that was very slow, but has since taken off, going by the large number of steganography software available:

1. Concealing messages within the lowest bits of [noisy](http://en.wikipedia.org/wiki/Image_noise) images or sound files.
2. Concealing data within encrypted data or within random data. The data to be concealed are first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the [one-time pad](http://en.wikipedia.org/wiki/One-time_pad) generates ciphertexts that look perfectly random if one does not have the private key).
3. [Chaffing and winnowing](http://en.wikipedia.org/wiki/Chaffing_and_winnowing).
4. [Mimic functions](http://en.wikipedia.org/wiki/Mimic_function) convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a [ciphertext only attack](http://en.wikipedia.org/wiki/Ciphertext-only_attack).
5. Concealed messages in tampered executable files, exploiting redundancy in the targeted [instruction set](http://en.wikipedia.org/wiki/Instruction_set).
6. Pictures embedded in video material (optionally played at slower or faster speed).
7. Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in keypresses in some applications ([telnet](http://en.wikipedia.org/wiki/Telnet" \o "Telnet) or[remote desktop software](http://en.wikipedia.org/wiki/Remote_desktop_software)) can mean a delay in packets, and the delays in the packets can be used to encode data.
8. Changing the order of elements in a set.
9. Content Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a non human adversary/warden.
10. [Blog](http://en.wikipedia.org/wiki/Blog) Steganography. Messages are [fractionalized](http://en.wikipedia.org/w/index.php?title=Fractionalized&action=edit&redlink=1) and the (encrypted) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole [blogosphere](http://en.wikipedia.org/wiki/Blogosphere).
11. Modifying the echo of a sound file (Echo Steganography).
12. Secure Steganography for Audio Signals.
13. Image [bit-plane complexity segmentation steganography](http://en.wikipedia.org/wiki/BPCS-Steganography)
14. Including data in ignored sections of a file, such as after the logical end of the carrier file.
15. Making text the same color as the background in word processor documents, e-mails, and forum posts.

NETWORK

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. This nomenclature was originally introduced by [Krzysztof Szczypiorski](http://en.wikipedia.org/w/index.php?title=Krzysztof_Szczypiorski&action=edit&redlink=1) in 2003. Contrary to the typical steganographic methods which utilize digital media (images, audio and video files) as a cover for hidden data, network steganography utilizes communication protocols control elements and their basic intrinsic functionality. As a result, such methods are harder to detect and eliminate.

Typical network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU ([Protocol Data Unit](http://en.wikipedia.org/wiki/Protocol_Data_Unit" \o "Protocol Data Unit)), to the time relations between the exchanged PDUs, or both (hybrid methods).

More over, it is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term interprotocol steganography.

Network steganography covers a broad spectrum of techniques, which include, among others:

1. Steganophony : the concealment of messages in [Voice-over-IP](http://en.wikipedia.org/wiki/Voice-over-IP) conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver (this method is called LACK - Lost Audio Packets Steganography), or, alternatively, hiding information in unused header fields.
2. WLAN Steganography : the utilization of methods that may be exercised to transmit steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks)

PRINTED

Digital steganography output may be in the form of printed documents. A message, the [plaintext](http://en.wikipedia.org/wiki/Plaintext), may be first encrypted by traditional means, producing a [ciphertext](http://en.wikipedia.org/wiki/Ciphertext). Then, an innocuous covertext is modified in some way so as to contain the ciphertext, resulting in the stegotext. For example, the letter size, spacing, [typeface](http://en.wikipedia.org/wiki/Typeface), or other characteristics of a covertext can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it. [Francis Bacon](http://en.wikipedia.org/wiki/Francis_Bacon) developed [Bacon's cipher](http://en.wikipedia.org/wiki/Bacon%27s_cipher) as such a technique.

The ciphertext produced by most digital steganography methods, however, is not printable. Traditional digital methods rely on perturbing noise in the channel file to hide the message, as such, the channel file must be transmitted to the recipient with no additional noise from the transmission. Printing introduces much noise in the ciphertext, generally rendering the message unrecoverable. There are techniques that address this limitation, one notable example is ASCII Art Steganography.

DIGITAL TEXT

[Unicode](http://en.wikipedia.org/wiki/Unicode) steganography uses look a like characters of the usual [ASCII](http://en.wikipedia.org/wiki/ASCII) set to look normal, while really carrying extra bits of information. If the text is displayed correctly, there should be no visual difference from ordinary text. Some systems, however, may display the fonts differently, and the extra information would be easily spotted.

Alternately, hidden (e.g., control) characters, and redundant use of markup (e.g., empty bold, underline or italics) can add embedded within a body of text to hide information that wouldn't be visually apparent when displayed, but can be discovered by examining the document source. HTML pages can contain code for extra blank spaces and tabs at the end of lines, as well as different colours, fonts and sizes, which will not be visible when displayed. A more trivial example is white text on a white background, which can be revealed by "selecting ".

One such method is based on the non-printing Unicode characters [Zero-Width Joiner](http://en.wikipedia.org/wiki/Zero-Width_Joiner) (ZWJ) and [Zero-Width Non-Joiner](http://en.wikipedia.org/wiki/Zero-Width_Non-Joiner) (ZWNJ). These characters are used for joining and disjoining letters in Arabic, but can be used in Roman alphabets for hiding information because they have no meaning in Roman alphabets, and because they are "zero-width" and thus not displayed. The embedding of ZWJ in the cover-text represents "1" and the embedding of ZWNJ represents "0". Groups of characters can be used to represent the letters A (giving it the code "0", and thus represented by ZWNJ) to Z (giving it the code "1011", and thus represented by ZWJ,ZWNJ,ZWJ,ZWJ). These character groups can be inserted between each character of the cover text, thereby hiding a message.

**METHOD OF STEGANOGRAPHY**

There are four types of Steganography methods , namely :

1. Least Significant Bit insertion ( LSB )

The method used to hide messages in digital media is different . For example , the image file message can be hidden by using the paste method at low bit or the rightmost bits ( LSB ) on the pixel data that make up the file .

Disadvantages of LSB Invertion : Can be concluded from the example of 8 -bit pixels , using the LSB Insertion can drastically change the color of the pixel constituent . It can show a marked difference from the cover image into stego image , so that the sign shows the state of steganography

The advantages of LSB Insertion : The greatest gains from the LSB algorithm is fast and easy . And the algorithm also has a steganographic software that supports the work of the principal elements of the LSB color palette through manipulation ( painting ) .

1. Algorithms and Transformation

Compression algorithm is a method of steganography to hide data in a mathematical function . Two of these functions is the Discrete Cosine Transformation ( DCT ) and Wavelet Transformation . DCT and wavelet functions that transform the data from one place ( the domain ) to the ( domain ) to another. DCT function is to transform the data from the spatial (spatial domain ) to the frequency ( frequency domain)

1. Redundant Encoding Pattern

Redundant Encoding Pattern is drawing a small message on most images .

The advantage of this method is that it can withstand the cropping ( failure ) .

The disadvantage is not able to draw a larger message .

1. Spread Spectrum method

Spread Spectrum Steganography scattered as the messages are scrambled (encrypted ) through images (unlike in the LSB ) . To read a message , the receiver requires that crypto -key algorithm and stego -key . This method is also still vulnerable to destruction or the destruction of the compression and the image ( the image ) .

REFERENCE

http://en.wikipedia.org/wiki/Steganography

http://www.google.com

http://www.wikipedia.com

http://[www.ilmukomputer.com](http://WWW.ILMUKOMPUTER.COM)

ACADEMIC OF INFORMATICA COMPUTER

ENGLISH ASSIGMENT GROUP

12.2A.37

Lecture : Muji Endah Palupi, SS

SEMESTER 2

“ STEGANOGRAPHY ”

CHAPTER 10



GRUP 10

Member :

ANTON IRAWAN (12133937)

ANGGI PRICILIA EKADEVI (12133976)

SITI NUR KHOMARIAH (12133845)

ZULFARIZAL ANDREA (12133859)