Seminar Report

On

**STEGANOGRAPHY**

In partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology in Computer Science & Engineering

Under

MAULANA ABUL KALAM AZAD

University of Technology,

WEST BENGAL

Submitted By

ANKITA GUPTA

Department of Computer Science & Engineering

Semester VI

Roll No: 11900113011

*email:ankitagupta9505 @gmail.com*

Y E A R : 2 0 1 6



S I L I G U R I I N S T I T U T E O F T E C H N O L O G Y

S I L I G U R I, W E S T B E N G A L

I N D I A

**ACKNOWLEGEMENT**

With great pleasure and deep sense of gratitude, I express my indebtedness to **Prof.**

**Mithun Roy** for his invaluable guidance and constant encouragement at each and

every step of my project work. He exposed me to the intricacies of relevant topics

through paper counseling and discussions and always showed great interest in providing

timely support and suitable suggestions.

I would also like to express my gratitude to all my friends in the Department of Computer

Science and Mr. Aniruddha Das for their constant support and encouragement. Words are not

enough to express my gratitude towards my parents to whom I owe every success and

achievements of my life. Their constant support and encouragement under all odds has

brought me where I stand today.

Date: April 12th 2016.

**Ankita Gupta**

11900113011

Department of CSE

Siliguri Institute of Technology

**ABSTRACT**

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

**CONTENTS**

|  |  |  |
| --- | --- | --- |
| SL NO | TITLE | PAGE NO |

**1. INTRODUCTION………………………………………... 5**

**2. HISTORY……………………………................................ 6**

**3. TECHNIQUE…………………………………………….. 6**

**3.1. PHYSICAL……………………………………… 7-8**

**3.2. DIGITAL MESSAGES…………….................... 8-10**

**3.3. NETWORK……………...................................... 11**

**3.4. PRINTED………………………………………. 11**

**3.5. USING PUZZLE………………………………. 12**

**4. GRAPHICAL REPRESENTATION…......................... 12**

**5. SYSTEM ANALYSIS & DESIGN…………………….. 12-13**

**6. APPLICATION**

**6.1. USE IN MODERN PRINTERS.….................. 13.**

**6.2. EXAMPLE FOR MODERN PRACTISE…… 13-14**

**6.3. Alleged use by Intelligence Services…………. 15**

**6.4. Distributed Steganography…………………... 15**

**6.5. Online Challenge……………………………… 15**

**7. WORKING…………………………………………….. 15-20**

**8. ADVANTAGE…………………………....................... 21**

**9. DISADVANTAGE…………………………………….. 21**

**10. CONCLUSION………………………………………. 22**

**11. REFERENCES………………………………………. 23**

**1. INTRODUCTION**

**Steganography** is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word *steganography* combines the [Greek](https://en.wikipedia.org/wiki/Greek_language) words *steganos*, meaning "covered, concealed, or protected", and *graphein*  meaning "writing".

The first recorded use of the term was in 1499 by [Johannes Trithemius](https://en.wikipedia.org/wiki/Johannes_Trithemius) in his [*Steganographia*](https://en.wikipedia.org/wiki/Johannes_Trithemius#Steganographia), a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages 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](https://en.wikipedia.org/wiki/Invisible_ink) between the visible lines of a private letter. Some implementations of steganography that lack a [shared secret](https://en.wikipedia.org/wiki/Shared_secret) are forms of [security through obscurity](https://en.wikipedia.org/wiki/Security_through_obscurity), whereas key-dependent steganographic schemes adhere to [Kerckhoffs's principle](https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle).

The advantage of steganography over [cryptography](https://en.wikipedia.org/wiki/Cryptography) alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where [encryption](https://en.wikipedia.org/wiki/Encryption) is illegal. Thus, whereas 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](https://en.wikipedia.org/wiki/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.

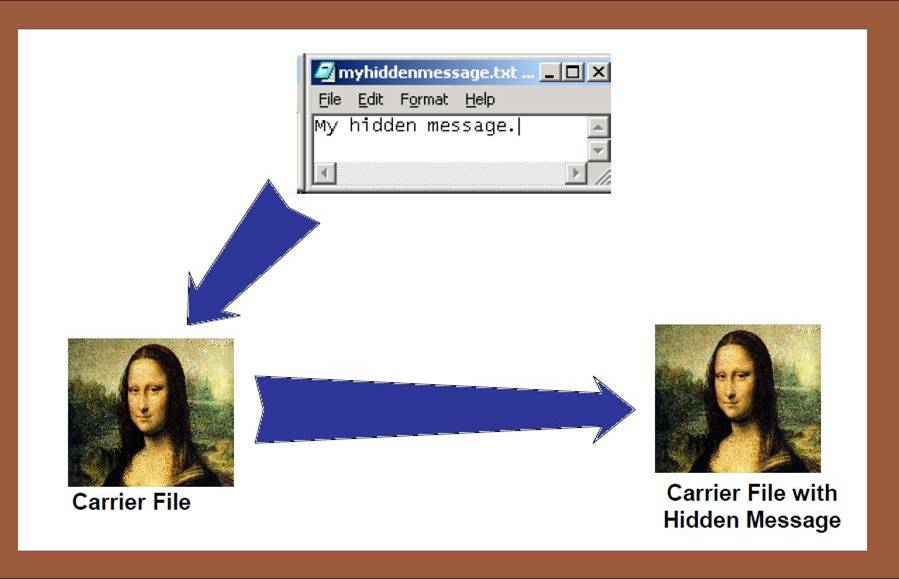


Figure 1: Example of steganography

**2. HISTORY**

[](https://en.wikipedia.org/wiki/File:Chart_in_the_hand_of_Dr_John_Dee._Steganographiae.png)

Figure2: A chart from [Johannes Trithemius](https://en.wikipedia.org/wiki/Johannes_Trithemius)'s[Steganographia](https://en.wikipedia.org/wiki/Steganographia) copied by [Dr John Dee](https://en.wikipedia.org/wiki/Dr_John_Dee" \o "Dr John Dee)in 1591

The first recorded uses of steganography can be traced back to 440 BC when [Herodotus](https://en.wikipedia.org/wiki/Herodotus) mentions two examples in his [*Histories*](https://en.wikipedia.org/wiki/The_Histories_of_Herodotus).[Demaratus](https://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](https://en.wikipedia.org/wiki/Wax_tablet) were in common use then as reusable writing surfaces, sometimes used for shorthand.

In his work *Polygraphiae* [Johannes Trithemius](https://en.wikipedia.org/wiki/Johannes_Trithemius) developed his so-called "[Ave-Maria-Cipher](https://en.wikipedia.org/w/index.php?title=Ave_Maria_Cipher&action=edit&redlink=1)" that 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*.

**3. TECHNIQUE**

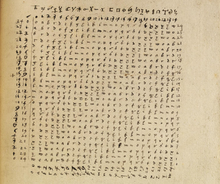
[](https://en.wikipedia.org/wiki/File:Steganography_in_the_hand_of_John_Dee.png)

Figure 3: Deciphering the code.*Steganographia*

**3.1 PHYSICAL**

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

* Hidden messages within [wax tablet](https://en.wikipedia.org/wiki/Wax_tablet)—in ancient [Greece](https://en.wikipedia.org/wiki/Greece), people wrote messages on wood and covered it with [wax](https://en.wikipedia.org/wiki/Wax) that bore an innocent covering message.
* Hidden messages on messenger's body—also used in ancient Greece. [Herodotus](https://en.wikipedia.org/wiki/Herodotus) tells the story of a message tattooed on the shaved head of a slave of [Histiaeus](https://en.wikipedia.org/wiki/Histiaeus), hidden by the hair that afterwards grew over it, and exposed by shaving the head. 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 restrictions on the number and size of messages that can be encoded on one person's scalp.
* During [World War II](https://en.wikipedia.org/wiki/World_War_II), the French Resistance sent some messages written on the backs of couriers in invisible ink.
* Hidden messages on paper written in [secret inks](https://en.wikipedia.org/wiki/Invisible_ink), under other messages or on the blank parts of other messages
* Messages written in [Morse code](https://en.wikipedia.org/wiki/Morse_code) on [yarn](https://en.wikipedia.org/wiki/Yarn) and then knitted into a piece of clothing worn by a courier.
* Messages written on envelopes in the area covered by [postage stamps](https://en.wikipedia.org/wiki/Postage_stamp).
* In the early days of the printing press, it was common to mix different typefaces on a printed page due to the printer not having enough copies of some letters in one typeface. Because of this, a message could be hidden using two (or more) different typefaces, such as normal or italic.
* During and after World War II, [espionage](https://en.wikipedia.org/wiki/Espionage) agents used photographically produced [microdots](https://en.wikipedia.org/wiki/Microdot) to send information back and forth. Microdots were typically minute (less than the size of the [period](https://en.wikipedia.org/wiki/Full_stop) produced by a [typewriter](https://en.wikipedia.org/wiki/Typewriter)). World War II microdots were embedded in the paper and covered with an adhesive, such as [collodion](https://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.
* During WWII, [Velva lee Dickinson](https://en.wikipedia.org/wiki/Velvalee_Dickinson), a spy for [Japan](https://en.wikipedia.org/wiki/Japan) in [New York City](https://en.wikipedia.org/wiki/New_York_City), sent information to accommodation addresses in neutral [South America](https://en.wikipedia.org/wiki/South_America). She was a dealer in [dolls](https://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.
* [Jeremiah Denton](https://en.wikipedia.org/wiki/Jeremiah_Denton) repeatedly blinked his eyes in [Morse Code](https://en.wikipedia.org/wiki/Morse_Code) during the 1966 televised press conference that he was forced into as an American [POW](https://en.wikipedia.org/wiki/POW) by his North Vietnamese captors, spelling out "T-O-R-T-U-R-E". This confirmed for the first time to the U.S. Military (naval intelligence) and Americans that the North Vietnamese were torturing American POWs.
* Cold War counter-propaganda. In 1968, crew members of the [USS *Pueblo*](https://en.wikipedia.org/wiki/USS_Pueblo_(AGER-2)) intelligence ship held as prisoners by [North Korea](https://en.wikipedia.org/wiki/North_Korea), communicated in sign language during staged photo opportunities, informing the [United States](https://en.wikipedia.org/wiki/United_States) they were not defectors, but captives of the North Koreans. In other photos presented to the US, crew members gave "[the finger](https://en.wikipedia.org/wiki/The_finger)" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

**3.2 DIGITAL MESSAGE**

[](https://en.wikipedia.org/wiki/File:Steganography_original.png)

Figure 4: Image of a tree with a steganographically hidden image.

The hidden image is revealed by removing all but the two least significant [bits](https://en.wikipedia.org/wiki/Bit) of each [color component](https://en.wikipedia.org/wiki/Color_component) and a subsequent [normalization](https://en.wikipedia.org/wiki/Normalization_(image_processing)). The hidden image is shown below.

[](https://en.wikipedia.org/wiki/File:Steganography_recovered.png)

Figure 5: Image of a cat extracted from the tree image above.

Modern steganography entered the world in 1985 with the advent of 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:

* Concealing messages within the lowest bits of [noisy](https://en.wikipedia.org/wiki/Image_noise) images or sound files.
* Concealing data within encrypted data or within random data. The message to conceal is encrypted, then 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](https://en.wikipedia.org/wiki/One-time_pad) generates ciphertexts that look perfectly random without the private key).
* [Chaffing and winnowing](https://en.wikipedia.org/wiki/Chaffing_and_winnowing).
* [Mimic functions](https://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](https://en.wikipedia.org/wiki/Ciphertext-only_attack).
* Concealed messages in tampered executable files, exploiting redundancy in the targeted [instruction set](https://en.wikipedia.org/wiki/Instruction_set).
* Pictures embedded in video material (optionally played at slower or faster speed).
* Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in keypresses in some applications ([telnet](https://en.wikipedia.org/wiki/Telnet) or[remote desktop software](https://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.
* Changing the order of elements in a set.
* Content-Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a nonhuman adversary/warden.
* [Blog](https://en.wikipedia.org/wiki/Blog)-Steganography. Messages are [fractionalized](https://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](https://en.wikipedia.org/wiki/Blogosphere).
* Modifying the echo of a sound file (Echo Steganography).
* Steganography for audio signals.
* Image [bit-plane complexity segmentation steganography](https://en.wikipedia.org/wiki/BPCS-Steganography)
* Including data in ignored sections of a file, such as after the logical end of the carrier file.

**3.2.1 DIGITAL TEXT**

* Making text the same color as the background in word processor documents, e-mails, and forum posts.
* Using [Unicode](https://en.wikipedia.org/wiki/Unicode) characters that look like the standard [ASCII](https://en.wikipedia.org/wiki/ASCII) character set. On most systems, there is no visual difference from ordinary text. Some systems may display the fonts differently, and the extra information would then be easily spotted, of course.
* Using hidden (control) characters, and redundant use of markup (e.g., empty bold, underline or italics) to embed information within HTML, which is visible by examining the document source. HTML pages can contain code for extra blank spaces and tabs at the end of lines, and colours, fonts and sizes, which are not visible when displayed.
* Using non-printing Unicode characters [Zero-Width Joiner](https://en.wikipedia.org/wiki/Zero-Width_Joiner) (ZWJ) and [Zero-Width Non-Joiner](https://en.wikipedia.org/wiki/Zero-Width_Non-Joiner) (ZWNJ). These characters are used for joining and disjoining letters in Arabic and Persian, but can be used in Roman alphabets for hiding information because they have no meaning in Roman alphabets: because they are "zero-width" they are not displayed. ZWJ and ZWNJ can represent "1" and "0".

**3.2.2 Social Steganography**

In communities with social or government taboos or censorship, people use cultural steganography—hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers. Examples include:

* Hiding a message in the title and context of a shared video or image
* Misspelling names or words that are popular in the media in a given week, to suggest an alternate meaning
* Hiding a Picture which can be traced by using Paint or any other Drawing tool.

****

FIGURE 6: IMAGE STEGANOGRAPHY

**3.3. 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](https://en.wikipedia.org/w/index.php?title=Krzysztof_Szczypiorski&action=edit&redlink=1) in 2003. Contrary to typical steganographic methods that use digital media (images, audio and video files) to hide data, network steganography uses communication protocols' control elements and their 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](https://en.wikipedia.org/wiki/Protocol_Data_Unit)), to the time relations between the exchanged PDUs, or both (hybrid methods).

Moreover, it is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term inter-protocol steganography.

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

* Steganophony — the concealment of messages in [Voice-over-IP](https://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.
* WLAN Steganography – transmission of steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks).

**3.4 PRINTED**

Digital steganography output may be in the form of printed documents. A message, the [*plaintext*](https://en.wikipedia.org/wiki/Plaintext), may be first encrypted by traditional means, producing a [*cipher text*](https://en.wikipedia.org/wiki/Ciphertext). Then, an innocuous *cover text* is modified in some way so as to contain the ciphertext, resulting in the *stegotext*. For example, the letter size, spacing, [typeface](https://en.wikipedia.org/wiki/Typeface), or other characteristics of a cover text 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](https://en.wikipedia.org/wiki/Francis_Bacon) developed [Bacon's cipher](https://en.wikipedia.org/wiki/Bacon%27s_cipher) as such a technique.

The cipher text 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.

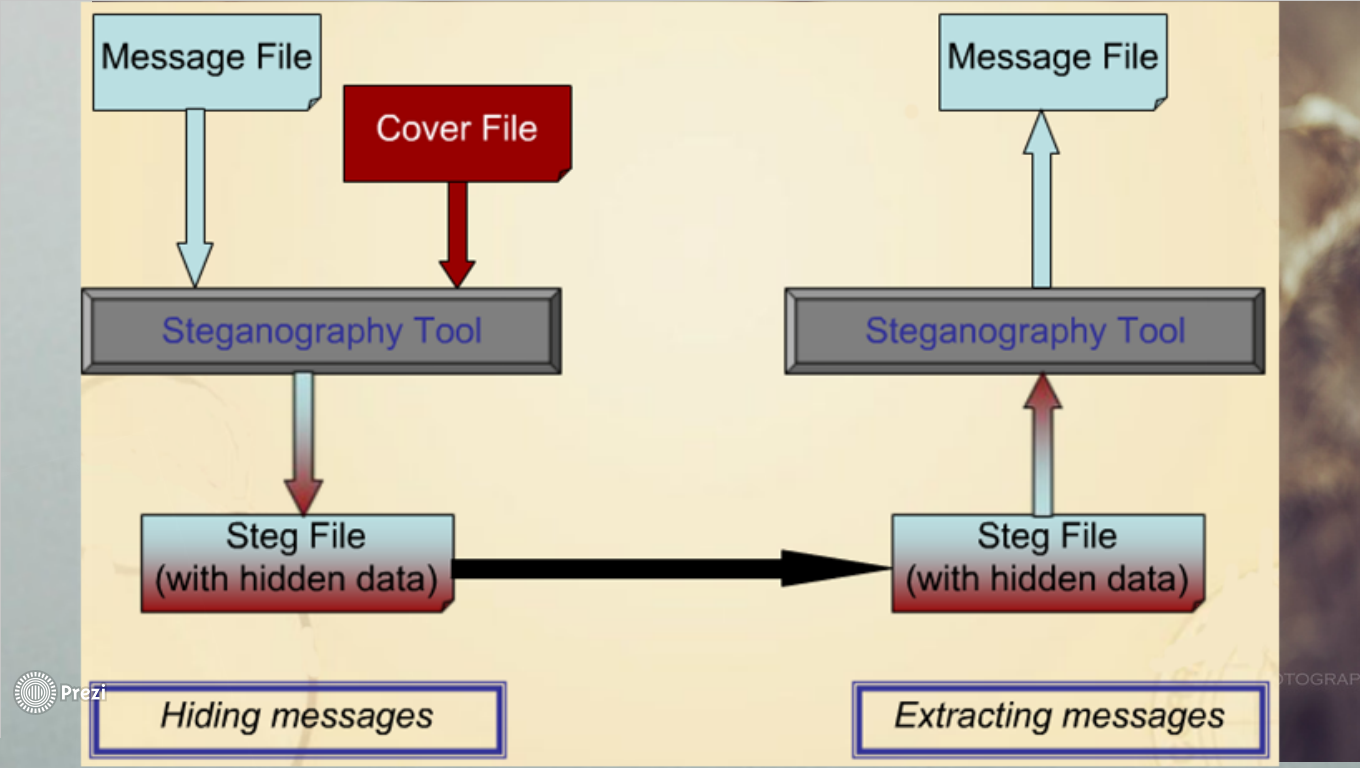
**3.5 USING PUZZLES**

The art of concealing data in a puzzle can take advantage of the degrees of freedom in stating the puzzle, using the starting information to encode a key within the puzzle / puzzle image.

For instance, steganography using sudoku puzzles has as many keys as there are possible solutions of a sudoku puzzle, which is 6.71×1021. This is equivalent to around 70 bits, making it much stronger than the [DES](https://en.wikipedia.org/wiki/Data_Encryption_Standard) method, which uses a 56 bit key.

**4. Graphical Representation**

The graphical representation of Steganography system is as follows:



**Figure 7: Steps involved in Steganography**

**5. SYSTEM ANALYSIS & DESIGN**

Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt. Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simples programming. One of .Net tools for pictures and images is auto-converting most types of pictures to BMP format. I used this tool in this software called “Steganography” that is written in C#.Net language and you can use this software to hide your information in any type of pictures without any converting its format to BMP (software converts inside it).

The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires.  
  
The **encrypt module** is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.  
The **decrypt module** is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that.

**6. APPLICATION**

**6.1 Use in modern printers**

*Main article:*[*Printer steganography*](https://en.wikipedia.org/wiki/Printer_steganography)

Some modern computer printers use steganography, including [HP](https://en.wikipedia.org/wiki/Hewlett-Packard) and [Xerox](https://en.wikipedia.org/wiki/Xerox) brand color laser printers. These printers add tiny yellow dots to each page. The barely-visible dots contain encoded printer serial numbers and date and time stamps.

**6.2. Example from Modern Practice**

The larger the cover message (in binary data, the number of [bits](https://en.wikipedia.org/wiki/Bit)) relative to the hidden message, the easier it is to hide the latter. For this reason, [digital pictures](https://en.wikipedia.org/wiki/Digital_image) (which contain large amounts of data) are used to hide messages on the [Internet](https://en.wikipedia.org/wiki/Internet) and on other communication media. It is not clear how common this actually is. For example: a 24-bit bitmap uses 8 bits to represent each of the three color values (red, green, and blue) at each [pixel](https://en.wikipedia.org/wiki/Pixel). The blue alone has 28 different levels of blue intensity. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the [least significant bit](https://en.wikipedia.org/wiki/Least_significant_bit) can be used more or less undetectably for something else other than color information. If this is repeated for the green and the red elements of each pixel as well, it is possible to encode one letter of [ASCII](https://en.wikipedia.org/wiki/ASCII) text for every three [pixels](https://en.wikipedia.org/wiki/Pixel).

Stated somewhat more formally, the objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (the original signal) due to the injection of the payload (the signal to covertly embed) are visually (and ideally, statistically) negligible; that is to say, the changes are indistinguishable from the [noise floor](https://en.wikipedia.org/wiki/Noise_floor) of the carrier. Any medium can be a carrier, but media with a large amount of redundant or compressible information are better suited.

From an [information theoretical](https://en.wikipedia.org/wiki/Information_theory) point of view, this means that the [channel](https://en.wikipedia.org/wiki/Channel_(communications)) must have more [capacity](https://en.wikipedia.org/wiki/Channel_capacity) than the "surface" [signal](https://en.wikipedia.org/wiki/Signal_(information_theory)) requires; that is, there must be [redundancy](https://en.wikipedia.org/wiki/Redundancy_(information_theory)). For a digital image, this may be [noise](https://en.wikipedia.org/wiki/Noise) from the imaging element; for [digital audio](https://en.wikipedia.org/wiki/Digital_audio), it may be noise from recording techniques or [amplification](https://en.wikipedia.org/wiki/Amplifier) equipment. In general, electronics that digitize an [analog signal](https://en.wikipedia.org/wiki/Analog_(signal)) suffer from several noise sources such as [thermal noise](https://en.wikipedia.org/wiki/Johnson-Nyquist_noise), [flicker noise](https://en.wikipedia.org/wiki/Flicker_noise), and [shot noise](https://en.wikipedia.org/wiki/Shot_noise). This noise provides enough variation in the captured digital information that it can be exploited as a noise cover for hidden data. In addition, [lossy compression](https://en.wikipedia.org/wiki/Lossy_compression) schemes (such as [JPEG](https://en.wikipedia.org/wiki/JPEG)) always introduce some error into the decompressed data; it is possible to exploit this for steganographic use as well.

Steganography can be used for [digital watermarking](https://en.wikipedia.org/wiki/Digital_watermark), where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified (for example, [Coded Anti-Piracy](https://en.wikipedia.org/wiki/Coded_Anti-Piracy)), or even just to identify an image (as in the [EURion constellation](https://en.wikipedia.org/wiki/EURion_constellation)).

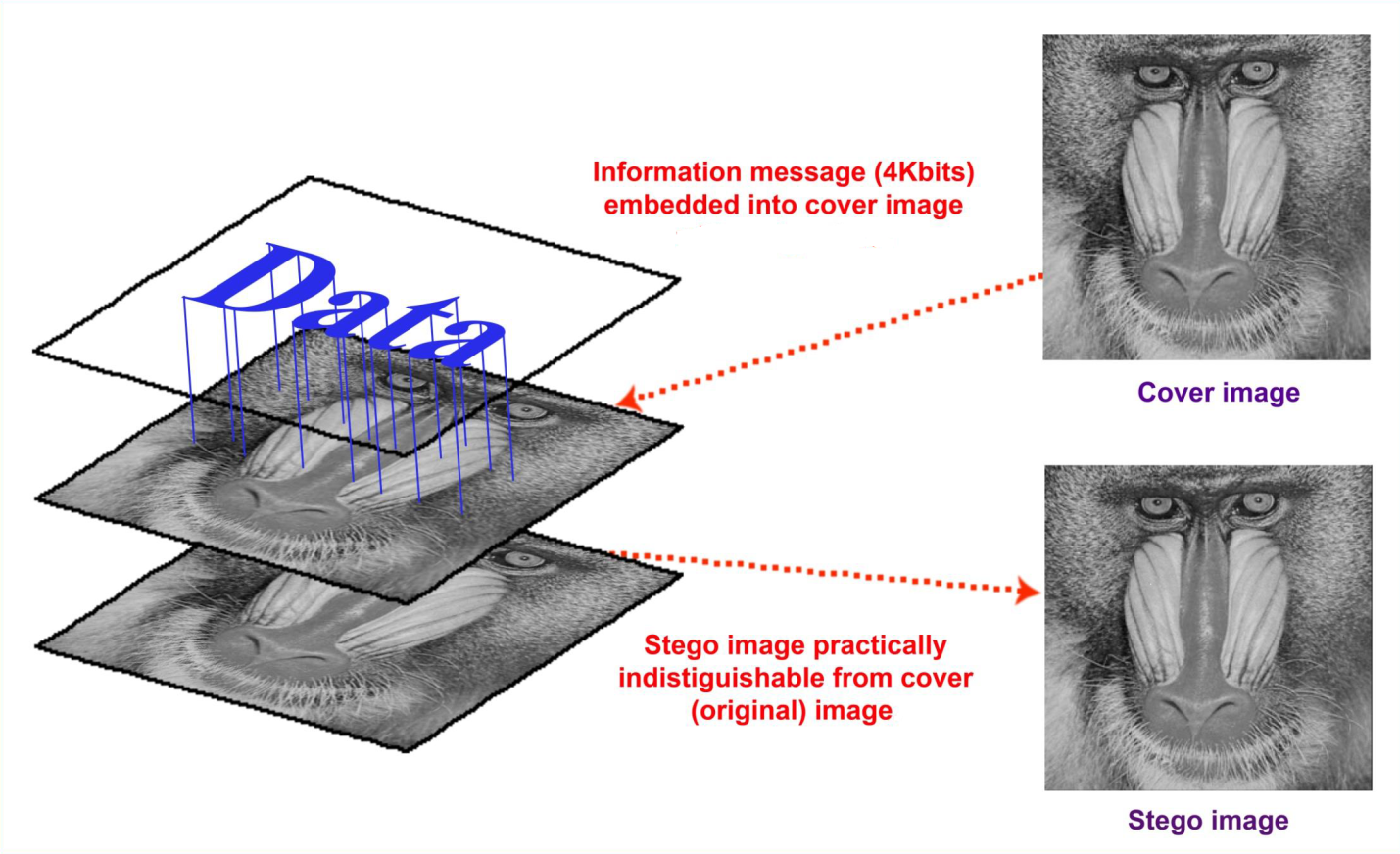


FIGURE 8: COVER IMAGE AND STEGO IMAGE

**6.3 Alleged use by Intelligence Services**

In 2010, the [Federal Bureau of Investigation](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) alleged that the [Russian foreign intelligence service](https://en.wikipedia.org/wiki/Foreign_Intelligence_Service_(Russia)) uses customized steganography software for embedding encrypted text messages inside image files for certain communications with "illegal agents" (agents under non-diplomatic cover) stationed abroad.

**6.4 Distributed Steganography**

There are distributed steganography methods, including methodologies that distribute the payload through multiple carrier files in diverse locations to make detection more difficult. For example, [U.S. Patent 8,527,779](https://www.google.com/patents/US8527779) by cryptographer William Easttom (Chuck Easttom).

**6.5 Online challenge**

The puzzles presented by [Cicada 3301](https://en.wikipedia.org/wiki/Cicada_3301) incorporates steganography with cryptography and other solving techniques since 2012.

**7. WORKING**

**7.1 DATA HIDING**

target=imread('image.jpg');

fid = fopen('messeage.txt','r');

F = fread(fid);

s = char ('F');

fclose (fid);

original=target;

sz1=size (original);

size1=sz1 (1)\*sz1 (2);

sz2=size (F);

size2=sz2 (1);

if size2> size1

fprintf ('\nImage File Size %d\n',size1);

fprintf('Text File Size %d\n',size2);

disp('Text File is too Large');

else

fprintf('\nImage File Size %d\n',size1);

fprintf('Text File Size %d\n',size2);

disp('Text File is Small');

i=1;j=1;k=1;

while k<=size2

a=F(k);

o1=original(i,j,1);

o2=original(i,j,2);

o3=original(i,j,3);

[r1,r2,r3]=hidetext(o1,o2,o3,a);

target(i,j,1)=r1;

target(i,j,2)=r2;

target(i,j,3)=r3;

if(i<sz1(1))

i=i+1;

else

i=1;

j=j+1;

end

k=k+1;

end

width=sz1(1);

txtsz=size2;

n=size(original);

target(n(1),n(2),1)=txtsz;% Text Size

target(n(1),n(2),2)=width;% Image's Width

%save secret.mat target; % txtsz width;

imwrite(target,'secret.bmp','bmp');

imshow(target)

end

****

**FIGURE 9: ORIGNAL IMAGE (image.jpg)**

**7.2 DATA RETRIVAL**

target=imread('secret.bmp');

n=size (target);

txtsz=target(n(1),n(2),1);% Text Size

width=target(n(1),n(2),2);% Image's Width

i=1;j=1;k=1;

while k<=txtsz

r1=target(i,j,1);

r2=target(i,j,2);

r3=target(i,j,3);

R(k)=findtext(r1,r2,r3);

if(i<width)

i=i+1;

else

i=1;

j=j+1;

end

k=k+1;

end

fid = fopen('secret.txt','wb');

fwrite(fid,char(R),'char');

fclose(fid);

**7.3 FUNCTION OF HIDETEXT**

function[red,green,blue]=hidetext(redc,greenc,bluec,text)

red=bitand(redc,248);

green=bitand(greenc,248);

blue=bitand(bluec,252);

txt=0;

if bitand(text,128)== 128

red=bitor(red,4);

end

if bitand(text,64)== 64

red=bitor(red,2);

end

if bitand(text,32)== 32

red=bitor(red,1);

end

if bitand(text,16)== 16

green=bitor(green,4);

end

if bitand(text,8)== 8

green=bitor(green,2);

end

if bitand(text,4)== 4

green=bitor(green,1);

end

if bitand(text,2)== 2

blue=bitor(blue,2);

end

if bitand(text,1)== 1

blue=bitor(blue,1);

end

return

**7.4 FUNCTION OF FINDTEXT**

function data = findtext(redc,greenc,bluec)

txt=0;

if bitand(redc,4)== 4

txt=bitor(txt,128);

end

if bitand(redc,2)== 2

txt=bitor(txt,64);

end

if bitand(redc,1)== 1

txt=bitor(txt,32);

end

if bitand(greenc,4)== 4

txt=bitor(txt,16);

end

if bitand(greenc,2)== 2

txt=bitor(txt,8);

end

if bitand(greenc,1)== 1

txt=bitor(txt,4);

end

if bitand(bluec,2)== 2

txt=bitor(txt,2);

end

if bitand(bluec,1)== 1

txt=bitor(txt,1);

end

data=txt;

return

****

**FIGURE 10:RECEIVED IMAGE(secret.bmp)**

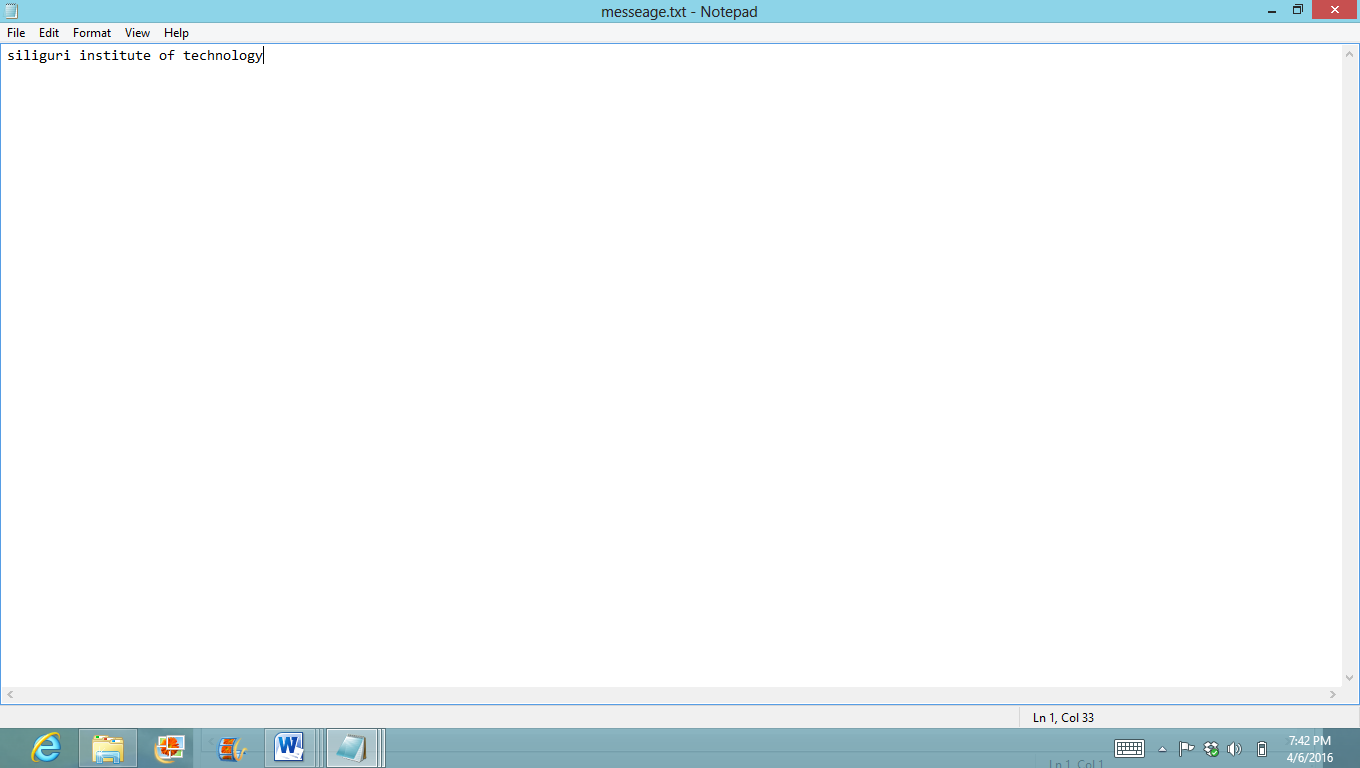
****

FIGURE 11:HIDDEN MESSAGE

**9. ADVANTAGES**

* Difficult to detect and only receiver can detect.
* It can be done faster with large number of software.
* Provides better security for sharing data in LAN, MAN & WAN.

**10. DISADVANTAGES**

* The confidentiality of information is maintained by the algorithms, and if the algorithms are known then this technique is of no use.
* Password leakage may occur and it leads to the unauthorized access of data.
* If the technique is gone in the wrong hands like hackers can be very much dangerous for all.

**11. CONCLUSION**

* This seminar provides an overview of steganalysis and introduced some characteristics of steganographic software that point signs of information hiding.
* The ease in use and abundant availability of steganography tools has law enforcement concerned in trafficking of illicit material via web page images, audio, and other transmissions over the internet.
* Where standard cryptography and encryption is outlawed, steganography can be used.
* Formerly, just an interest of the military, steganography is now gaining popularity among the masses.

**12. REFERENCES**

* <https://en.wikipedia.org/wiki/Steganography>
* <http://www.sarc-wv.com/news.aspx>
* <http://www.strangehorizons.com/2001/20011008/steganography.shtml>
* [http://\vww.jjtc.com/stegdoc](http://vww.jjtc.com/stegdoc)
* Hide & Seek: An Introduction to Steganography: Niles Provos and Peter Honeyman.