

INSTITUTE OF INFORMATION TECHNOLOGY



Jahangirnagar University

জাহাঙ্গীরনগর বিশ্ববিদ্যালয়

IT-4259: Computer Network Security

for

4th Year 2nd Semester of B.Sc (Honors) in IT (5th Batch)

Lecture: 06

Steganography- A Security Mechanism

Prepared by:

K M Akkas Ali

akkas_khan@yahoo.com, akkas@juniv.edu

Associate Professor

Institute of Information Technology (IIT)

Jahangirnagar University, Dhaka-1342

Objectives of this Lecture:

- ❖ To know the general idea behind steganography.
- ❖ To be familiar with basic terminology related to steganography.
- ❖ To introduce the concepts of historical use of steganography.
- ❖ To be familiar with some steganographic examples.
- ❖ To distinguish between cryptography and steganography.
- ❖ To discuss about **The Third Eye**- an steganographic application.

Steganography: An Introduction

What is Steganography:

- Steganography is a Greek word which means “covered or hidden writing”. It is the art of hiding a message within another medium in such a way that prevents the detection of hidden messages.
- It keeps third parties out from knowing that the intended message is even there. Only the intended recipients know it is there and intelligible to them only.

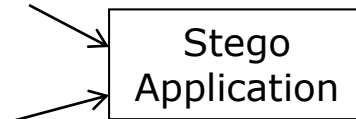
Steganography: An Introduction

General Idea Behind Steganography:

In steganography, the message "Set up the bomb" may be concealed by **covering** it with another Sentence to convey the original.

Carrier or Cover media
(text, image, audio or video)

Message or data to hide
(text, image, audio, video etc.)



Stego object

Carrier or Cover media

Sharif eats tablets under pressure, that helps everything before offering Malaysian beer.

message

Original message

Set up the bomb

Sharif **e**ats **t**ablets under **p**ressure, **t**hat **h**elps **e**verything **b**efore offering **M**alaysian **b**eer.

Set up the bomb

Stego object

Sender: Alice

Recipient: Bob

Basic Terminology Related to Steganography

❖ **Carrier, Container, Cover Media or Unobtrusive media:**

The innocent-looking media in which an original message is hidden is called **cover**, **carrier** or **container**. That is, the files hiding other files are usually referred to as “carrier” files. Cover may be text (coverttext), image (coverimage), audio, video etc.

These files are made so that, whilst containing the hidden information, they are still mostly functional and will not arouse suspicion to anyone not specifically looking for them.

❖ **Message/ Embedded Object:**

The data that is to be hidden inside the carrier is the message. Observe that a message need not be text. It can as well be another picture, a sound, video or a zip file or a word document or anything else that is a “file”.

❖ **Stego or Stego Object:**

When the message is hidden in the cover, the resulting object is called a stego-object. The Carrier becomes a “**Stego**” or stego medium after it hides data into itself.

Historical Usage of Steganography:

History is full of facts and myths about the use of steganography. People in the past used steganography for secret communication purpose in a variety of ways. Some of them includes:

The Greeks and wax-covered tablets:

- Steganography as hidden writing was used to refer to practices of leaders hiding messages sent to other leaders.
- In ancient Greece, text was written in wooden tablets and covered them with wax upon which an innocent covering message was written.
- To pass a hidden message, a person would scrape the wax off of a tablet, write a message on the underlying wood and again cover the tablet with wax to make it appear blank and unused so it passed inspection by sentries without question.

Historical Usage of Steganography:

Hidden messages on messenger's body:

- During the Roman Empire, secret information was tattooed on a messenger's shaved head.
- A messenger's head was shaved, a message tattooed upon it.
- Several weeks later, the messenger's hair has grown in and completely concealed the secret information.
- After that, the messenger is sent to remote place to intended person to deliver the message by shaving his head again.
- Other people would not be aware he was carrying a message.
- 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 its one-off use since additional messages requires additional slaves.

Historical Usage of Steganography:

Invisible inks in WWII:

- Invisible inks offered a common form of invisible writing.
- Early in World War II, steganographic technology consisted almost exclusively of these inks. Invisible inks were used to write a secret message between the lines of the covering message. The secret message was exposed when the paper was heated or treated with another substance.
- With invisible ink, a seemingly innocent letter could contain a very different message written between the lines.
- Common sources for invisible inks are lemon juice, onion juice, milk, vinegar, urine etc. All of these turn dark when heated or held over a flame.
- If, as a child, you ever wrote an invisible message in lemon juice and had your friend hold it next to a light bulb in order to watch the message magically appear, you've used steganography.
- Invisible inks are often used as anti-counterfeit devices. For example, "VOID" is printed on checks and other official documents in an ink that appears under the strong ultraviolet light used for photocopies.

Historical Usage of Steganography:

Letters with pencil lead:

- Some letters in an innocuous message might be **overwritten** in a **pencil lead** that is visible only **when exposed to light at an angle**.

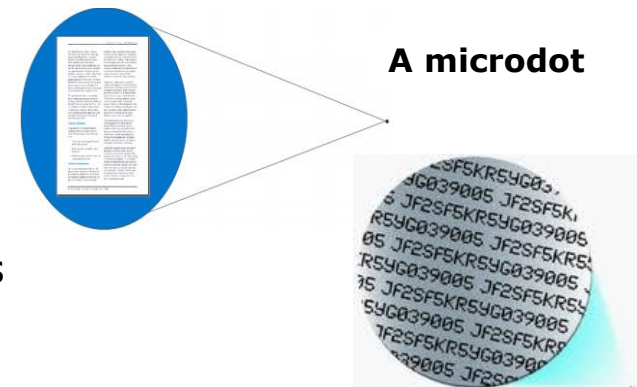
Spoken Language Steganography:

- The way language is spoken may encode a message.
- **Pauses**, **throat clearing**, and **enunciations** may all be used to trigger hidden messages to an intended listener.

Historical Usage of Steganography:

Microdot between WWI and WWII:

- A **microdot** is text or an image photographically reduced to the size and shape of a typographical dot and stuck to an otherwise innocuous typescript or under a postage stamp to prevent detection by unintended recipients.
- The **Germans developed microdot technology** for steganographic purposes between World War I and World War II.
- The **espionage agents** used microdots to send information back and forth.
- Using this technique, **message is photographed using "reverse microscope"** to generate microdots.
- Photographic **dot is cut** out with a hypodermic needle.
- Microdot is then placed on a period in a cover message and sent via normal means.
- These microdots often went unnoticed by inspectors, and information could be read by the intended recipient using a microscope.
- **Being so small** as to not draw attention, microdot technology permits the transmission of large amounts of data, including drawings and photographs



Enlarge view of a microdot

Historical Usage of Steganography:

Open coded messages (1st, 2nd etc letter steganography):

- Null cipher (unencrypted or open coded message) can be used to hide information, since it sounds innocent and is used as ordinary occurrences.
- The real message is "camouflaged" or hidden in an innocent-sounding message.
- Because many open-coded messages don't seem to be cause for suspicion, and therefore sound normal and innocent, the suspect communications can be detected by mail filters while "innocent" messages are allowed to flow through.
- For example, the following null-cipher message was actually sent by a German spy in WWII:

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.

- Decoding this message by extracting the second letter in each word reveals the following, hidden message:

Pershing sails from NY June 1.

Some Steganographic Examples:

Illustrations of some methods for implementing steganography:

- Assume that two prisoners, **Alice** and **Bob**, are trying to plan a jail escape while under the watchful eye of jail police Eve.
- **Eve** will not tolerate suspicious behavior, such as passing notes that are clearly encrypted.
- So Alice and Bob communicate such that it seems they are talking about something harmless (such as the weather or their families) when they are actually planning an escape.
- From this simple theoretical example, many steganographic techniques and practices have spawned and have helped improve data security in the real world.
- Some **examples** are described below.

Some Steganographic Examples:

Example-1: 1st Letter Steganography

- In cryptography, the message "Set up the bomb" may be concealed by the secret writing "Rds to sgd anla" through shifting to one character before the actual character.
- In steganography, the same message may be concealed by covering it with another sentence to convey the original. For example: Set up the bomb is concealed as:

Sharif **e**ats **t**ablets **u**nder **p**ressure, **t**hat **h**elps **e**verything **b**efore
offering **M**alaysian **b**eer.

Some Steganographic Examples:

Example-2: 2nd Letter Steganography

- "Run and hide" is embedded by taking the second letter of each word in the sentence, as shown below:

Around July, anyone may encounter odd white lights
adorning sea-skies.

Example-3: Using different types of fonts

- "I can sing" is embedded by using two type fonts with slight differences: Arial and Verdana.

Computer is a multitasking electronic device which is capable of
performing a lot of tasks within a single moment.

Some Steganographic Examples:

Example-4: Inserting binary data using open space Steganography

- Consider the following innocuous short message:
“This lecture is mostly about cryptography, not for steganography”
- If we use single space between words to represent the binary digit 0 and double space to represent binary digit 1, then message can hide the bit stream 01000001 which is letter A (since, 8-bit binary representation of the letter **A** in ASCII code is 01000001):

This lecture is mostly about cryptography, not for steganography

0 1 0 0 0 0 0 1 = A

Some Steganographic Examples:

Example-5: Open or extra space Steganography

- "Made it out. Send money" is embedded by taking the first letter of every word that follows an extra space, as shown below by underlining the extra spaces and bolding the letters following:

Hidden **m**essages could also **a**ppear in the form of miniscule typeface, size, or spacing **d**ifferences. **E**xtra spaces before certain words could **i**ndicate that **t**hose words **o**r the first letters of those words should be taken apart from the entire message to reveal a secret embedded **u**tterance. **T**his is especially handy in html files **s**ince **e**xtra spaces show up only in the source file and **n**ot on the webpage **d**isplay. Letters that are slightly larger **m**ight similarly be taken to reveal a hidden message. It could even be that, through use of invisible ink between lines **o**f text or tiny print within underlining or punctuation, the true message is **n**ot visible at all. Some of these methods may be **e**asier to detect than others, but they have had their own practical uses in history, as we will saw in the previous section. Can **y**ou find the message hidden in this paragraph?

Some Steganographic Examples:

Example-6: Steganography using Dictionary

- We can use a dictionary of words organized according to their grammatical usages.
- For example, we can have a dictionary containing 2 articles, 8 verbs, 32 nouns, and 4 prepositions.
- Then we agree to use cover text that always use sentences with the pattern:
article-noun-verb-article-noun
- The secret binary data can be divided into 16-bit chunks:
 - ❑ The **first bit** of binary data can be represented by an article (for example, 0 for a and 1 for the).
 - ❑ The **next five bits** can be represented by a noun (subject of the sentence).
 - ❑ The **next 4 bits** can be represented by a verb.
 - ❑ The **next bit** can be represented by the second article.
 - ❑ The **last five bits** can be represented by another noun (object).
- Using this technique, the message "HI" can be concealed in the sentence like the following:

Ascii code of HI	0100100001001001				
Divisions of the bits	0	10010	0001	0	01001
Sentence pattern	article	noun	verb	article	noun
Stego object	a	friend	called	a	doctor

Some Steganographic Examples:

Example-7: Word shifting Steganography

- Consider the following sentence and termed it as S_1 :

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.

- Apply word-shifting algorithm in S_1 :

- ❖ Expanding the space before **explore**, world, **wide** and **web** by one point.
- ❖ Condense the space after **explore**, world, **wide** and **web** by one point.

- We get the modified sentence S_2 as:

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 combining or overlapping S_1 and S_2 , produces a different message: **explore the world wide web**. The sentences containing the shifted words appear harmless.

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.

Some Steganographic Examples:

Example-8: Ave Maria Steganography

- Ave Maria cipher is a clever message encryption method used in ancient time.
- The cipher is a table of 384 parallel columns of Latin words.
- Each word on the table represents a plaintext character.
- To code a message, the message letters are replaced by the corresponding words on the table. The coded message then looks like innocent religious litanies.
- For example, let us consider the 26 alphabets of English where each character represents a word listed below.





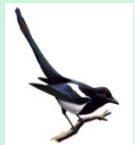





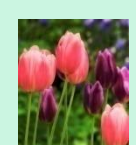















A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
America	Bangladesh	Canada	Denmark	England	France	Germany	Hong Kong	India	Japan	Korea	Libya	Malaysia	Nepal	Oman	Portugal	Qatar	Romania	Sri Lanka	Thailand	Uganda	Venezuela	West Indies	Xinjiang	Yemen	Zimbabwe

- For example, the plaintext "LOVE" is encrypted as "Libya Oman Venezuela England" using the above table.

Some Steganographic Examples:

Example-9: Image Label Steganography

- For example, let us consider the 26 alphabets of English where each character represents an image listed below.

A	B	C	D	E	F	G	H	I	J	K	L	M
												
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
												

- For example, using the above table, the plaintext "Hit them" is encrypted as:

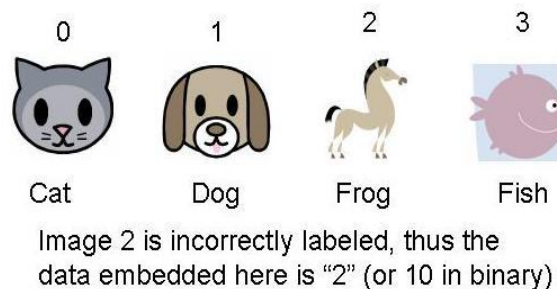


= Hit them

Some Steganographic Examples:

Example-10: Image Label Steganography

- In the past, steganography has hidden data in unimportant parts of files and altered the "syntax" of covers without being concerned with "semantics."
- The goal was to hide messages from humans who did not know to look for them, and this goal was achieved quite well.
- However, computers were very good at detecting the secret communications. So it makes more sense to focus on fooling machines than to focus on fooling men.
- Image labeling steganography may be obvious to humans but not to current artificial intelligence (AI) tactics which is shown below:



- In the case (illustrated in figure above), the human recipient detects which of a series of textual labels for different images is actually incorrect and the position of this image in the list of images embeds part of a message. This method can be repeated multiple times to reveal a full message.

Some Steganographic Examples:

Example-11: Audio Embedding Steganography

Hiding Information in Audio: Uses least significant bits in wav file

It is simple to encode a message **by** varying byte values in an audio.

- Let us assume an audio file had the following 8 bytes of data somewhere in it:

180, 229, 139, 172, 209, 151, 21, 104

- In binary, this would be:

10110100-11100101-10001011-10101100-11010001-10010111-00010101- 01101000

- If we wanted to hide the byte value 11010110, we use the least significant bit from each byte to hide our byte:

10110101-11100101-10001010-10101101-11010000-10010111-00010101- 01101000

- The changes result in the following bytes, which are so close to the originals that the difference will be inaudible:

Modified: 181, 229, 138, 173, 208, 151, 21, 104

Original: 180, 229, 139, 172, 209, 151, 21, 104

- Similarly, a message can also be hidden or embedded in image (Using slightly different colors to hide a message) or video formatted file.

Some Steganographic Examples:

Example-12: Image Embedding Steganography

Hiding a message in an image file: Uses least significant bits in image file.

It is simple to encode a message by varying lines, colors or other elements in an image. Least Significant Bit of each pixel is used to encode characters, with 8 pixels per character.

- Let us assume that an image file had the following three pixels (9 bytes) of data somewhere in it:

Pixel-1 (RGB): 0101001**0**, 1001011**0**, 1010010**0**

Pixel-2 (RGB): 1011010**0**, 1001000**1**, 0100111**0**

Pixel-3 (RGB): 1011011**0**, 0010111**0**, 11010001

- If we want to hide the letter A (whose binary value is 10000011) in the three pixels of the image, we insert the binary value for A in the three pixels using the least-significant bits of each byte to hide A:

Pixel-1 (RGB): 0101001**1**, 1001011**0**, 1010010**0**

Pixel-2 (RGB): 1011010**0**, 1001000**0**, 0100111**0**

Pixel-3 (RGB): 1011011**1**, 0010111**1**, 11010001

- Only half of the least significant bits of the pixels changed. The numeric value of each byte changed very little. The changes result in the image are so close to the originals that the difference will not be identified with naked eye. To the human eye, the resulting stego-image will look identical to the cover image.

Difference Between Cryptography and Steganography

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Cryptography	Steganography
Cryptography is a Greek word which means "secret writing".	Steganography is also a Greek word which means "covered or hidden writing".
Cryptography is a security technique in which the contents of a message is concealed by enciphering.	Steganography is also a security technique in which a message is concealed by covering it with something else.
Here the original data (called plaintext) is passed through a series of mathematical operations that generate an alternate form of the original data known as ciphertext.	It is the art of hiding a message within another medium in such a way that prevent the detection of hidden messages. The resulting file is called a "stego file."
Encryption doesn't hide data, but it does make it hard to read. The encrypted data can only be read by parties who have been given the necessary key to decrypt the ciphertext back into its original plaintext form.	Steganography hides data. It keeps third parties out from knowing that the intended message is even there. Only the intended recipients know it is there and intelligible to them only.

Difference Between Cryptography and Steganography

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Cryptography	Steganography
Cryptography provides privacy	Steganography is intended to provide secrecy.
(Privacy is what you need when you use your credit card on the Internet - you don't want your number revealed to the public. For this, you use cryptography, and send a coded pile of gibberish that only the web site can decipher. Though your code may be unbreakable, any hacker can look and see you've sent a message. For true secrecy, you don't want anyone to know you're sending a message at all).	
Cryptography "scrambles" a message so if intercepted, it cannot be understood.	Steganography "camouflages" a message to hide its existence, so it cannot be seen.
Encryption only obscures a message's meaning, not its existence. Although encrypted data is difficult to decipher, it is relatively easy to detect. An encrypted message, for instance, may draw suspicion on the part of the recipient though third parties may not be able to read the message, but they know one was sent.	Steganography is not meant to obscure the message, but to obscure the fact that there is a message at all. So, an "invisible" message created with steganographic methods will not arouse suspicion. Therefore, steganography is often used to supplement encryption.

Difference Between Cryptography and Steganography

Prepared by: K M Akkas Ali, Assistant Professor, IIT, JU

Cryptography	Steganography
<p>In cryptography, the original message that is to be sent from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext or encrypted text. In case of symmetric key cryptography, to create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key.</p>	<p>In steganography, the original message that is to be sent from Alice to Bob is called original or embedded message which may be plaintext, ciphertext, image, audio, video etc. The innocent-looking media in which an original message is hidden is called cover or carrier. Cover may be text (coverttext), image (coverimage), audio, video etc. When the plaintext message is hidden in the cover, the resulting object is called a stego-object. A stego-key (a type of password) may also be used to hide, then later decode, the message.</p>
<p>Attacks against cryptography take what is known to be an encrypted message and attempt to decrypt the message.</p>	<p>Attacks against steganography take what seems to be an ordinary image, text, multimedia file, or other document and determine whether or not there is another message hidden within.</p>

Difference Between Cryptography and Steganography

Prepared by: K M Akkas Ali, Assistant Professor, HIT, JU

Cryptography	Steganography
As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes.	As steganography is the art of hiding a message within another medium, steganalysis is the art of analyzing potential stego-mediums for the traces of steganographic modifications.
Cryptanalysis or steganalysis is needed, not to break other people's code, but to learn how vulnerable our cryptosystem or stegosystem is. It helps us create better secret codes.	

Cryptography with Steganography:

- Hiding a message with steganography methods **reduces the chance of a message being detected**. Steganography is not intended to replace cryptography but supplement it. **They are strongest when combined**. A message sent in secret (steganography) in an encrypted form (cryptography) is much more secure than the message sent by secret means.
- Imagine the common situation when you encrypt your important business data. Suddenly robbers capture and torture you into revealing cryptographic keys. As well police power may be abused. They ask you to give them the private keys or you are highly suspicious of committing crime. Next, **what if the police is bribed**. Would not it be better, if you can plausibly deny the existence of important data?
- **Cryptography along with steganography** goes a step further and makes the ciphertext invisible to unauthorized users.

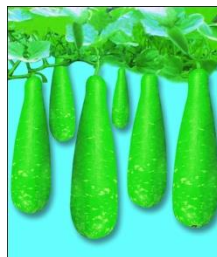
Plaintext

Just shoot him

Cryptography

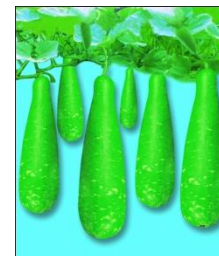
Ciphertext

Itrs rgns ghl



***Carrier image/
Unobtrusive media***

Stego object



steganography

From Alice

To Bob

What is Steganography used for:

- Steganography is a fascinating and effective method of hiding data that has been used throughout history.
- **The aim of steganography is** to conceal information inside other data that is harmless (or not secret) and thus, it secure data from the adversary.
- Like many security tools, it can be used for a variety of reasons for both legitimate or criminal purposes.
 - Covert communications
 - **Watermarks and signatures for copyright protection**
 - Terrorism, espionage and pornography.

What is Steganography used for:

Steganography for Legitimate Purpose:

- In legitimate purpose, steganography can be used for-
 - ✓ Covert communications
 - ✓ Watermarks and signatures for copyright protection
- For **copyright protection**, steganography can be used as watermarking images. Digital watermarks (also known as "fingerprinting") are similar to steganography in that they are overlaid in files, which appear to be part of the original file and therefore are not easily detectable by the average person.
- Further, steganography can be used **to tag notes to online images** like post-it notes attached to paper files.
- Finally, steganography can be used **to maintain the confidentiality** of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

What is Steganography used for:

Steganography for Criminal Purpose:

Unfortunately, steganography can also be used to hide illicit, unauthorized or unwanted activity for illegitimate purposes:

- ❑ For instance, if someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer.
- ❑ The most common misuse of steganography is the hiding of malware into seemingly safe files such as pictures, audio and email attachments. This method is used to hide any type of malware ranging from viruses to worms from spyware to Trojans.
- ❑ Furthermore, a person with a hobby of saving pornography, or worse, to their hard drive, may choose to hide the evidence through the use of steganography.
- ❑ Steganography can be used as a means of covert (secret) communication by terrorists.
- ❑ FBI has arrested 11 suspected Russian agents who were using steganography to spy in the US (June 2010)

Steganography : Tips and Tricks:

- Always encrypt your message prior to using steganography to hide it.
- Hide your **stego-medium** among other media **of the same type**, or in a unsuspecting location.
- Destroy the original cover-medium so that the only version of it that remains is the stego-medium. If it is exposed, a comparison between the cover and stego media immediately reveals the changes.

The Third Eye: An Application of Steganography

The Third Eye is an steganographic application that hides information in pictures.

- Take a look at the following two images:



Image-1



Image-2

- The first picture is quite normal. The second picture looks exactly like the first.
- However, the second picture is not a normal picture at all. It contains a text file which is embedded in the image using a Steganography program and is nearly undetectable.
- Not only can you not see a visual difference in the picture, the file size of the original and the stego medium (image with the hidden text) is exactly the same.
- There are several programs on the Internet that may be able to detect a small anomaly in the picture, like "The Third Eye", "Stegdetect" etc, but the method used to embed the secret document is protected by a key, or password, as well.