Steganography

Rocco DE NICOLA
IMT Lucca

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Outline

- Information Hiding
- Steganography in history
- Steganographic models
  - Injective vs Generative
- Steganographic Techniques
  - Substitutive, selective, constructive
- Watermarking

Information Hiding

- The circulation and sharing of information is important as is the desire or need to keep certain information confidential.
- The most commonly used approach to make the conversation private is to make the message incomprehensible to those who are not the recipient
- The advent of digital has also brought new paradigms of implementation of already known theories and techniques to the area of information privacy.

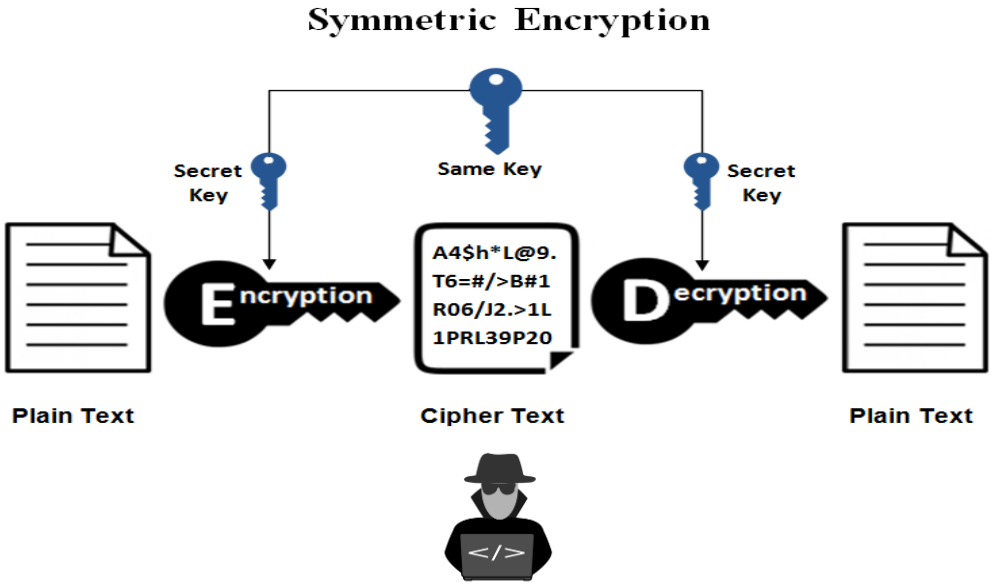
Three techniques

- Cryptography: encodes messages by means of special encryption algorithms that make it incomprehensible to those who are not aware of the relevant decryption systems.
- Steganography: hides the very existence of the message, including it in a “neutral” medium and thus guaranteeing the secrecy of the communication itself.
- Watermarking: inserts appropriate information (often hidden) in texts, images or videos, to signal its originality or owner.

Cryptography

- Cryptography is the science that studies techniques and methodologies to encrypt a plain text in order to produce an encrypted text understandable only to a legitimate recipient.
- The receiver must have sufficient information (key) to decipher the cipher text, thus retrieving the plain text.
- The purpose of encryption is to hide the content of a message, BUT encrypted (incomprehensible) texts generates suspicion.
- Cryptography fails when the content of the transmitted ciphertext is decrypted

Cryptography



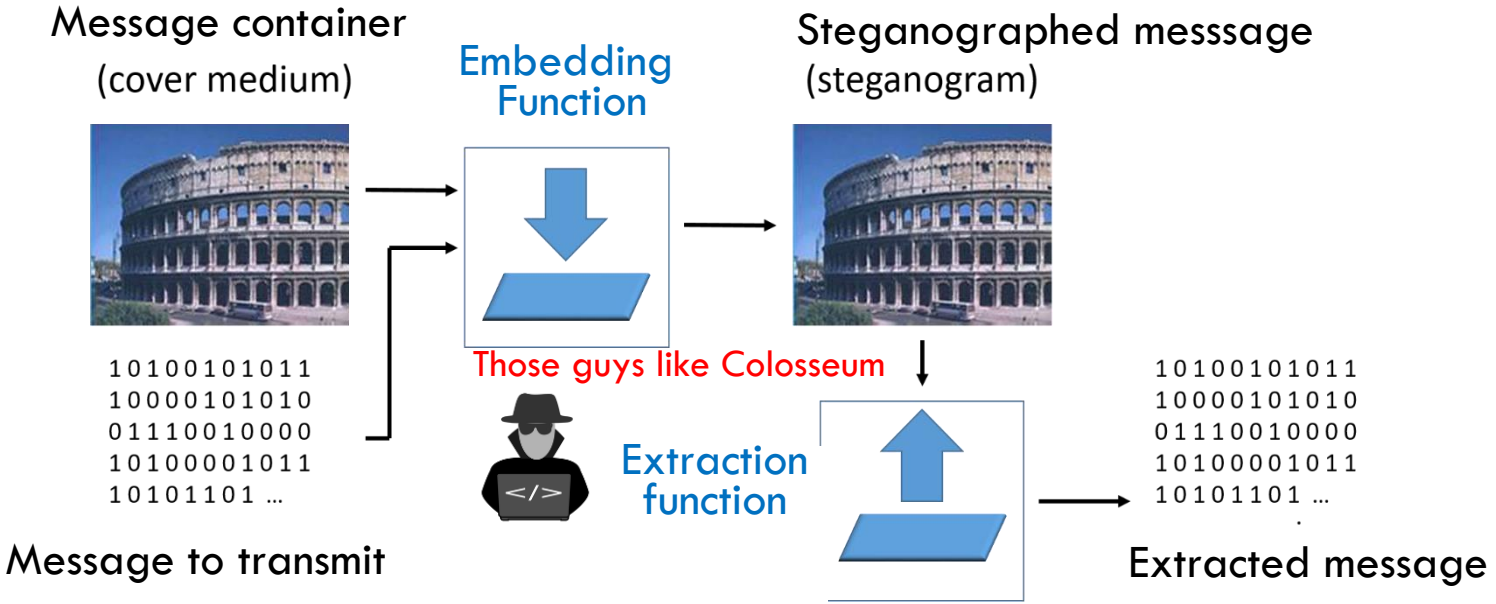
I do not understand this
but it is suspicious

Steganography

- Steganography is the art of hiding a message (which has to remain secret) within a message container that can be public and is not suspicious.
- The container can also look totally different from the secret message and must be able to hide the very existence of the communication.

Steganography fails if the transmition of confidential material is discovered, even if one is unable to decrypt its contents.

Steganographic System



Steganography in history

Herodotus writes that:

- Histieus, around 440 B.C., shaved the head of a trusted slave and tattooed it with a message for Aristagora of Miletus; the message disappeared as soon as the hair grew back.
- Demeratus, a Greek at the court of the king of Persia Xerxes, warned Sparta of an imminent attack.
  - After removing the wax from a pair of wooden tablets, he engraved a message and covered the tablets with wax again, so that they looked like new.
  - At destination, no one imagined the presence of the message, until after the wife of Leonidas, after a premonition suggested scratching away the wax.

Invisible inks

- The ancient Romans used to write between the lines of a text using an ink made with natural substances such as lemon juice, vinegar or milk. The hidden message became visible once the text was brought close to a heat source.
- The scientist Giambattista Della Porta (16th century) explained how to communicate through a boiled egg, preparing an ink with 30 grams of alum (a chemical substance containing aluminium) in half a litre of vinegar, and using it to write on the shell.

Microdots

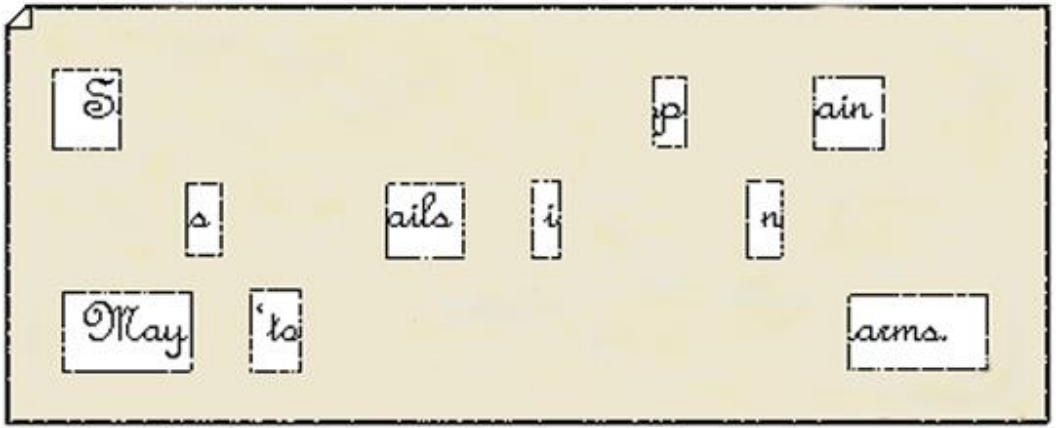
- Photographs the size of a typewritten dot that, once developed and enlarged, can become good quality printed pages.
- The first microdot was discovered by the FBI only in 1941, thanks to a tip-off

Cardano’s Grids

- Cardano's grids (1501 - 1626) were sheets of rigid material in which rectangular holes were cut out at irregular intervals.
- The secret message was written in the holes (each hole could contain one or more letters), after which the grid was removed and an attempt was made to complete the writing of the rest of the sheet in order to obtain a complete message, which was then sent to its destination.
- By applying an exact copy of the original grid to the sheet, it was possible to read the hidden message.

Example of Cardano's Grid

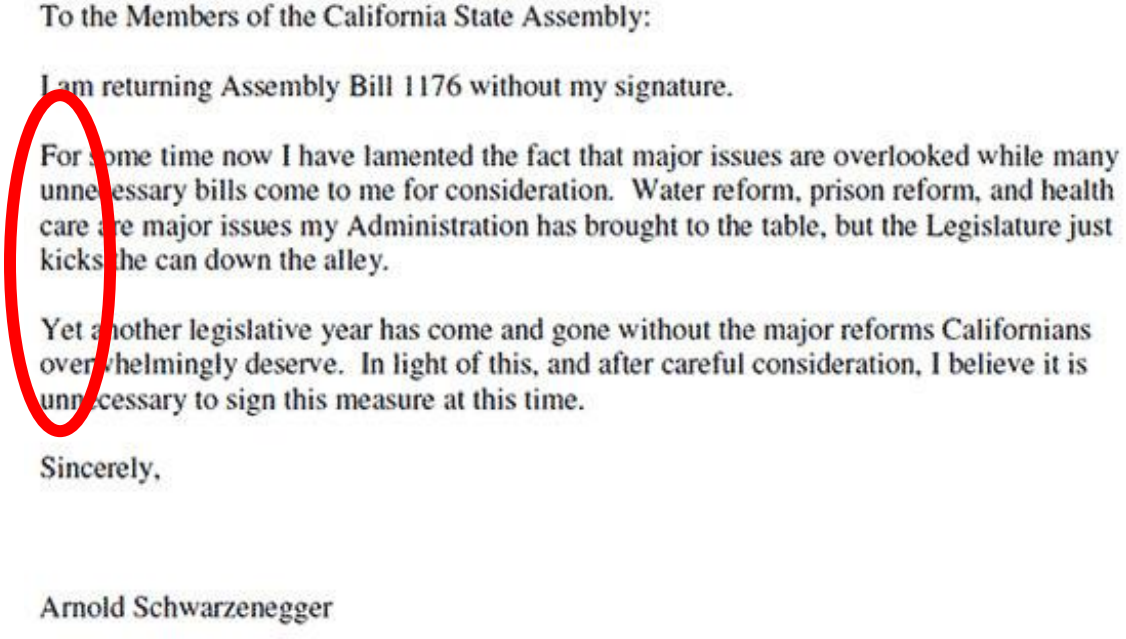
Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.



Acrostic

The acrostic (from the Greek ákros, "extreme" and stíchos, "verse") is a poetic composition within which the syllables or initial letters of each verse form a vertical word, a name, a sentence.

For an example read the first letters of each line of the message of Governor Schwarzenegger



To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked while many unnecessary bills come to me for consideration. Water reform, prison reform, and health care are major issues my Administration has brought to the table, but the Legislature just kicks the can down the alley.

Yet another legislative year has come and gone without the major reforms Californians overwhelmingly deserve. In light of this, and after careful consideration, I believe it is unnecessary to sign this measure at this time.

Sincerely,

Arnold Schwarzenegger

Null Cyphers

- A null cypher is a concealment cipher in which plain text is mixed with a large amount of unencrypted material.
- Example: Stringing together the first letter of every third word of the following cover text reveals "Wikipedia" as the hidden message:
  - It's important **w**e allow anyone **i**nterested in gaining **k**nowledge accesst o **i**nformation which is **p**ublished freely. There **e**xists a website **d**evoted to this **i**dea, and you **a**re on it!

Trithemius/1

- The three volumes essay Steganographia (written c. 1499; published 1606), by the German benedectine Trithemius was placed on the Index Librorum Prohibitorum in 1609 because it appeared to be about magic—specifically, about using spirits to communicate over long distances.
- After the publication of the decryption key for the first two volumes, they have been known to be actually concerned with cryptography and steganography.

Trithemius/1

- Until recently, the third volume was still believed to be solely about magic, but the "magical" formulae have now been shown to be covertexts for yet more cryptographic content.
- John Dee (mathematician, astrologer and occultist, 1527 – 1608) used Trithemius steganography to conceal his communication with Queen Elizabeth I.
- One of the codes used in this book is the Ave Maria cipher where each coded letter is replaced by a short sentence about Jesus in Latin.

Steganalysis

- Steganalysis is the set of methods and techniques capable of attacking a steganographic system.
- Just as cryptanalysis has the task of revealing the encrypted output of a cryptographic system, the purpose of steganalysis is to label an object with certainty as suspect (containing, that is, an occult message inside it) or as harmless (without hidden information).

"If the purpose of cryptanalysis is to reveal the datum, the purpose of steganalysis is to discover its presence."

Steganalysis

- The modern formulation of the steganographic studies is due to the work of G.J. Simmons who, in 1984, proposed the prisoners problem.
- Alice and Bob are kept in separate cells and can communicate only through the warden (Eve), who punishes them if the exchanged message contains malicious contents such as an escape plan
- Eve, besides being able to examine all the messages that the two prisoners exchange, can take an active or passive role.
  - passive if she merely examines the message the two prisoners exchange.
  - active if she can alter the messages exchanged

Outline

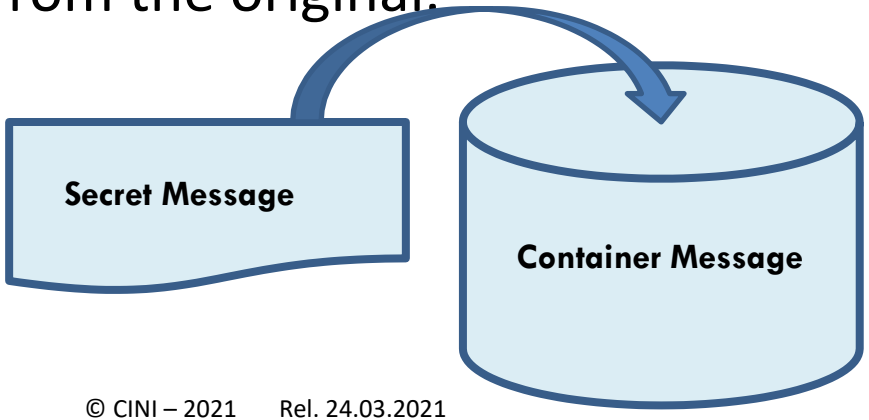
- Information Hiding
- Steganography in history
- Steganographic models
  - Injective vs Generative
- Steganographic Techniques
  - Substitutive, selective, constructive
- Watermarking

Steganographic models: Containers

- The basic scheme of steganography assumes the existence of two messages:
  - Secret Message
  - Container Message
- Depending on the way the container is handled we talk about:
  - *Injective* Steganography
  - *Generative* Steganography

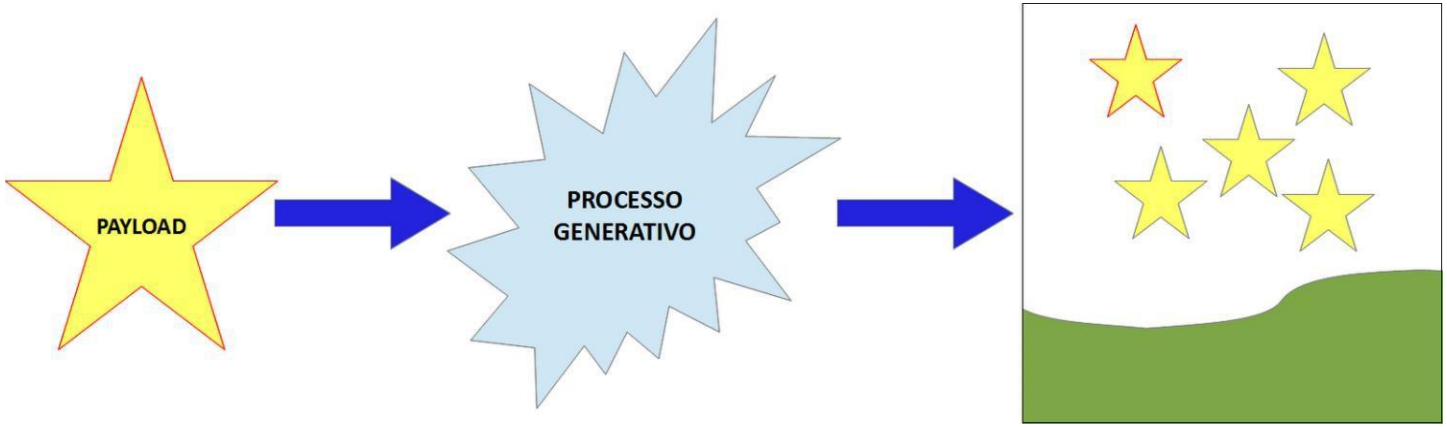
Injective Steganography

- Injective steganography (the most used) allows to insert secret messages in an existing container message modifying it in such a way to contain the secret message, and to result, at the level perceived by the human senses, practically indistinguishable from the original.



Generative Steganography

- The generative steganography allows to generate, starting from the secret message, a container message able to hide that secret message in the best way.



Steganographic models

- The image designated to contain the message is called the cover image (container).
- The message is called payload
- The result of paylod insertion in the cover image is called stego-image.

```
Stego-image = F (G(cover), H(Payload))
```

  - F is the steganographic function
  - G is a function that processes the image cover
  - H is a function that processes the message to be inserted, e.g., a cryptographic function.

Outline

- Information Hiding
- Steganography in history
- Steganographic models
  - Injective vs Generative
- Steganographic Techniques
  - Substitutive, selective, constructive
- Watermarking

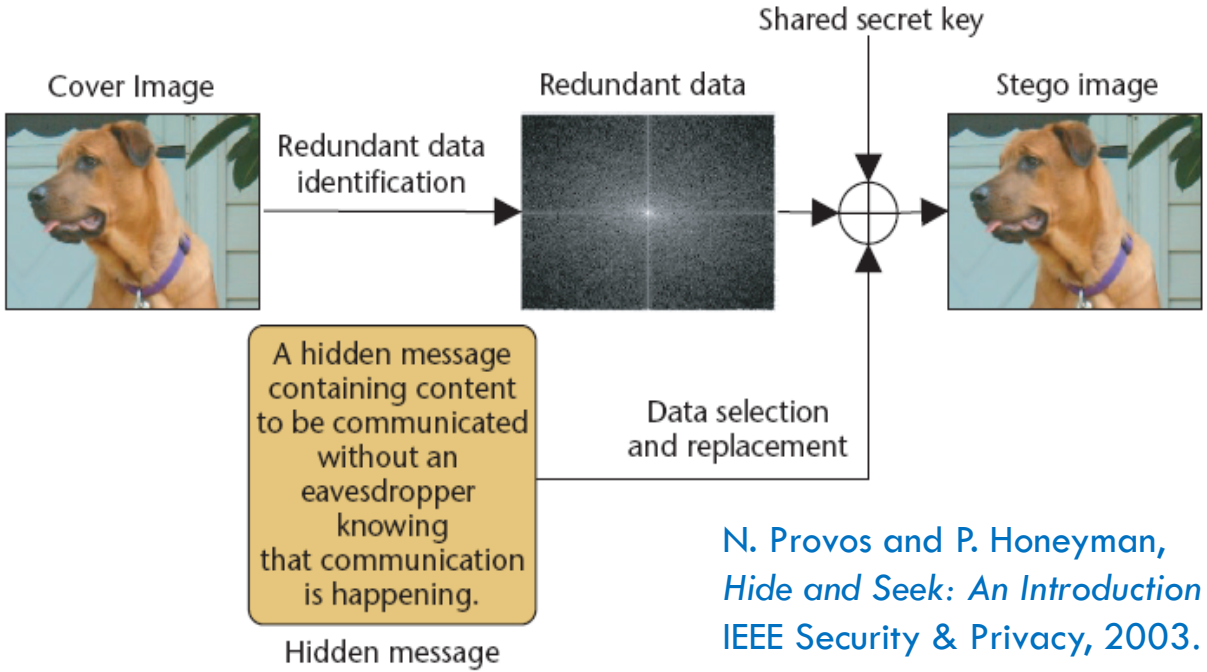
Steganographic Techniques

- An alternative classification to container-based classification is based on the techniques used for adding information to the container:
  - substitutive steganography
  - selective steganography
  - constructive steganography.

Substitutive Steganography

- The goal is to replace a minor element of the cover medium with an element of the secret message to be hidden.
- Substitutive techniques are the most widely used and are so widespread that the term steganography often implicitly refers to them.
- The main defect of these techniques lies in the possible alteration of the statistical characteristics of the container.

Substitutive Steganography



N. Provos and P. Honeyman,
Hide and Seek: An Introduction to Steganography,
IEEE Security & Privacy, 2003.

Selective Steganography

- The basic idea is to choose the support according to the message to be hidden by trial and error, repeating the same procedure until the result meets a certain condition.
- The stego medium that survived the selection process actually contains the secret information, but it is a "natural" container.
- The problem with this technique is that it is very expensive compared to the amount of information that can be hidden.

Selective Steganography

Secret Bits	1110011
Cover Text	Česká republika jekrásné místo
Steganographic Text	Česká republik a jekrásné místo 1 1 1 0 0 1 1

S. Khan et al. "Czech Text Steganography Method by Selective Hiding Technique" Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1-3, 2015, London, U.K.

The secret bit 'zero' is stored in the un-pointed letters and the secret information bit 'one' is stored in the pointed letters (with additional annotation in the ASCII representation, using extension characters not visible to the reader but only to the computer).

Constructive Steganography

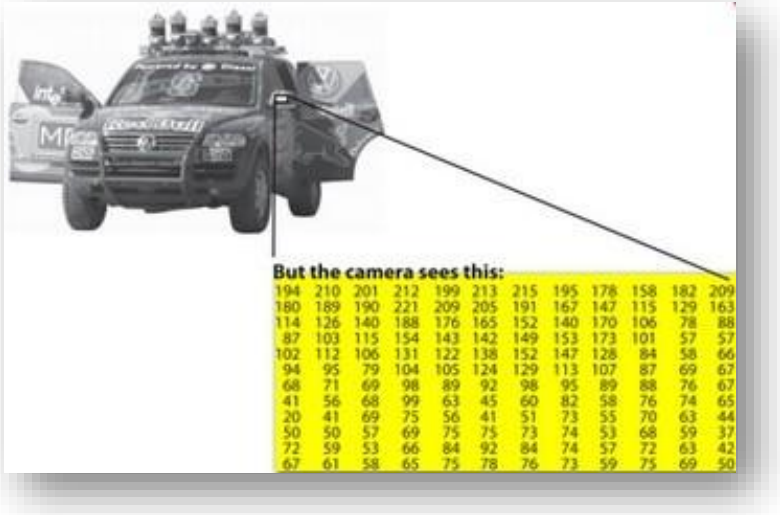
- The objective is to replace the noise in the medium used with secret information appropriately modified to imitate the statistical characteristics of the original noise.
  - It is not easy to build a noise model and it is possible that someone with better resources may be able to build a more accurate model and distinguish between the original noise and its substitute.
  - If the noise model used falls into opponents' hands, they may use it to check that a message conforms to it.

Choice of cover

- Steganography needs to use cover objects that are possibly unpublished and never used before.
- The most used covers are the images.
- Multimedia data (audio and video) are excellent containers: in fact, following digitization, they contain quantization noise that provides the necessary room for manoeuvre for data entry.
- The most common technique of injective steganography on images is the one based on the least significant bit modification (LSB).
- Lossy compression is able to introduce additional amounts of noise, but may also destroy the hidden message

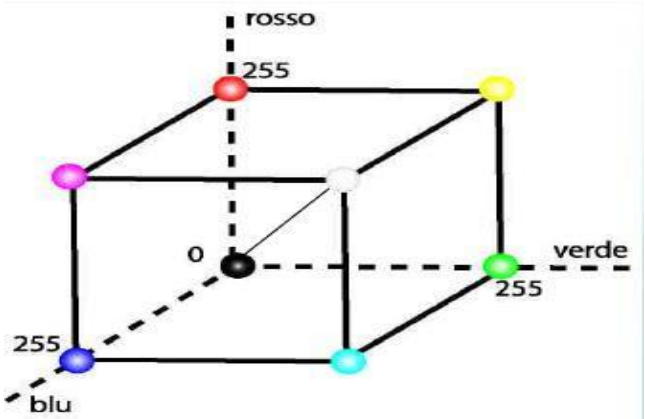
Images as cover

- A digital image is an array of pixels
- The term pixel comes from picture element
  - The pixel contains the information related to the representation of reality that has been captured by a scanner, or another machine

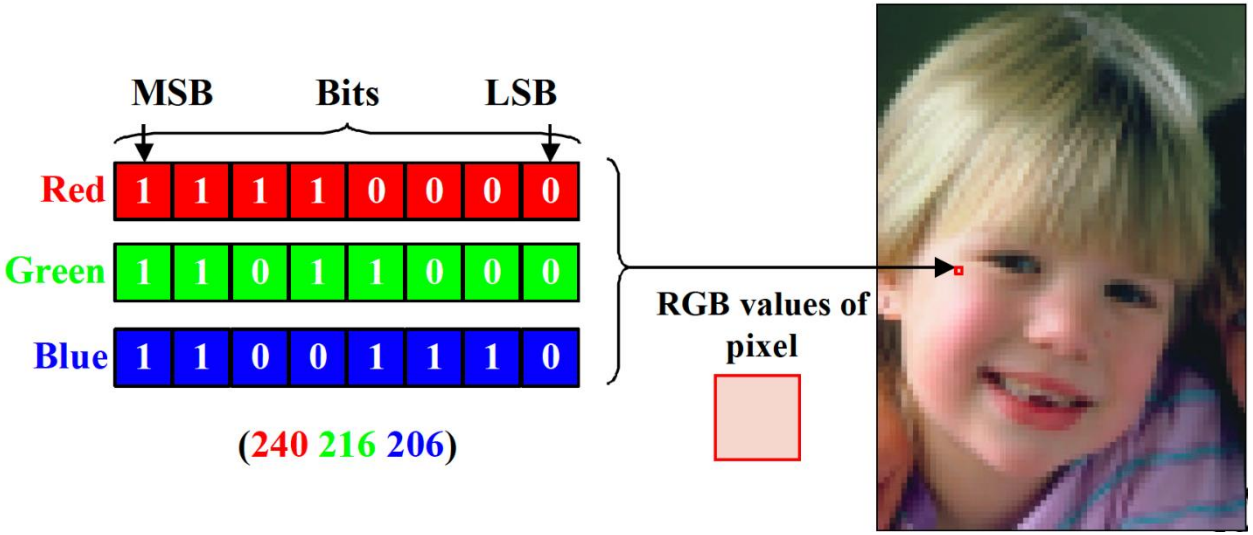


Images as cover

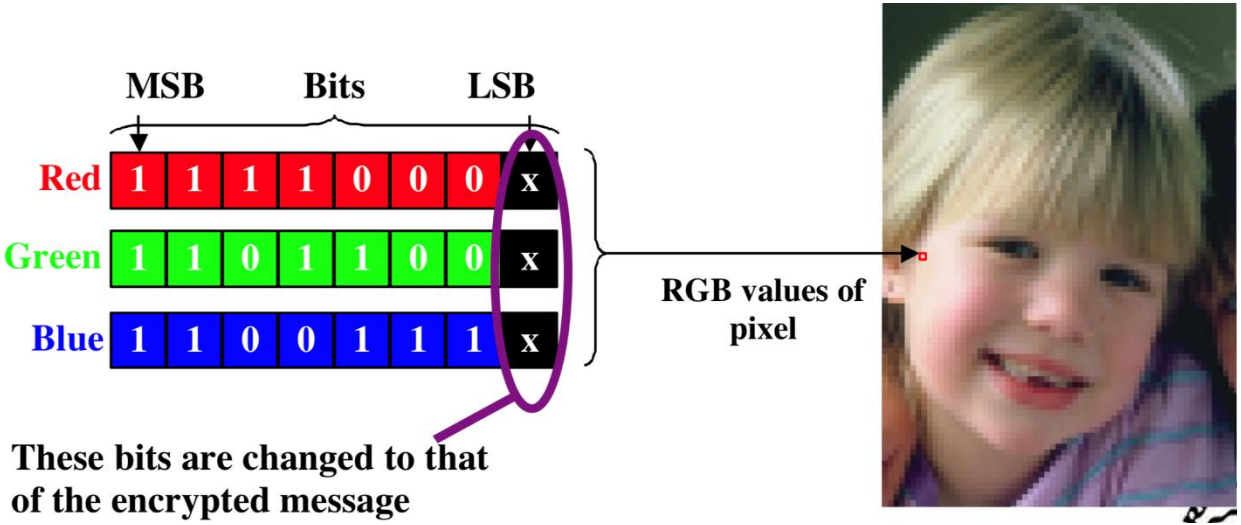
- Digital color images are arrays of values of pixels in the spatial domain (many different formats)
- In personal computers the common color space is RGB (Red, Green, Blue).
- In images with 24 bit/pixel a color is assigned to each pixel position
  - Each color component has a value of 8 bits between 0 and 255
  - (0,0,0) corresponds to darker black
  - (255,255,255) corresponds to lighter white



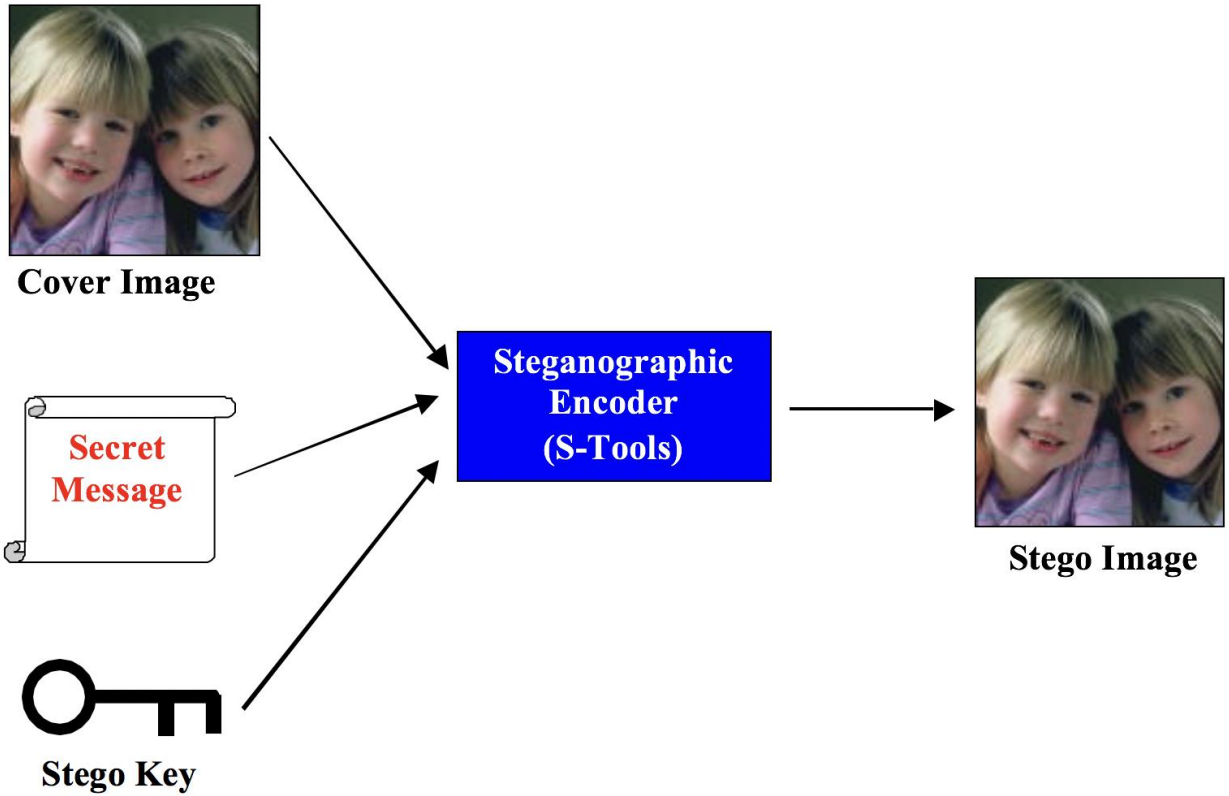
RGB 24 bit/pixel



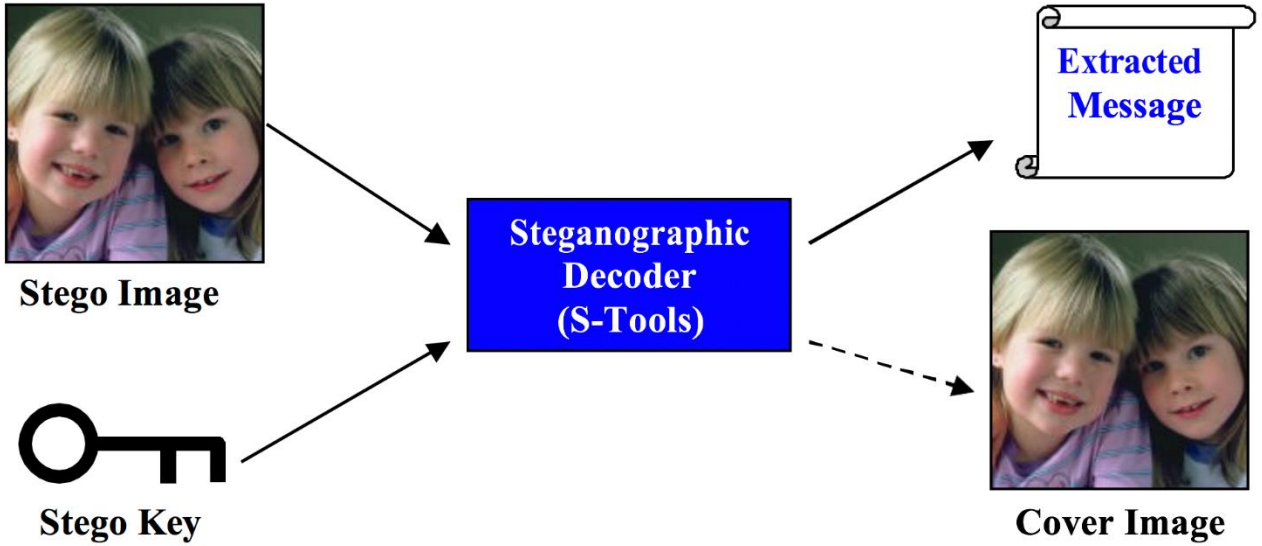
Substitutive encryption



Steganographic Encryption



Stenographic decryption



Tools for steganalysis

- There are tools that allow you to locate, extract and/or destroy messages hidden within suspicious covers.
- 2Mosaic, StirMark Benchmark: remove messages from images.
  - http://www.petitcolas.net/fabien/watermarking/2mosaic/index.html
  - http://www.petitcolas.net/fabien/watermarking/stirmark/
- StegDetect: attacks steganographed files using statistical attacks.
  - http://www.outguess.org/detection.php
- StegBreak: detects and extracts secret messages inserted by various software.
  - http://manpages.ubuntu.com/manpages/hardy/man1/stegbreak.1.html

Outline

- Information Hiding
- Steganography in history
- Steganographic models
  - Injective vs Generative
- Steganographic Techniques
  - Substitutive, selective, constructive
- Watermarking

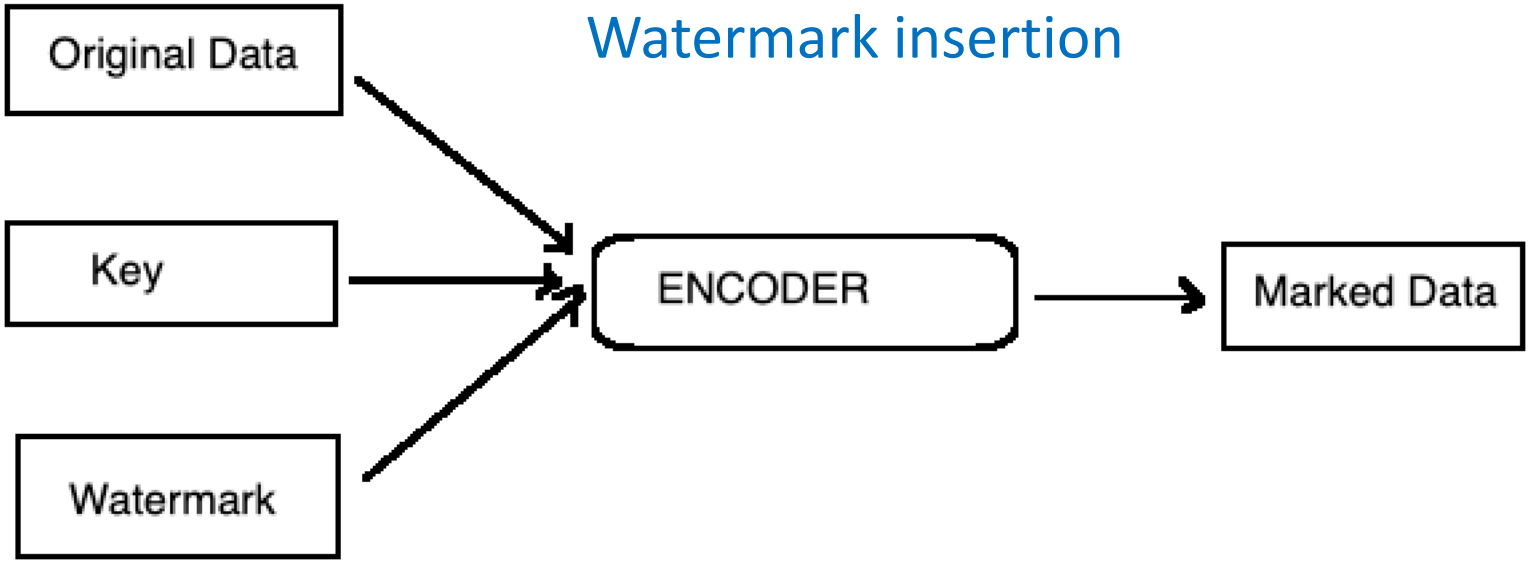
Watermarking

- A set of techniques and methods for the inclusion of information in a multimedia file, which can then be detected or extracted to obtain information about its origin and/or provenance.
- Watermarking is used to insert appropriate information into a signal, in particular on multimedia files, possibly to indicate its originality or to indicate the owner of the property rights.
- A watermark, just like banknote watermarks, must be visible only under certain conditions - for example after the application of appropriate algorithms.

Watermarking goals

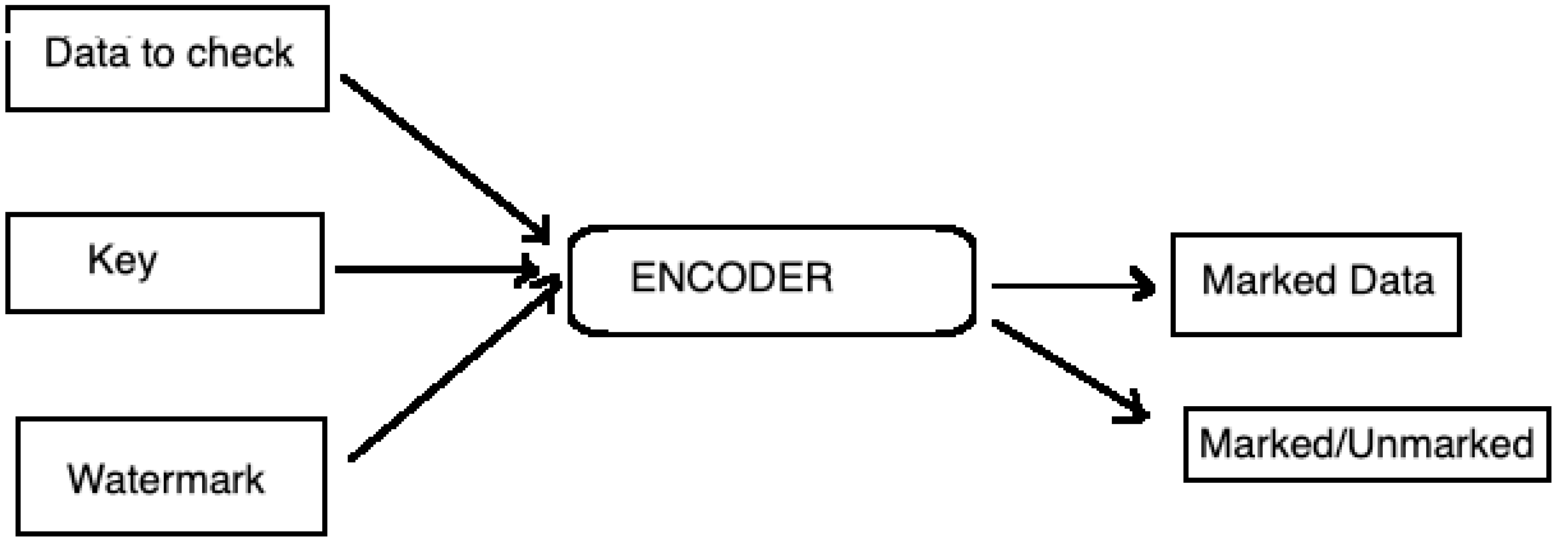
- Make it clear to all users who is the legitimate owner of the document (if the trademark is visible);
- Prove the originality of a non-counterfeit document;
- Avoid distribution of unauthorized copies;
- Mark some specific features of the document;
- Mark the sales path of the document, using a different trademark for each buyer.

Examples of usage



EXAMPLES OF USAGE

Extraction and Detection



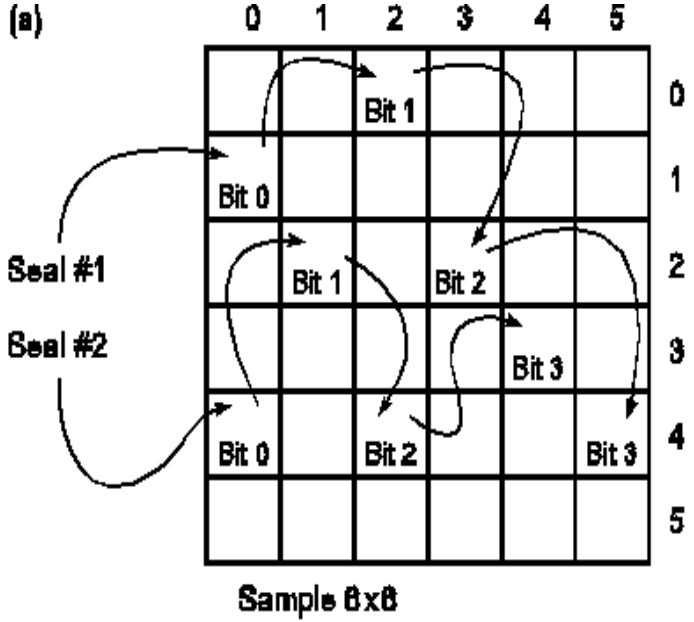
Features

- Little intrusive: invisible enough not to degrade the quality of the data and to prevent it from being found and deleted.
- Sufficiently Visible: visible enough to discourage theft.
- Easily detectable: the owner of the data or an independent supervisory authority must be able to identify it easily.
- Unique: its recovery should unambiguously identify the owner of the data.
- Multiple: it must be possible to generate several watermarks
- Robust: difficult to remove from anyone who wants to counterfeit the copyright of the data.

Watermarking of images

- The positions of a few pixels and a checksum are the watermark:
  - You choose the 7 most significant bits of 8 different pixels
  - The segments are concatenated to get a checksum of 56 bits
  - The checksum bits are written in the last bit of 56 randomly chosen pixels

Watermarking images: an example



(b)

0	1	2	3	4	5	
55	73	71 71	123	123	205	0
120 121	123	70	72	147	199	1
130	123 123	67	68 68	73	123	2
140	133	120	72	70 70	117	3
156 159	142	123 122	123	69	71 70	4
195	178	150	112	67	70	5

71 ← Original pixel value
70 ← Pixel value after embedding a checksum bit

Advantages of the checksum

- Quick and easy
  - The checksum insertion changes (on average) only half the number of pixels; visual distortion is limited
  - One can have multiple watermarks as long as they do not overlap
- Fragile
  - The entire watermark can be removed by setting all LSBs to zero
  - Does not work in case of compression with loss of information

Steganography

Rocco DE NICOLA
IMT Lucca

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it