

Information Systems Security

Steganography

Summary

- ▶ Early uses of steganography
- ▶ Modern applications
- ▶ Domains of insertion
- ▶ Example of information hidden in an image
- ▶ Watermarking (Copyright)
- ▶ Steganalysis

Steganography

- ▶ **Art of hiding data in other data**

- From the Greek 'steganos' (hidden or secret) and 'graphy' (writing or drawing)

- ▶ **Hidden messages in a medium**

- Ignorance of the existence of the secret

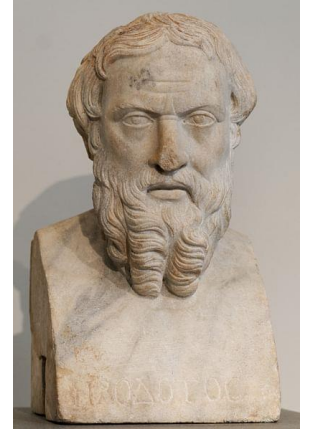
- ▶ **Cryptography: message impossible to understand**

- ▶ **Steganography: message impossible to found**

First use of steganography

► 5th century BC (Herodotus):

- Histiaeus chose a devoted slave, shaved his head, and wrote on it the message to be transmitted to his son-in-law Aristagoras of Miletus
- He waited for his hair to grow back before sending him to Aristagoras with instructions to have his head shaved



► Again according to Herodotus

- To inform the Spartans of the impending attack of the Persians, Demaratus took tablets, scraped off the wax and engraved the secret message on the wood, then covered the tablets with wax
- The tablets, apparently blank, did not attract attention



Example of steganography



Je suis très émue de vous dire que j'ai bien compris, l'autre jour, que vous avez toujours une envie folle de me faire danser. Je garde un souvenir de votre baiser et je voudrais que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à vous montrer mon affection toute désintéressée et sans calcul. Si vous voulez me voir ainsi dévoiler, sans aucun artifice mon âme toute nue, daignez donc me faire une visite et nous causerons en amis et en chemin. [...]

Lettre de George Sand à Alfred de Musset

Modern applications of steganography

► Information protection

- Prevent people with significant resources from reading private documents
- Allowing free speech in countries where cryptography is banned
- Allowing military or intelligence communications without detection by the enemy

► Data Leak Detection

- Enable the detection of a leak of confidential data by marking documents
- Insertion of a marking to identify the owner of the rights of a work (watermarking)

Modern applications of steganography

- ▶ **Cryptography:** Effective way to protect secret data, however, the simple act of communicating with encrypted messages attracts attention
- ▶ **When a communication channel is monitored by a third party, they can, on the slightest suspicion, destroy the communication between the two parties**
 - A communication containing a secret message **should seem normal** to the person controlling the channel



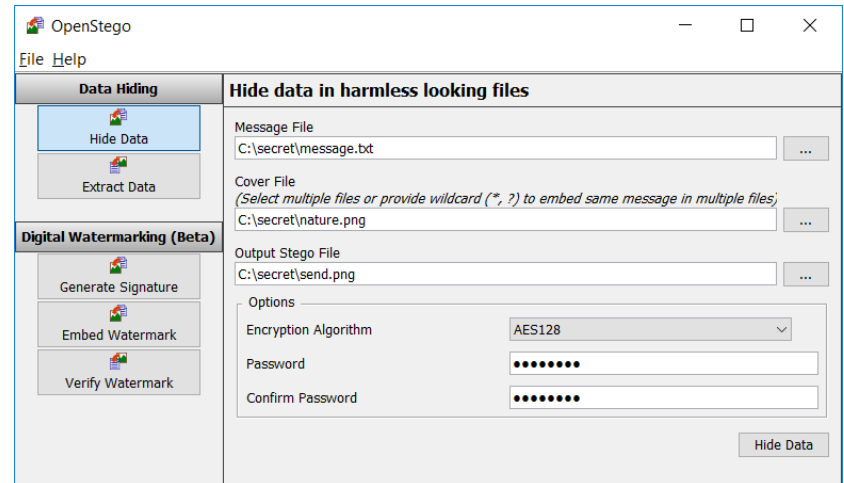
Properties of steganography

- ▶ **Robustness:** ensures that secret information cannot be destroyed without severely degrading the medium
- ▶ **Invisibility:** aims to ensure that the medium is not disturbed by the secret information inserted
- ▶ **Capacity:** defines the amount of information that can be integrated into the medium without visible deterioration
 - These three characteristics are closely and inversely related
 - ✓ For example, improved capacity usually has a negative influence on invisibility

Softwares

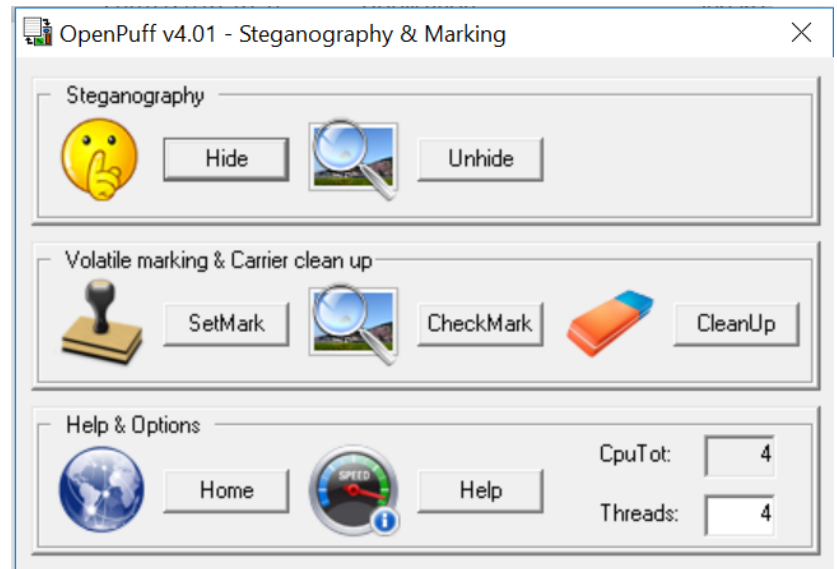
OpenStego

- Java-based and open-source
- Created in 2015
- Hide files or messages in PNG, BMP, GIF, or JPG images
- Digital watermarking



OpenPuff

- Opensource software
- Created in 2004
- Hide files in lot of formats without plugin (audio, video, etc.)



The main mediums

► Different mediums are possible to hide information

➤ Text

- ✓ Punctuation placement, choice of synonyms, spacing between words are simple ways to add information without disrupting the original information

➤ Sound

- ✓ Variations that are imperceptible to the ear can contain a large amount of information (low frequencies)

➤ Image

- ✓ Image encoding details, such as the color palette, may contain information

➤ Other

- ✓ There are as many places to hide information as there are formats and types of data

Domains of insertion







- ▶ **Secret information can be hidden essentially in two possible domains of insertion: the spatial domain, and the frequency domain**
- ▶ **Spatial domain: Perform the hiding directly in the bits of the pixels of the carrier image**
- ▶ **Frequency domain: encodes data through the frequency of the image, and hides information in areas of the image that are less sensitive to compression, cropping, and various image processing**
 - This allows for an increased robustness

Domains of insertion

- ▶ **The most well-known space technique is LSB (Least Significant Bit)**
 - Consists of hiding a secret message in the least significant bits of the pixels of the image, so that the distortions brought about by the insertion process remain imperceptible
 - To the human eye, changes in the LSB value are almost imperceptible
 - Direct insertion methods in this area are inexpensive in terms of computational time since they do not require a prior transformation step
- ▶ **Spatial steganography methods are generally susceptible to attack**

Composition of an image

- ▶ A digital image is a file that describes an image as a succession of dots, the pixels, indicating what color each pixel is
 - An image file contains a header giving the width and height among other things and a table indicating the color that each point (pixel) of the rectangle in which the image is to be displayed
 - The simplest way to encode a color is to give its RGB components (red, green, blue) as an integer varying from 0 to 255 (i.e. 8 bits : $2^8=256$)

Color	R	G	B	Byte 1	Byte 2	Byte 3
	0	0	0	00000000	00000000	00000000
	255	255	255	11111111	11111111	11111111
	255	0	0	11111111	00000000	00000000
	0	255	0	00000000	11111111	00000000
	0	0	255	00000000	00000000	11111111
	132	122	191	10000100	01111010	10111111

Example

► Hiding one image in another

- We try to hide the image of the train within the image of the landscape



Example

- ▶ The four most significant bits of the train image replace the four least significant bits of the landscape image :



Example

- ▶ Hidden image extracted from the previous image:

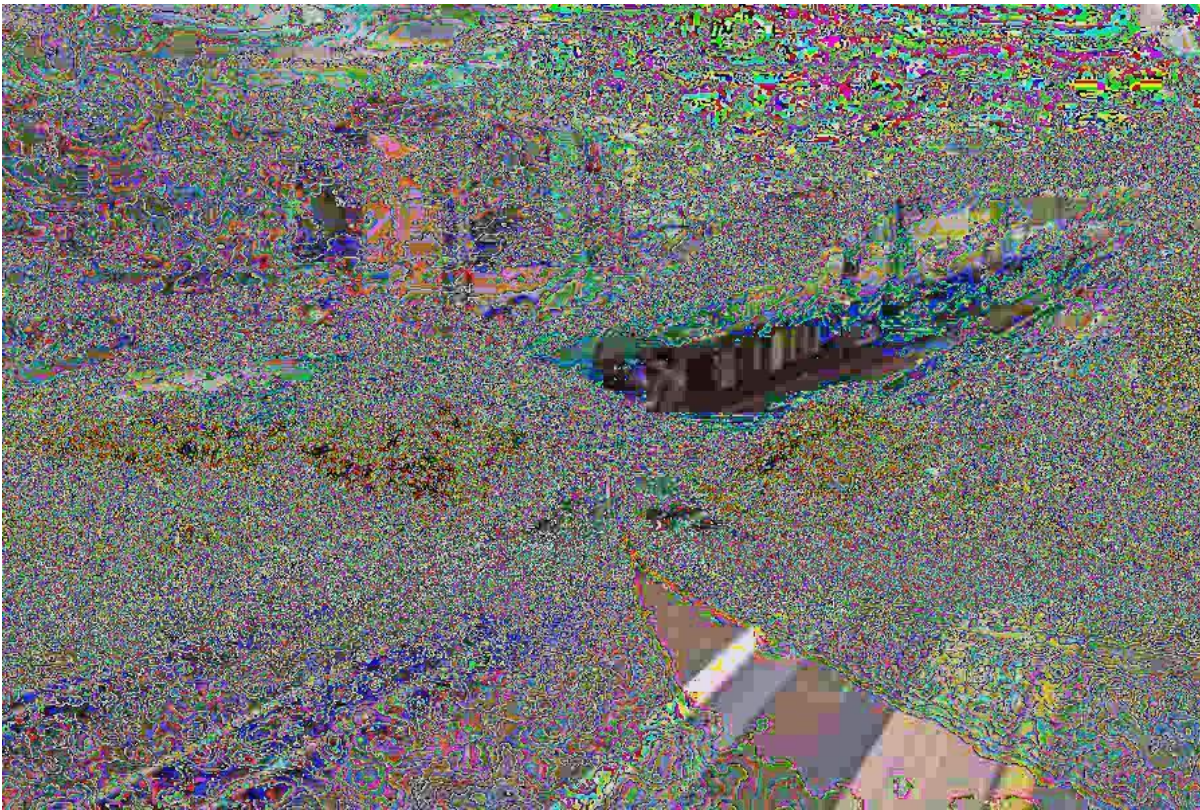


Example

- ▶ The passage of the secret into the container was carried out in the following way :
 - Removing least significant bits from the container
 - Shift from most significant bits to least significant bits of the secret
 - Adding the container's most significant bits to the least significant bits of the secret
 - For example, for the pixel (10,10) :
 - ✓ Container RGB (174, 176, 191) → (1010 1110, 1011 0000, 1011 1111)
 - ✓ Removing least significant bits from the container (160, 176, 176) → (1010 0000, 1011 0000, 1011 0000)
 - ✓ Secret RGB (160, 163, 154) → (1010 0000, 1010 0011, 1001 1010)
 - ✓ Secret shift in least significant bit (10, 10, 9) → (0000 1010, 0000 1010, 0000 1001)
 - ✓ Final pixel for Stegano image (170, 186, 185) → (1010 1010, 1011 1010, 1011 1001)

Example

- ▶ The previous spatial transformation is sensitive to the compression of the steganographed image (containing the secret):



Hiding information in an image

► A GIF (Graphical Interchange Format) image is made up of 256 colors

- The GIF89a format uses a color palette. To use this format, you must therefore reduce the number of colors used to 256
- To do this, the GIF compressing software will define the 256 most used colors in the image
- Each pixel is therefore encoded on 1 byte because it takes one of the colors of the palette between 0 and 255 (i.e. 8 bits)

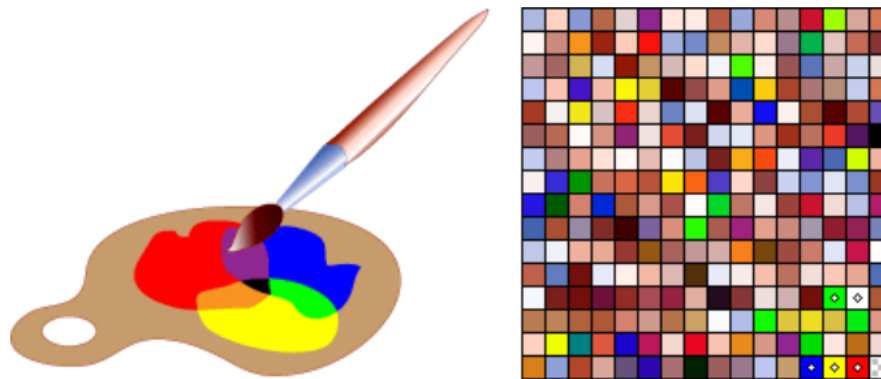
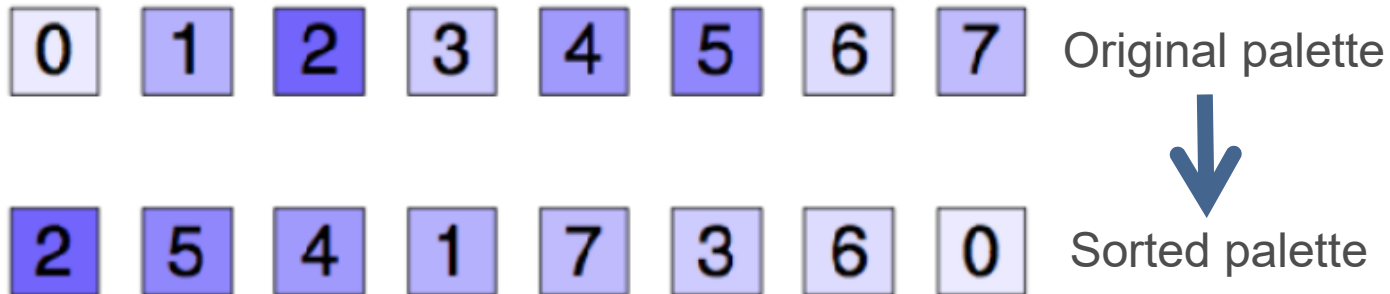


Image saved as a GIF with a palette of 256 colors

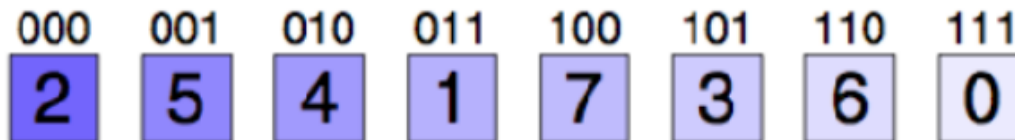
Hiding information in an image

► EzStego consists of hiding information in a GIF

- To do this, we create a sorted copy of the palette of 256 colors
- The sorting of the palette is done in such a way that the difference between 2 colors next to each other is almost imperceptible

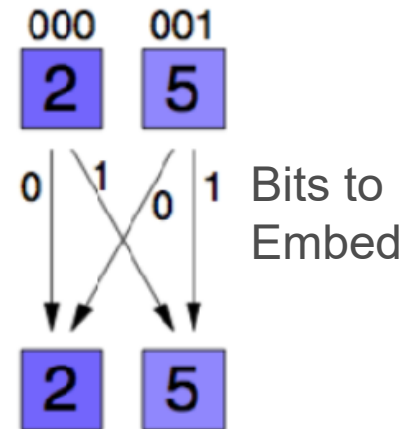


- The sorted palette then has a new index :

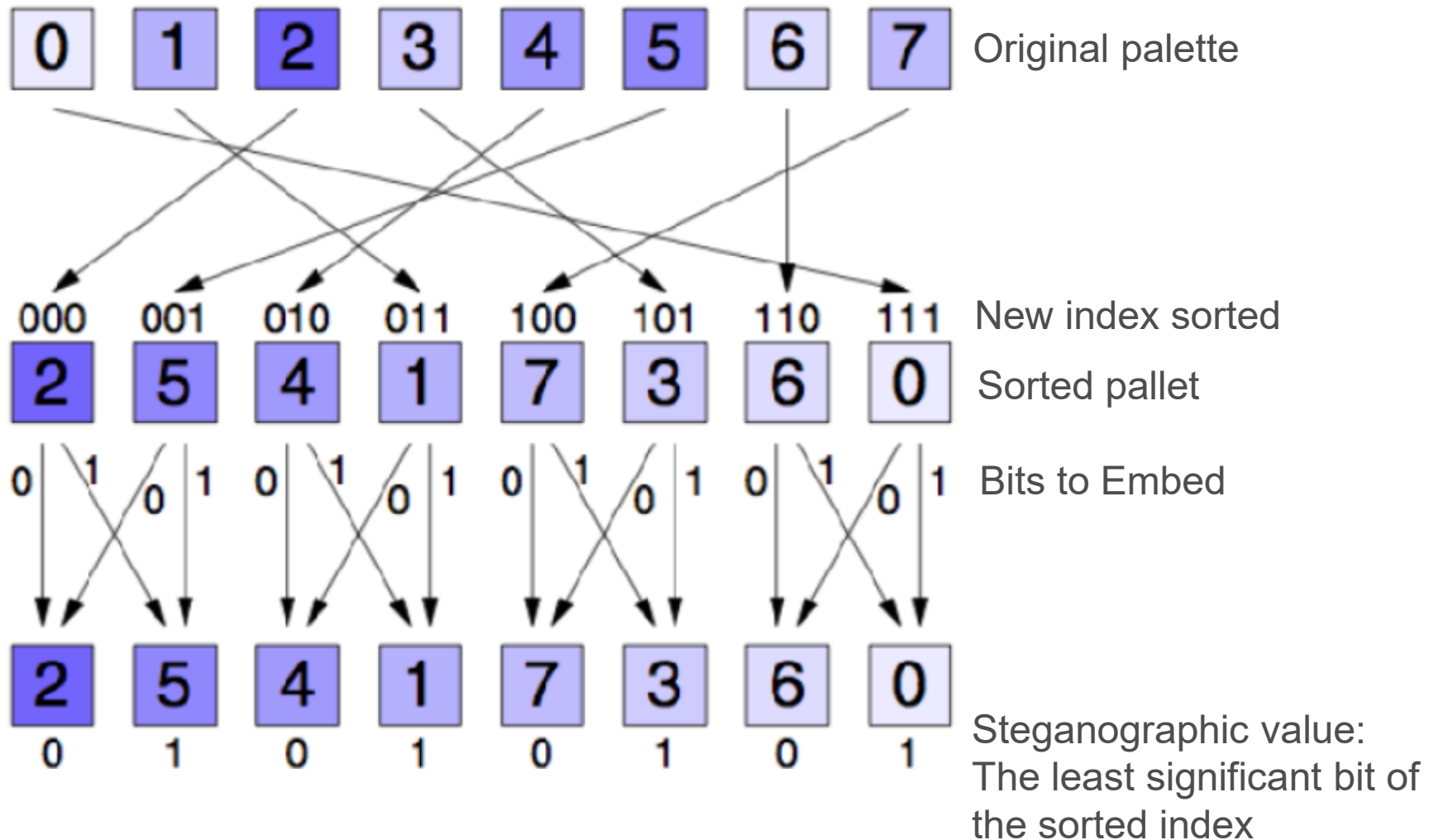


Hiding information in an image

- To include the desired information, we go through each pixel of the image
- For each pixel, we look for the index in the sorted palette
- We look at which bit we need to incorporate on the current pixel and we put this bit on the low bit of the current byte (the one of the index of the sorted palette)
- You may or may not shift by one index in the sorted palette
- If the palette is well sorted, then the difference between the two colors will be **imperceptible**
- This new index in the sorted palette corresponds to an index in the unsorted palette
- We then replace the current pixel with the index of the unsorted palette



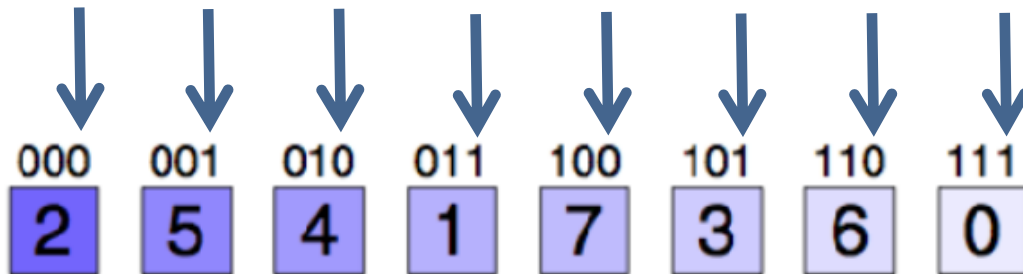
Hiding information in an image



Find the information in the image

► To find the information in the image, proceed as follows:

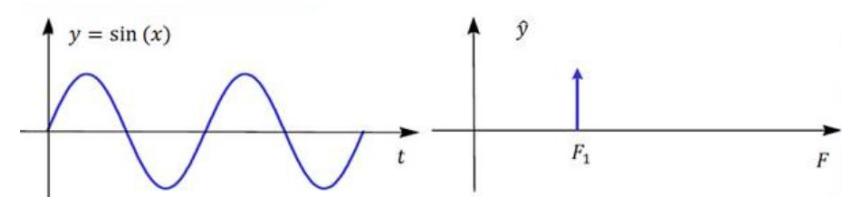
- We create the same sorted copy of the palette of 256 colors
- We look for the index of the current pixel in the sorted palette
- The least significant bit in this index comes from the mask applied to the image



Domains of insertion

Frequency domain techniques are :

- DFT (Discret Fourier Transform)
- DCT (Discret Cosine Transform)
- DWT (Discret Wavelet Transform)



These techniques encode data through the overall frequency of the image

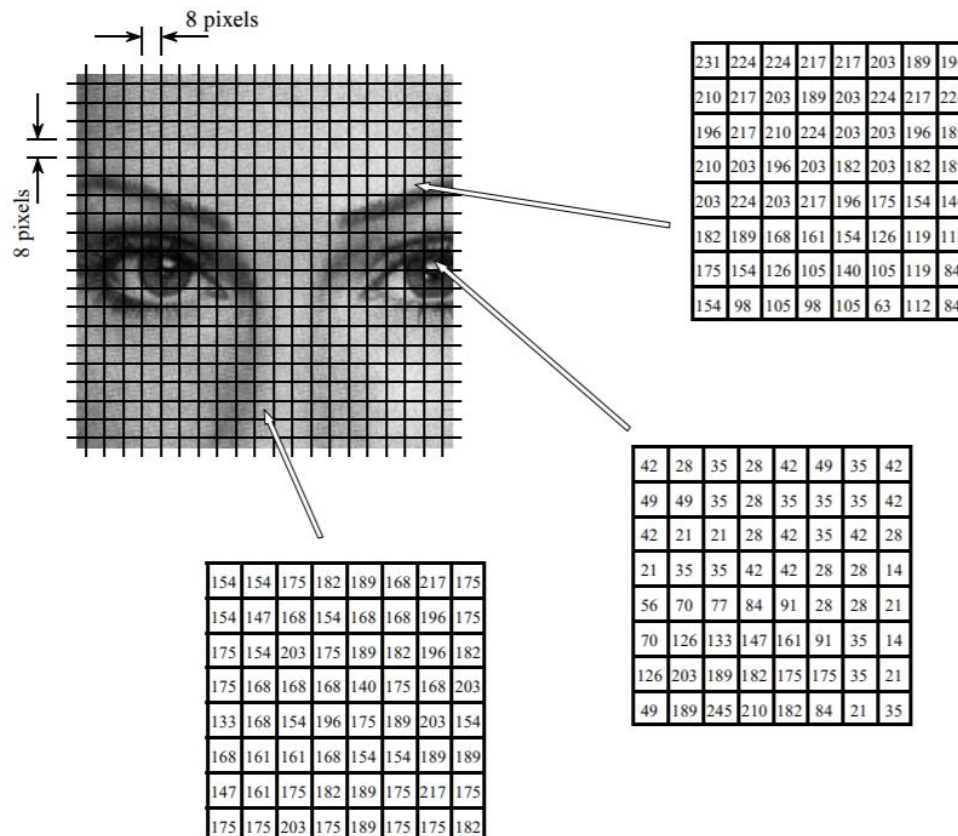
- Hide information in areas of the image that are less sensitive to compression, cropping, and various image processing

Greatly increased robustness

JPEG compression

- ▶ JPEG uses the discrete cosine transform (DCT) to encode the image

- The image is first cut into 8x8 pixel blocks



JPEG compression

- To each of these blocks is then applied a discrete cosine transformation
- This transformation replaces the 64 levels of grey in the block with 64 other coefficients
 - ✓ The element (0,0) of the DCT matrix represents the average value of the block, the others indicate the spectral power for each spatial frequency

231	224	224	217	217	203	189	196
210	217	203	189	203	224	217	224
196	217	210	224	203	203	196	189
210	203	196	203	182	203	182	189
203	224	203	217	196	175	154	140
182	189	168	161	154	126	119	112
175	154	126	105	140	105	119	84
154	98	105	98	105	63	112	84

Gray scale Matrix

174	19	0	3	1	0	-3	1
52	-13	-3	-4	-4	-4	5	-8
-18	-4	8	3	3	2	0	9
5	12	-4	0	0	-5	-1	0
1	2	-2	-1	4	4	2	0
-1	2	1	3	0	0	1	1
-2	5	-5	-5	3	2	-1	-1
3	5	-7	0	0	0	-4	0

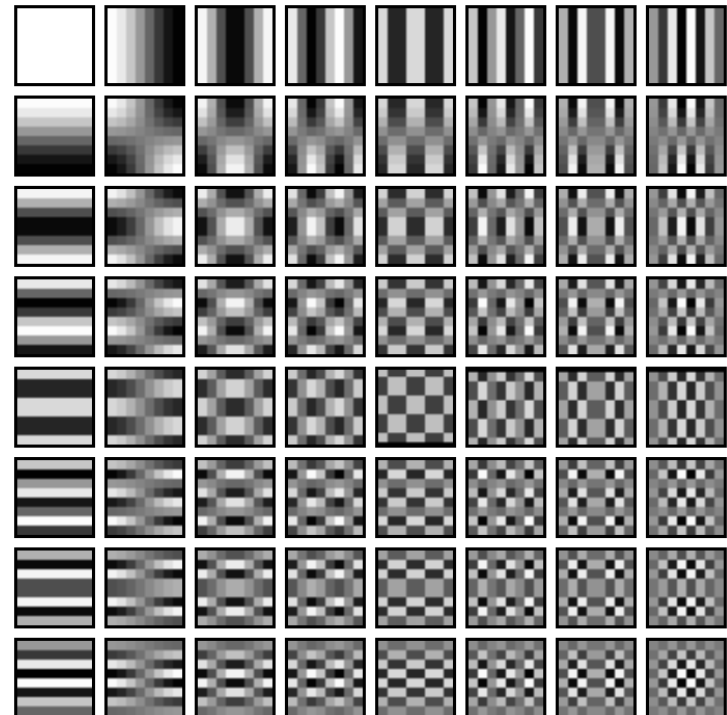
DCT Matrix

JPEG compression

- Each coefficient in the DCT matrix below defines the amplitude of the basic functions

174	19	0	3	1	0	-3	1
52	-13	-3	-4	-4	-4	5	-8
-18	-4	8	3	3	2	0	9
5	12	-4	0	0	-5	-1	0
1	2	-2	-1	4	4	2	0
-1	2	1	3	0	0	1	1
-2	5	-5	-5	3	2	-1	-1
3	5	-7	0	0	0	-4	0

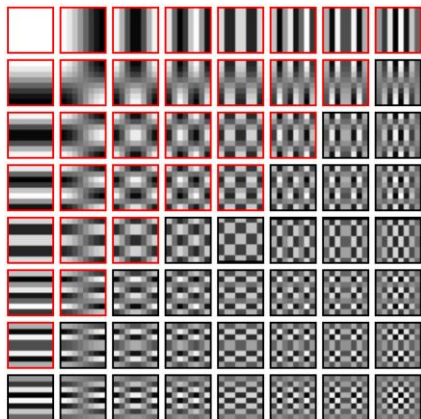
DCT matrix: amplitude of basic functions



Basic Functions

JPEG compression

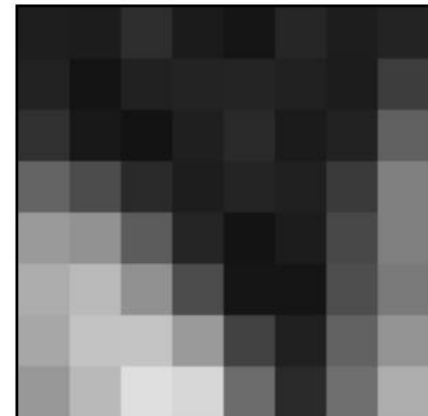
- The coefficients of the **low frequencies** are in the **upper left** corner while the **high frequencies** will be in the **lower right** corner
- However, the **low frequencies** of a signal are **more important** than the high frequencies for the human eye
 - ✓ Removing 50% of the high-frequency bits only removes 5% of the encoded information



Selection of 50%
of functions



Initial bloc 8x8



Reconstituted block

JPEG compression

- To achieve image compression, **the number of bits of high frequencies is reduced**
- The following tables are used depending on the expected level of compression :

1	1	1	1	1	2	2	4
1	1	1	1	1	2	2	4
1	1	1	1	2	2	2	4
1	1	1	1	2	2	4	8
1	1	2	2	2	2	4	8
2	2	2	2	2	4	8	8
2	2	2	4	4	8	8	16
4	4	4	4	8	8	16	16

Low compression

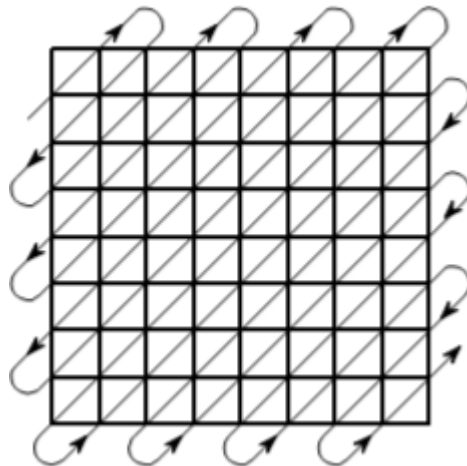
1	2	4	8	16	32	64	128
2	4	4	8	16	32	64	128
4	4	8	16	32	64	128	128
8	8	16	32	64	128	128	256
16	16	32	64	128	128	256	256
32	32	64	128	128	256	256	256
64	64	128	128	256	256	256	256
128	128	128	256	256	256	256	256

High compression

- The reduction of the high frequencies by a coefficient of 16 allows the information to be encoded on 4 bits instead of the original 8 bits
- The coefficient 256 indicates the suppression of high frequencies

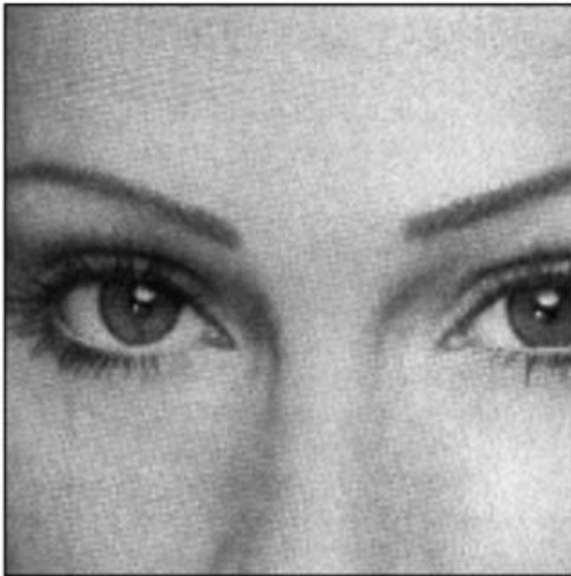
JPEG compression

- The final step is to convert the 8x8 matrix into a linear sequence
- Allows small amplitudes to be grouped together and thus to decrease the size of the 8x8 matrix
- A compression ratio of 45:1 allows the 8x8 matrix to be represented with 12 bits instead of 512 bits

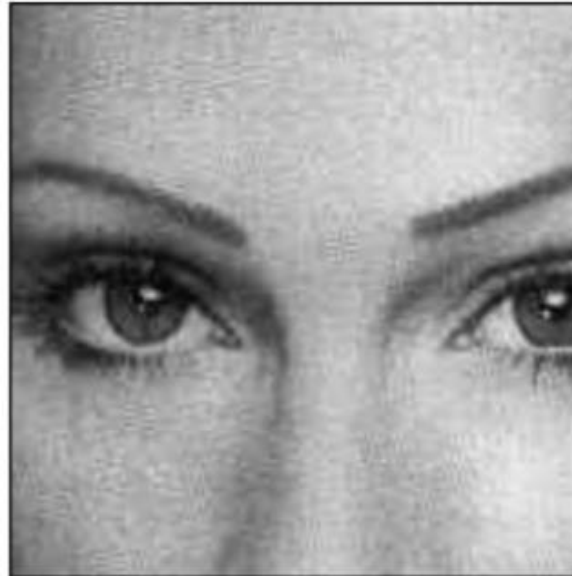


JPEG compression

- Example of distortion due to JPEG compression



Original image



Compression ratio of
10:1



Compression ratio of
45:1
(2.3% of the original
image size)

Malicious use of steganography

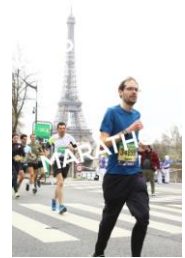
- ▶ This hiding technique is used in the malware world to infect computers with seemingly innocent files
- ▶ Example: An attacker group linked to APT10 uses the [Backdoor.Stegmap](#) tool (Sept 2022) that retrieves an image from a Github directory in which the payload is located
 - An XOR of this file with a key is used to **decrypt malicious payload** to pass any type of command on the victim machine (create/delete files, registry keys, processes, etc.)
 - Hiding the payload in the image allows attackers to **easily host** this file on trusted sites such as Github and is less likely to raise an alert than a download from a command and control (C&C) server



Digital watermark

► Watermarking aims to protect the copyright of a work on a digital medium

- Visible watermark : Do not use steganography (e.g., photo tagging on paid photo preview versions)
- Invisible watermark : serves as a signature to identify the owner of the image, at the same time conferring a copyright
 - ✓ In this case, steganography is used to hide a message (e.g. the buyer's ID) **without degrading the medium**



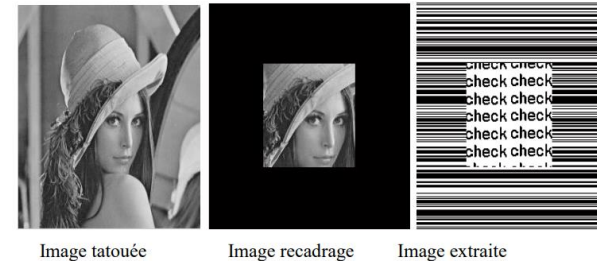
► Watermarking includes two types: the fragile watermark and the robust watermark

Digital watermark

- ▶ **The fragile watermark is only used to prove the integrity of the data**
 - The protection of the data hidden being very weak, the message it carries is not really important but allows any modification to be detected
 - Used in the fight against document counterfeiting

- ▶ **The robust watermark is harder to get around and must withstand various attacks**

- It must have the following two properties:
 - ✓ The data hidden must be very resistant to the various known attacks (resampling, printing and scanning, compression, cutting, noise and format changes)
 - ✓ The data hidden must be easily recognizable after extraction, despite the damage suffered by the various attacks



Steganalysis

- ▶ Unlike steganography, stegananalysis is the art and science of detecting if a given medium is hiding a secret message, and if possible, retrieving that hidden message
- ▶ Steganalysis is analogous to cryptanalysis applied to cryptography
- ▶ This is a very difficult task, due to:
 - The great diversity of mediums
 - The wide variation in data
 - The different insertion algorithms
 - The low distortion due to the integration of the message in general



Preventing steganography

- ▶ **The observer can compare the statistical properties of the suspected communication and compare them with those of a communication that does not contain hidden messages**
 - Too many differences can be an indication of hidden communication
- ▶ **To prohibit all covert communications, it is necessary to be able to intercept and transform or prohibit all communications**
 - Since background noise or low frequencies are good hiding places, you will have to add your own noise, or filter out the existing noise
 - We can also uncompress and then compress the message

Document Marking

► Possibility to tag documents to detect possible data leaks

- Simple : document header or footer (Confidential)
- Complex : Inserting a markup in the document's metadata (invisible in the document's properties)
 - ✓ For example, PDF documents contain a dictionary (set of keys/values), just add a particular key/value
 - ✓ Since Office 2007, use of the Office Open XML file format that stores document data in zipped XML files: simply add XML properties to these files in a place that is resistant to editing the document



Data exfiltration detection

► Infrastructure is needed to detect the leakage of previously tagged documents

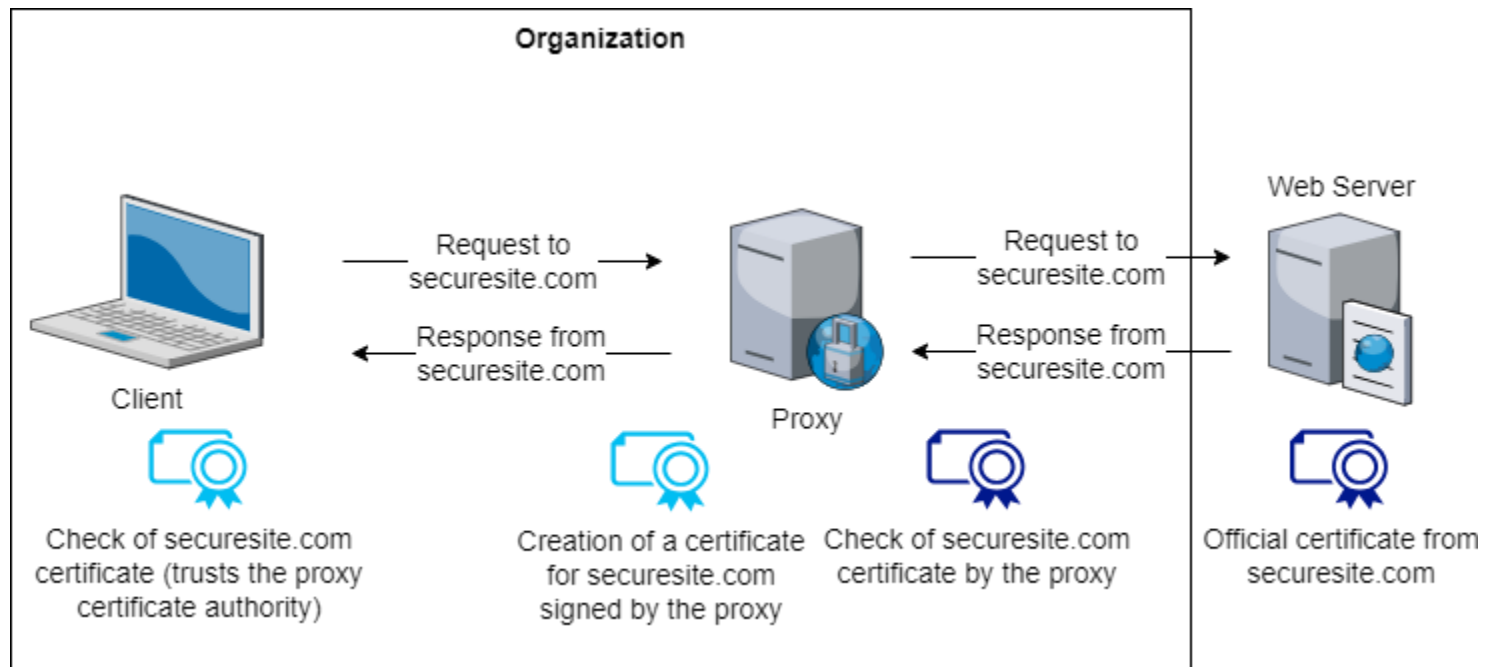
- Web proxy
- Mail proxy
- USB protection (DLP agent or port restrictions)
- Detecting attempts to remove the tag

► Issue related to the encryption of flows if network detection is used

- Requires decrypting streams so that outgoing files can be scanned for the signature that matches the tag
- Leads new risks: this operation causes to **break a secure channel** and exposes unencrypted data on the device in charge of the operation

Decryption of flows

- To inspect encrypted traffic, the communication channel must stop at the proxy, be inspected, and then re-encrypted, and sent to the final destination



Conclusion

- ▶ **Steganography allows a message to be hidden to avoid attracting attention, unlike cryptography**
 - Eliminates some controls (antivirus) and makes it more difficult to scan for malware
- ▶ **The more robustness and invisibility are requested, the less the medium will allow the transport of a large amount of information**
- ▶ **Allows you to watermark information**
 - Identify the source of a data breach
 - Fight against counterfeiting