Lecture 9 and 10

Image Cryptography and Steganography

R. Rhouma

UTAS
Sultanate of Oman
September 2022

CSSY2201 : Introduction to Cryptography

جامعة التقنية
والعلوم التطبيقية
University of Technology
and Applied Sciences
Salalah صلالة

Plan

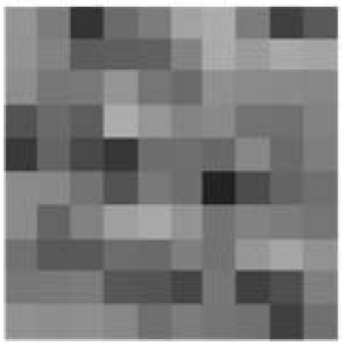
What is an Image ?

2-dimensional matrix of Intensity (gray or color) values

Set of Intensity values

Image coordinates are integers

$$I(u,v) \in \mathbb{P} \quad \text{and} \quad u,v \in \mathbb{N}.$$



$F(x,y)$

$\rightarrow$

148	123	52	107	123	162	172	123	64	89 ···
147	130	92	95	98	130	171	155	169	163 ···
141	118	121	148	117	107	144	137	136	134 ···
82	106	93	172	149	131	138	114	113	129 ···
57	101	72	54	109	111	104	135	106	125 ···
138	135	114	82	121	110	34	76	101	111 ···
138	102	128	159	168	147	116	129	124	117 ···
113	89	89	109	106	126	114	150	164	145 ···
120	121	123	87	85	70	119	64	79	127 ···
145	141	143	134	111	124	117	113	64	112 ···
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

$I(u,v)$

Digital Image

Common image formats include :

- 1 values per point/pixel (B&W or Grayscale)
- 3 values per point/pixel (Red, Green, and Blue)
- 4 values per point/pixel (Red, Green, Blue, + "Alpha" or Opacity)

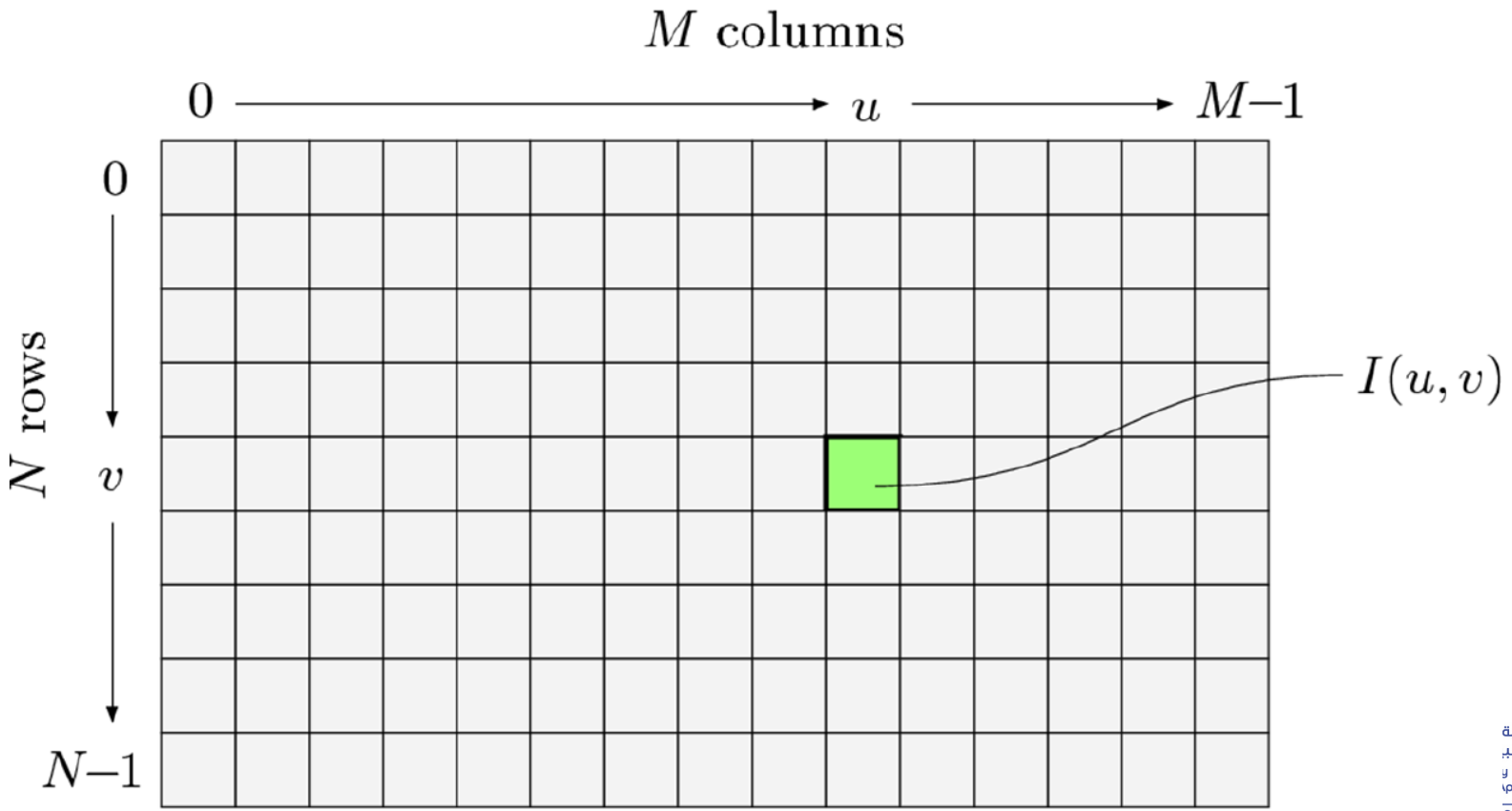
Grayscale

RGB

RGBA

Representing Images

- Image data structure is 2D array of pixel values
- Pixel values are gray levels in range 0-255 or RGB colors
- Array values can be any data type (bit, byte, int, float, double, etc.)



Intensity Level Resolution

- Intensity level resolution : number of intensity levels used to represent the image
  - The more intensity levels used, the finer the level of detail discernable in an image
  - Intensity level resolution usually given in terms of number of bits used to store each intensity level

Number of Bits	Number of Intensity Levels	Examples
1	2	0, 1
2	4	00, 01, 10, 11
4	16	0000, 0101, 1111
8	256	00110011, 01010101
16	65,536	1010101010101010

Intensity Level Resolution

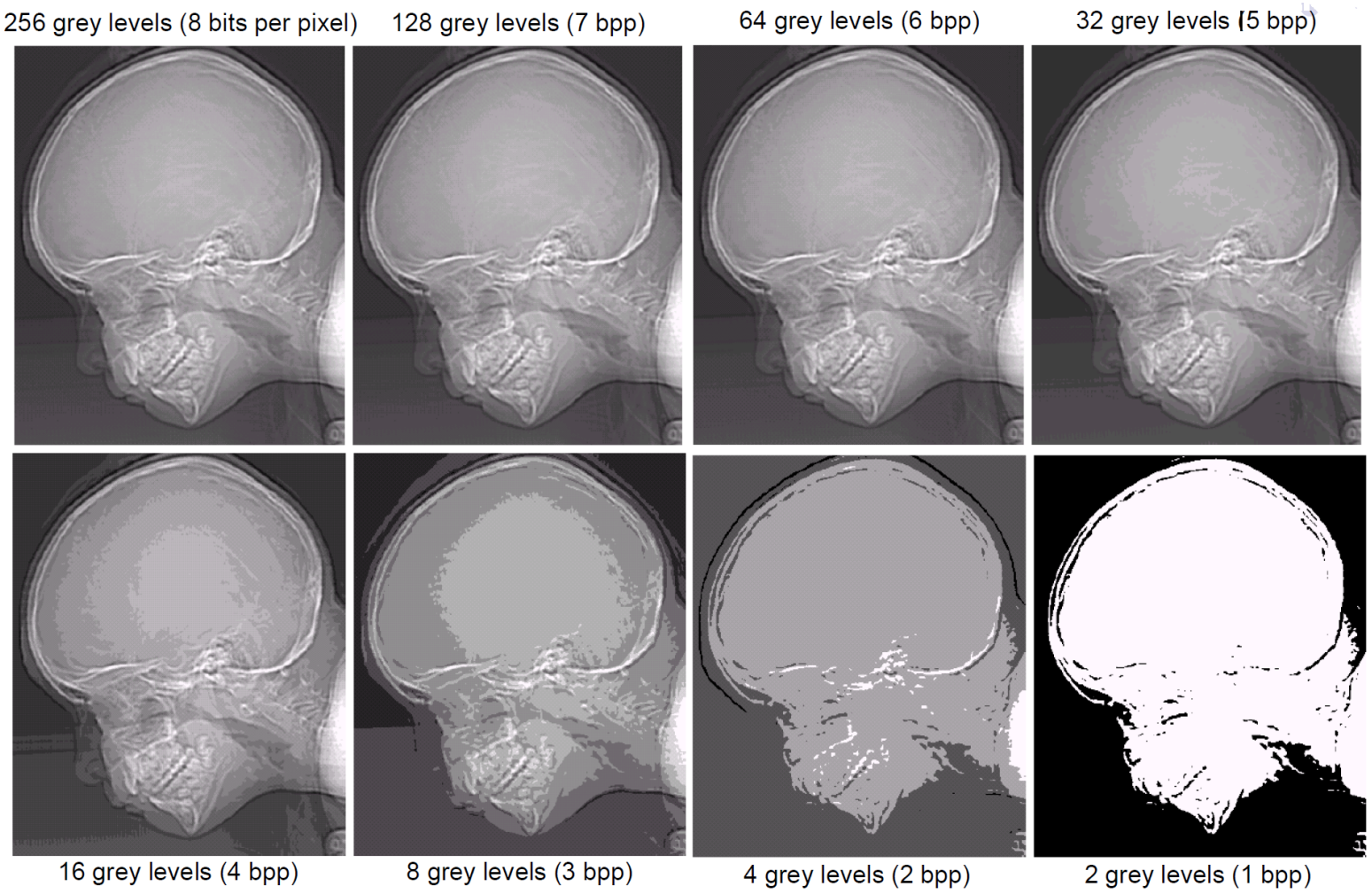


Image File Formats

- Hundreds of image file formats. Examples
  - Tagged Image File Format (TIFF)
  - Graphics Interchange Format (GIF)
  - Portable Network Graphics (PNG)
  - PEG, BMP, Portable Bitmap Format (PBM), etc
- Image pixel values can be
  - Grayscale : 0 - 255 range
  - Binary : 0 or 1
  - Color : RGB colors in 0-255 range (or other color model)
  - Application specific (e.g. floating point values in astronomy)

How many Bits Per Image Element ?

Grayscale (Intensity Images):

Chan.	*Bits/Pix.*	*Range*	*Use*
1	1	0...1	Binary image: document, illustration, fax
1	8	0...255	Universal: photo, scan, print
1	12	0...4095	High quality: photo, scan, print
1	14	0...16383	Professional: photo, scan, print
1	16	0...65535	Highest quality: medicine, astronomy

Color Images:

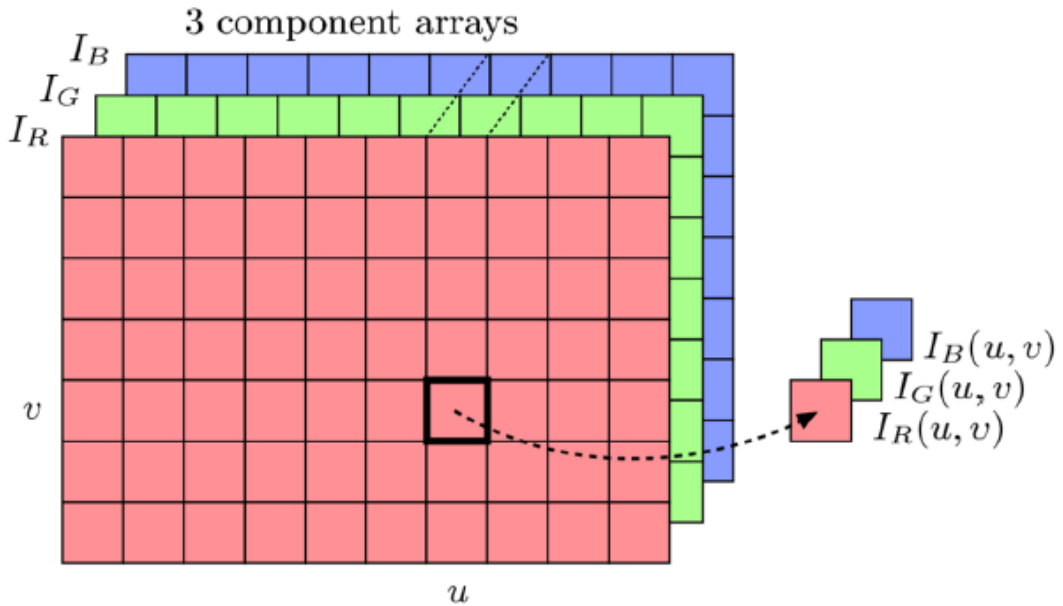
Chan.	*Bits/Pix.*	*Range*	*Use*
3	24	$[0...255]^3$	RGB, universal: photo, scan, print
3	36	$[0...4095]^3$	RGB, high quality: photo, scan, print
3	42	$[0...16383]^3$	RGB, professional: photo, scan, print
4	32	$[0...255]^4$	CMYK, digital prepress

Special Images:

Chan.	*Bits/Pix.*	*Range*	*Use*
1	16	$-32768...32767$	Whole numbers pos./neg., increased range
1	32	$\pm 3.4 \cdot 10^{38}$	Floating point: medicine, astronomy
1	64	$\pm 1.8 \cdot 10^{308}$	Floating point: internal processing

True Color

- Colors in 3 separate arrays of similar length
- Retrieve same location (u,v) in each R, G and B array



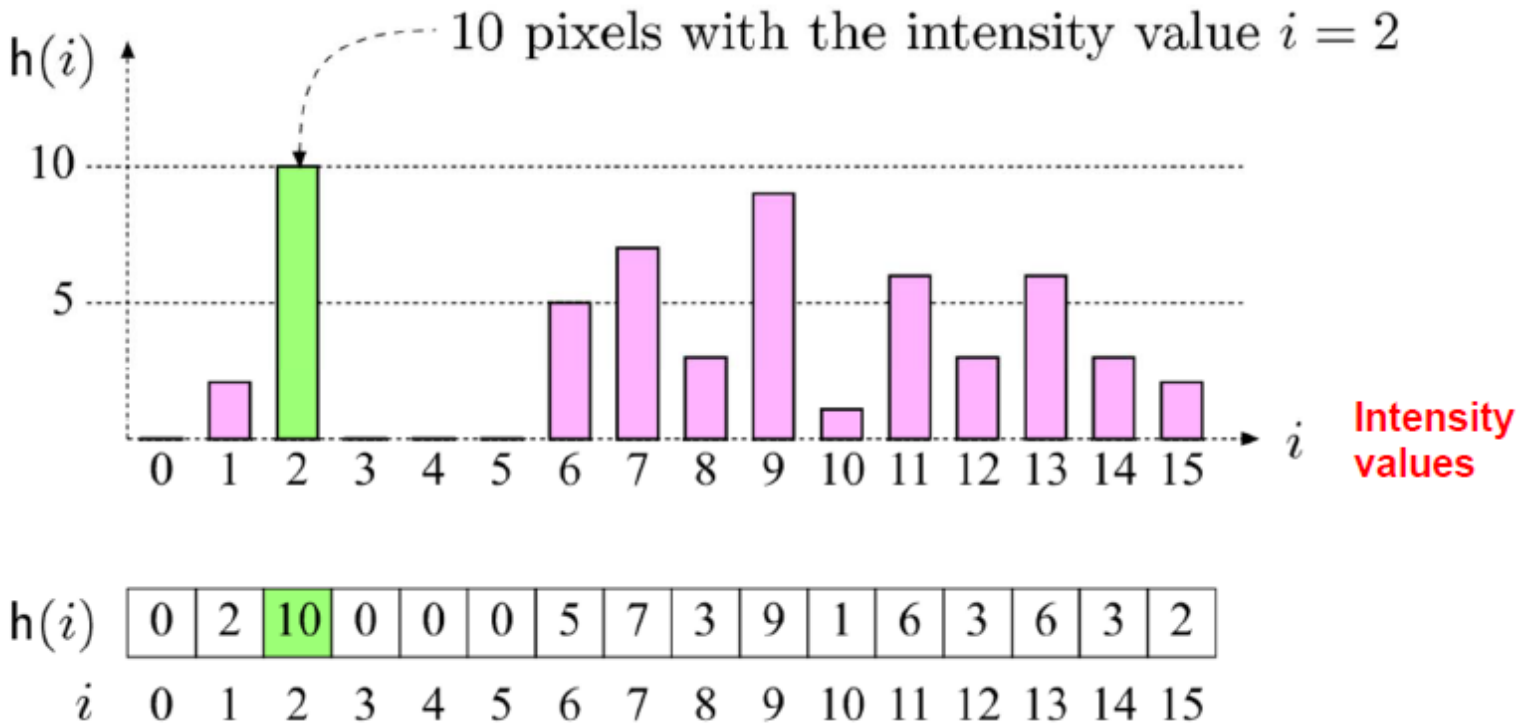
$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} \leftarrow \begin{pmatrix} I_R(u,v) \\ I_G(u,v) \\ I_B(u,v) \end{pmatrix}$$

color images

- RGB full-color images (24-bit "RGB color"),
  - packed order
  - Supports TIFF, BMP, JPEG, PNG and RAW file formats
- Indexed images ("8-bit color")
  - Up to 256 colors max (8 bits)
  - Supports GIF, PNG, BMP and TIFF (uncompressed) file formats

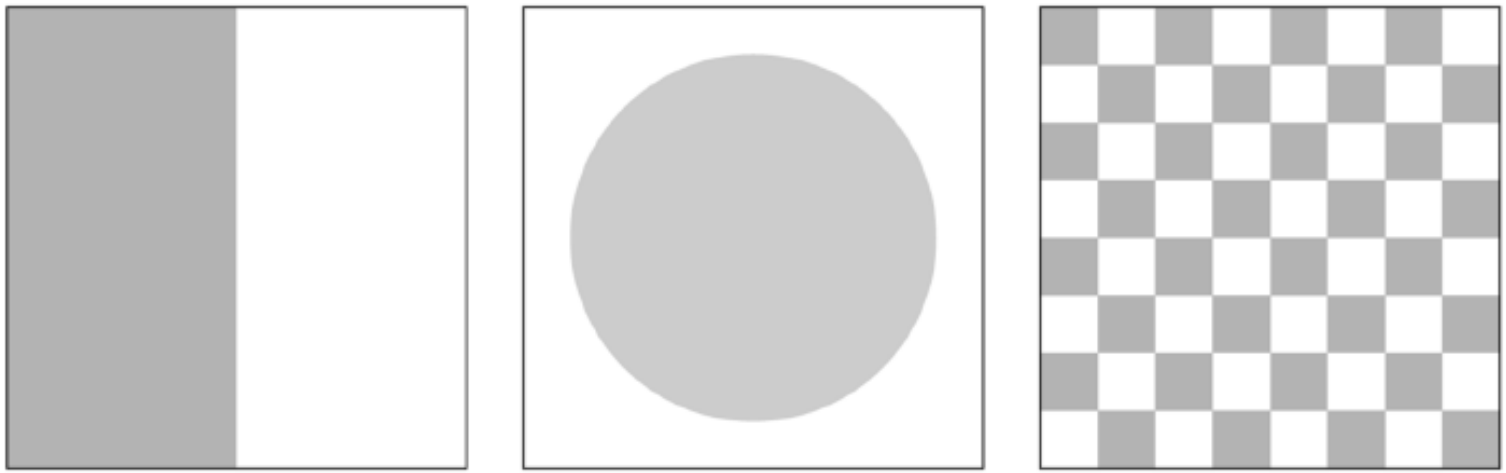
Histograms

- Histograms plots how many times (frequency) each intensity value in image occurs
- Example :
  - Image (left) has 256 distinct gray levels (8 bits)
  - Histogram (right) shows frequency (how many times) each gray level occurs



- E.g. K = 16, 10 pixels have intensity value = 2
- Histograms : only statistical information
- No indication of location of pixels

- Different images can have same histogram
- 3 images below have same histogram



- Half of pixels are gray, half are white
  - Same histogram = same statisics
  - Distribution of intensities could be different
- Can we reconstruct image from histogram ? No !

- So, a histogram for a grayscale image with intensity values in range

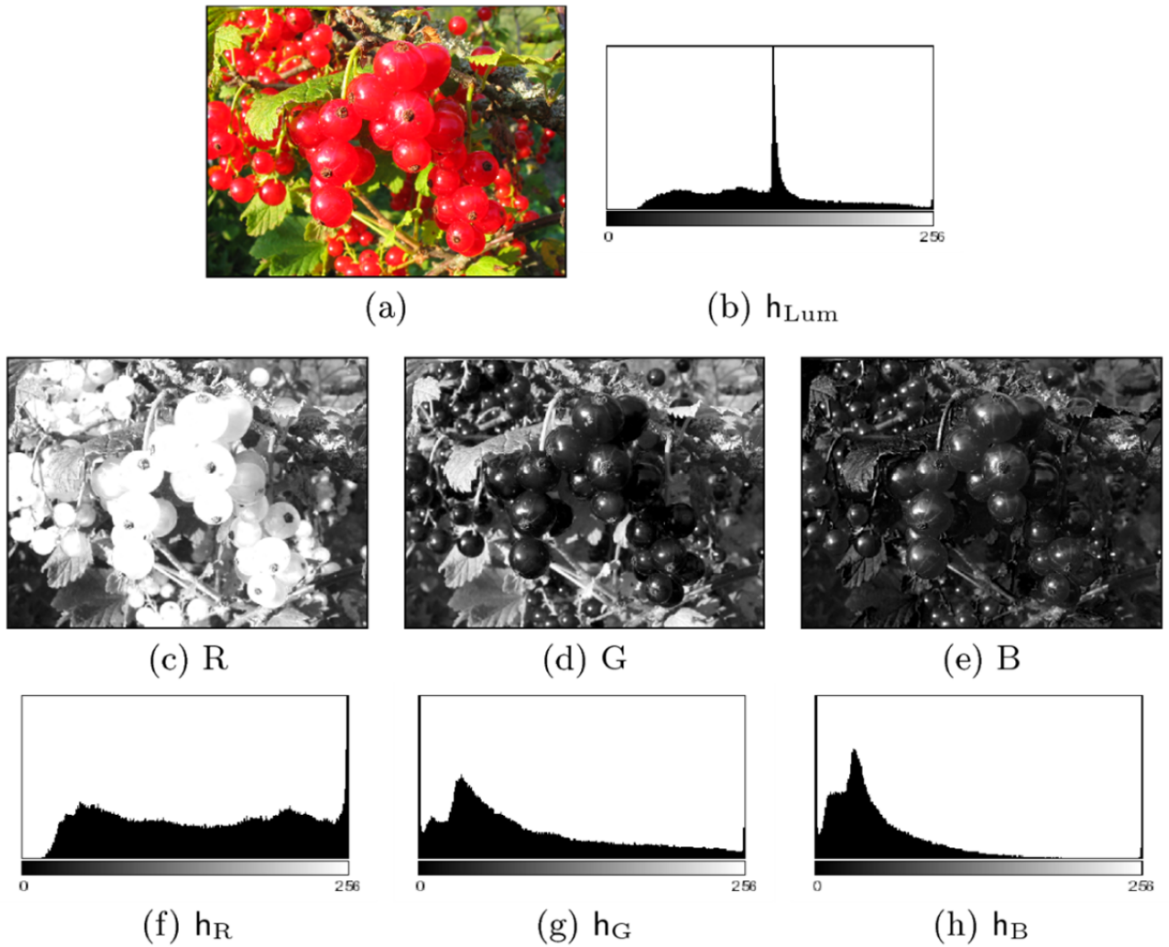
$$I(u, v) \in [0, K - 1]$$

  would contain exactly K entries
- E.g. 8-bit grayscale image, $K = 2^8 = 256$
- Each histogram entry is defined as :
  h(i) = number of pixels with intensity i
- E.g : h(255) = number of pixels with intensity 255
- formal definition : $h(i) = card\{(u, v)|I(u, v) = i\}$

Color Image Histograms

Two types :

1. Intensity histogram :
   - Convert color image to gray scale
   - Display histogram of gray scale
2. Individual Color Channel Histograms : 3 histograms (R,G,B)



PSNR and MSE

- Peak Signal to Noise Ratio (PSNR) is an engineering formulation determined through mean square error (MSE). It is generally utilized for image quality evaluation as follows :

$$PSNR = 10 \log_{10} \frac{d^2}{MSE}$$

where

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - Y(i,j))^2$$

- d stands for the maximal intensity value that can be taken. for example in a gray scale image $d = 255$.
- M and N are the height and width of the images.
- To use PSNR and MSE, the two compared images should be with the same dimensions.
- values of PSNR between 30 dB and 40 dB (decibels) indicate that images are very similar.

NPCR

Number of Pixels Change Rate (NPCR) :

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%$$

M and N are the height and width of the images

$$D(i,j) = \begin{cases} 0 \ if \ S(i,j) = S'(i,j) \\ 1 \ if \ S(i,j) \neq S'(i,j) \end{cases}$$

$S(i,j)$ and $S'(i,j)$ are the values of pixels.
for two random images : $NPCR = 99.609375\%$

UACI

Unified Average Changing Intensity (UACI) :

$$UACI = \frac{1}{M \times N}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|S(i,j) - S'(i,j)|}{2^B - 1}\right) \times 100\%$$

M and N are the height and width of the images.
$S(i,j)$ and $S'(i,j)$ are the values of pixels.
and B is the intensity level (E.g for a gray scale image $B = 8$).
For two random images : $UACI = 33.46354\%$

Example : Image cryptosystem

Let's take an example of an image cryptosystem

- which uses CBC mode : Cipher Block Chaining
- also use a random source genertor from a map lattice x_n
- We will analyse its security through statistical tests like :
  - Correlation Coefficient
  - NPCR : Number of Pixel Change Rate
  - UACI : Unified Average Changing Intensity
  - Entropy

Encryption and Decryption

From the keys, a map x_n is iterated

- Encryption :

$$C_n(1) = (R_n + int(x_n(1) \times L) + C_{n-1}(1)) mod\, 256$$

$$C_n(2) = (G_n + int(x_n(2) \times L) + C_{n-1}(2)) mod\, 256$$

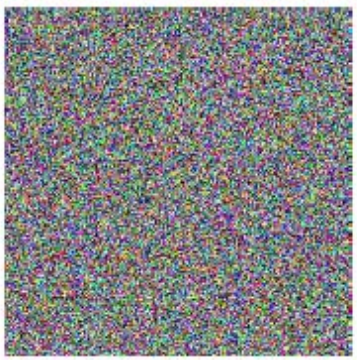
$$C_n(3) = (B_n + int(x_n(3) \times L) + C_{n-1}(3)) mod\, 256$$

- Decryption :

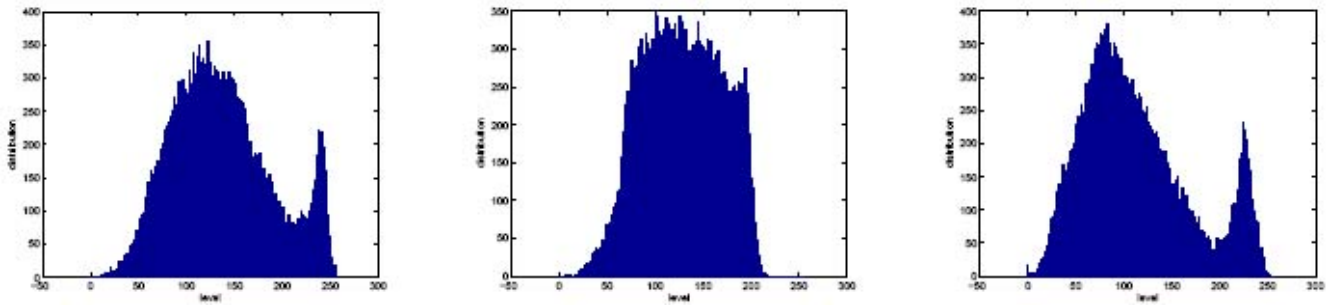
$$R_n = (C_n(1) - int(y_n(1) \times L) - C_{n-1}(1)) mod\, 256$$

$$G_n = (C_n(2) - int(y_n(2) \times L) - C_{n-1}(2)) mod\, 256$$

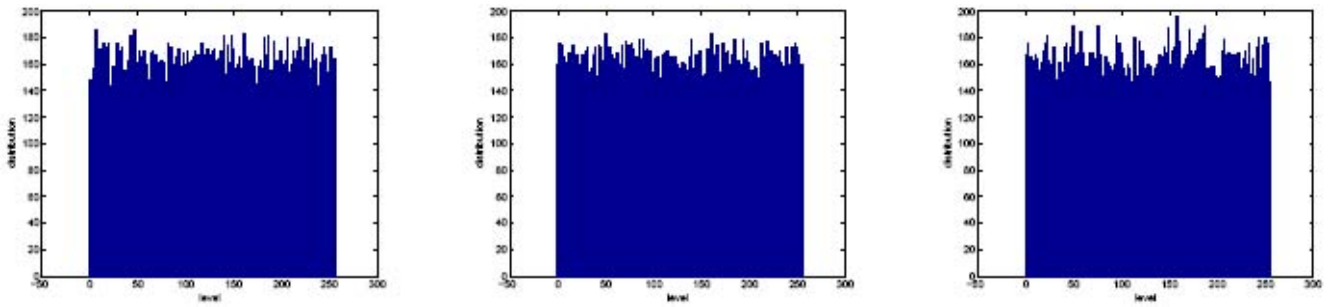
$$B_n = (C_n(3) - int(y_n(3) \times L) - C_{n-1}(3)) mod\, 256$$


Histogram



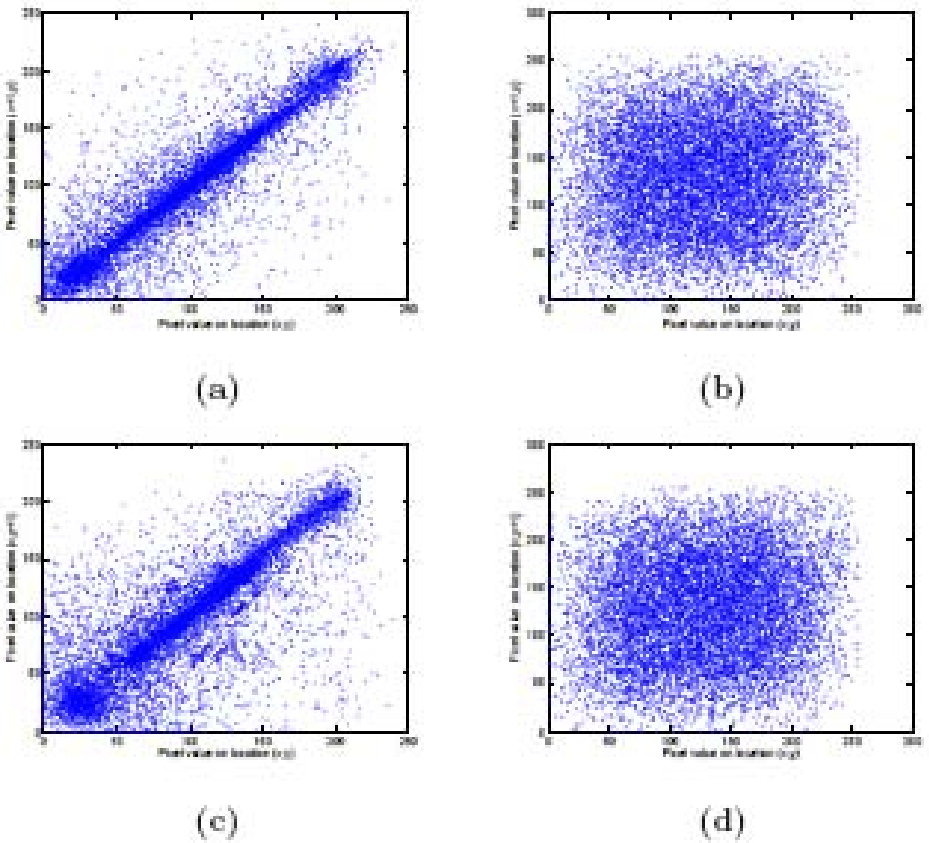
Histogram of plain image for colour R, G and B.



Histogram of cipher image for colour R, G and B.

Histogram of cipher image should look uniform to be sure that the cryptosystem mimic a random source.

Correlations of adjacent pixels



- Drawing X(i+1)=f(X(i)) in horizontal or vertical show a graph following the line y=x. this is expected in plain image because every pixel is highly correlated with its adjacent pixel (figure (a) horizontal, (b) vertical)
- the same plot X(i+1)=f(X(i)) shown a random dispersion for the cipher-image ((b) horizontal (d) vertical)

Correlation Coefficient

$$r = \frac{cov(p,q)}{\sqrt{D(p)}\sqrt{D(q)}}$$

where,

$$D(p) = \frac{1}{S}\sum_{i=1}^{S}(p_i - \bar{p})^2$$

$$cov(p,q) = \frac{1}{S}\sum_{i=1}^{S}(p_i - \bar{p})(q_i - \bar{q})$$

- q_i and p_i are adjacent pixels (horizontal or vertical).
- S is the total number of pairs (p_i, q_i) obtained from the image ;
- $\bar{p}$ and $\bar{q}$ are the mean values of p_i et q_i, respectively.

Correlation coefficient	Plain image	Cipher image
horizontal	0.9006	0.0681
vertical	0.8071	0.0845

- r for plain-image is naturally close to 1
- r for random images should be close to 0
- the experience shows that the cipher-image is very like a random image.

NPCR and UACI measures

- measuring NPCR and UACI between plain-images and cipher-images for every color component. To be sure that the cryptosystem transform the plain-image on a random-like output.
- For 2 gray-scale random images : $NPCR = 99.609375\%$ and $UACI = 33.46354\%$

Image	Mean NPCR (%)			Mean UACI (%)		
	R	G	B	R	G	B
Lena	99.5660	99.5860	99.6010	33.4137	33.2980	33.4148
Baboon	99.5469	99.6265	99.5776	33.4600	33.4525	33.3468
Jet	99.6005	99.6085	99.6080	33.4124	33.4665	33.4633
Peppers	99.6100	99.5790	99.5880	33.4111	33.4236	33.4163

Entropy : Randomness Measure

- Entropy : the cipher image should look random. A pure random source using N-bit for each pixel will reach Entropy=N according to Claude Shannon

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) log(\frac{1}{p(m_i)})$$

$\Rightarrow$

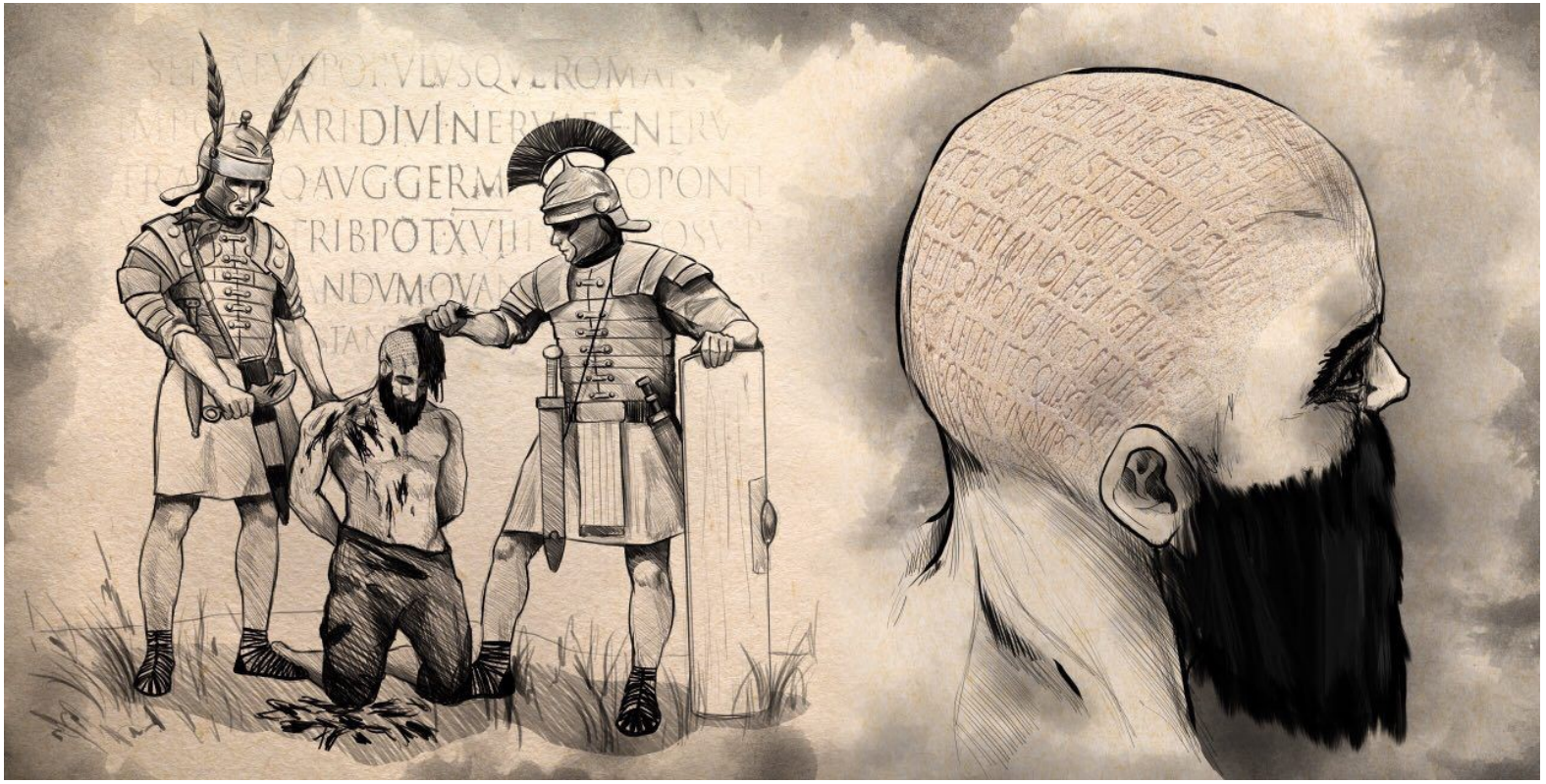
$$H_R(m) = \sum_{i=0}^{2^8-1} p(R_i) log(\frac{1}{p(R_i)}) = 7.9732 \simeq 8$$

$$H_G(m) = \sum_{i=0}^{2^8-1} p(G_i) log(\frac{1}{p(G_i)}) = 7.9750 \simeq 8$$

$$H_B(m) = \sum_{i=0}^{2^8-1} p(B_i) log(\frac{1}{p(B_i)}) = 7.9715 \simeq 8$$

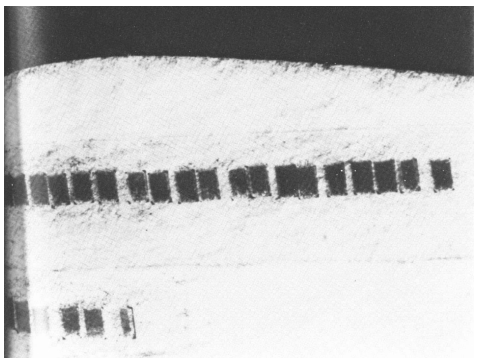
Data Hiding of confidential messages

Data hiding technique from the Greek era : Write secret texts on the shaved head of a slave. Let the hair grow to hide the message



Historical Forms of Steganography

- Tattoos (Herodotus)
- Invisible Inks (lemon juice, milk, urine,..)
- Microdots in paper
- text (reconstitute the secret from some letters in text)



Modern Steganography

- Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.
- Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, html) with the bits of invisible information
- This hidden information can be plain text, cipher text or even images.
- In modern steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image, Bitmap image.

Steganography process

Cover-media + Hidden data + Stego-key = Stego-medium

- Cover media : It is the file in which we will hide the hidden data. Cover-media can be image or audio file.
- stego-key : the key to embed and to extract hiden information
- stego-medium. The resultant file is of above process called stego medium.

Why use Steganography rather than Cryptography ?

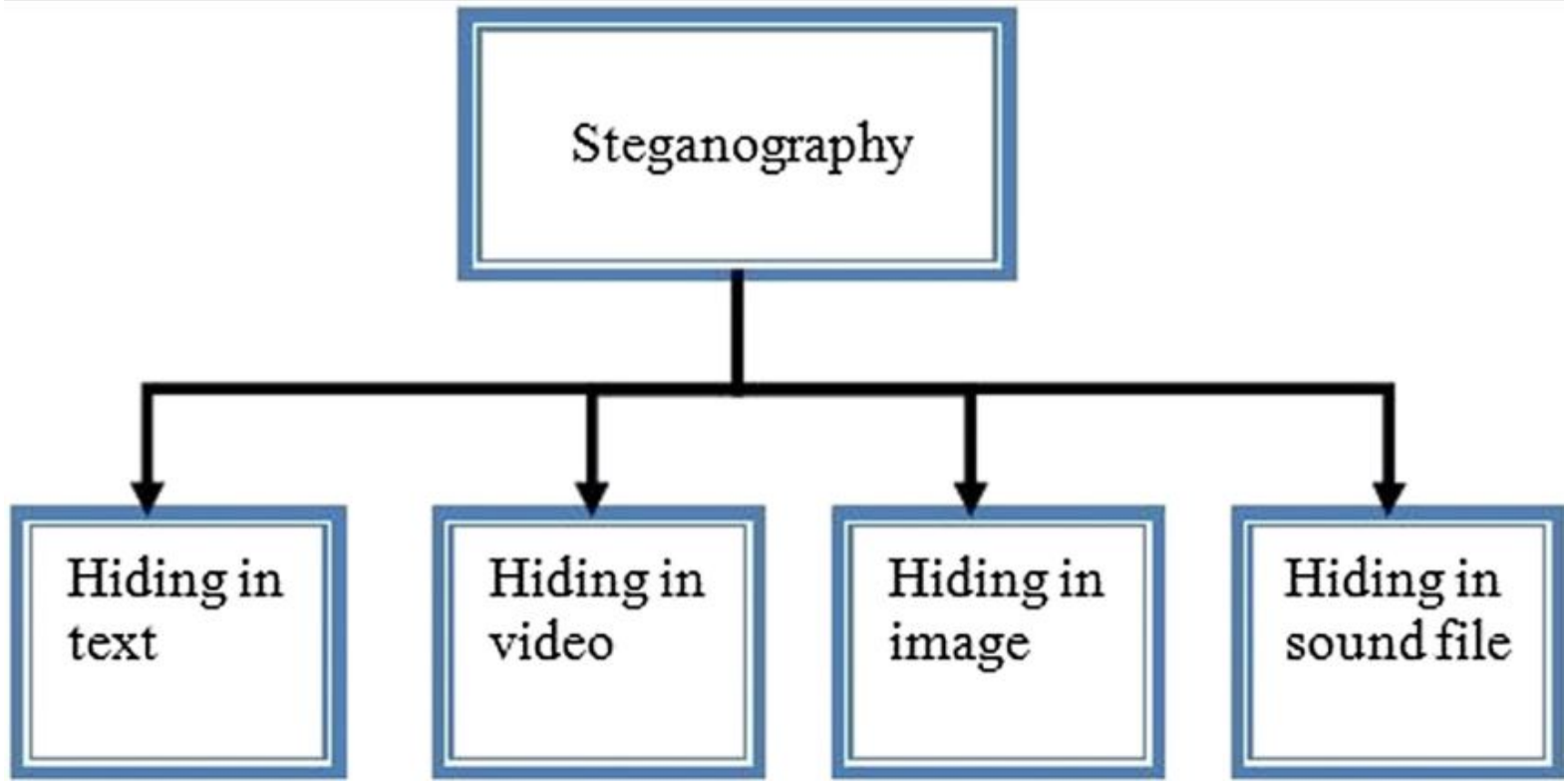
- Advantages : i) No one suspects existence of message ii) Highly secure
- Disadvantages : It requires a lot of overhead to hide a relatively few bits of information

Important factors in Steganography

Three main factors should be considered in any successful stego system :

1. Imperceptibility
2. Robustness
3. Embedding Capacity

Types of Steganography



Cryptography vs Steganography vs. Watermarking

- Cryptography is about protecting the content of messages (their meaning).
- Steganography is about concealing the existence of messages
- Watermarking is about establishing identity of information to prevent unauthorized use
  - They are imperceptible
  - They are inseparable from the works they are embedded in
  - They remain embedded in the work even during transformation

Steganography vs Cryptography

Steganography	Cryptography
Unknown message passing	Known message passing
Steganography prevents discovery of the very existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being develop for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithm are resistant to attacks ,larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

Text Steganography : example

Since everyone can read, encoding text
in neutral sentences is doubtfully effective

Since Everyone Can Read, Encoding Text
In Neutral Sentences Is Doubtfully Effective

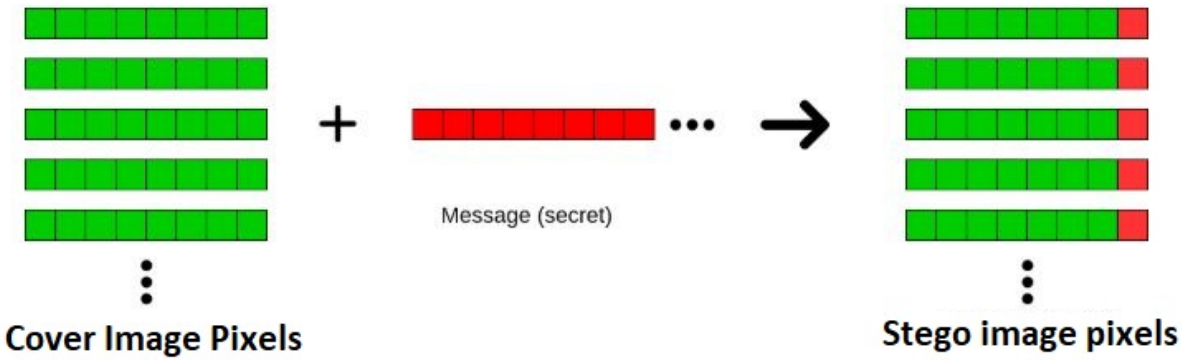
'Secret inside'

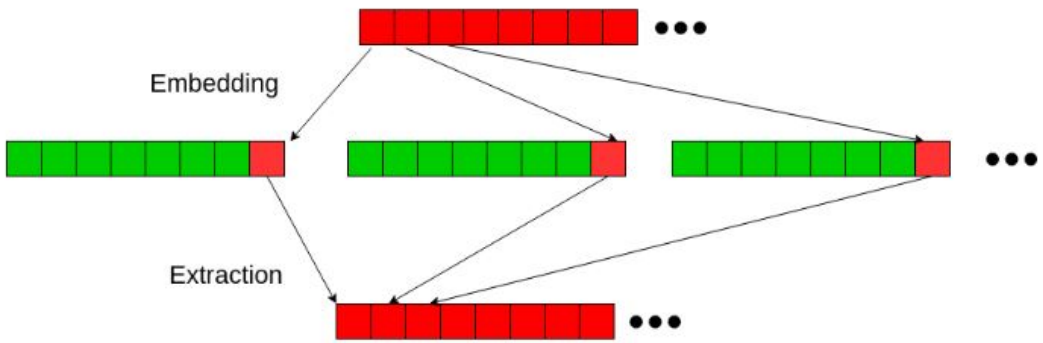
Steganography in images

1. Hiding information in an image
2. Embed the secret data in bit pixels : dealing with 8-bit based image (Gray) or 24-bit images (RGB)

Steganography in images

- Least significant bit insertion (GIF, BMP) : Changing the least significant bit in order to store secret data





- Discrete Cosine Transform (JPG) : Applying a Cosine function to approximate hidden data
- also using other transform using wavelets, fractals, etc

Imperceptibility measure

- PSNR between cover (X) and stego (Y) images of size $M \times M$:

$$PSNR = 10 \log_{10} \frac{255^2}{EQM}$$

$$EQM = \frac{1}{M \times M} \sum_{i=1}^{M} \sum_{j=1}^{M} (X(i,j) - Y(i,j))^2$$

PSNR=38.83

PSNR=35.15

- PSNR of "good" quality images varies between 30 and 40 dB.

Robustness assessment

- ability to extraxt the hidden data despite the distortion made on the stego image.

Rotation resizing cutting Noising blurring JPEG compression