Image Compression and Watermarking

ICT4201: DIP

Preview

- The art and science of reducing the amount of data required to represent an image
- The process of inserting visible and invisible data (such as copyright information) into images

Image Compression

- Why we need this?
  - Suppose a Standard definition (SD) movie using 720×480×24 bits pixel array where a video player has frame size 30 frames/sce. Then the size of the movie will be 30×720×480×3 bytes/pixel= 31104000 bytes/sec
  - Duration of movie is 2 Hrs, then $31104000 \times 2 \times 60 \times 60 = 2.24 \times 10^{11}$ bytes = 224 GB
  - For example, images on web page, HD images should be compressed to reduce storage and transmission rate.
- When there are irrelevant or repeated information, we can compress it
- Data with no redundancy cannot be compressed.
- Compression is a technique which increases efficiency by removing redundancy from any representation.
- Decompression is the reverse operation performed to the redundant parts are put back into the original representation to restore it in its initial form.

Lossless vs. Lossy Compression

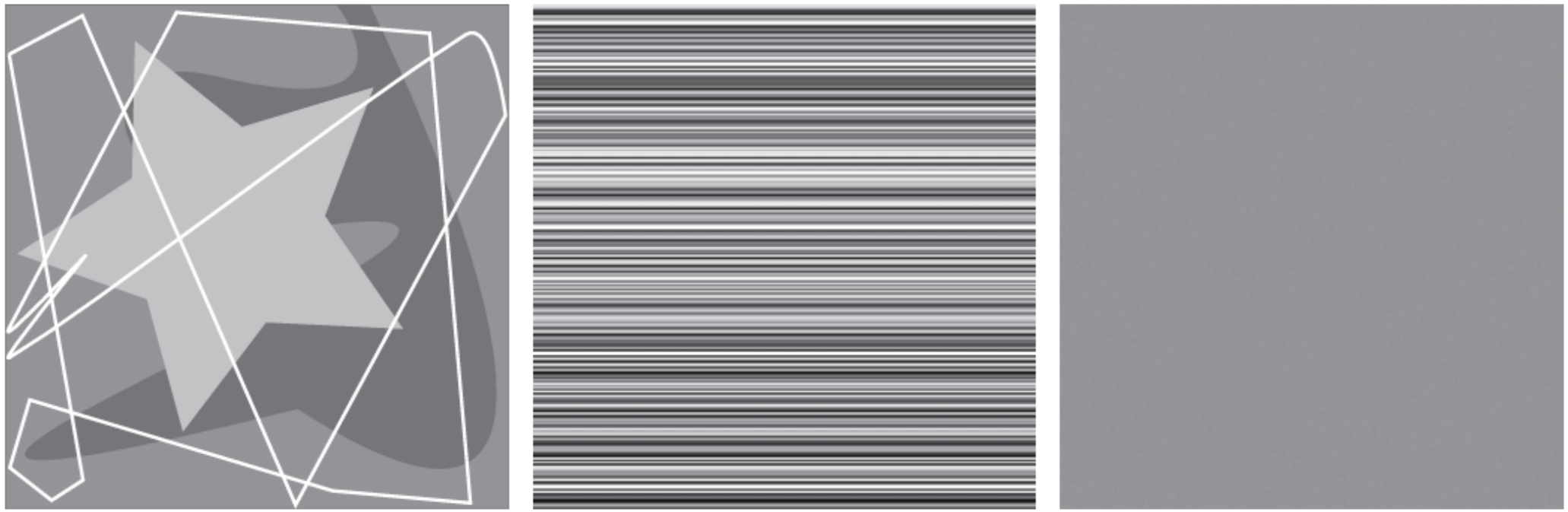
- Lossless: zero error tolerance
  - No information loss
  - Shannon's entropy formula
  - For photographic images, compression ratio is modest (about 2:1)
- Lossy: the goal is to preserve the visual quality of images
  - Information loss visually acceptable
  - Shannon's rate-distortion function
  - For photographic images, compression ratio is typically around 10-100

Fundamentals of Image compression

- The term data compression refers to the process of reducing the amount of data required to represent a given quantity of information.
- Data and information are not the same; data are the means by which information is conveyed.
- Because various amounts of data can be used to represent the same amount of information, representations that contain irrelevant or repeated information are said to contain redundant data.
- If we let *b* and *b'* denote the number of bits (or information- carrying units) in two representations of the same information, the relative data redundancy, *R*, of the representation with b bits is $R = 1 - \frac{1}{C}$
- Where *C* is compression ratio, $C = \frac{b}{b'}$
  - If C= 10 (10:1) then R= 0.9 or 90% redundant data.

Fundamentals of Image compression

- Two-dimensional intensity arrays suffer from three principal types of data redundancies that can be identified and exploited:
  1. **Coding redundancy:** A code is a system of symbols (letters, numbers, bits, and the like) used to represent a body of information or set of events. Each piece of information or event is assigned a sequence of code symbols, called a code word.
  2. **Spatial and temporal redundancy:** Spatial and temporal correlation between pixels is unnecessarily replicated in the representations of the correlated images or sequence of images causes unnecessary redundancy of information.
  3. **Irrelevant information:** Most 2-D intensity arrays contain information that is ignored by the human visual system and/or extraneous to the intended use of the image. It is redundant in the sense that it is not used.



a b c

FIGURE 8.1 Computer generated $256 \times 256 \times 8$ bit images with (a) coding redundancy, (b) spatial redundancy, and (c) irrelevant information. (Each was designed to demonstrate one principal redundancy, but may exhibit others as well.)

CODING REDUNDANCY

- Assume that a discrete random variable r_k in the interval [0, L-1] resent the intensities of an M×N image, and that each r_k occurs with probability $p_r(r_k)$,
- As normalized histogram we can write, $p_r(r_k) = \frac{n_k}{MN}$, k= 0,1,2,3,……..,L-1.
  - where L is the number of intensity values, and n_k is the number of times that the kth intensity appears in the image. If the number of bits used to represent each value of r_k is $l(r_k)$, then the average number of bits required to represent each pixel is

$$L_{avg} = \sum_{k=0}^{L-1} l(r_k) p_r(r_k)$$

  - $l(r_k)$ can be variable or fixed.

CODING REDUNDANCY--- Example

r_k	$p_r(r_k)$	Code 1	$l_1(r_k)$	Code 2	$l_2(r_k)$
$r_{87} = 87$	0.25	01010111	8	01	2
$r_{128} = 128$	0.47	01010111	8	1	1
$r_{186} = 186$	0.25	01010111	8	000	3
$r_{255} = 255$	0.03	01010111	8	001	3
r_k for $k = 87, 128, 186, 255$	0	—	8	—	0

- For Code 1, L_{avg} = 8 bits,
- For Code 2, L_{avg} = 2(0.25)+1(0.47)+3(0.25)+3(0.03)= 1.81 bits
  - $C = \frac{256\times256\times8}{256\times256\times1.81} = \frac{8}{1.81} = 4.42$; [Size of total image = MNL_{avg}]
  - $R = 1 - \frac{1}{C} = 1 - \frac{1}{4.42} = 0.774$; 77.4% of the data in the original 8-bit 2-D intensity array is redundant

SPATIAL AND TEMPORAL REDUNDANCY

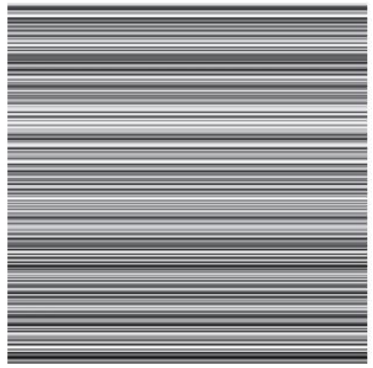
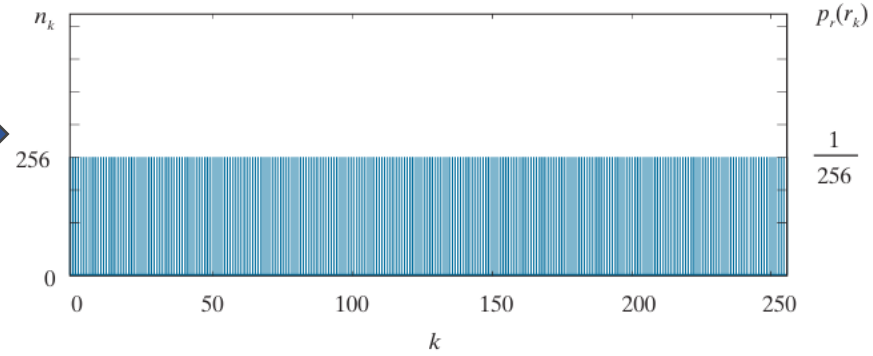


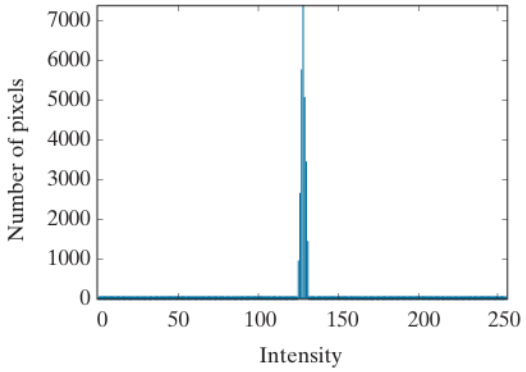
Image Histogram

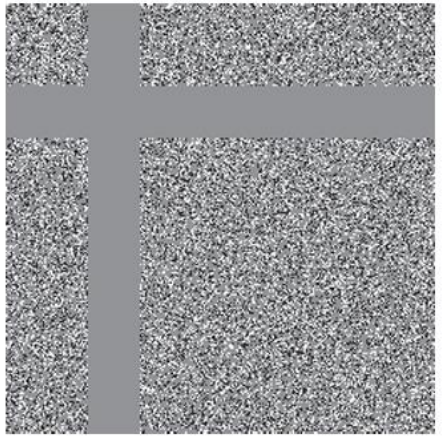


- All 256 intensities are equally probable. As Fig. shows, the histogram of the image is uniform.
- Because the intensity of each line was selected randomly, its pixels are independent of one another in the vertical direction.
- Because the pixels along each line are identical, they are maximally correlated (completely dependent on one another) in the horizontal direction
- Using run-length pairs, where each run-length pair specifies the start of a new intensity and the number of consecutive pixels that have that intensity.
  - It compressed a 2-D image intensity array by [256×256×8] /[(256+256)×8] or 128:1. Each 256-pixel line of the original representation is replaced by a single 8-bit intensity value and length 256 in the run-length representation.

IRRELEVANT INFORMATION

- it appears to be a homogeneous field of gray, can be represented by its average intensity alone—a single 8-bit value.
- a histogram equalized version of the image makes the intensity changes visible and reveals two previously undetected regions of constant intensity—one oriented vertically, and the other horizontally.
- If the image represented by its average value alone, this “invisible” structure (i.e., the constant intensity regions) and the random intensity variations surrounding them (real information) is lost. Whether or not this information should be preserved is application dependent.





MEASURING IMAGE INFORMATION

- In accordance with this supposition, a random event *E* with probability *P*(*E*) is said to contain

$$I(E) = \log \frac{1}{P(E)} = -\log P(E)$$

Given a source of statistically independent random events from a discrete set of possible events $\{a_1, a_1, \ldots, a_J\}$ with associated probabilities $\{P(a_1), P(a_1), \ldots, P(a_J)\}$, the average information per source output, called the *entropy* of the source, is

$$H = -\sum_{j=1}^{J} P(a_j) \log P(a_j) \qquad (8\text{-}6)$$

If an image is considered to be the output of an imaginary zero-memory "intensity source," we can use the histogram of the observed image to estimate the symbol probabilities of the source. Then, the intensity source's entropy becomes

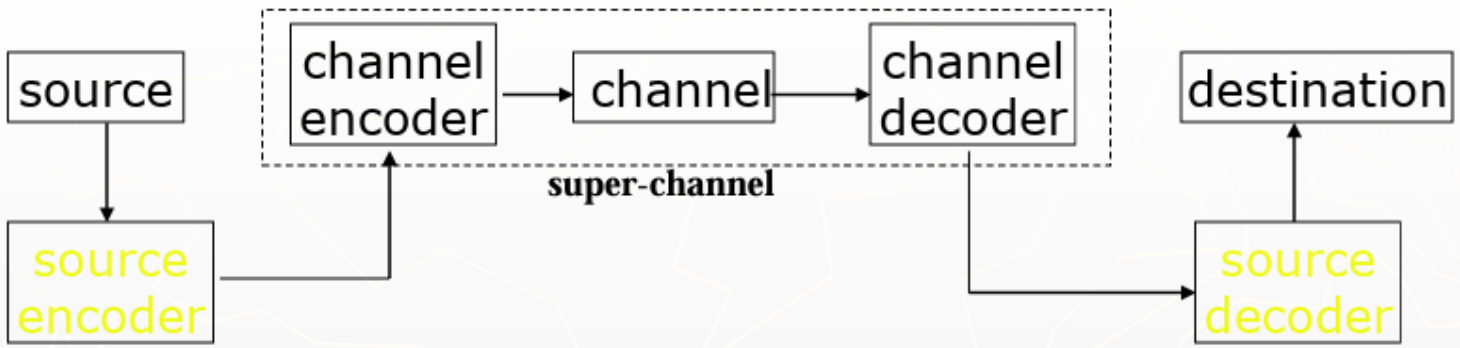
$$\tilde{H} = -\sum_{k=0}^{L-1} p_r(r_k) \log_2 p_r(r_k) \qquad (8\text{-}7)$$

Example

- From the previous example

$$
\begin{aligned}
\tilde{H} &= -\left[0.25\log_2 0.25 + 0.47\log_2 0.47 + 0.25\log_2 0.25 + 0.03\log_2 0.03\right] \\
&= -\left[0.25(-2) + 0.47(-1.09) + 0.25(-2) + 0.03(-5.06)\right] \\
&\approx 1.6614 \text{ bits/pixel}
\end{aligned}
$$

Shannon's Picture on Communication (1948)



The goal of communication is to move information from here to there and from now to then

Examples of source:
Human speeches, photos, text messages, computer programs …

Examples of channel:
storage media, telephone lines, wireless transmission …

FIDELITY CRITERIA

- Compression can loss information.
- Two types of criteria can be used for such an assessment: (1) objective fidelity criteria, and (2) subjective fidelity criteria.
- When information loss can be expressed as a mathematical function of the input and output of a compression process, it is said to be based on an objective fidelity criterion. An example is the root-mean-squared (rms) error between two images.
- Subjective is judged by human.

Let $f(x,y)$ be an input image, and $\hat{f}(x,y)$ be an approximation of $f(x,y)$ that results from compressing and subsequently decompressing the input. For any value of x and y, the error $e(x,y)$ between $f(x,y)$ and $\hat{f}(x,y)$ is

$$e(x,y) = \hat{f}(x,y) - f(x,y) \tag{8-9}$$

so that the total error between the two images is

$$\sum_{x=0}^{M-1-} \sum_{y=0}^{N-1} \left[\hat{f}(x,y) - f(x,y) \right]$$

where the images are of size $M \times N$. The *root-mean-squared error*, e_{rms}, between $f(x,y)$ and $\hat{f}(x,y)$ is then the square root of the squared error averaged over the $M \times N$ array, or

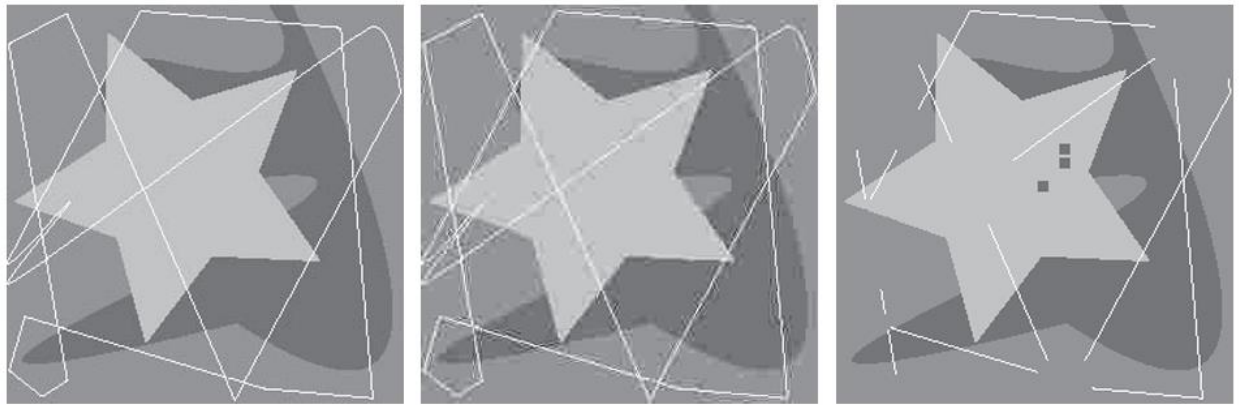
$$e_{\text{rms}} = \left[\frac{1}{MN} \sum_{x=0}^{M-1-} \sum_{y=0}^{N-1} \left[\hat{f}(x,y) - f(x,y) \right]^2 \right]^{1/2} \tag{8-10}$$

If $\hat{f}(x,y)$ is considered [by a simple rearrangement of the terms in Eq. (8-9)] to be the sum of the original image $f(x,y)$ and an error or "noise" signal $e(x,y)$, the *mean-squared signal-to-noise ratio* of the output image, denoted SNR_{ms}, can be defined as in Section 5.8:

$$\text{SNR}_{\text{ms}} = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \hat{f}(x,y)^2}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[\hat{f}(x,y) - f(x,y) \right]^2} \tag{8-11}$$

The rms value of the signal-to-noise ratio, denoted SNR_{rms}, is obtained by taking the square root of Eq. (8-11).

FIDELITY CRITERIA-- Example



rms errors are 5.17, 15.67, and 14.17 intensity levels,

Value	Rating	Description
1	Excellent	An image of extremely high quality, as good as you could desire.
2	Fine	An image of high quality, providing enjoyable viewing. Interference is not objectionable.
3	Passable	An image of acceptable quality. Interference is not objectionable.
4	Marginal	An image of poor quality; you wish you could improve it. Interference is somewhat objectionable.
5	Inferior	A very poor image, but you could watch it. Objectionable interference is definitely present.
6	Unusable	An image so bad that you could not watch it.

Image Compression Model

- an image compression system is composed of two distinct functional components: an encoder and a decoder.
- The encoder performs compression, and the decoder performs the complementary operation of decompression. Both operations can be performed in software, as is the case in Web browsers and many commercial image-editing applications, or in a combination of hardware and firm ware, as in commercial DVD players.
  - A codec is a device or program that is capable of both encoding and decoding

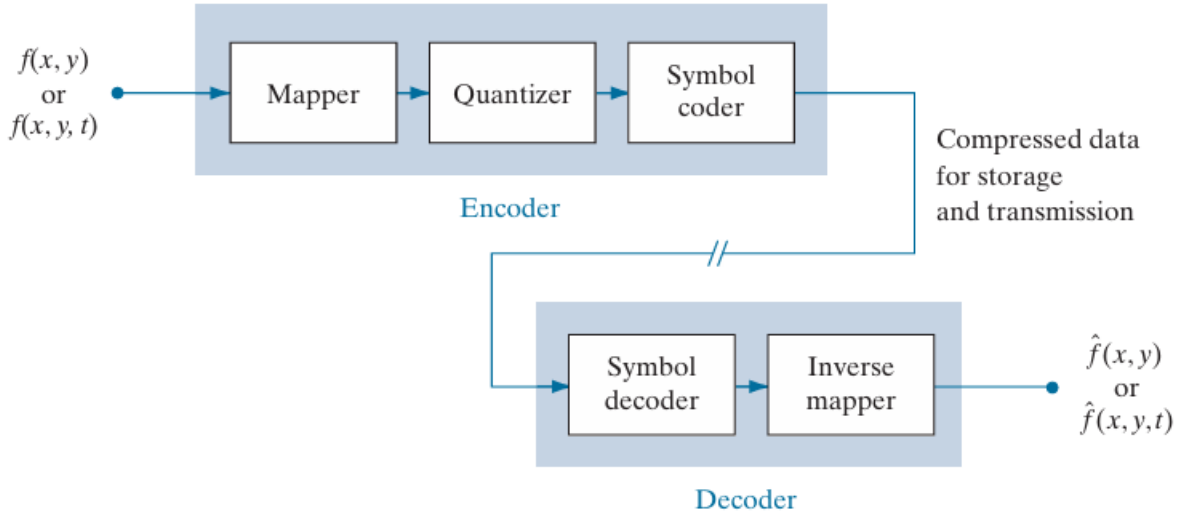


Image Compression Model

- A mapper transforms input into a (usually nonvisual) for mat designed to reduce spatial and temporal redundancy. This operation generally is reversible, and may or may not directly reduce the amount of data required to represent the image.
- The quantizer in Fig. 8.5 reduces the accuracy of the mapper’s output in accor dance with a pre-established fidelity criterion. The goal is to keep irrelevant information out of the compressed representation. As noted earlier, this operation is irreversible.
- In the third and final stage of the encoding process, the symbol coder generates a fixed-length or variable-length code to represent the quantizer output, and maps the output in accordance with the code. This operation is reversible.

Compression Standard

FIGURE 8.6
Some popular image compression standards, file formats, and containers. Internationally sanctioned entries are shown in blue; all others are in black.

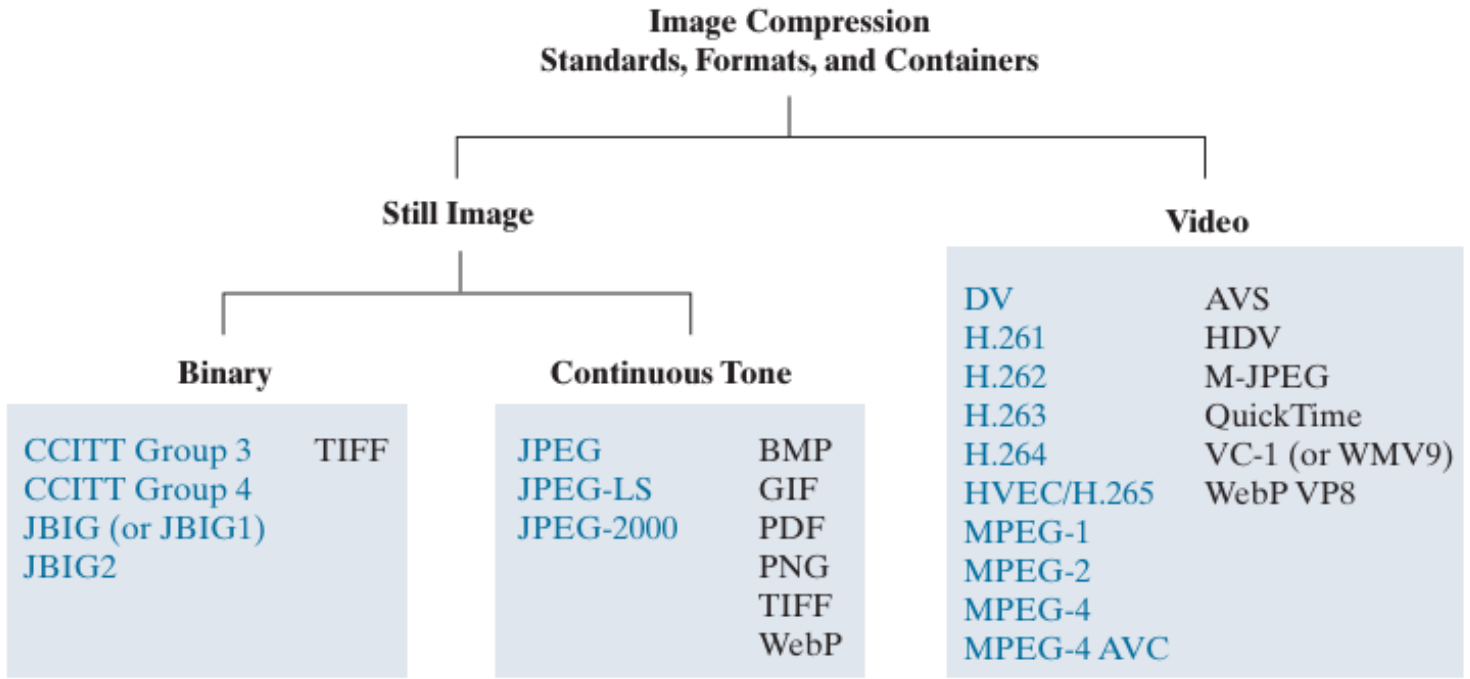


Image Watermarking

- Images distributed in the internet can be copied repeatedly and without error, putting the rights of their owners at risk.
- Even encrypted images becomes unprotected after decryption.
- One way to discourage illegal duplication is to insert one or more items of information, collectively called a watermark.
- *Digital image watermarking* is the process of inserting data into an image in such a way that it can be used to make an assertion about the image.
  - Watermarking is opposite to compression.

Different ways of watermarking

1. Copyright identification-- Watermarks can provide information that serves as proof of ownership when the rights of the owner have been infringed.
2. User identification or fingerprinting -- The identity of legal users can be encoded in watermarks and used to identify sources of illegal copies.
3. Authenticity determination -- The presence of a watermark can guarantee that an image has not been altered, assuming the watermark is designed to be destroyed by any modification of the image.
4. Automated monitoring -- Watermarks can be monitored by systems that track when and where images are used (e.g., programs that search the Web for images placed on Web pages). Monitoring is useful for royalty collection and/or the location of illegal users.
5. Copy protection -- Watermarks can specify rules of image usage and copying (e.g., to DVD players).

Types of watermarking

1. Visible Watermarks – These watermarks are visible. It is an opaque or semi-transparent sub image or image that is placed on top of another image (i.e., the image being watermarked) so that it is obvious to the viewer. Television networks often place visible watermarks (fashioned after their logos) in the upper or lower right-hand corner of the television screen.
2. Invisible Watermarks – These watermarks are embedded in the media and use steganography technique. They are not visible by naked eyes.
3. Public Watermarks – These can be understood and modified by anyone using certain algorithms. These are not secure.
4. Fragile Watermarks – These watermarks are destroyed by data manipulation. There must be a system which can detect all changes in the data if fragile watermarks are to be used.

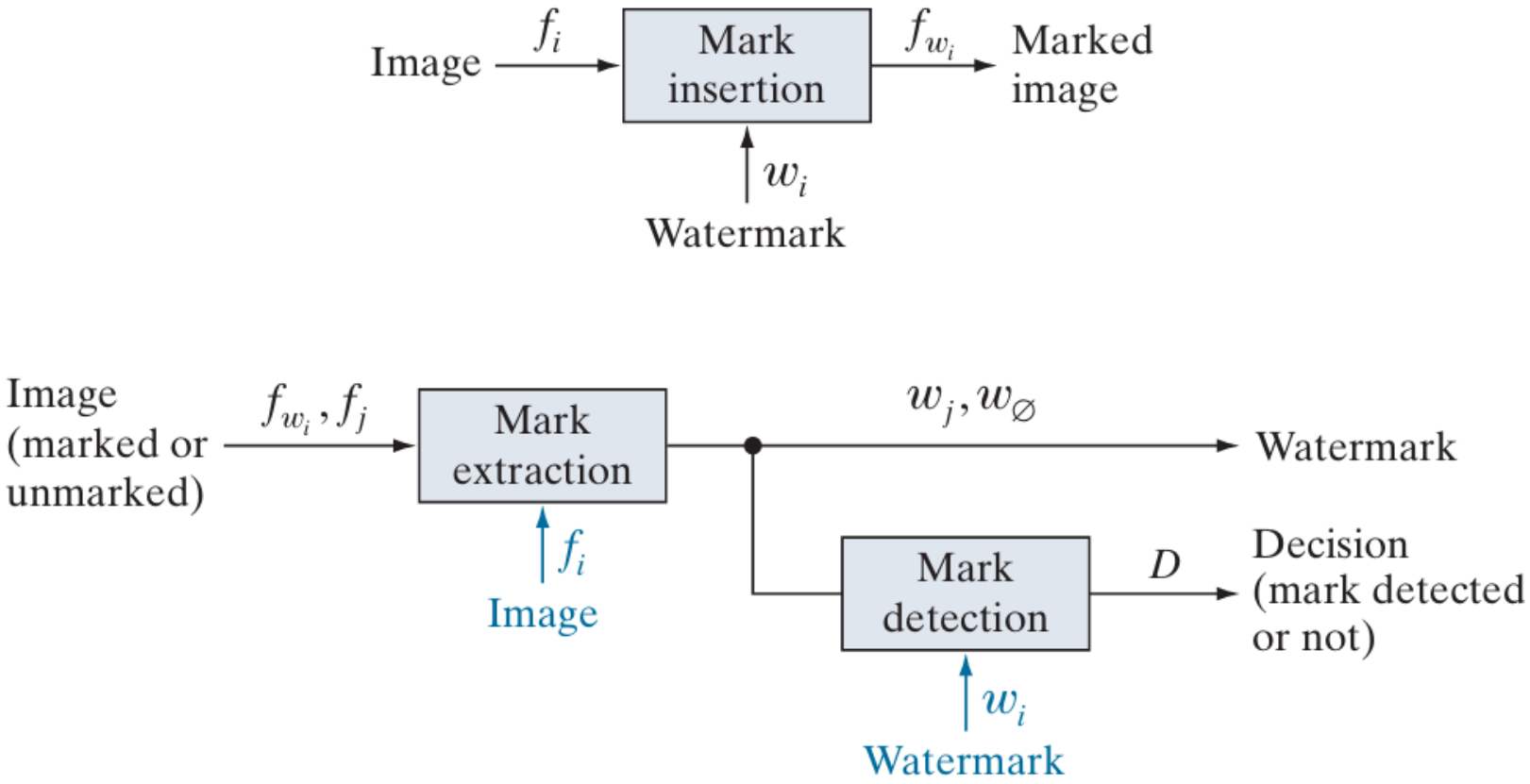
Digital watermarking process (Life cycle) :

- The information needs be embedded in the media. The signal which is embedded is the host signal and the information is called digital watermark. The process has 3 main parts:
  - Embed – In this part, the digital signal is embedded with the digital watermark.
  - Attack – The moment when the transmitted media is changed, it becomes a threat and is called an attack to the watermarking system.
  - Protection – The detection of the watermark from the noisy signal which might have altered media (JPEG compression, rotation, cropping, and adding noise) is called Protection.

Applications

- Watermarks are used in forensics. Tampered evidence is unacceptable in forensics and Watermarked images are acceptable.
- This is used by brands. The Digital Watermarking is done so that the authority of the digital media is intact.
- Digital Watermarking prevents copying of the data.
- Video editing software use watermarks so that people buy the full version of it.
- It is used in video authentication. News channels often show videos of other agencies which are watermarked. It is also used for ID card security.
- It is used for content management in social media.

Watermarking system



Thank You