Département Informatique
Année Universitaire 2022-2023

Chapitre 3

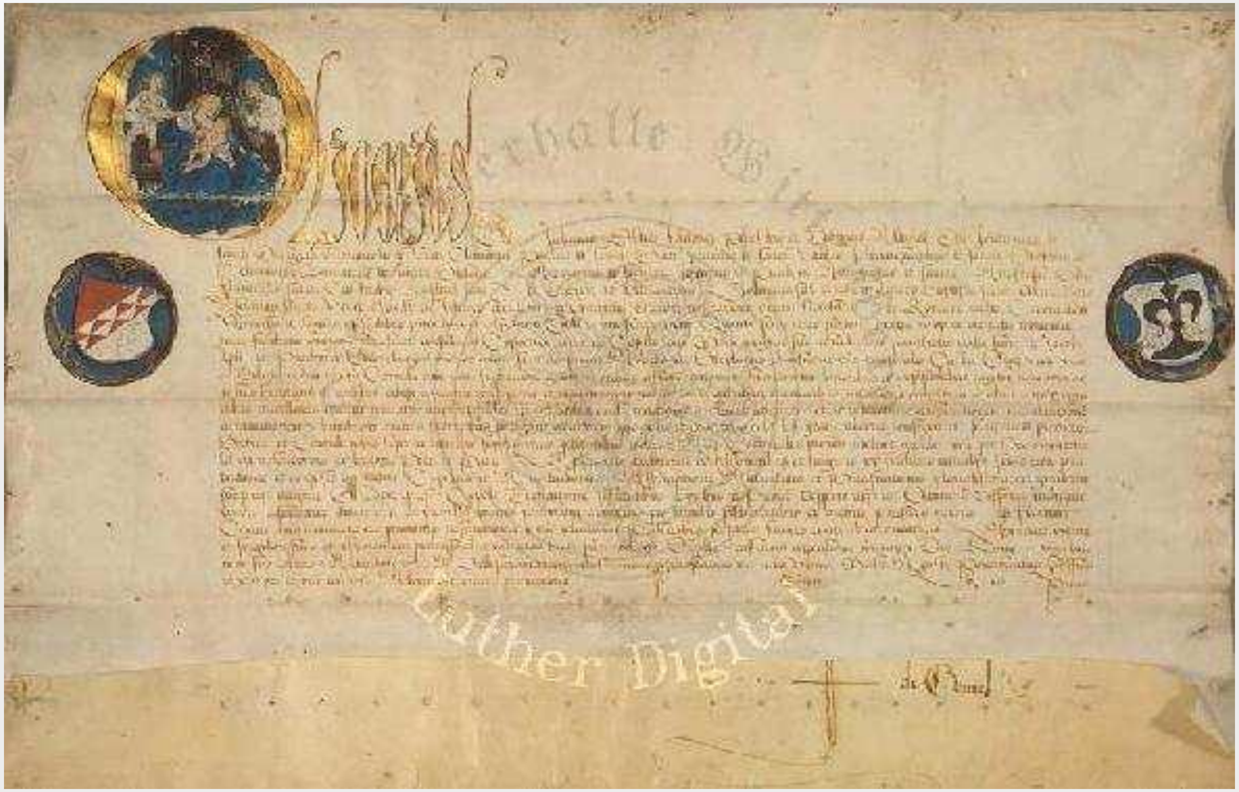
DIGITAL WATERMARKING

Outline

- Watermarking – Introduction
- Basic information hiding method – Least Significant Bit (LSB) Methods
- Spread Spectrum Modulation
- Error Correction Coding
- Human Visual System Models

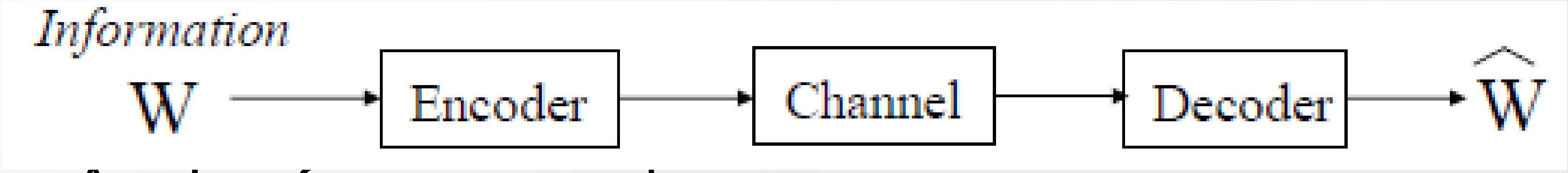
Watermarking

- Embedding Visible/Invisible Codes in Multimedia Data for Security Purpose



What is Watermarking ?
Multimedia as a Communication Channel

- Basic communication system:

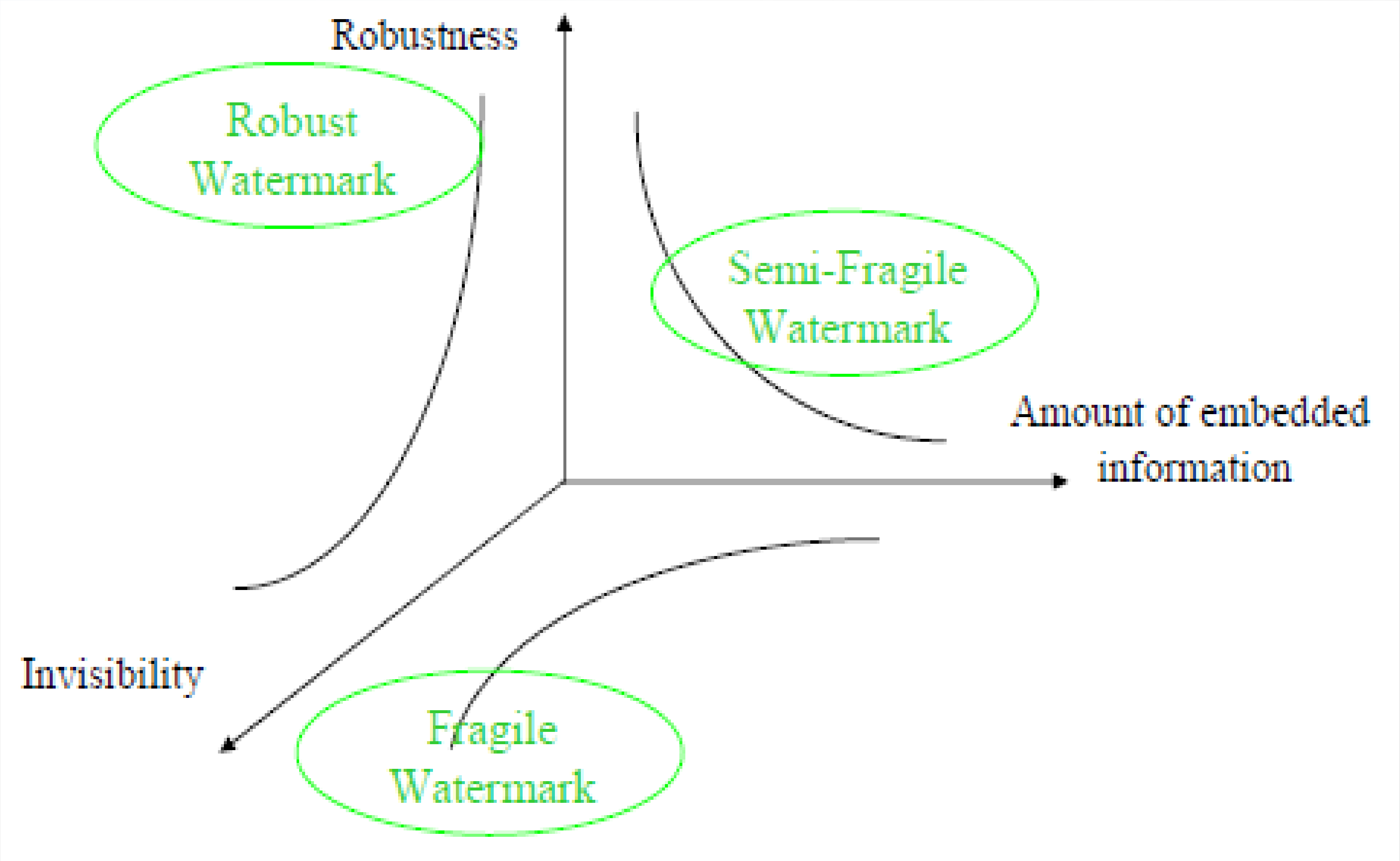


- Analog Communication --
- Encoder/ Decoder:
  - Amplitude Modulation (AM),
  - Frequency Modulation (FM).
  - Multiplexing: use different carrier frequencies.
- Channel: air, wire, water, space, ...

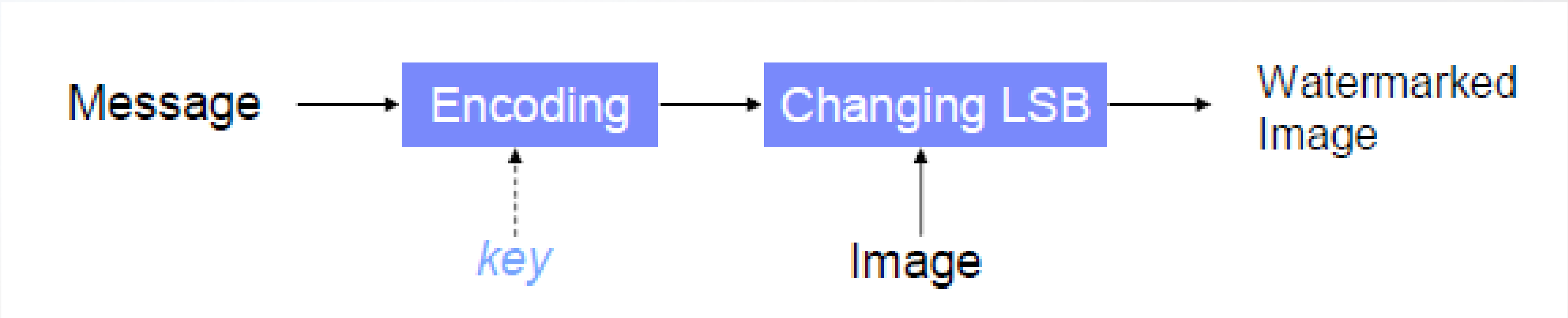
Invisible Watermark

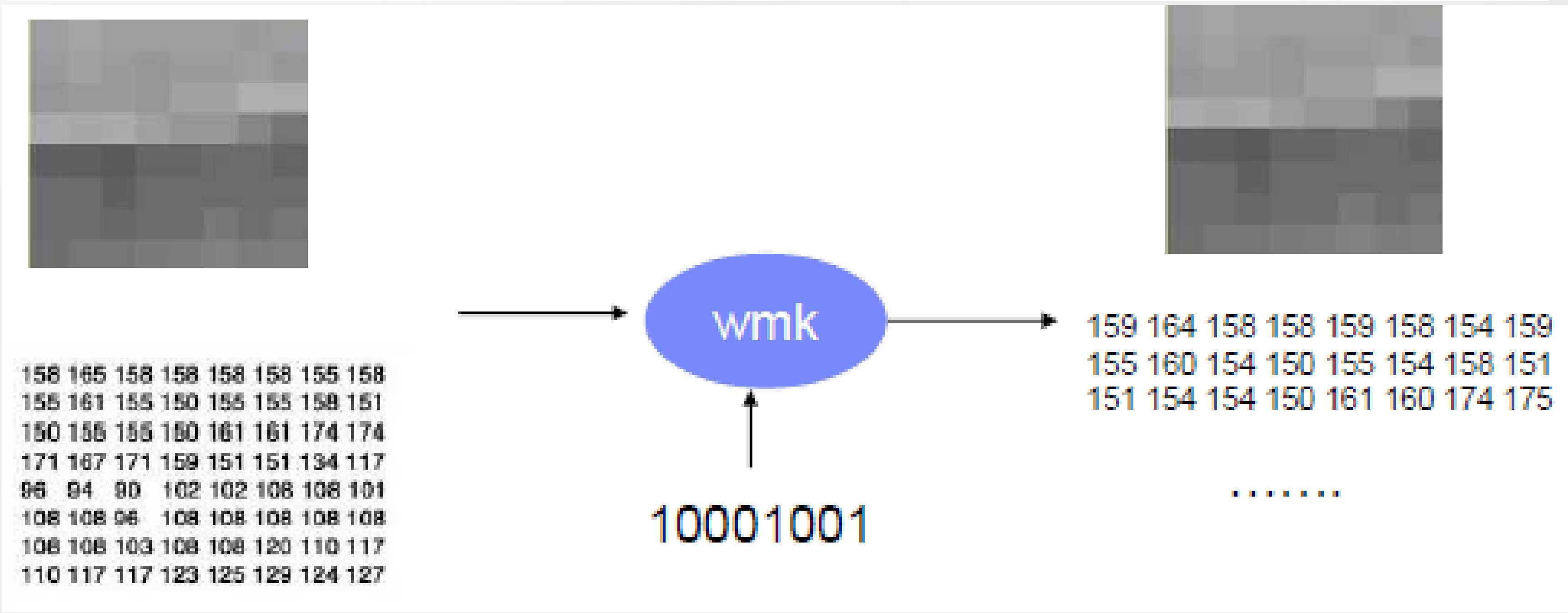
- **Purpose:**
  - Protect ownership and trace illegal use.
  - (Content) Authentication
  - Copy/ Playback control
- **Properties** -- Transmit a bitstream through a very noisy channel, i.e. the original picture.
  - **Robust:** The watermark must be very difficult, if not impossible, to remove. It must be able to survive manipulations to the images, such as: lossy compression, format transformation, shifting, scaling, cropping, quantization, filtering, xeroxing, printing, and scanning.
  - **Invisible:** The watermark should not visually affect the image/video content.

Three Metrics of Watermarking

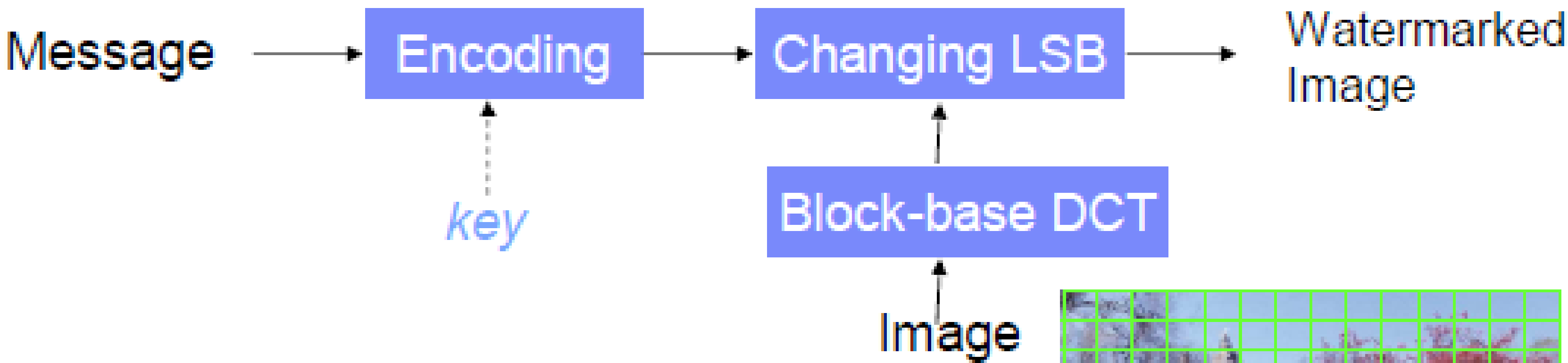


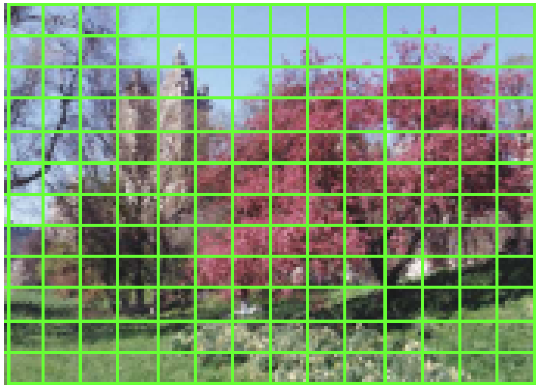
Simplest Watermark – Changing Least Significant Bits



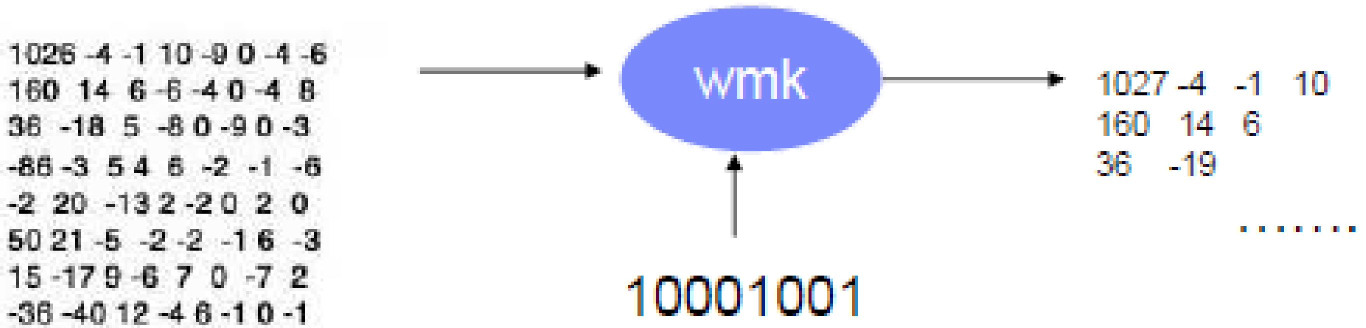


Changing LSB in the block-based frequency domain

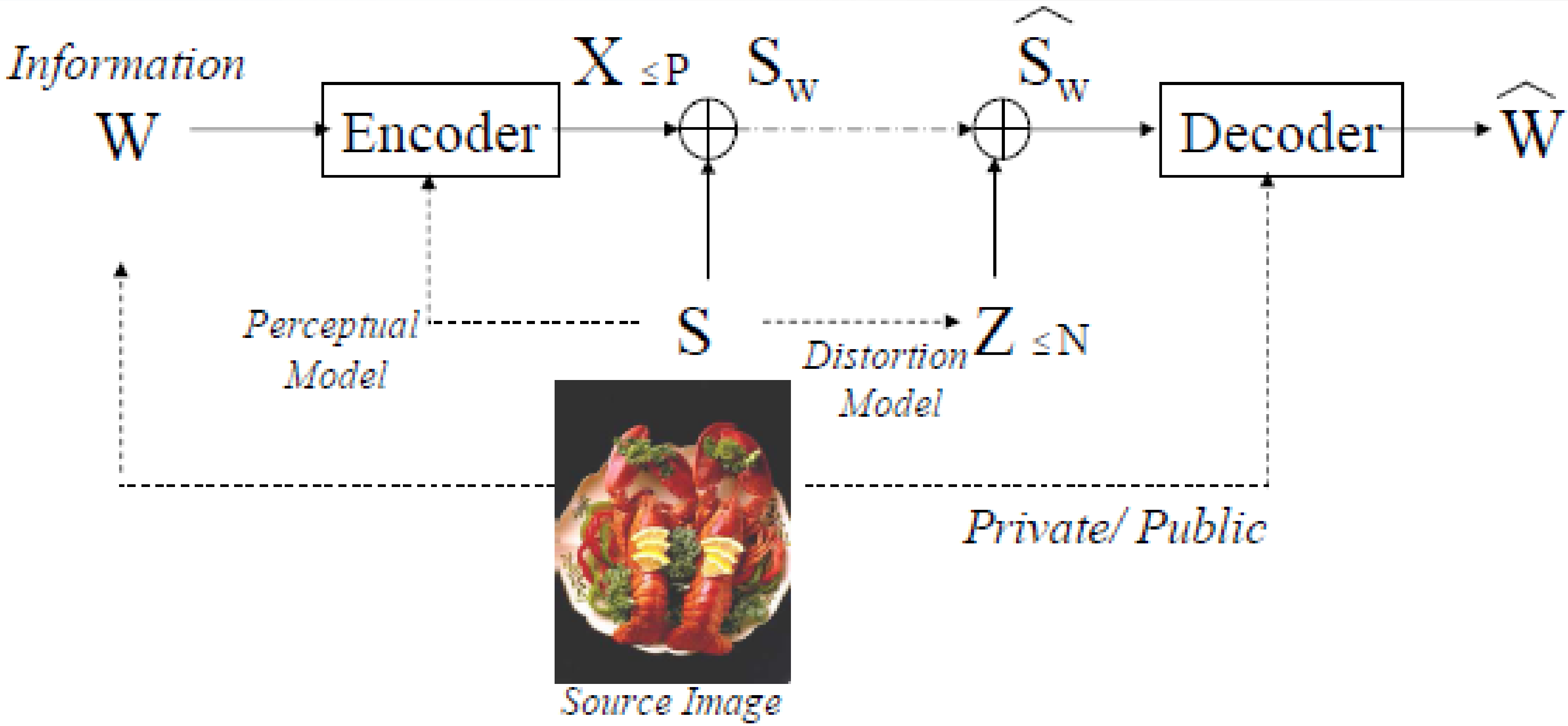




- Embed one bit at one DCT coefficient
- Extension -1: embed one bit at one DCT coefficient after quantization
- Extension -2: embed one bit per DCT block

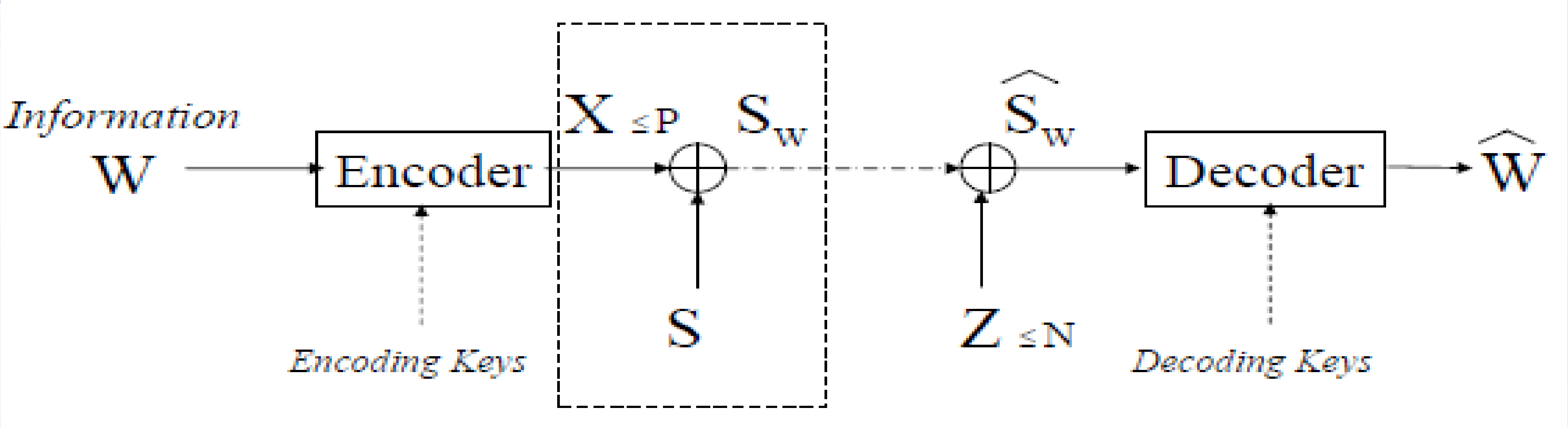


Watermarking on Multimedia Content



S: Source Image (Side Information)
W: Embedded Information
X: Watermark (Power/Magnitude Constraint: P)
Z: Noise (Power/Magnitude Constraint: N)

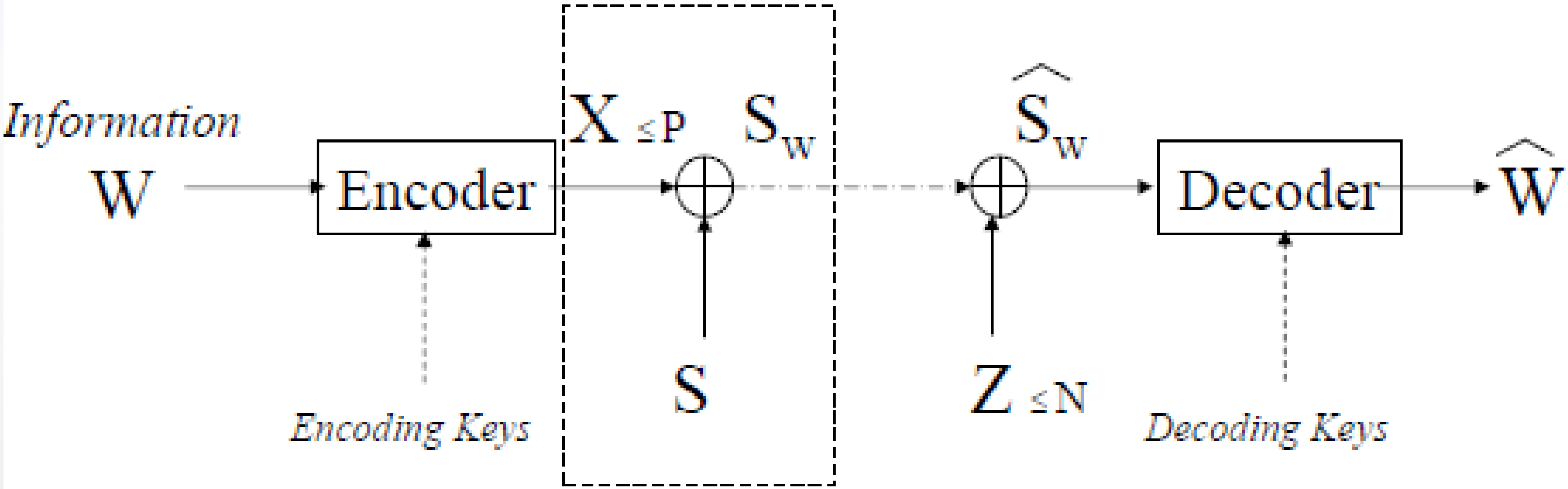
Digital Communication



Encoder may include two stages: Coding and Modulation.

- **Coding:**
  - Scrambling (use cryptographic keys) and Error Correction Coding.
- **Modulation:**
  - Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA).
  - Spread Spectrum is a CDMA technique, which needs modulation keys for Frequency Hopping or other specific codes

Spread Spectrum Communication



- Spread Spectrum Communication:
  - Orthogonal codebooks, $E[f_i \cdot f_j] = 0$
  - e.g.:
    - $f_1 = 1\ 1\ -1\ 1\ 1\ -1\ -1\ -1\ -1\ 1$
    - $f_2 = -1\ 1\ -1\ 1\ -1\ 1\ 1\ -1\ 1\ 1$
- Detection:
  - maxarg (n) correlation coefficient ($\hat{S}_w - S$, f_n) or ($\hat{S}_w$, f_n)

Spread Spectrum Watermarking
(Cox et. al. 1997)

- **Spread Spectrum**: T(Sw) = T(S) + T(X)
  - T can be any spatial-frequency transforms.
  - E.g. Fourier Transforms (DFT, DCT), Wavelet Transforms
- **Objectives**:
  - Detect the existence of a specific code, which is served as the copyright information.
  - Watermark detection needs the original source.
- **Implementation**:
  - Add a specific code on the 1000 largest or the 1000 lowest frequency DCT coefficients of the image.
  - E.g. T(X) = 1 1 -1 1 1 –1 –1 –1 –1 1 .....
- **Detection**:
  - correlation coefficient (T(Sw) – T (S) , T(X))

Increase Robustness via Coding - Error Correction Coding (I)

- Allow decoder being able to correctly decode the message in a noisy environment
- E.g.: original codewords:
    - A -> 00
    - B -> 01
    - C -> 10
    - D -> 11
- E.g.: [5,4] ECC codes
    - A -> 00 -> 00000
    - B -> 01 -> 10110
    - C -> 10 -> 01011
    - D -> 11 -> 11101
- **Definition**: The rate of an [n, M]–code which encodes information k-tuples *is* $R = k/n$, where n is the number of bits and M is the number of codewords.

Increase Robustness via Coding - Error Correction Coding (II)

- The Hamming distance d(x,y) of two codewords x and y is the number of coordinate positions in which they differ
  - E.g.: in the previous example: d(A,B) = 3, d(A,D) = 4,…
- Let C be an [n, M]-code. The Hamming distance d of the code C is:

$$d = \min \{ d(x,y) \mid x,y \text{ belongs to } C, x \neq y \}$$

- E.g.: the Hamming distance of the above code is 3.
- **Theorem:** Let C be an [n, M]-code having distance *d=2e+1.* Then, C can correct *e* errors. If used for error detection, C can detect *2e* errors.

Generic Human Vision Model

- 1972: Stockham proposed a vision model for image processing, which is based on the nonlinear brightness adapting mechanism.
- 1970s – 1980s: Adding more components to the Human Vision Models:
  - Frequency domain
  - Color information
  - Orientation
- 1990s: More complete models
  - Lubin’s model
  - Daly’s model
- 1990s: Application-oriented models
  - Compression
  - watermarking

Just Noticeable Distortion (JND)
Chou and Li's JND (1995)

- Definition of JND is not consistent:
- In the early literatures (especially before 1997):
  - A measurement unit to indicate the visibility of the changes of a specific pixel (or the whole image) in two images.
  - A posterior measurement.
- In some recent papers:
  - Assumes to be the maximum amount of invisible changes in a specific pixel (or frequency coefficients) of an image.
  - A prior estimation.
- Many watermarking papers adopt the second definition. However, no rigorous physical and psychological experiments have ever shown this concept in their design. (by 2001).

Properties of human masking effects

- Decided by luminance, contrast and orientation
- **Luminance masking:** (Weber's effect)
  - The brighter the background, the higher the luminance masking threshold
  - Detection threshold for a luminance pattern typically depends upon the mean luminance of the local image region.
  - Also known as light adaptation of human cortex.
- **Contrast masking**:
  - The reduction in the visibility of one image component by the presence of another.
  - This masking is strongest when both components are of the same spatial frequency, orientation and location.
- **Orientation**-selective channels affects the visibility.