Digital Watermarking

Alexander Hasslacher, 0056448

EMT-Institut, JKU-Linz, 2004

What is a Watermark

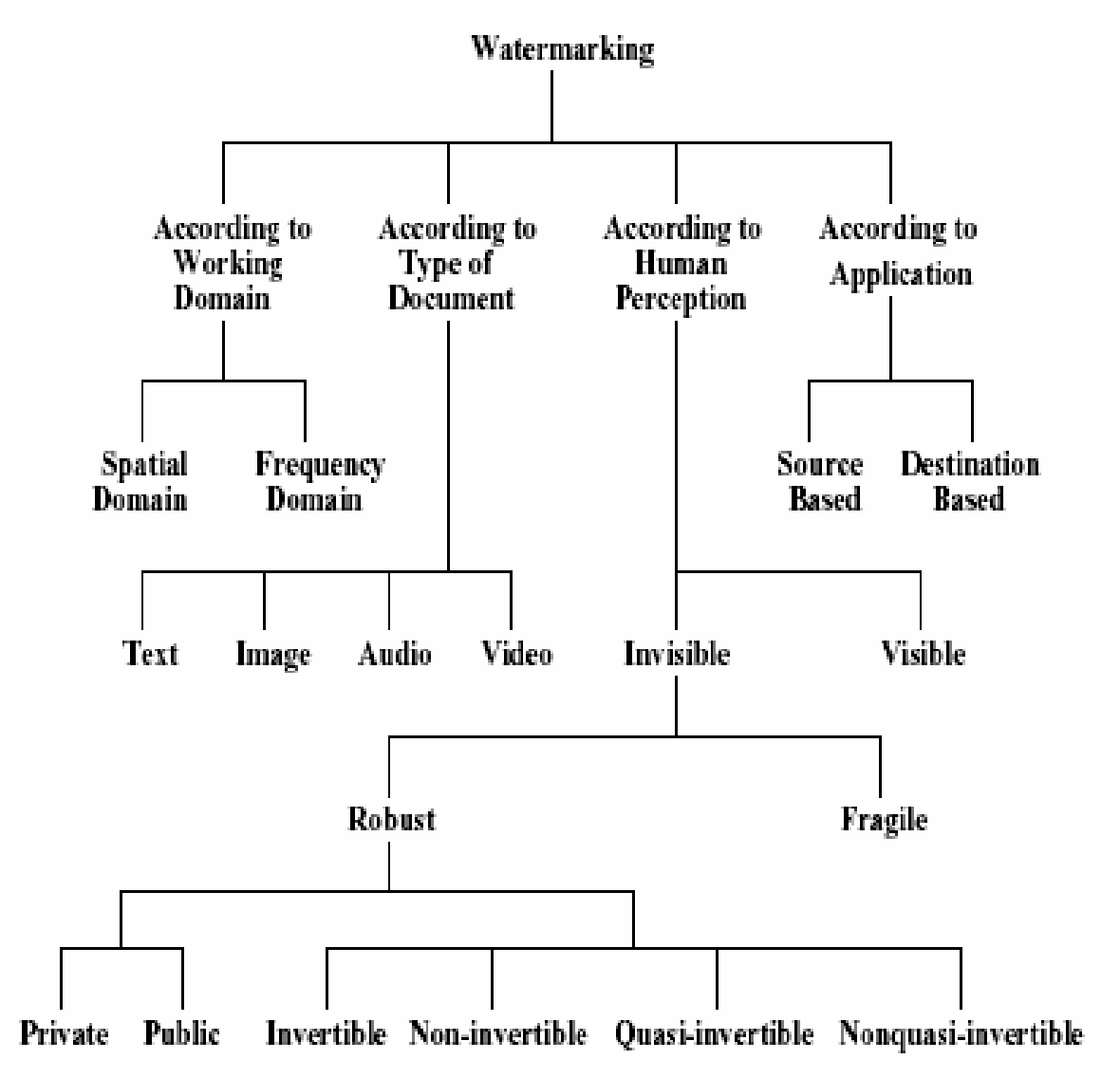
Original Image (I)

Encoder

Signatur (S)

Watermarked Image (I')

Types of Digital Watermarks



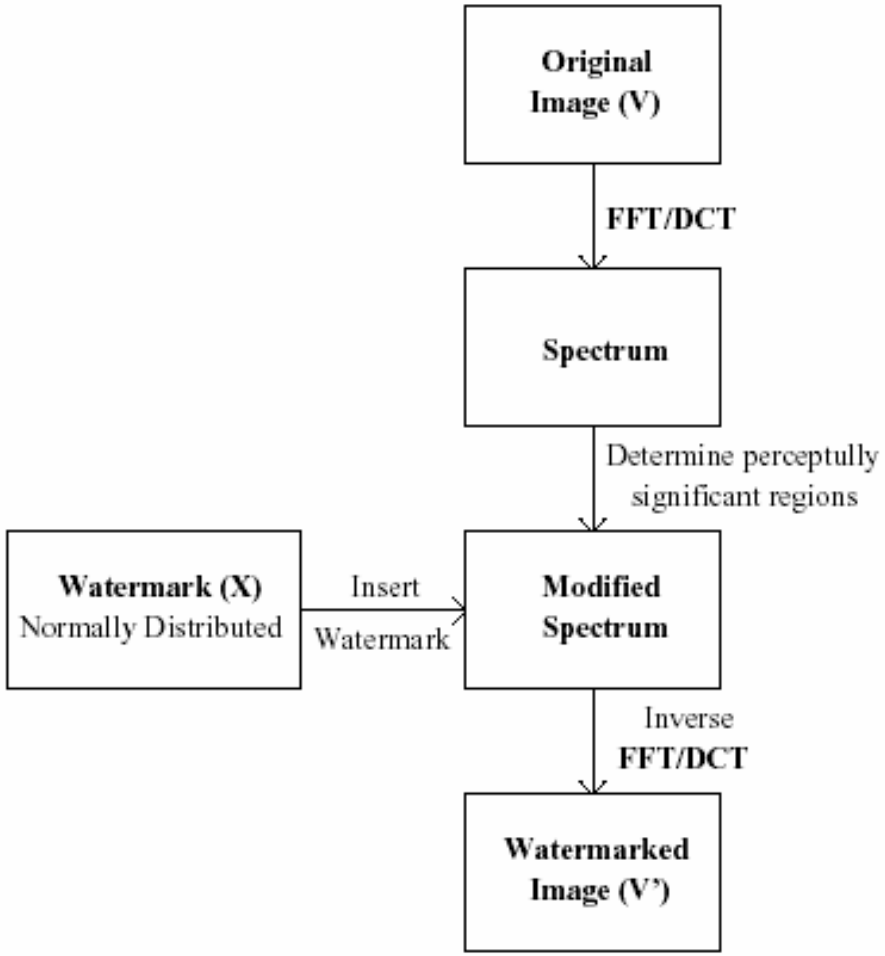
Visible and invisible Watermark

LSB for *.BMP

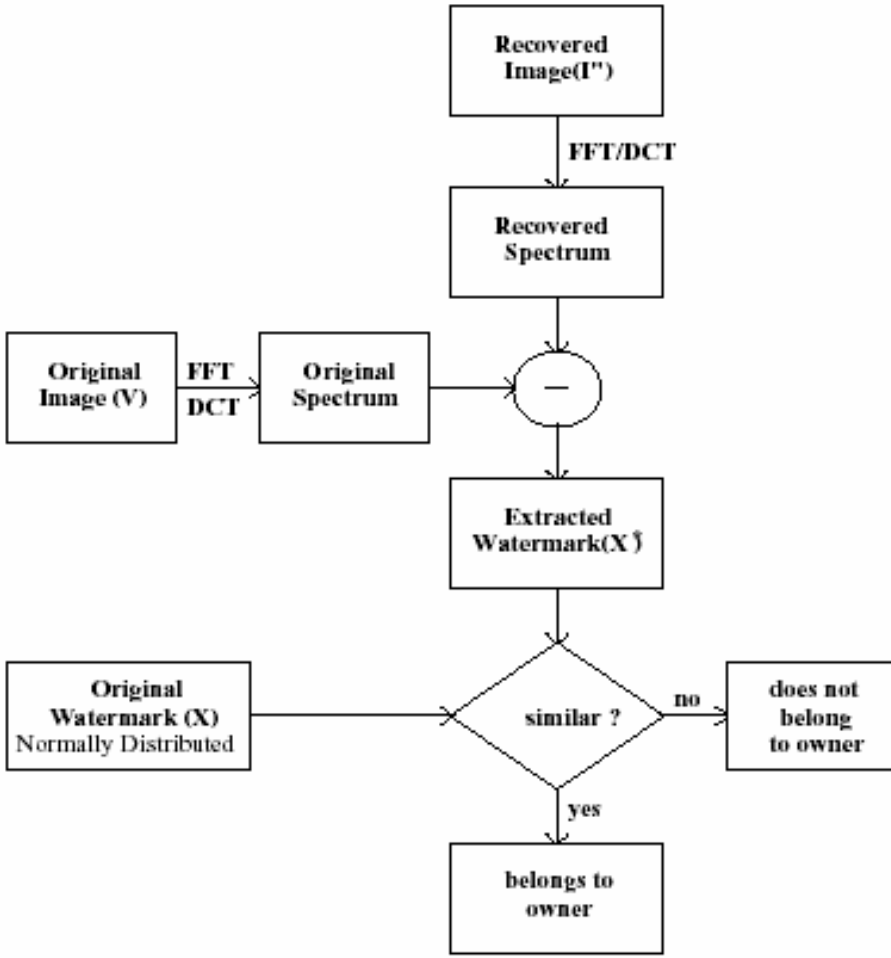
- LSB
  - 00100111 11101001 11001000
  - 00100111 11001000 11101001
  - 11001000 00100111 11101001
    - Hide a binary value for 'A' 10000011
  - 00100111 11101000 11001000
  - 00100110 11001000 11101000
  - 11001000 00100111 11101001

fragile against noise & compression

FFT, DCT

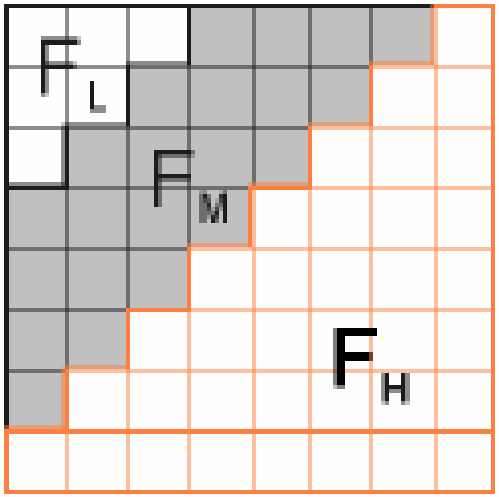


(a) Insertion process



(b) Extraction process

Frequency-Based Techniques



DCT Coefficients

Random Pattern generated using a secret key

4 16 4 4 36 0 1 0 16 ..... 1 36 25

1 0 1 1 1 0 1 0 1 ..... 1 0 0

5 16 5 5 37 0 2 0 17 ..... 2 36 25

Watermarked Coefficients

DCT Domain Watermarking

- Watermark embedding
  - W: watermark to be embedded.
  - X: sequence of pixel values
  - X_d and Y_d: row-concatenated DCT coefficients of X and Y
  - A=scaling factor: Determines the intensity of the watermark
    - $Y_d(i) = X_d(i)(1+aW)$
- Watermark extraction
  - W*: extracted version of the watermark
  - Z_d: possibly forged watermarked image.

$$W^*(i) = \frac{1}{a}\frac{Z_d(i)}{X_d(i)} - 1 \Longrightarrow S(W, W^*) = \frac{W * W^*}{\sqrt{W * W^*}}$$

  - T=user-defined threshold
  - If S > T, image is authentic

SCALING FACTOR a = 0.1, 0.5, 1.0, 5.0

Original image

a = 0.1

a = 0.5

a = 1.0

a = 5.0

Conclusions

- Modification of all DCT coefficients distorts the image drastically
- The scaling factor a is a critical system parameter.
  - If a is too small. The image is not distorted but the robustness of the scheme is low
  - If a is too large, the image is distorted but the robustness of the scheme is high
- Modification of low-frequency coefficients
  - Distorts the image
  - Gives the hacker a clue about where the watermark is embedded
- Modification of high-frequency coefficients
  - No distortion
  - The watermakr cannot be detected after attacks like JPEG compression

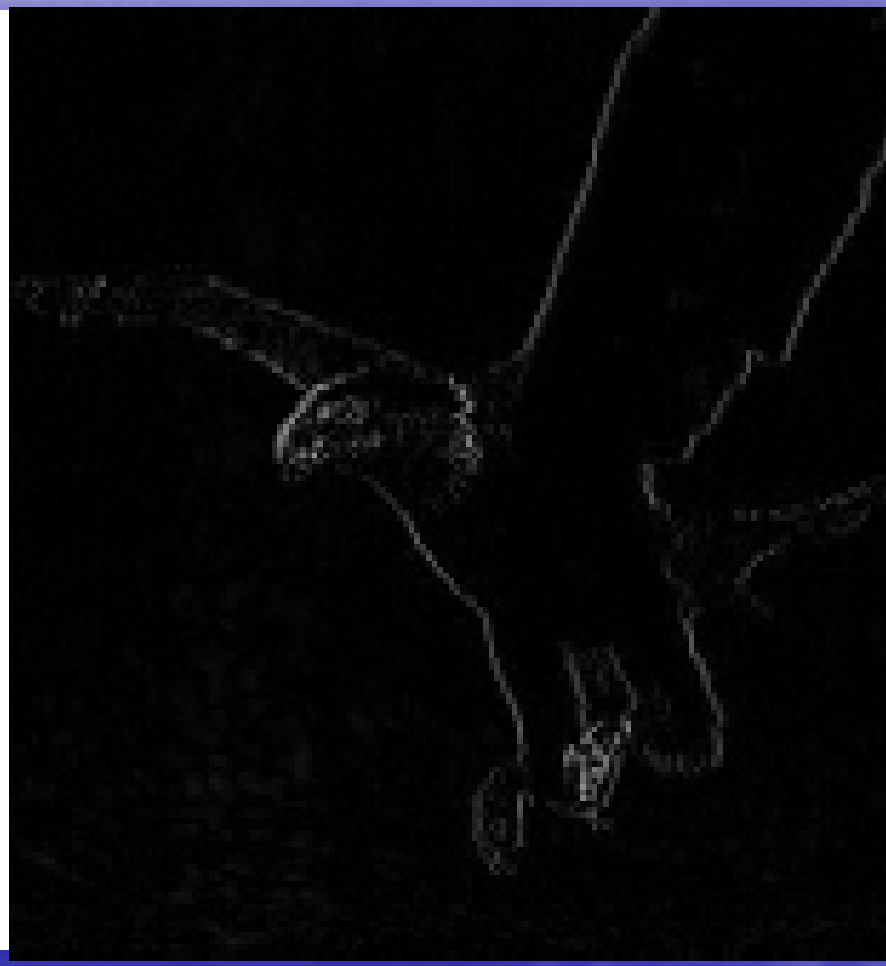
Examples Invisible Watermarking

(a) Original

(b) Watermarked

Example 2 Invisible WM

(a) Original



Visible Watermarking

(c) Bigger watermark

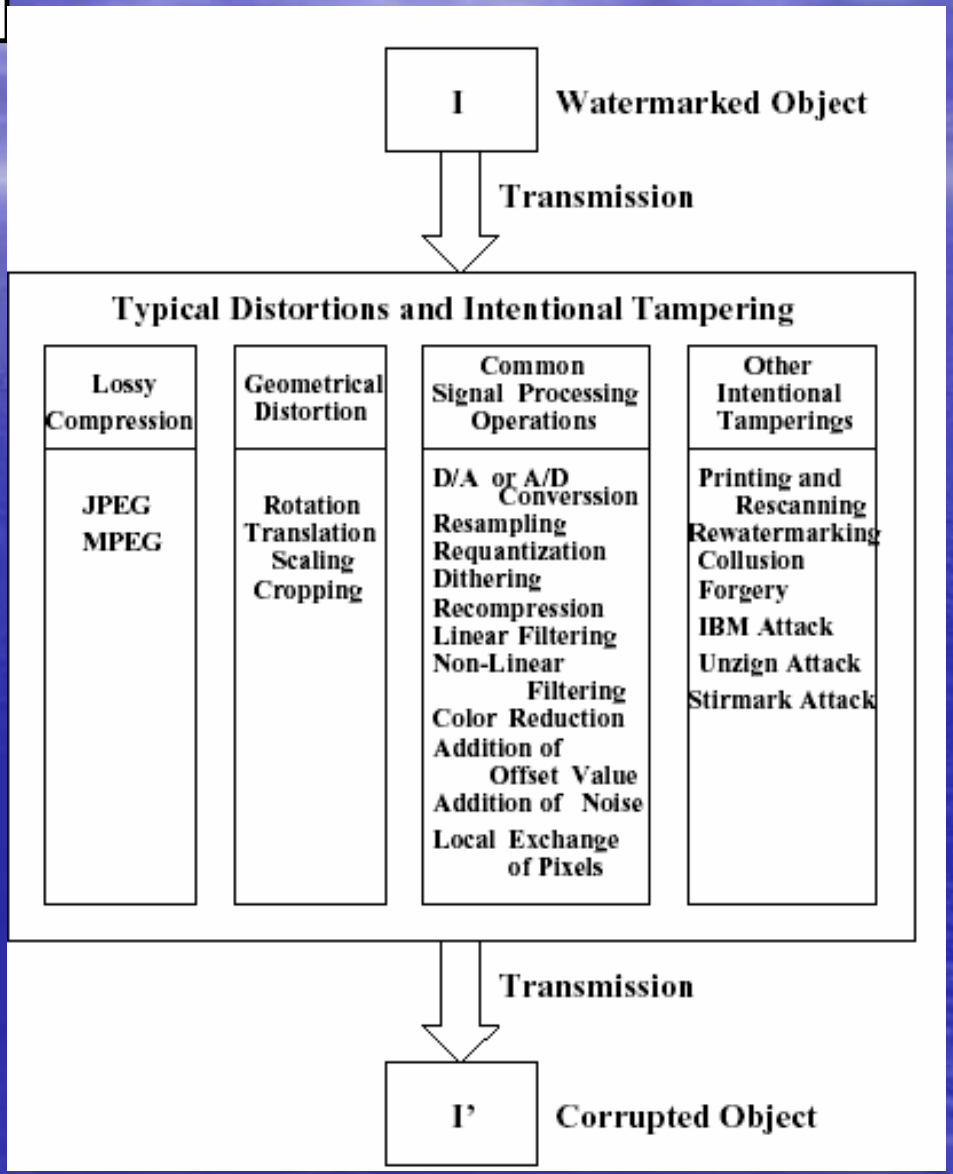
(d) Smaller watermark

Both, Invisible and Visible WM

(a) Lena

(b) Bird

Attacks on WM



Audio Watermarking

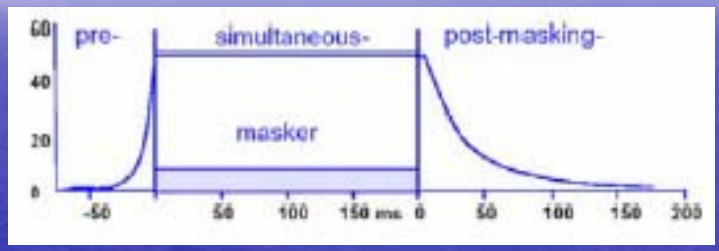
- Uses
  - DRM (Digital Right Manamement)
    - Proof of ownership
    - Access control for digital media
    - Tracing illegal copies …
  - Transmitting Metadata
    - Like composer, soloist, genre of music,…

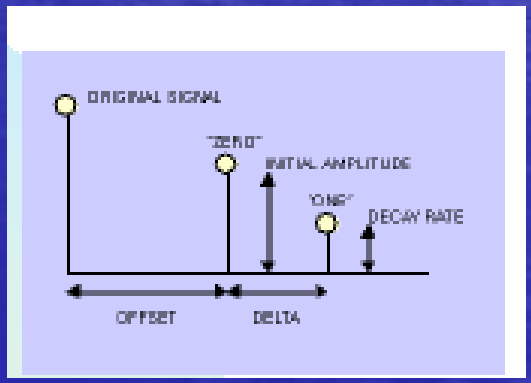
Audio Watermarking

- Requirements
  - Hidden, in case of music inaudible
  - Statistically invisible
  - Robust against signal processing operations
  - Directly connected to the music, not in a header
  - Key dependent

Inaudible Signals in Audio WM

- Temporal masking
  - 5-20ms before a loud signal
  - 50-200ms after a loud signal
- A silent sound after a loud sound
- Adding a echo
  - 0 = 0.5ms after a sound
  - 1 = 1.0ms after a sound
- MP3Stego
  - WAV -> MPEG-3 + additional Data





MP3Stego

```
C:\WINDOWS\System32\cmd.exe
24.11.2004  09:28         1.823.640 svega.wav
24.11.2004  09:30    <DIR>          tables
19.03.2002  10:56                64 vssver.scc
              12 Datei(en)      3.412.954 Bytes
               7 Verzeichnis(se),  1.681.666.048 Bytes frei

C:\mp3stego\DEVELO~1\MP3Stego>sound.mp3

C:\mp3stego\DEVELO~1\MP3Stego>decode -X sound.mp3
MP3StegoEncoder 1.1.16
See README file for copyright info
Input file = 'sound.mp3'  output file = 'sound.mp3.pcm'
Will attempt to extract hidden information. Output: sound.mp3.txt
Enter a passphrase: ****
Confirm your passphrase: ****
the bit stream file sound.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame   791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "sound.mp3" is finished
The decoded PCM output file name is "sound.mp3.pcm"

C:\mp3stego\DEVELO~1\MP3Stego>edit sound.mp3.txt

C:\mp3stego\DEVELO~1\MP3Stego>_
```

Versteckter Text: Dies ist Alex sein File

i.E: Google Imagesearch

- Webcrawler looking for Watermarked pictures on Homepages
- Money for Photographers
- Microsoft´s picturetank

Questions ?

Thank´s for coming!!