CGI 98
Hannover
June 1998

Digital Watermarking of Text, Image and Video Documents

Bernd Girod
Frank Hartung
Jonathan Su

Telecommunications Laboratory
University of Erlangen-Nuremberg
http://www-nt.e-technik.uni-erlangen.de/

Copyright in the Digital Age

Copyrights are threatened by potentially unlimited copying of digital data without loss of fidelity

Severe financial implications for copyright holders

- Example 1: In April 1998 illegally copied audio CDs worth $ 85,000,000 were discovered and confiscated in Hongkong
- Example 2: In June 1998 illegally copied software and multimedia CDs worth $ 1,900,000 were discovered and confiscated in Berlin

How to Prevent Copyright Infringements?

Encryption / Conditional Access

- protects the data only on the transmission channel
- the paying recipient has in general access to the decrypted data

Copy Prevention Mechanisms

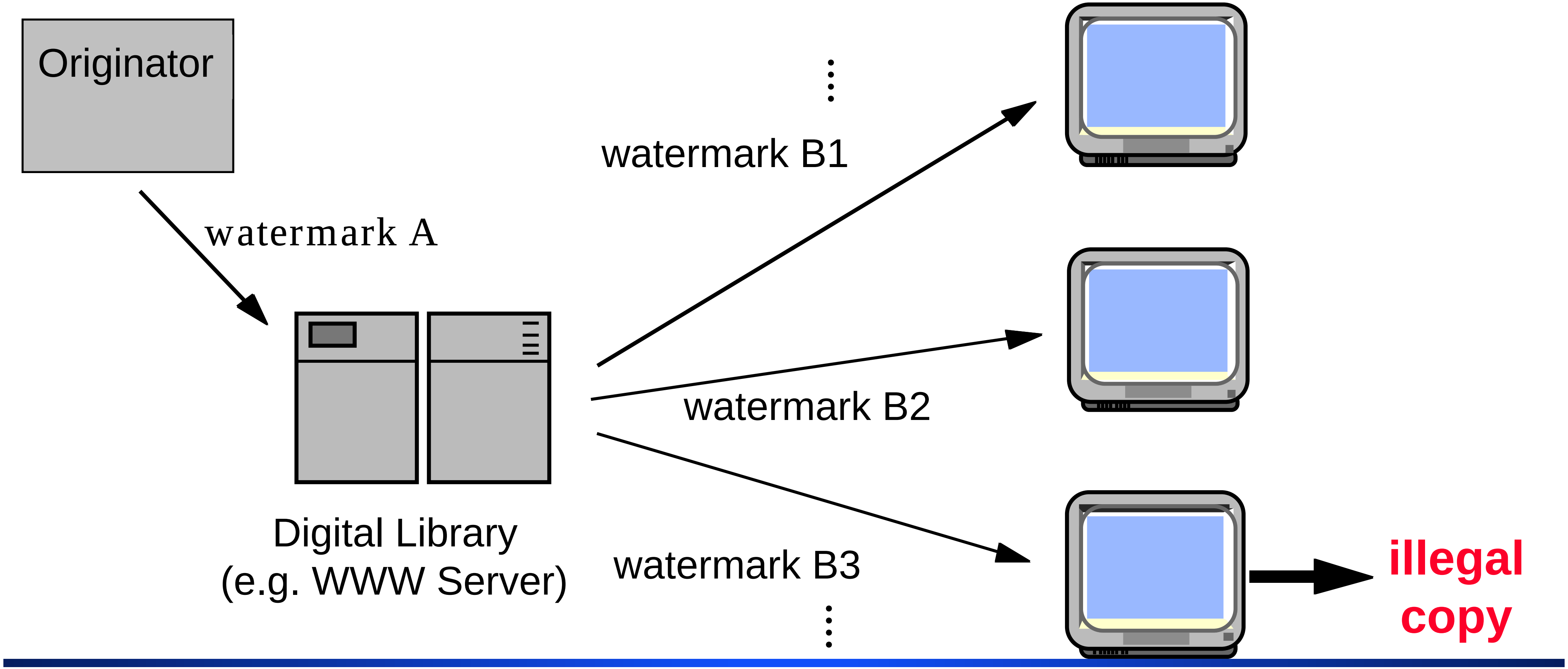
- difficult in open systems
- often, copy prevention mechanisms are circumvented

Digital Watermarking

- marking of multimedia data with information about origin and recipient
- does not prevent copying, but, illegal copies can be traced back
- “last line of defense”

Watermarks as Fingerprints

Identification of legal recipient with help of individual watermarks:



Digital Watermarking Requirements

Below perceptual threshold

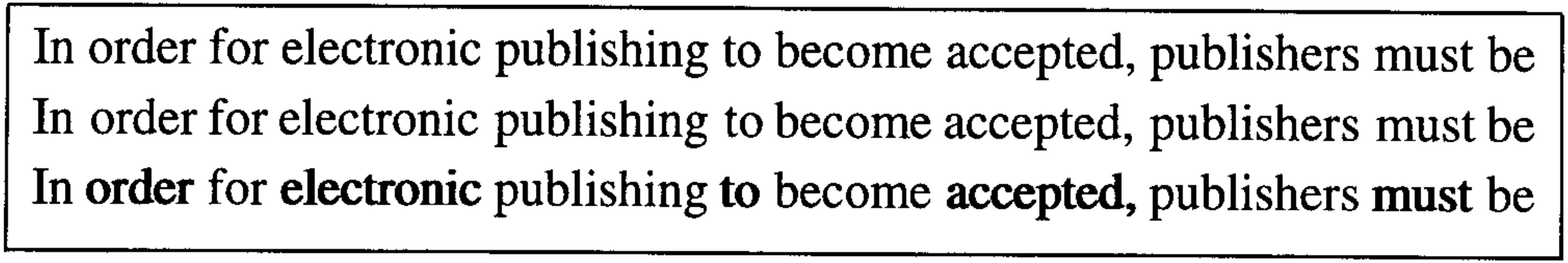
Robust against unattempted and hostile modification of the data, e.g.

- format conversion (Postscript -> PDF, JPEG -> GIF)
- compression
- D/A und A/D conversion
- additive noise
- scaling, rotation, cropping, composition (images)
- hostile attacks on the watermark

Low complexity for embedding (less critical for extraction)

Text Document Watermarking: Examples

Modulate word spacing



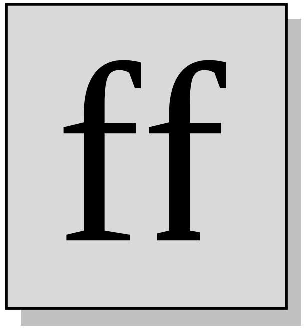
In order for electronic publishing to become accepted, publishers must be

In order for electronic publishing to become accepted, publishers must be

In **order** for **electronic** publishing **to** become **accepted,** publishers **must** be

(source: Brassil et al., AT&T)

Character feature watermarking

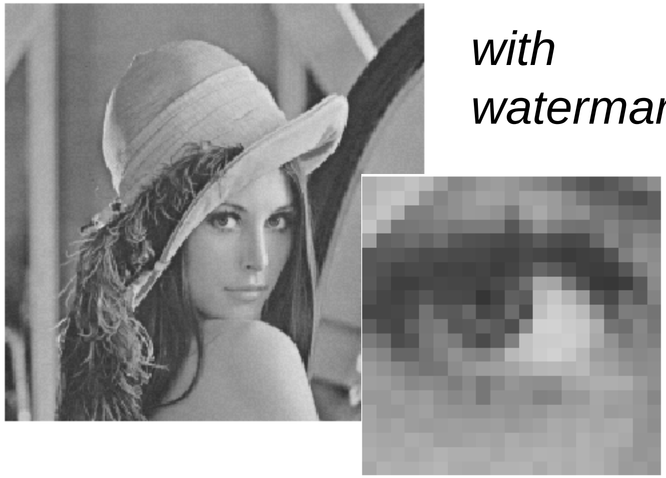


Image/Video Watermarking

Idea: small, pseudo-random changes of pixel amplitudes

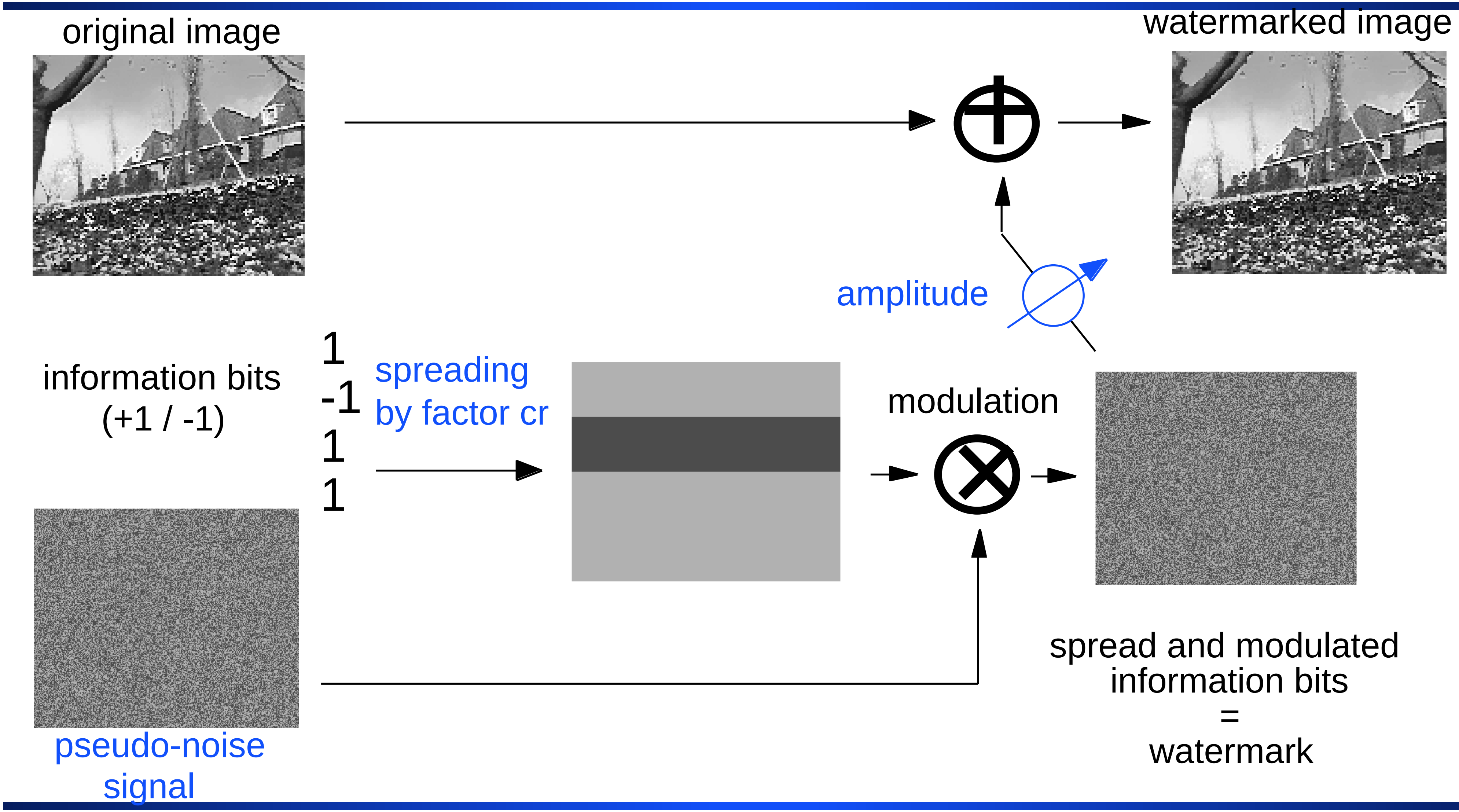
Each embedded information bit distributed over many pixels
-> redundancy + robustness

without watermark



with watermark

Spread Spectrum Image/Video Watermarking



original image

watermarked image

amplitude

information bits
(+1 / -1)

1
-1
1
1

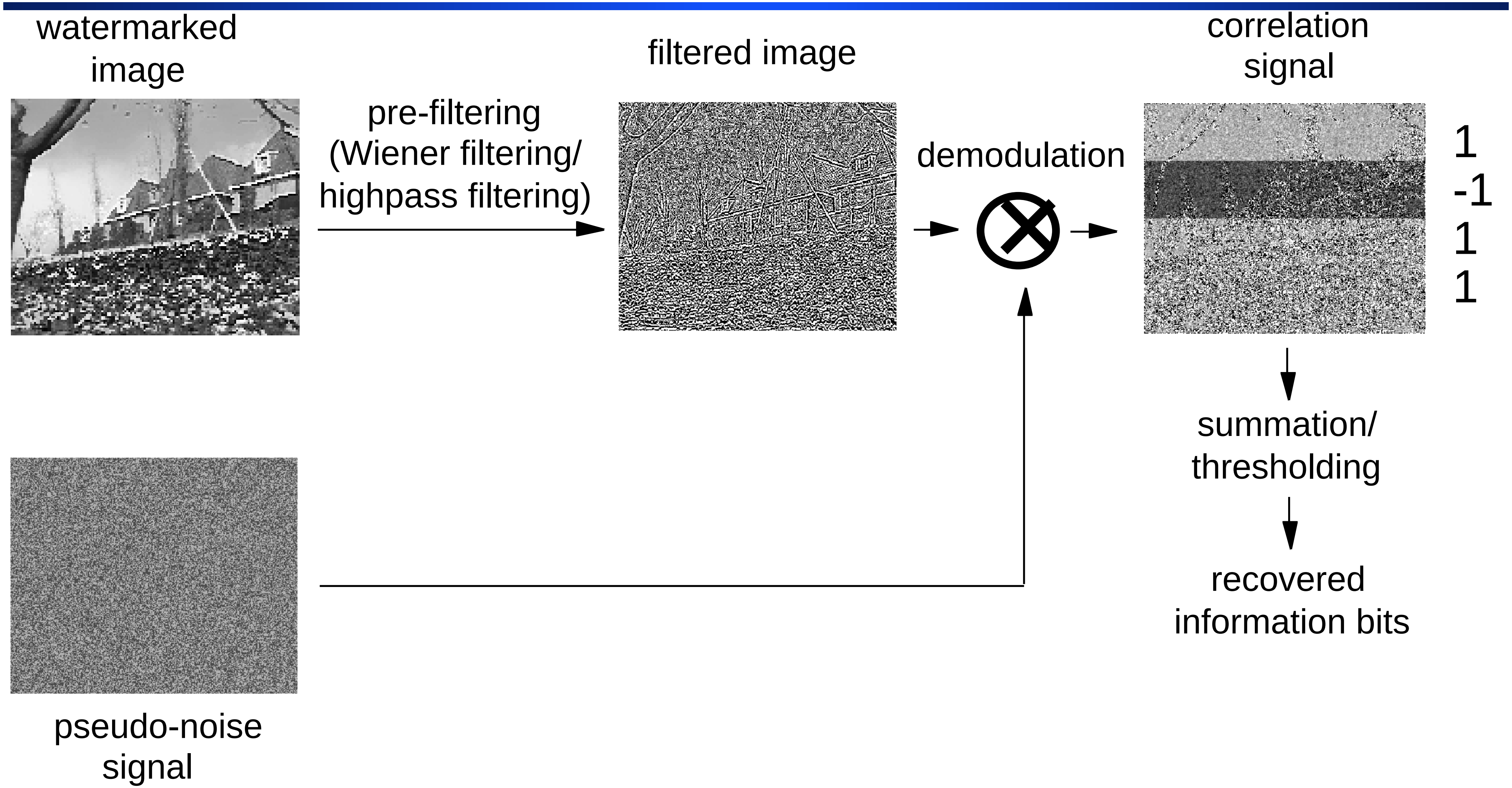
spreading
by factor cr

modulation

spread and modulated
information bits
=
watermark

pseudo-noise
signal

Decoding of
Spread Spectrum Watermarks



watermarked image

pre-filtering (Wiener filtering/ highpass filtering)

filtered image

demodulation

correlation signal

1
-1
1
1

summation/ thresholding

recovered information bits

pseudo-noise signal

How Many Bits Can Be Embedded?

Bit error rate estimate of the watermark channel:

$$\mathrm{BER} = \frac{1}{2}\,\mathrm{erfc}\left(\mathrm{const.}\,\frac{\sigma_{PN}\sqrt{cr}\ \ \mathrm{amplitude}}{\sigma_{\mathrm{filtered\ image}}}\right)$$

Example:

- amplitude = 3
- cr = 2400
- Gaussian PN signal, $\sigma^2_{PN} = 1$

⇒

BER = 5 * 10^{-7}

100 bits for 512x512 image

4 kbps for video

For robustness: choose parameters conservatively

Robustness of Spread Spectrum Watermarks in the Presence of Attacks

Malicious attacks

- filtering, addition of noise,...: not successful due to built-in robustness
- collusion attacks: modify pseudo-noise sequence to be collusion secure [Boneh and Shaw 1995, Boneh and Shaw 1997]
- attacks that attempt to destroy correlation (zoom/shift/rotation, frame swap): watermark recovery by blockwise multidimensional sliding correlator

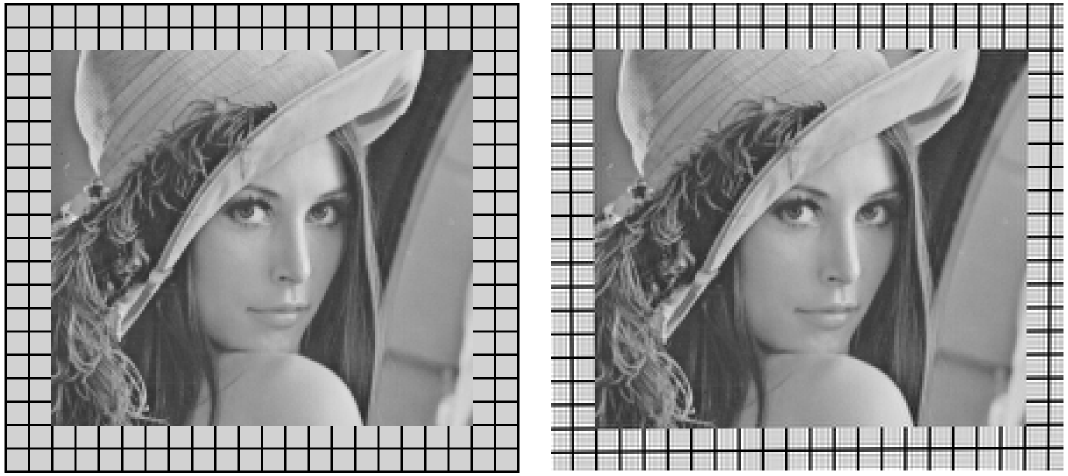


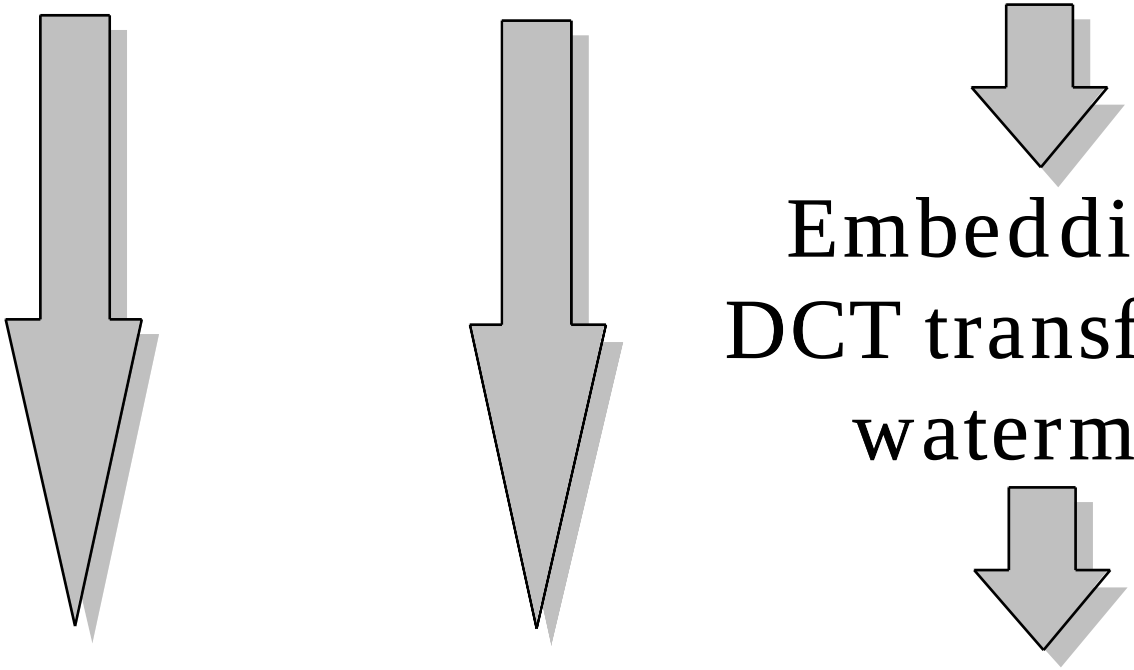
Image attacked using the StirMark attack software available on the Internet

So far: no known attack that successfully defeats spread spectrum watermarking without destroying the image/video

Watermarking of Compressed Video

Original video bitstream

...10101101101011011110010011001111100010101001101010101010101010...



header information

motion vectors

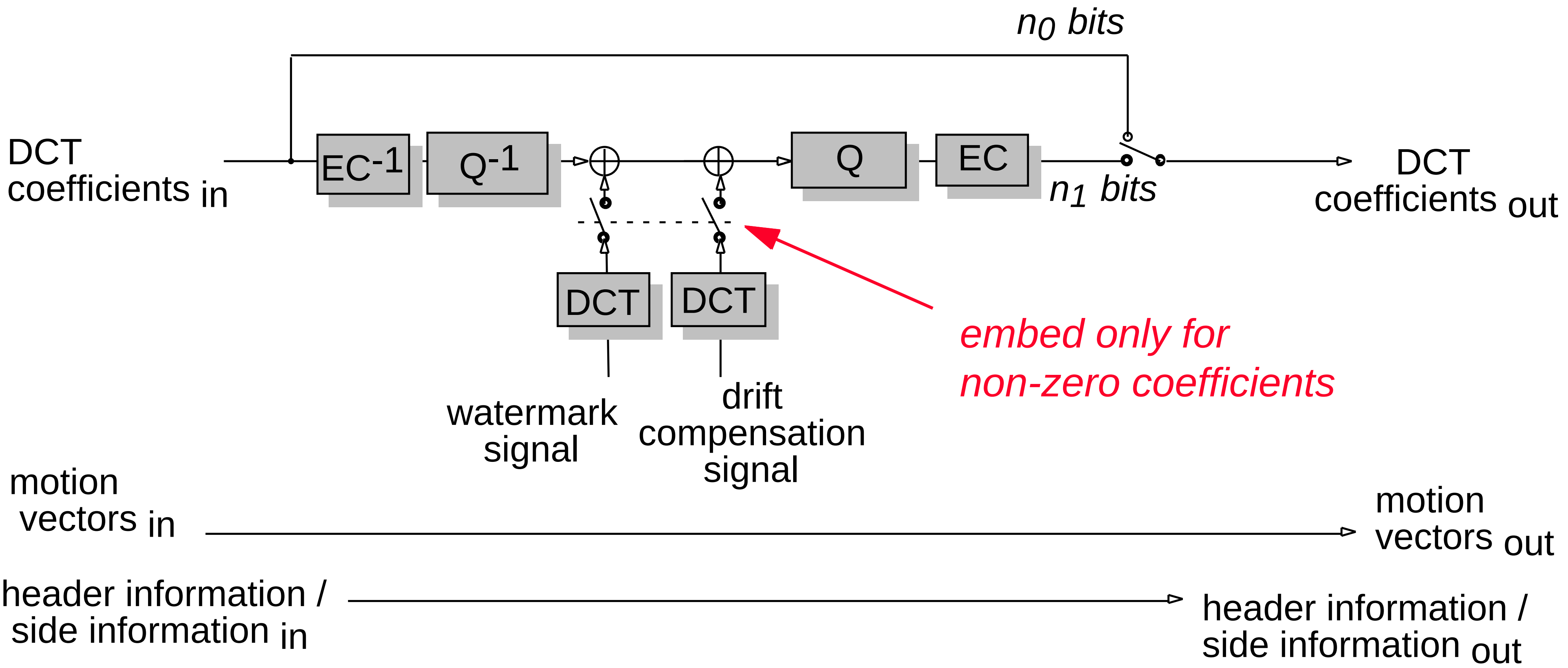
8x8 DCT block

Embedding of DCT transformed watermark

...1010110110101101111001001100111001010001111100011101010101010...

Watermarked video bitstream

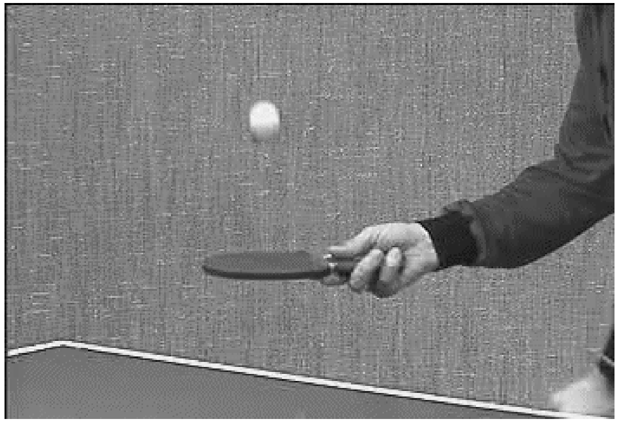
Embedding of Watermark and Drift Compensation Signal



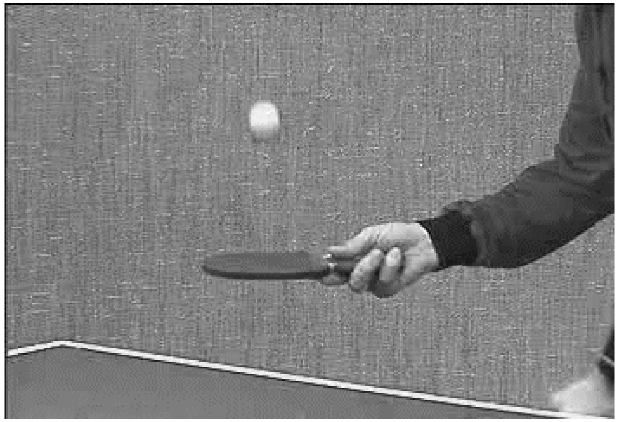
embed only for non-zero coefficients

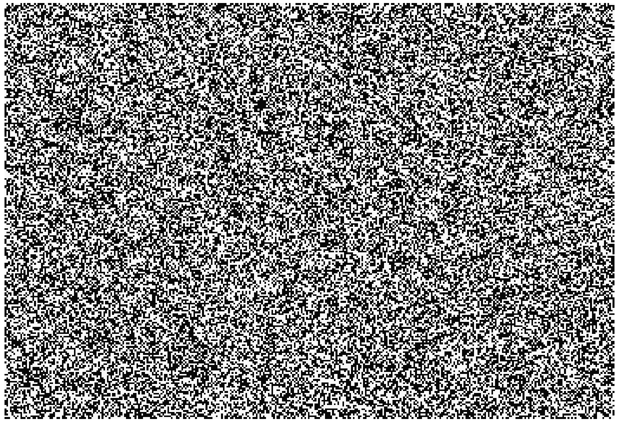
Example I

MPEG-2 coded frame

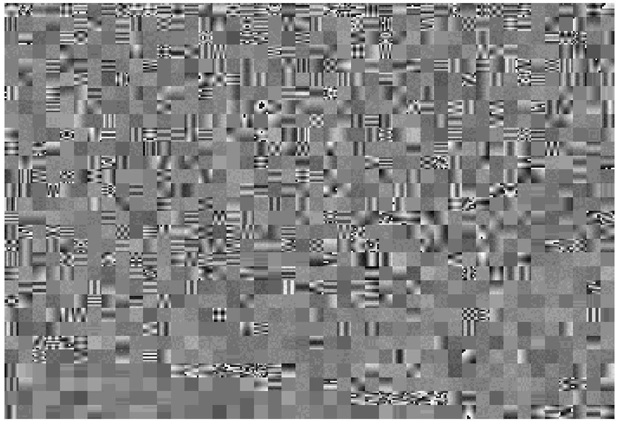


MPEG-2 coded frame with watermark





original watermark



embedded watermark

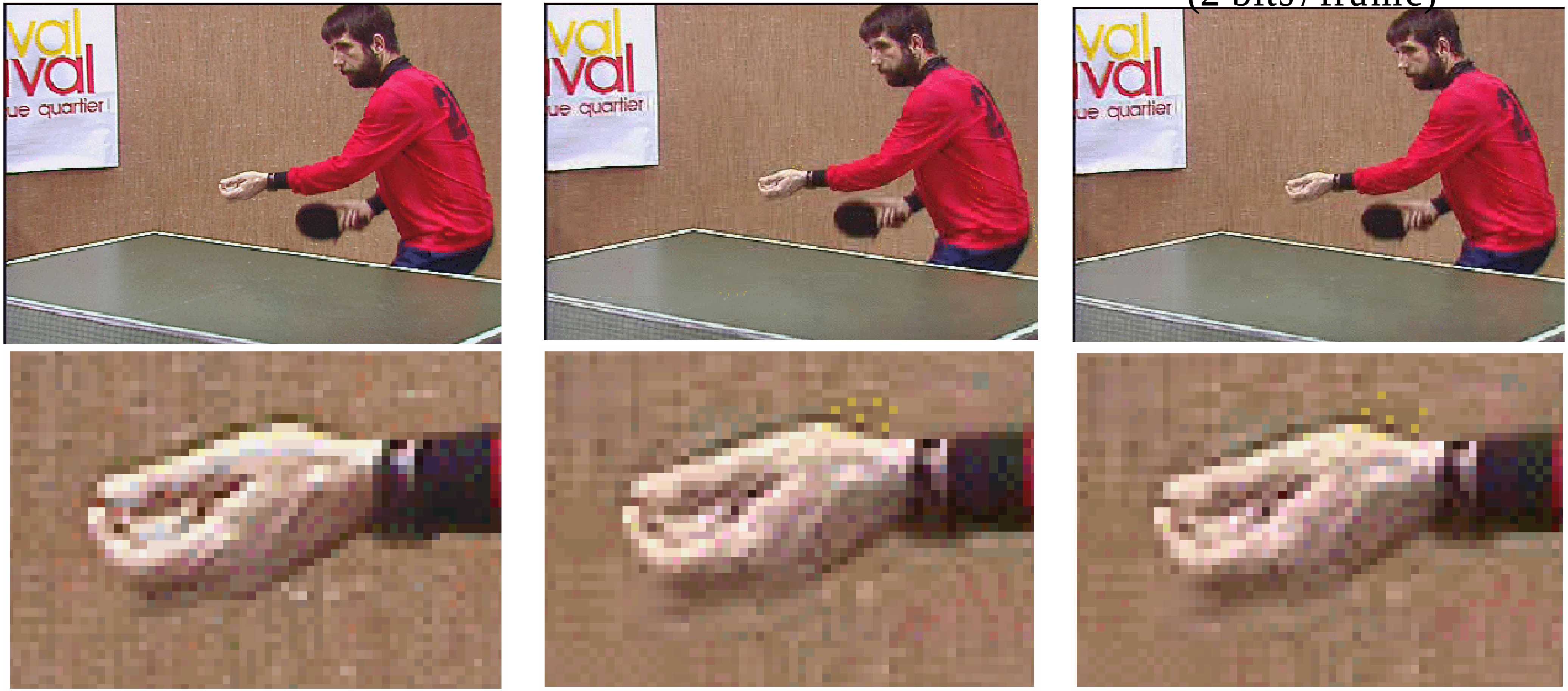
→ watermark embedded in compressed domain adapted to scene contents (→ less visible)

Example II

Original

MPEG-2 coded, without watermark

MPEG-2 coded, watermarked (2 bits / frame)



Conclusions

Digital Watermarking is the last line of defense which allows tracing of illegally produced copies of multimedia data

Text document watermarking

- small changes of layout (word spacing, line spacing, ...)

Image and Video Watermarking

- Spread spectrum approach
- Watermark recovery without the original
- Robust, even against attacks

Watermarking of compressed video

- addition of DCT coefficients with or without rate constraint
- no decoding and re-encoding necessary

http://www-nt.e-technik.uni-erlangen.de/