Telecommunications Seminar WS 1998

"Data Hiding, Digital Watermarking and Secure Communications"

Image and Video Watermarking

Herbert Buchner

University of Erlangen-Nuremberg

16.12.1998

Outline

1. Introduction: Watermarking of Visual Data
2. Some Approaches for Image Data
    - Spread spectrum concept
    - Image adaptive schemes
    - Robustness to geometric distortions
3. Watermarking of Video Data
    - Uncompressed video
    - Compressed video
4. Conclusions

1.Watermarking of Images and Video

- Data embedding / data hiding
  - Watermarking
  - Steganography
- ... in host signal:
  - Image
  - Video
  - Audio
  - Formatted text
  - ...

General Requirements

- Invisibility for the human visual system (HVS)
- Robustness to intentional and unintentional attacks:
  - Lossy compression schemes (JPEG, MPEG,...)
  - Linear and nonlinear filtering
  - Geometric distortions (scaling, cropping, rotation...)
  - Collusion
  - ...
- Security

Building a Watermark I

consists of two parts:

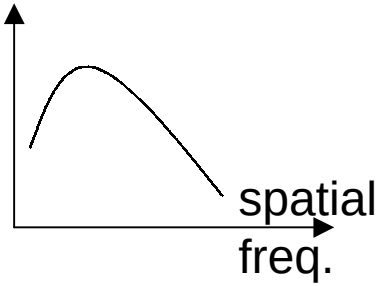
INSERTION STRATEGY	**WATERMARK STRUCTURE**
Where in the host signal shall we place the information?	*How* shall we place the additional information into the signal?

in order to comply with the requirements

Building a Watermark II

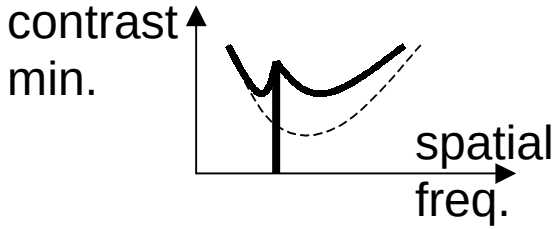
➡ Basic principle of **all** approaches for data embedding: exploitation of the limitations of the HVS:

- Minimum intensity or contrast sensitivity



- ‘Masking’ phenomena:
  - spatial masking

  - temporal masking
  - freq. masking



☞ Note: framework has no general optimum solution !

2. Some Approaches for Image Data

LSB-type methods - one of the simplest concepts for data embedding in noise-free environments.

➪ LSBs of the image are replaced by other data bits.

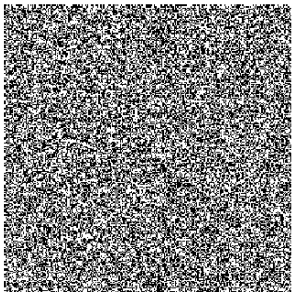
- Embedded data invisible (LSBs=**least perceptible** bits!)


original


bit plane 8


bit plane 5


bit plane 4

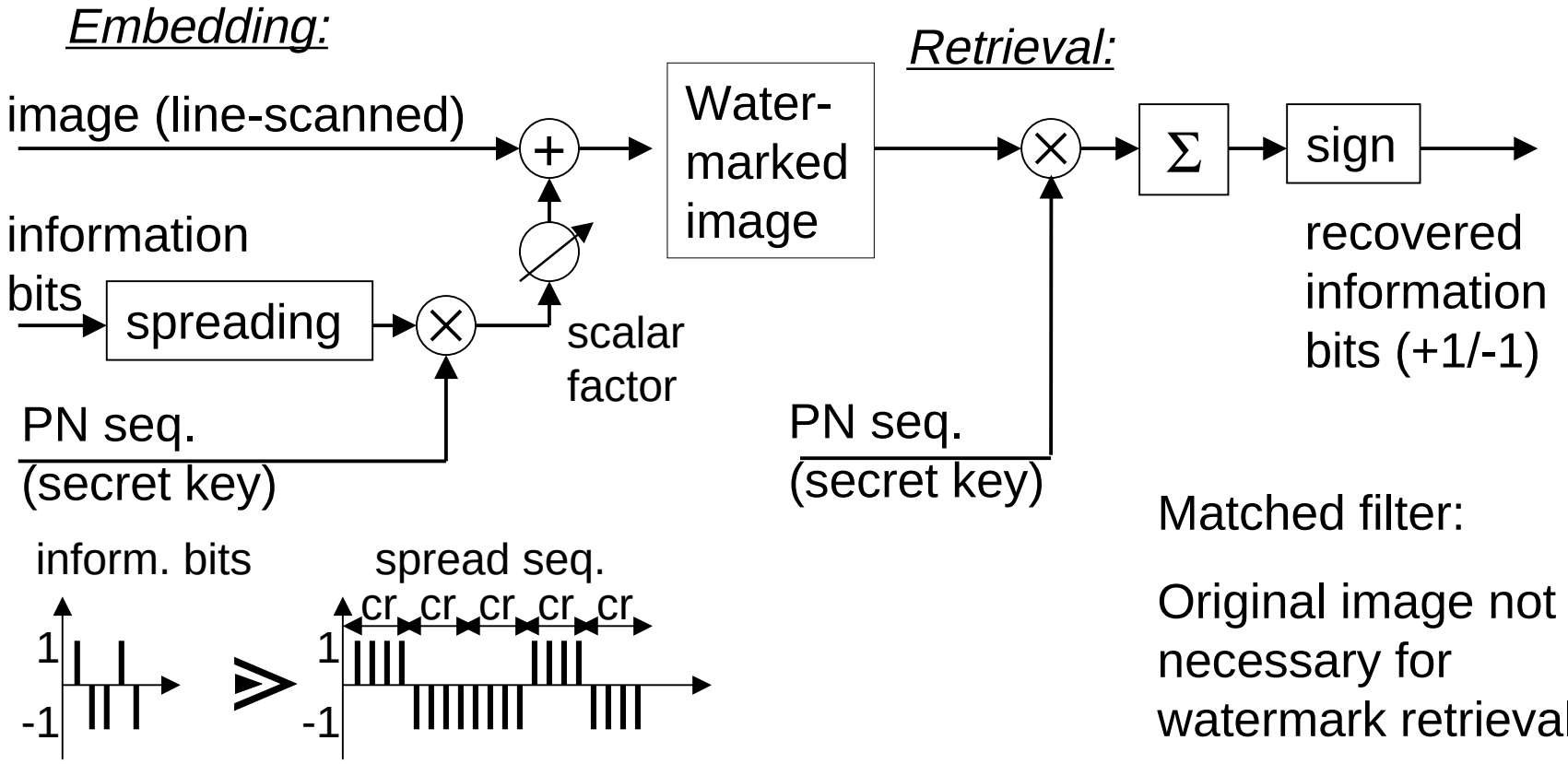

bit plane 1

- **INSECURE**: it is known where the information bits are
- **NOT ROBUST**: since changes of LSBs invisible !

Spread Spectrum Concept I

Greater robustness: How to imperceptibly insert a watermark into perceptually significant portions of the image?

Spread spectrum approach in the spatial domain (1D watermark)

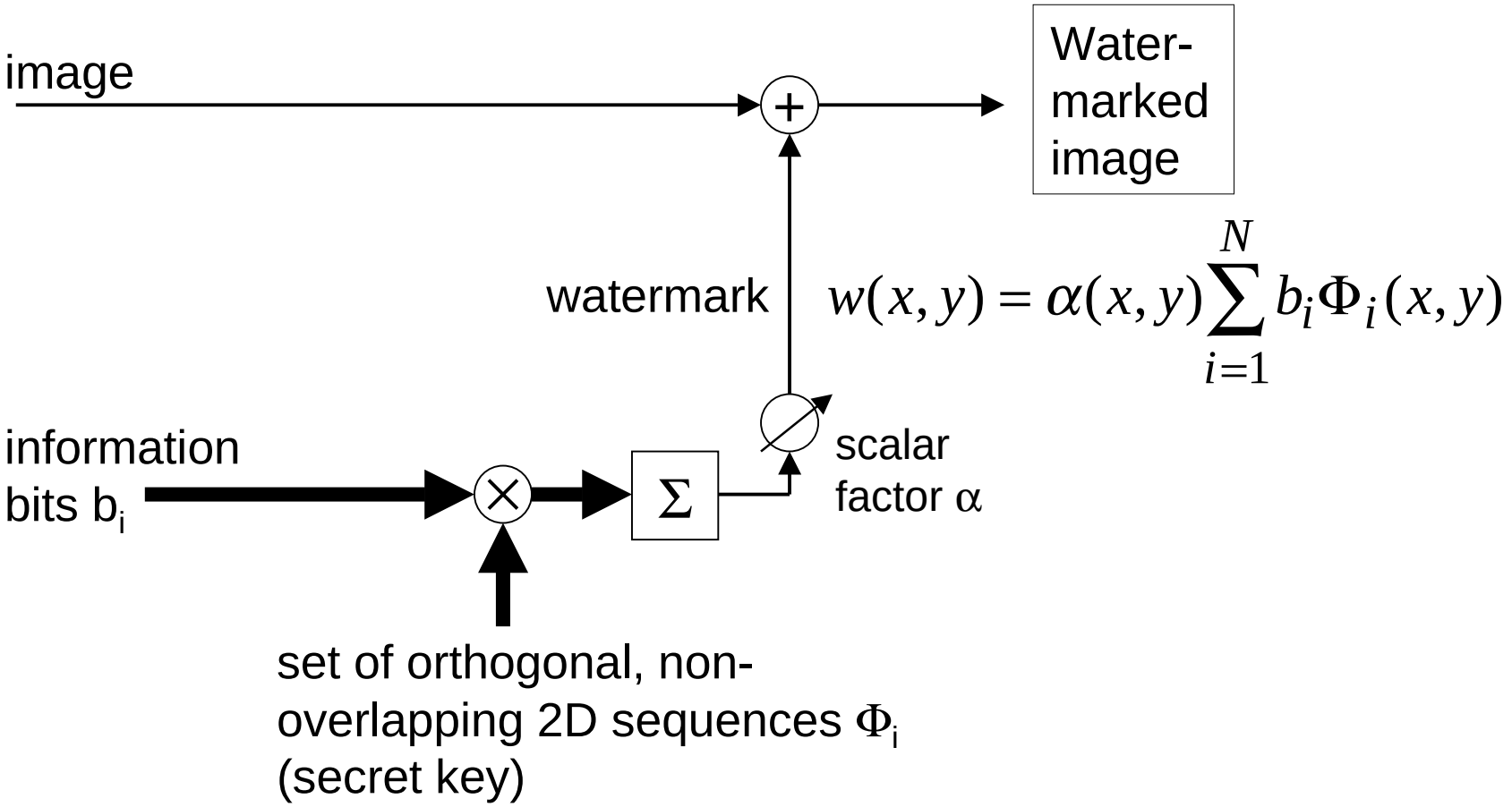


Matched filter:

Original image not necessary for watermark retrieval.

Spread Spectrum Concept II

Extension: 2D watermark in the spatial domain *(by Kutter)*



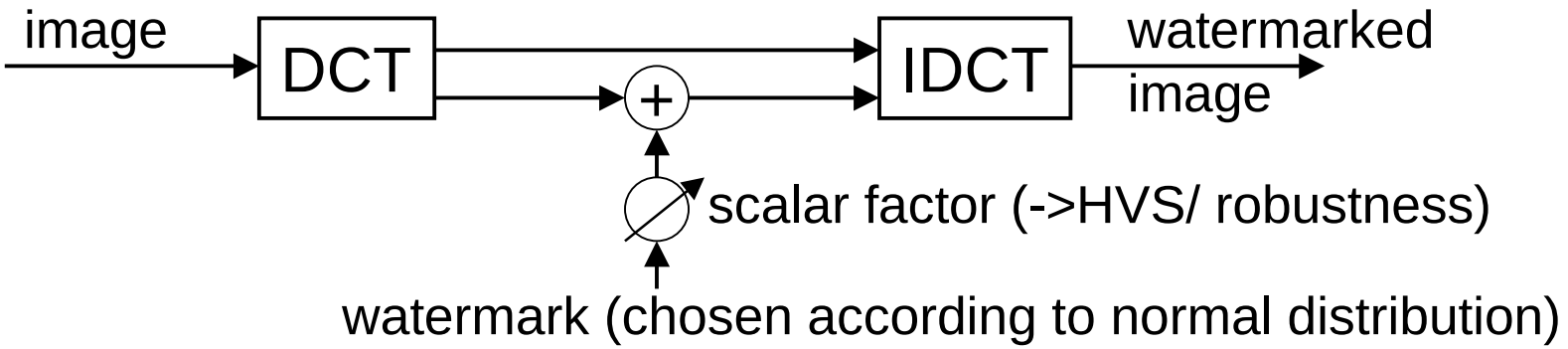
Spread Spectrum Concept III

Watermarking in frequency domain increases robustness

- Robustness to cropping: watermark spread over whole spatial extent
- Lossy compression (JPEG) usually eliminates non-salient spectral comp.
- Shrinking leads to loss in HF components only

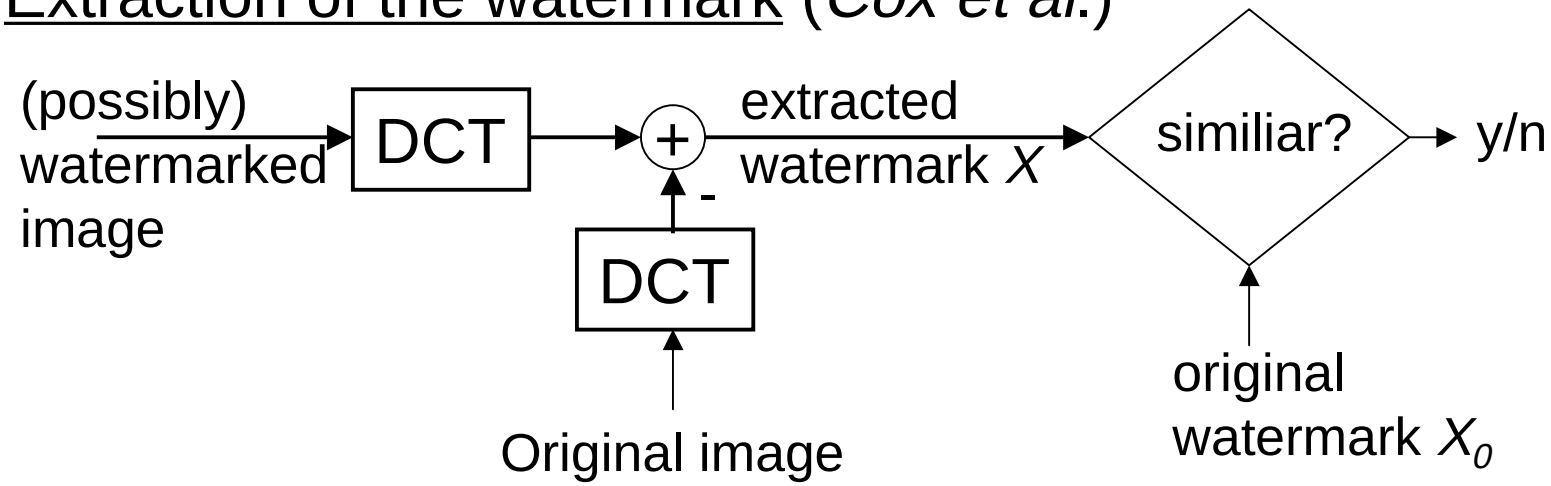
Approach by *Cox et al*.:

Watermark embedded in largest magnitude DCT coefficients (>1000 coeff. recommended) ⇨ frequency spreading !



Spread Spectrum Concept IV

Extraction of the watermark (*Cox et al.*)



Properties of the method:

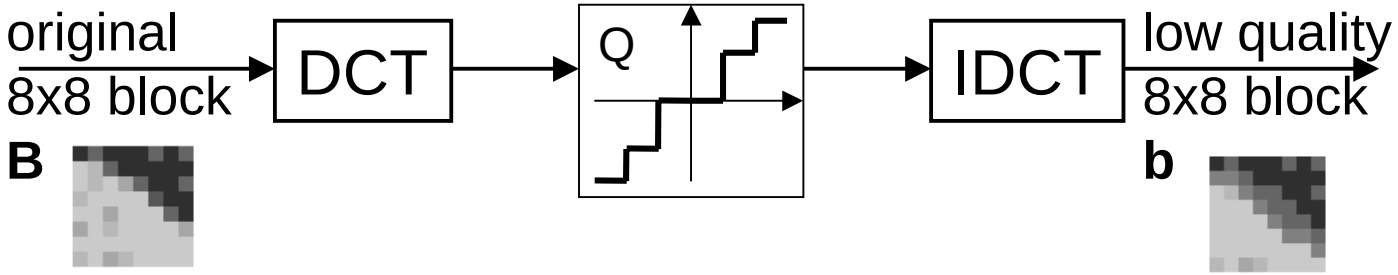
- Very reliable (robust to JPEG encoding, dithering, clipping with JPEG encoding, averaging of separately watermarked images, and combination of printing, photocopying, subsequent rescanning and rescaling)
- Major drawback: watermarked **and** original images necessary!

Image Adaptive Schemes I

Can make *explicit* use of characteristics of the image and/or HVS.

Simple example in spatial domain: image adaptive separation in histogram (by *Langelaar et al.*):

- Select (**secret key 1**) one 8x8 block **B** of the image
- Create a low quality copy of the block (preventive simulation of JPEG image to increase the robustness!):

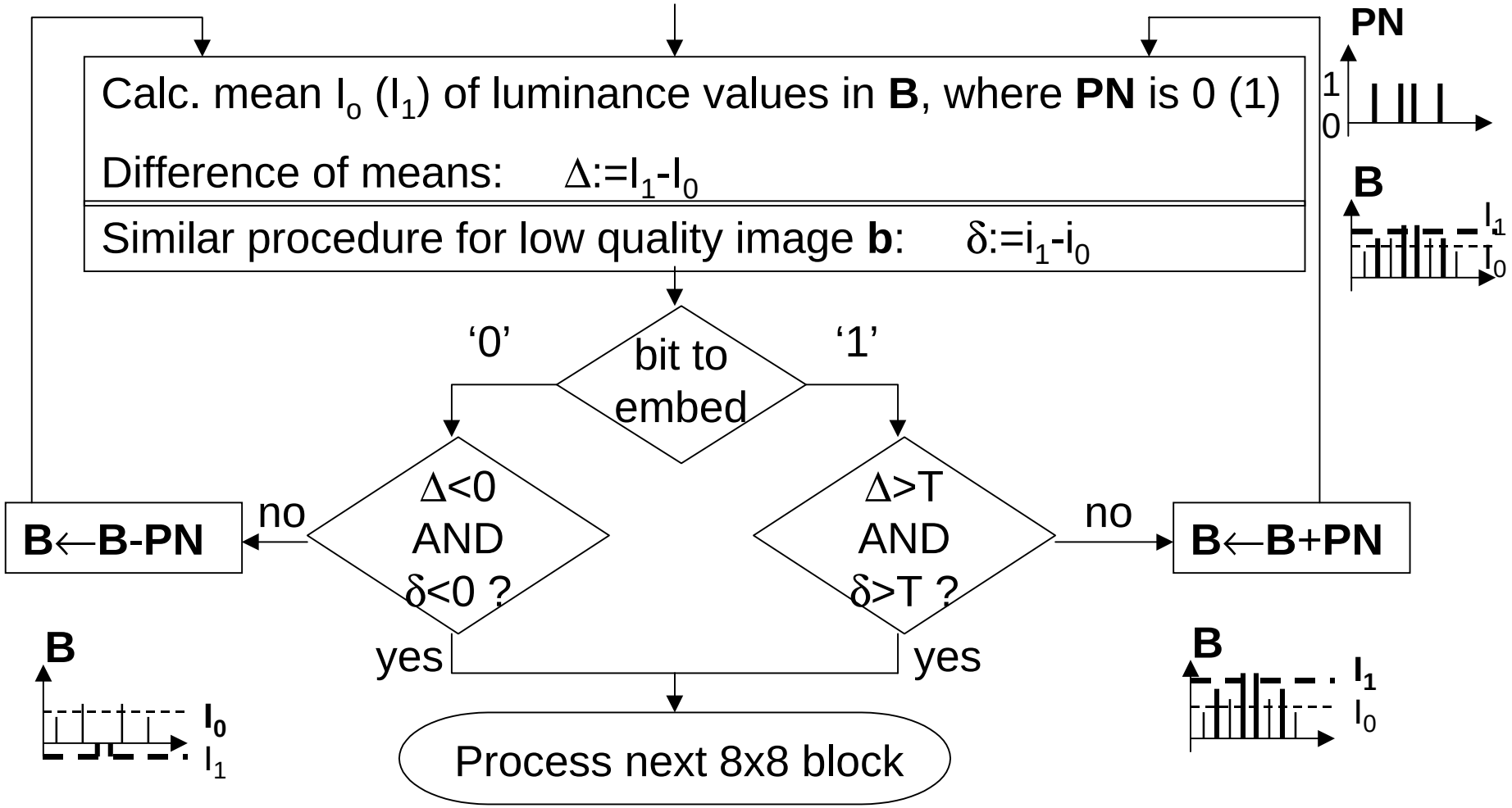


- Create a binary 8x8 pseudo-random pattern (**secret key 2**) **PN**:

"stencil"

Image Adaptive Schemes II

Watermarking procedure for each bit:



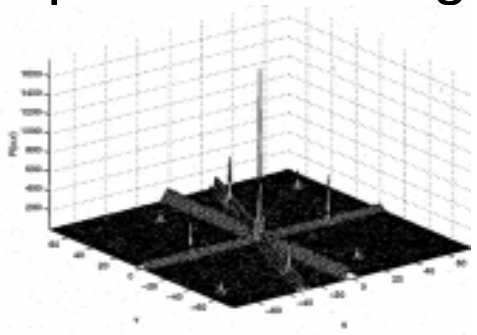
Robustness to Geometric Distortions

Two different types of approaches possible:

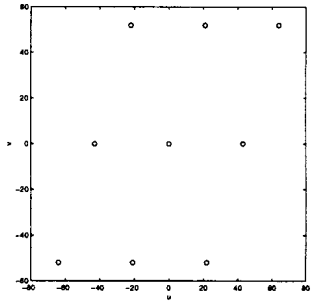
- Watermarking in a transformation invariant domain (e.g. magnitude of Fourier transform is shift invariant)
- Embedding some additional hidden grid to determine and invert the distortion before watermark retrieval

Method by *Kutter*: multiple embedding at shifted locations

watermarked image



autocorrelation funct.



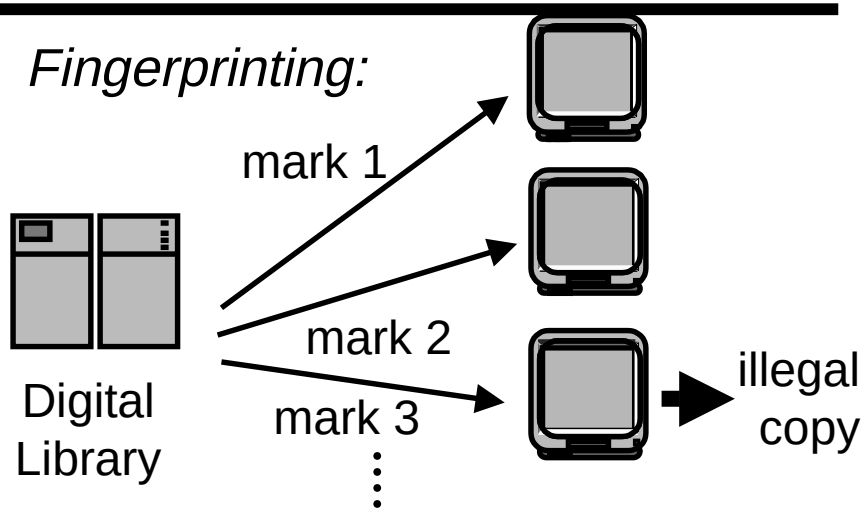
extracted peaks

Method allows watermark recovery after translation, cropping, scaling, rotation, shearing, change of aspect ratio

3. Watermarking of Video Data

<u>Main differences to image watermarking:</u>

- Much higher volume of data (bandwidth)
- Real-time embedding



<u>Possible requirements</u> (in addition to those of still image watermarking):

- Constant bit-rate (with/without watermark)
- Low complexity
- Compressed domain processing
- Interoperability

Watermarking of Uncompressed Video

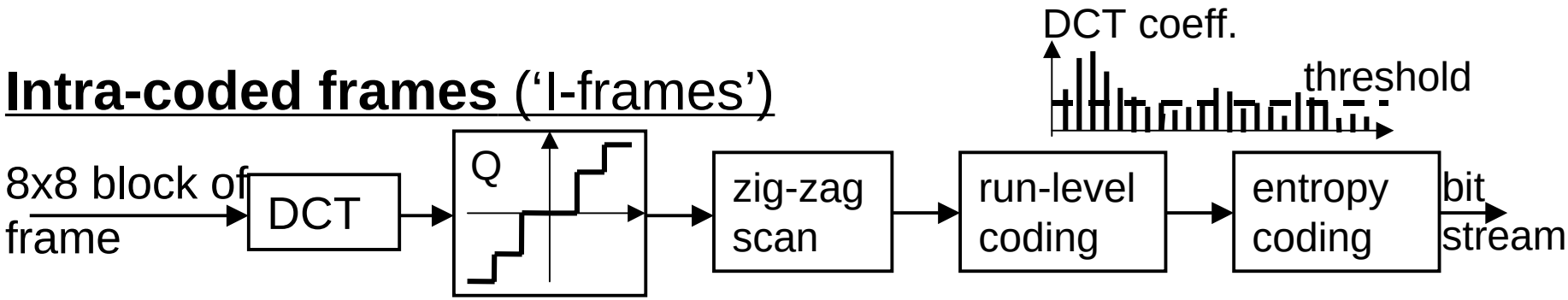
- If real-time embedding is not required: uncompressed video can be watermarked frame by frame using the conventional methods for still images
- One watermark bit can be distributed over several video frames to increase robustness

Hybrid Coding Schemes I

Basic principles: (MPEG, H.261, H.263)

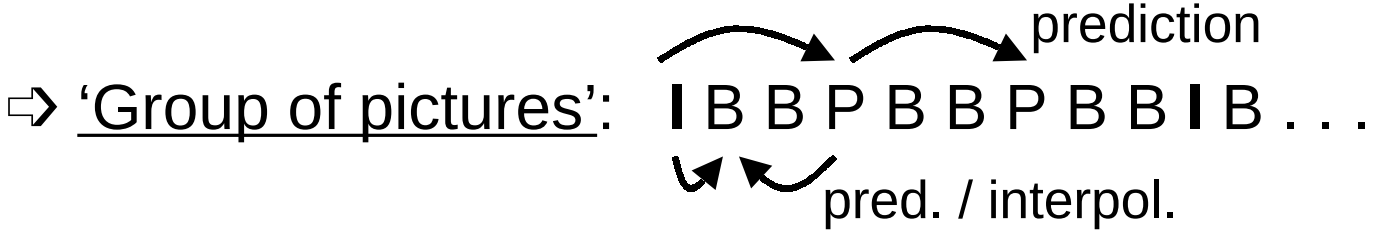
- Block-based transform coding (DCT)
- Motion compensated prediction

Intra-coded frames (‘I-frames’)



Inter-coded frames (‘P-frames’, ‘B-frames’)

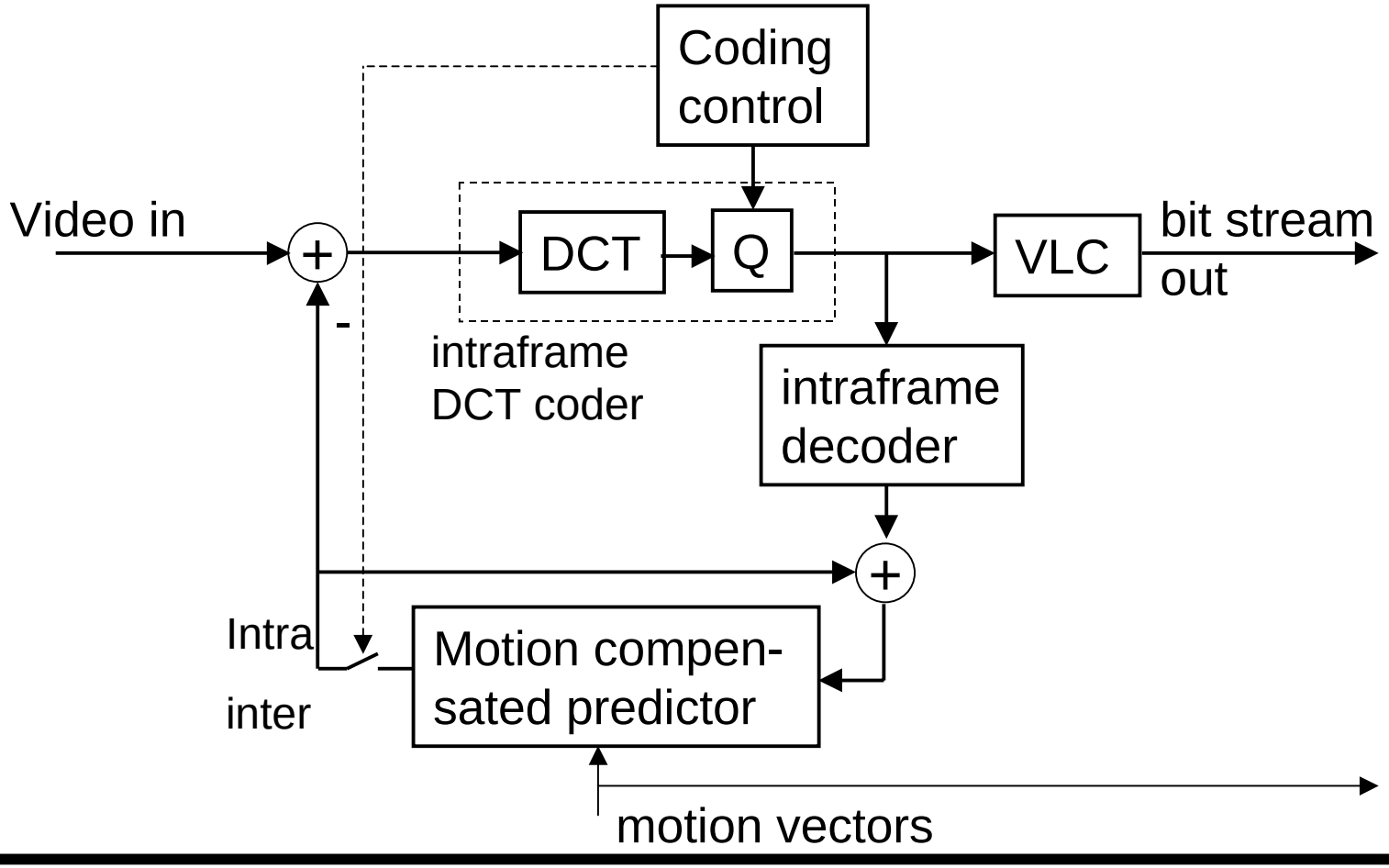
Residual prediction error signal frames are used



⇨ ‘Group of pictures’:

Hybrid Coding Schemes II

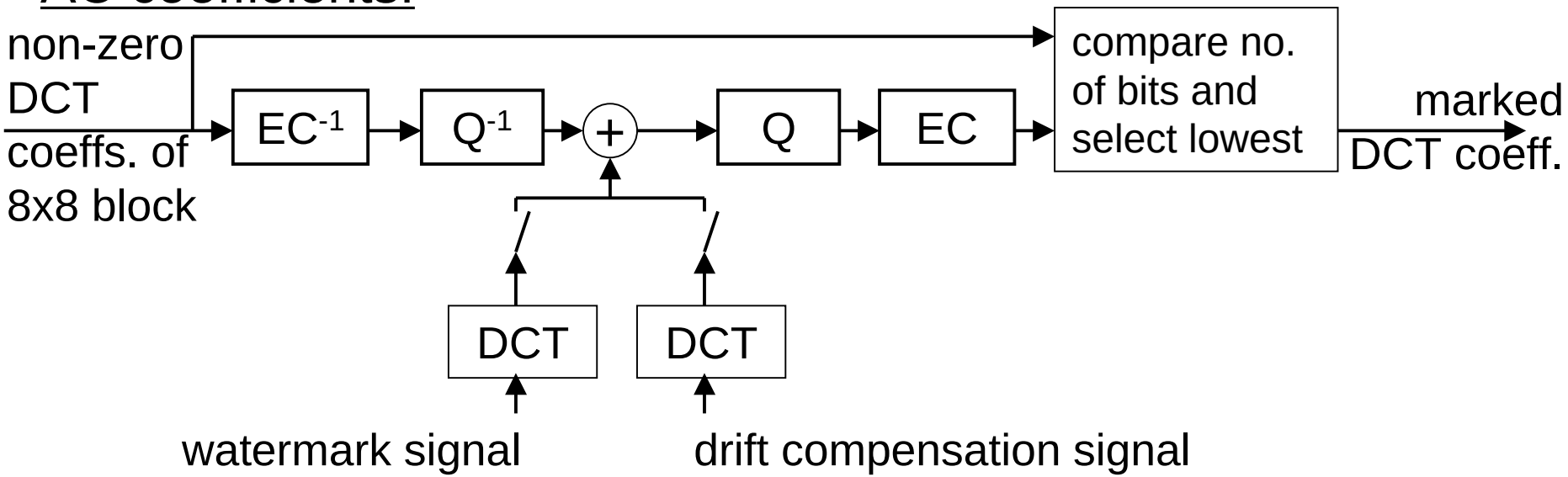
Simplified Block Diagram of a Generic Hybrid Coding Scheme:



Watermarking of Compressed Video I

Method for additive spread spectrum watermarkíng in hybrid coding schemes by *Hartung and Girod*: Adding video data and watermark for each 8x8 block in the DCT domain:

- AC coefficients:



- DC coefficients of I-blocks are always watermarked (fixed length code - comparison of code length not necessary)

Watermarking of Compressed Video II

- Scheme works with all additive watermark signals
- Visible artifacts avoided by addition of a drift compensation signal (motion-compensated hybrid coding works recursively!)
- Complexity comparable to MPEG decoding
- Method exploits masking characteristics indirectly, since only non-zero DCT coefficients are watermarked
- The watermark can be retrieved from the decoded sequence

4. Conclusions

- Watermarking is data embedding with several strict requirements
- Watermarks must be invisible:

  All approaches for watermarking of visual data implicitly or explicitly exploit the limitations of the human visual system
- Watermarks should be placed in perceptibly significant portions of the image/video to ensure robustness
- Most additive methods based on spread spectrum concept
- Applications for video watermarking usually require more sophisticated approaches if real time embedding is desired (embedding in the compressed domain)

References

- B. Girod, “Image Communication”, Lecture, Univ. of Erlangen-Nuremberg
- H. Niemann, “Mustererkennung”, Lecture, Univ. of Erlangen-Nuremberg
- M.D. Swanson, M. Kobayashi, A.H.Tewfik, “Multimedia Data-Embedding and Watermarking Technologies”, Proc. IEEE, vol. 86, no. 6, June 1998
- I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia”, IEEE Trans. Image Processing, vol. 6, no. 12, Dec. 1997
- F. Hartung, B. Girod, “Watermarking of uncompressed and compressed video”, Signal Processing, vol. 66, 1998
- F. Hartung, U. Horn, “Codierung digitaler Videosignale nach dem MPEG-Standard”, me, vol. 9, 1995 (in German)

References

- F. Hartung, B. Girod, “Digital watermarking of MPEG-2 coded video in the bitstream domain”, Proc. ICASSP97, Apr. 1997
- E. Koch, J. Zhao, “Towards Robust and Hidden Image Copyright Labeling”, Proc. Of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, June 1995 (available at: http://poseidon.csd.auth.gr/workshop/papers/p_19_1.html)
- G. C. Langelaar, J. C. A. van der Lubbe, J. Biemond, “Copy Protection for Multimedia Data based on Labeling Techniques” (available at: http:// www-it.et.tudelft.nl/html/research/smash/public/benlx96/benelux_cr.html)
- M. Kutter, F. Jordan, F. Bossen, “Digital Signature of Color Images using Amplitude Modulation”, Proc. SPIE-E197, 1997, pp. 518-526
- M. Kutter, “Watermarking resisting to translation, rotation and scaling”, Proc. of SPIE, Nov. 1998