Digital image watermarking

Peter Meerwald,
pmeerw@cosy.sbg.ac.at

August 19, 1999

Abstract

A brief introduction to image watermarking for copyright protection. After identifying the aims and requirements, a watermarking scheme is discussed to demonstrate applications and problems of this novel technology.

Digital media and the internet

- ✘ inexpensive copies
- ✘ no quality loss
- ✘ wide distribution but no control

a problem?

- ✘ how can intellectual property (eg. photography) be protected?
- ✘ how does the creator get the money?
- ✘ how to control distribution?

What is watermarking?

- ✘ embedding a mark (text, logo) into an image
- ✘ not dependent on file format
- ✘ no container, no encryption
- ✘ visible or invisible

Applications of watermarking

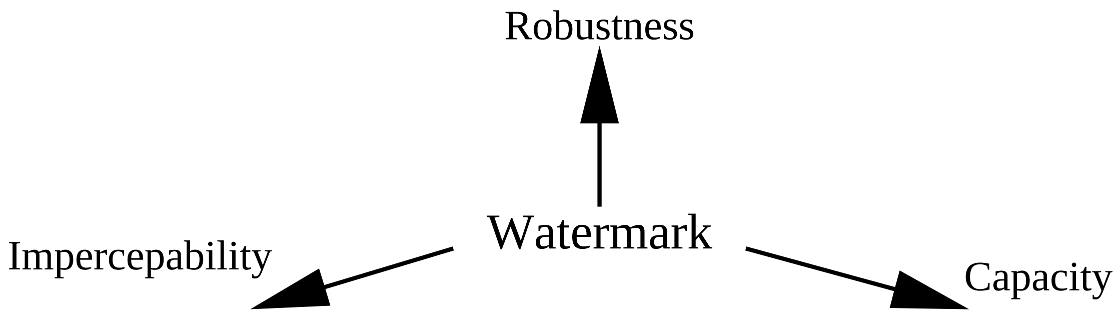
1. copyright protection / circulation tracking
   who owns an image? who leaked a copy? automatically scanning on the Web!

2. data hiding / steganography
   allows (encrypted) communication without attracting attention

3. authentication and tamper detection - has the image been modified?

Requirements

1. invisible
2. robust (attacks, compression)
3. high capacity
4. secure (collusion, confidence)
5. practical



How does it work?

1. generate watermark based on secret key
2. add redundancy
3. transform image (eg. DCT) or spatial domain
4. choose pseudo-random locations
5. make significant yet invisible changes
6. take human visual system (HVS) into account
7. inverse transformation

Human Visual System (HVS)

human eye not equally sensitive over luminance range

- ✘ noise: high frequency
- ✘ area luminance: low frequency

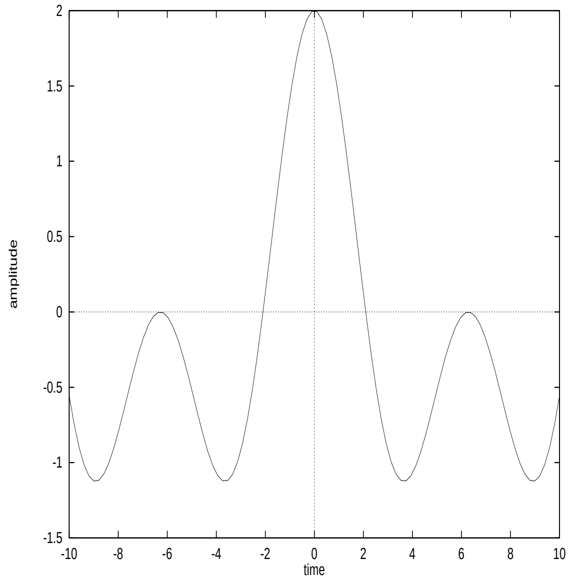
contrast sensitivity: perceptible luminance difference

color sensitivity: green most, blue least

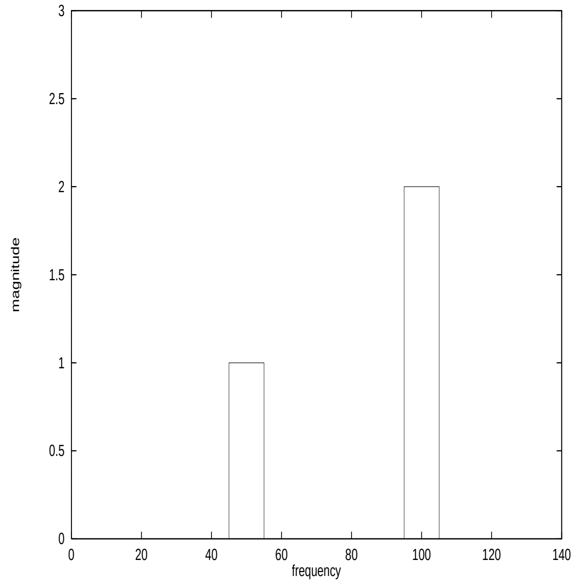
Discrete Cosine Transform (DCT)

spatial/pixel domain to frequency domain

$n \times m$ pixels to $n \times m$ real number coefficients



(a) time domain



(b) frequency domain

above signal is 1D but an image is a signal in 2D

DCT is computationally expensive

Watermark detection

1. blind or non-blind recovery (original image required)

2. get watermarked image, possibly altered

3. extracting embedded data

4. apply error correction

5. correlation

6. decision

In detail: Cox' algorithm

1. generate sequence of 1000 real numbers w_i, normal distribution, mean zero apply discrete cosine transform (DCT) on image

2. now in frequency domain, modification will spread over entire image

3. select 1000 DCT coeffients c_j from mid-frequency range (compromise between robustness and visibility; high freq. is noise and will be removed by JPEG)

4. embed watermark: $c'_j = c_j(1 + \alpha w_{i)}$

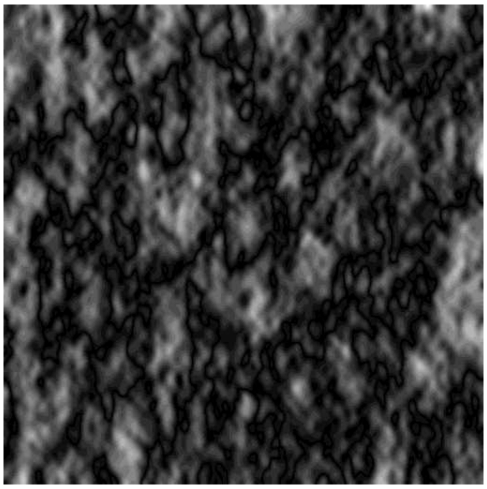
5. apply inverse cosine transform to get watermarked image

What does the watermark look like?

invisible but entire image altered (see difference image)

(c) original; A

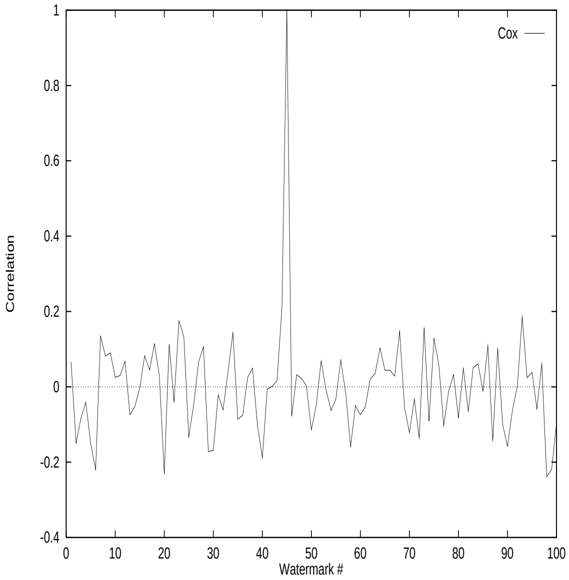
(d) watermarked; B

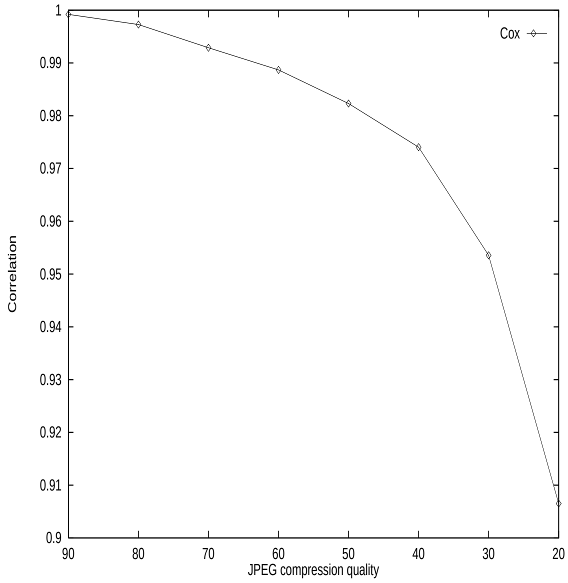


(e) difference image; $A - B$

Robustness against JPEG

watermark detectable (correlation)? image still usable?





Everything alright?

- ✘ Stirmark defeats all commercial watermarking schemes so far
- ✘ problems with geometric attacks (cropping, scaling)
- ✘ no courtroom experience

but:

- ✘ music industry will have audio watermarking to replace MP3
- ✘ ongoing research & improvements

Pointers

Visible Watermarking: Do it yourself
`http://webdesign.miningco.com/library/weekly/aa060997.htm`

Vatican Library
`http://www.research.ibm.com/journal/rd/mintz/mintzer.html`

Attack: StirMark
`http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark`

Stirmark - What's going on?
`http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/samples2.html`

Attack: UnZign `http://www.altern.com/watermark/`

Unzign samples `http://www.altern.com/watermark/pictures.html`

Authentication: Hillary or Monica?
`http://www.ctr.columbia.edu/~cylin/auth/auth.html`

Software system: Hacking Digimarc
`http://www.phase-one.com.au/fravia/frogdigi.htm`

Playboy `http://www.altern.com/watermark/playboy.html`

Commercial products
`http://www.cl.cam.ac.uk/~fapp2/watermarking/products.html`

References

[1] Cox, I. J., Killian, J., Leighton, T., Shamoon, T. Secure Spread Spectrum Watermark for Multimedia, 1995.

[2] Rao, K. R., Yip, P., Discrete Cosine Transform: Algorithms, Advantages, Applications, Academic Press, 1990.

[3] Petitcolas, F. A. P., Anderson, R. J., Kuhn, M. G., Attacks on copyright marking systems, Information Hiding Second International Workshop IH '98, Portland, Oregon, USA, 1998. `http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/`

[4] Lin, C. Y., Chang, S. F., Generating Robust Digital Signature for Image/Video Authentication, ACM Multimedia and Security Workshop, Bristol, UK, 1998. `http://www.ctr.columbia.edu/~cylin/auth/auth.html`