EE 6886: Topics in Signal Processing -- Multimedia Security System

Lecture 4: Digital Watermarking

Ching-Yung Lin
Dept. of Electrical Engineering
Columbia University, New York, NY 10027

© 2006 Columbia University

Course Outline

- Multimedia Security :
  - Multimedia Standards – Ubiquitous MM
  - Encryption – Confidential MM
  - Watermarking – Uninfringible MM
  - Authentication – Trustworthy MM
- Security Applications of Multimedia:
  - Audio-Visual Person Identification – Access Control, Identifying Suspects
  - Surveillance Applications – Abnormality Detection
  - Media Sensor Networks – Event Understanding, Information Aggregation

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

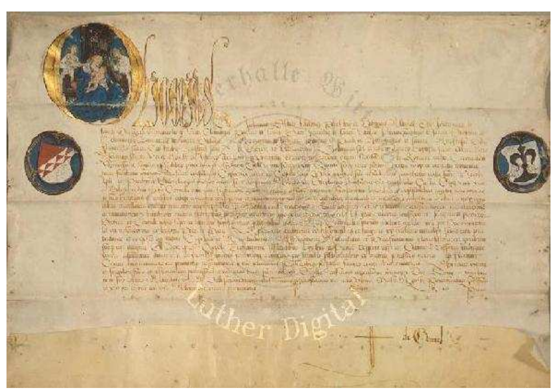
Lecture 4 Outline

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

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Watermarking

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



PIL or content- based feature codes

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

What is Watermarking ? –
Multimedia as a Communication Channel

- Basic communication system:

Information
W → Encoder → Channel → Decoder → $\widehat{W}$

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

Information
W → Encoder →  → Decoder → W

Image/Video/Audio

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Invisible Watermark

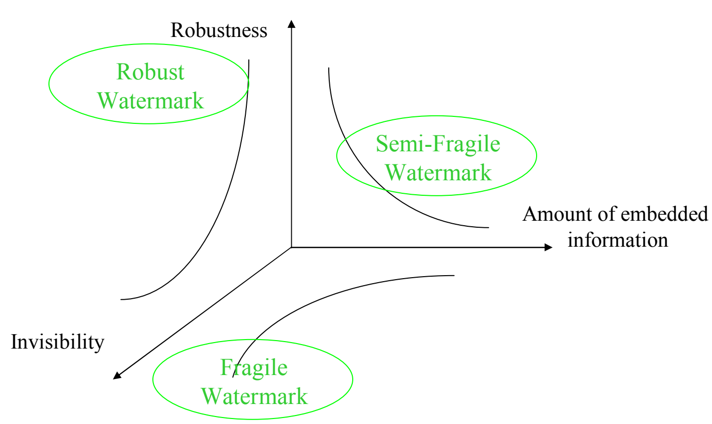
- Purpose:
  - Protect ownership and trace illegal use.
  - (Content) Authentication
  - Copy/ Playback control
- Properties -- *Transmit a bitstream through a very noisy channel, i.e. the original picture.*
  - Robust: The watermark must be very difficult, if not impossible, to remove. It must be able 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.

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Considerations for Watermarking System

- Security – *Kerchoff's assumption*
- Robustness
- Hiding Payload
- Application Scenario

Three Metrics of Watermarking



Steganography

- Information Hiding (no security concern)
- Watermarking (with security concern)
- Other applications:
  - Reversible information hiding
  - 3D watermarking
  - Halftoning

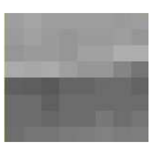
© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Simplest Watermark – Changing Least Significant Bits

Message → Encoding → Changing LSB → Watermarked Image

key → Encoding

Image → Changing LSB



158	165	158	158	158	158	155	158
155	161	155	150	155	155	158	151
150	155	155	150	161	161	174	174
171	167	171	159	151	151	134	117
96	94	90	102	102	108	108	101
108	108	96	108	108	108	108	108
108	108	103	108	108	120	110	117
110	117	117	123	125	129	124	127

→ wmk →

10001001 → wmk

159	164	158	158	159	158	154	159
155	160	154	150	155	154	158	151
151	154	154	150	161	160	174	175

…….

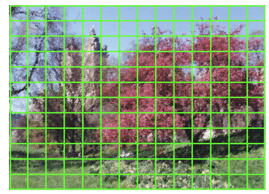
© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Changing LSB in the block-based frequency domain

Message → Encoding → Changing LSB → Watermarked Image

key → Encoding

Image → Block-base DCT → Changing LSB



- ❑ 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

1026	-4	-1	10	-9	0	-4	-6
160	14	6	-6	-4	0	-4	8
36	-18	5	-8	0	-9	0	-3
-86	-3	5	4	6	-2	-1	-6
-2	20	-13	2	-2	0	2	0
50	21	-5	-2	-2	-1	6	-3
15	-17	9	-6	7	0	-7	2
-36	-40	12	-4	6	-1	0	-1

→ wmk →

10001001 → wmk

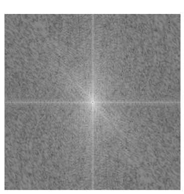
1027 -4 -1 10
160 14 6
36 -19
…….

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Changing LSB in the global frequency domain

Original Image

DFT Spectrum



- ❑ Convert Image to the global frequency domain
- ❑ Select some band for embedding coefficients
- ❑ Changing the least significant bit of the selected bands

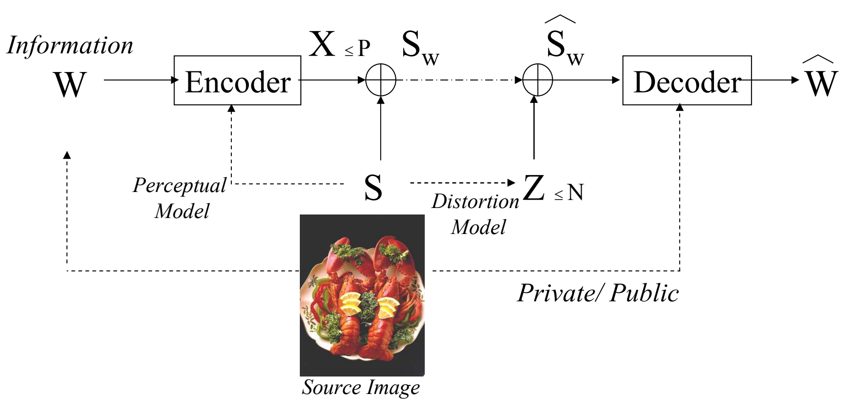
© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

What are the drawbacks of the LSB-based information hiding methods?

- Compare the previous three methods (changing LSBs at spatial domain, block-based frequency domain, and global frequency domain):
  - Robustness:
  - Security:
  - Hiding Payload:

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

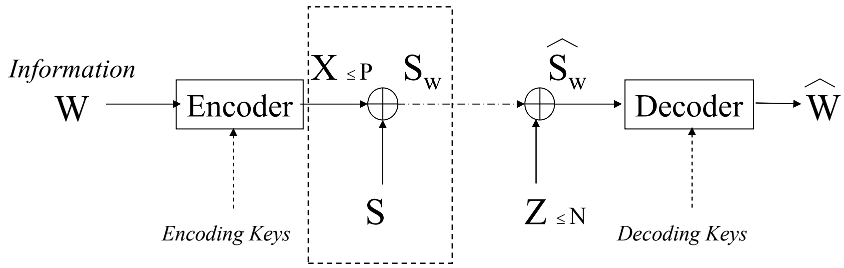
Watermarking on Multimedia Content



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

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

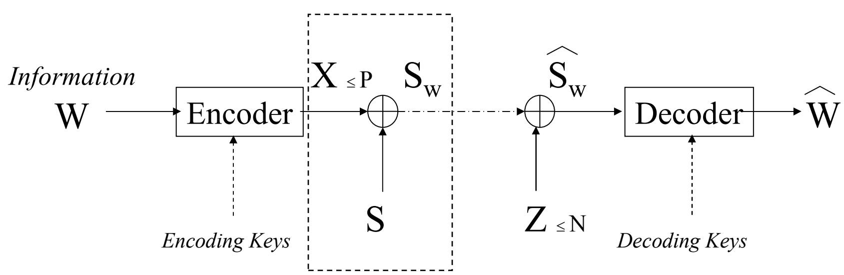
Digital Communication



- 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.

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

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 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)
- Examples

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Spread Spectrum Watermarking *(Cox et. al. 1997)*

- Spread Spectrum: $T(S_w) = T(S) + T(X)$
  - 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 ($T(S_w) – T(S)$, $T(X)$)

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Change of coefficients

- Change magnitudes based on a controllable parameter α.

$$v_i' = v_i + \alpha x_i$$

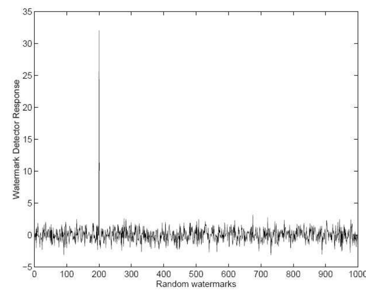
$$v_i' = v_i(1 + \alpha x_i)$$

$$v_i' = v_i(e^{\alpha x_i})$$

v_i: original value, x_i embedded value, v_i': imbedded result

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Spread Spectrum Watermarking Example

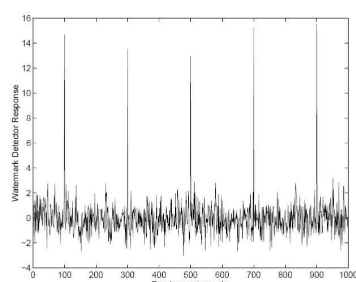


© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

E 6886 Topics in Signal Processing: Multimedia Security Systems

Spread Spectrum Watermarking Example

- Embedding multiple watermarks

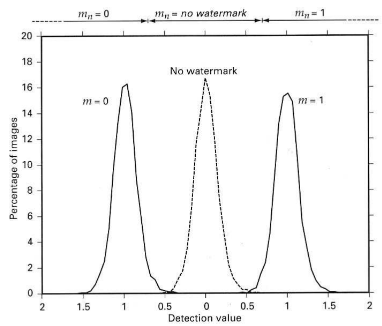


- The SS-based watermarks can survive compression, cropping, scaling, etc.
- However, it cannot survive rotation and need original data for watermark extraction.

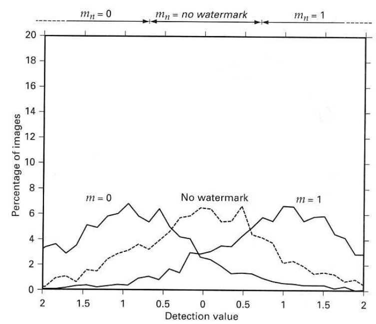
© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

How to evaluate a watermarking system

- Detection on the watermarks



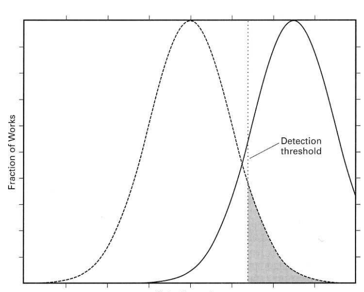
Before manipulation



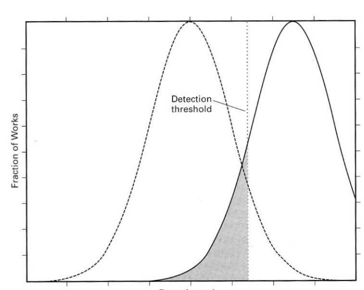
After low-pass filtering

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Performance Evaluation



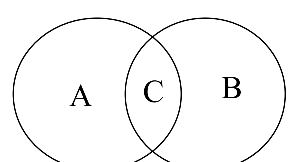
False Positive / False Alarm



False Negative / Miss

- What are False Positive (false alarm) and False Negative (miss)?
- What are ROC curves?

Detection Result

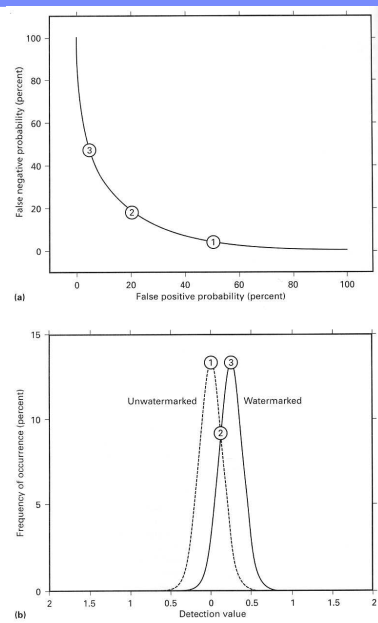


Fact

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

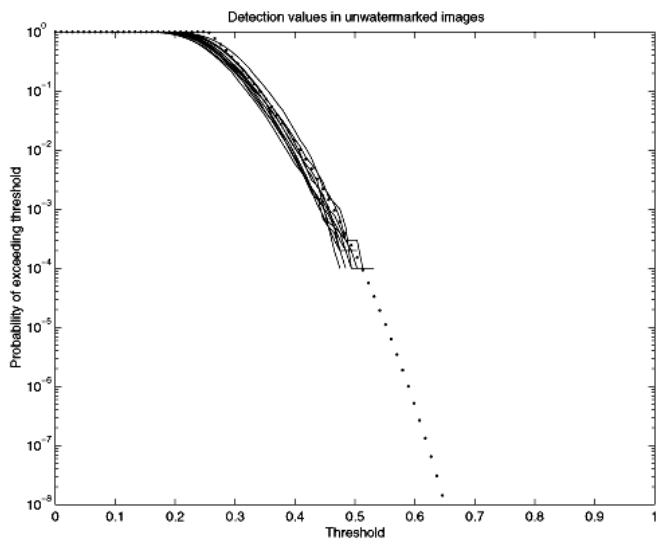
Region of Operation (ROC) curve

- False Negative v.s. False Positive
- Miss v.s. False Alarm
- Precision v.s. Recall



© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

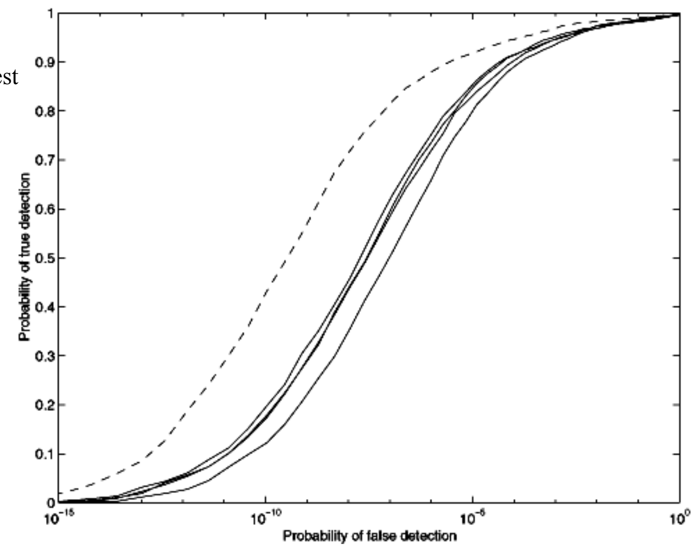
False Positive Example (10,000 images from Corel Image Library, 10 different watermarks)



© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Robustness Evaluation Example (ROC curves of 2,000 images)

Rotation Test
(4°, 8 °,
30 °, 45 °)



© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

E 6886 Topics in Signal Processing: Multimedia Security Systems

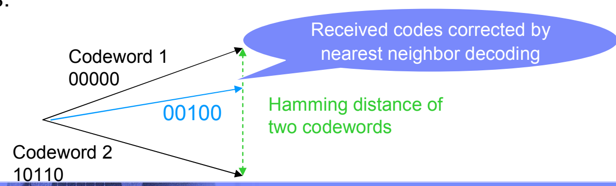
Increase Robustness via Coding -- Error Correction Coding (I)

- 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.

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

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.



© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

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

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Masking Effects on Human Vision System Models

e.g. JND model
PSNR = 32 dB

Specific Domains:
•Watson's DCT masking (1993)
• Watson's Wavelet masking (1997)
• Chou and Li's JND (1995)
• JPEG, QF =50

General models:
• Lubin's HVS model (1993)
• Daly's HVS model (1993)

Some properties of HVS models:

-- Amplitude nonlinearity, Inta-eye blurring, Re-sampling, Contrast sensitivity function, Subband decomposition, Masking, Pooling

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Just Noticeable Distortion (JND)

- 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).

Binary noise pattern with strength equal to Chou's JND bounds

Sinusoidal pattern with strength equal to Chou's JND bounds

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

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.

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Watson's JND Models

- Applied luminance masking and contrast masking.
- Consider specific domain coefficients.
- Use an original just-noticeable-change, called a mask, which is assumed to be the same in all blocks.
- Luminance masking:

$$t_{ijk} = t_{ij}\left(\frac{c_{00k}}{\bar{c}_{00}}\right)^{a_T}$$

t_{ij} is the original mask values, c_{00k} is the DC value of the block k and $\bar{c}_{00}$ Is the mean luminance of the display, $a_T = 0.648$ (suggested by Ahumada and peterson)

- Contrast masking:

$$m_{ijk} = max(t_{ijk}, |c_{ijk}|^{w_{ij}} t_{ijk}^{1-w_{ij}})$$

A typical empirical value of $w_{ij} = 0.7$

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Chou and Li's JND Model

$$JND(x,y) = max\{f_1(bg(x,y), mg(x,y)), f_2(bg(x,y))\}$$

where

$$f_1(bg(x,y), mg(x,y)) = mg(x,y) \cdot \alpha(bg(x,y)) + \beta(bg(x,y))$$

$$f_2(bg(x,y)) = \begin{cases} T_0 \cdot (1 - (bg(x,y)/127)^{0.5}) + 3 & for\ bg(x,y) \le 127 \\ \gamma \cdot (bg(x,y) - 127) + 3 & for\ bg(x,y) > 127 \end{cases}$$

$$\alpha(bg(x,y)) = bg(x,y) \cdot 0.0001 + 0.115$$

$$\beta(bg(x,y)) = \lambda - bg(x,y) \cdot 0.01$$

The experimental result of the parameters are, $T_0 = 17$, $\gamma = \frac{3}{128}$, and $\lambda = \frac{1}{2}$. In this model, $bg(x,y)$ is the average background luminance, and $mg(x,y)$ is the contrast value calculated from the output of high-pass filtering at four directions. f_1 and f_2 model the contrast and luminance masking effects, respectively.

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Comparison of Lubin's and Daly's Human Visual System Models (I)

	Amplitude Nonlinearity	Intra-eye blurring	Re-sampling	CSF
Daly's VDP	Local Normalization	N/A	N/A	SQRI
Lubin's VDM	N/A	optics	120 pxs/deg	SQRI

	Subband Decomposition	Masking Function	Pooling
Daly's VDP	Cortex Filters	coherence/learning effect	Probability Map
Lubin's VDM	Steerable Filters	dipper effect	JND Map

- Both systems include a calibration step, a masking measurement step in subbands and a pooling step
- Calibration step:
  - Daly's model: pixel amplitude normalization using a nonlinear curve based on the luminance adaption property of human retinal neurons, and a human contrast sensitivity function (CSF) calibration, which is a complex alternative to modulation transfer function.
  - Lubin's model: blurring function, which simulations the intra-eye optical point spread function (PSF) when the fixation distance differ from the image distance and a sampling function which simulates the fixed density of cones in the fovea, based on experiments on monkeys.

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Comparison of Lubin's and Daly's Human Visual System Models (II)

	Amplitude Nonlinearity	Intra-eye blurring	Re-sampling	CSF
Daly's VDP	Local Normalization	N/A	N/A	SQRI
Lubin's VDM	N/A	optics	120 pxs/deg	SQRI

	Subband Decomposition	Masking Function	Pooling
Daly's VDP	Cortex Filters	coherence/learning effect	Probability Map
Lubin's VDM	Steerable Filters	dipper effect	JND Map

- Masking step:
  - In both models, masking functions are applied to the intensity of spatial-frequency coefficients obtained by orientation-related filter banks.
  - Daly uses Watson's cortex filters, which are performed in the DFT domain.
    - divide the whole DFT spectrum into 5 circular subbands and each subband is divided into 6 orientation bands.
    - boundary of subbands are step functions convolved with Gaussian.
    - In total 31 subbands.
  - Lubin uses the steering myramid filters, which are similar to an extended wavelet decomposition.
    - 7 spatial-frequency decomposition and 4 orientation decomposition.
    - In total, 28 subbands.
  - As for the masking functions:
    - Daly uses a function that is controlled by the type of image (noise-like or sine-waves) and the number of learning (the visibility of a fixed change pattern would increase if the viewer observes it for multiple times).
    - Lubin uses a function considering the dipper effect

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Comparison of Lubin's and Daly's Human Visual System Models (III)

	Amplitude Nonlinearity	Intra-eye blurring	Re-sampling	CSF
Daly's VDP	Local Normalization	N/A	N/A	SQRI
Lubin's VDM	N/A	optics	120 pxs/deg	SQRI

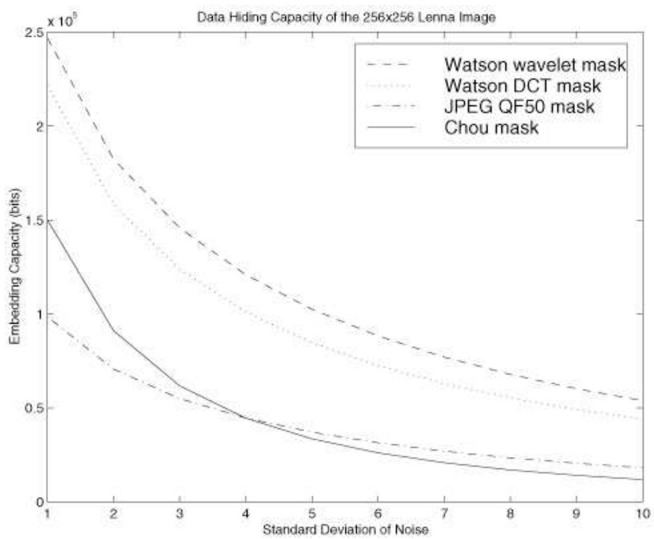
	Subband Decomposition	Masking Function	Pooling
Daly's VDP	Cortex Filters	coherence/learning effect	Probability Map
Lubin's VDM	Steerable Filters	dipper effect	JND Map

- CSF and masking functions are the most important parameters in deciding the masking effect of images.
  - CSF can be interpreted as a calibration function which is used to normalize the different perceptual importance in different spatial-frequency location.
  - Masking funcitons determine how much change is allowed in each spatial-frequency location based on its values
- Pooling:
  - Daly's result – Probability map of visibility
  - Lubin's model – a map of the JND unit value of each pixel. The distance measure is calculated based on the Minkowski metric of the output of masking function (Q is set to 2.4).

$$D_j = \{\sum_{k=1}^{m} |T_{j,k}(s_1) - T_{j,k}(s_2)|^Q\}^{\frac{1}{Q}}$$

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Watermarking capacity of power-constrained noisy environments



$\sigma_{noise} = 5$

WW: 102490 bits
WD: 84675 bits
JPG: 37086 bits
Chou: 33542 bits

Reference:
Zero-error capacity
JPG: 28672 bits

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

E 6886 Topics in Signal Processing: Multimedia Security Systems

Resources: Copyright Protection Forum

- The Copyright Protection Technical Working Group (CPTWG) : http://cptwg.org
- The Intellectual Property Management and Protection Group of the Moving Picture Experts Group (ISO/IEC JTC1/SC/29/WG11, IPMP group at MPEG) : http://www.cselt.it/mpeg and http://www.mpeg.org
- TV Anytime Forum: http://www.tv-anytime.org
- Digital Versatile Disk Forum: http://www.dvdforum.org
- Secure Digital Music Initiative's charter: http://www.sdmi.org
- Open Platform Initiative for Multimedia Access: http://www.cselt.it/ufv/leonardo/opima
- Digital Audio-Visual Council: http://www.davic.org

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Resources: Books

- Multimedia Security Technologies for Digital Rights Management
  by Wenjun Zeng, Heather Yu and Ching-Yung Lin (April 2006)
- Digital Watermarking
  by Ingemar Cox, Jeffrey Bloom, Matthew Miller (Oct. 2001)
- Information Hiding Techniques for Steganography and Digital Watermarking
  by Stefan Katzenbeisser and Fabien A. P. Petitcolas (Jan. 2000)
- Image and Video Database: Restoration, Watermarking and Retrieval
  by Hanjalic, Langelaar, Van Roosmalen and Biemond (July 2000)

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Resources: Papers

- H. Yu, D. Kundur, and C.-Y. Lin, "Spies, Thieves, and Lies: The Battle for Multimedia in the Digital Era," *IEEE Multimedia*, Vol.8, No. 3, July 2001.
- G. W. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting Publicly Available Images with a Visible Image Watermark," *SPIE Optical Security and Counterfeit Deterrence Techniques*, Vol. 2659, Jan. 1996.
- C.-H. Chou and Y.-C. Li, "A Perceptually Tuned Subband Image Coder Based on the Measure of Just-Noticeable-Distortion Profile," IEEE Trans. on Circuits and Systems on Video Technology, Vol. 5, No. 6, pp. 467-476, Dec. 1995.
- S. Daly, "The Visible Differences Predictor: An Algorithm for the Assesment of Image Fidelity," Digital Images and Human Vision, A. B. Watson, ed., pp. 179-206, MIT Press, 1993.
- J. Lubin, "The Use of Psychophysical Data and Models in the Analysis of Display System Performance," Digital Images and Human Vision, A. B. Watson, ed., pp 163-178, MIT Press, 1993.
- A. B. Watson, "DCT Quantization Matrices Visually Optimized for Individual Images," Proceeding of SPIE, Vol. 1913, pp. 202-216, 1993.
- A. B. Watson, G. Y. Yang, J. A. Solomon and J. Villasenor, "Visibility of Wavelet Quantization Noise," IEEE Trans. on Image Processing, Vol. 6, No. 8, August 1997.
- I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image Processing*, Vol. 6, No. 12, Dec. 1997.
- C.-Y. Lin, M. Wu, J. Bloom, M. L. Miller, I. J. Cox and Y. M. Lui, "Rotation, Scale, and Translation Resilient Watermarking for Images," *IEEE Trans. on Image Processing, Vol. 10, No. 5, May 2001.*
- F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding: A Survey," *Proceedings of the IEEE*, Vol. 87, No. 7, July 1999.

© 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.