Recent Trends on Multimedia Security

Ching-Yung Lin
IBM T. J. Watson Research Center

Outline

- Security in Digital Cinema and Next-Generation DVD Digital Rights Management
- Information Hiding Capacity and Human Vision System
- Enterprise Digital Rights Management

Outline

- Security in Digital Cinema and Next-Generation DVD Digital Rights Management
- Information Hiding Capacity and Human Vision System
- Enterprise Digital Rights Management

Digital Cinema

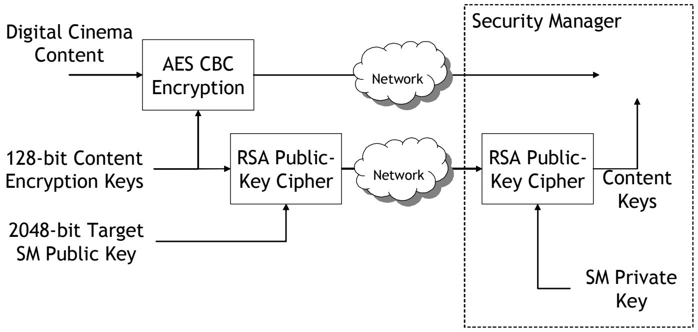
- Start of Digital Cinema: June 1999 → Start Wars: Episode I
- Digital Cinema Technology Committee (DC28): Jun3 2000 by the Society of Motion Picture and Television Engineers (SMPTE).
- Digital Cinema Specification: July 2005 by Disney, Fox, MGM, Paramount, Sony, Universal, and Warner Bros.
- Security in DC:
  - More restrictions in when, how, where the film can be played.
  - Traditionally, the business agreements have been protected by
    - legal and social mechanism.
    - the cost of copying device.
  - Technical barrier has been removed.

Digital Cinema Specification

- ❑ Images are represented in JPEG 2000.
- ❑ 2K (2048x1080) and 4K (4096x2160) at frame rates of 24 fps.
- ❑ 2K for 48 fps.
- ❑ Each pixel is represented with 36 bits: 12 bits in each of 3 color dimensions => uncompressed bitrates of 228 MBps, 456 MBps, or 911 MBps
- ❑ Audio uses 48 kHz and 96 kHz at 24 bits per sample. It allows maximally 16 channels.

Security in Digital Cinema Specification (I)

- ❑ Strong encryption of the content – Transport Encryption:
  - AES will be used in Cipher Block Chaining (CBC) mode with a key size of 128 bits.
- ❑ Methods for securely delivering decryption keys:
  - RSA public-key cipher will be used with a 2048-bit key



Digital Cinema Content

AES CBC Encryption

Network

Security Manager

128-bit Content Encryption Keys

RSA Public-Key Cipher

Network

RSA Public-Key Cipher

Content Keys

2048-bit Target SM Public Key

SM Private Key

Security in Digital Cinema Specification (II)

- Forensics: Logging
  - Secured logs in the XML format..
- Forensics: Watermarking
  - Image Media Block (IMB):
    - image decryption and decoding
    - add and detect forensic watermark to the imagery
  - Audio Media Block (AMB):
    - audio decryptoin and formatting to synchronize the audio and convert to AES3.
    - add foresic watermark
  - Requirements:
    - Watermark needs to indicate the time of exhibition to within 15 mins. ➔ 16 bits.
    - Needs to identify the location of exhibition ➔ 19 bits.
    - Payload needs to be embedded into every 5 minutes of content.
    - Needs to survive:
      - D/A, A/D, re-sampling, re-quantization, dithering, contrast and color enhancement, scaling, letterbox, aperture control, LPF, anti-aliasing filtering, brick wall filtering, noise reduction, frame-swapping, compression, scaling, cropping, additive noise, format conversion, change in frame rate, shifting, change in aspect ratio, etc.
      - Camcorder by low bit rate compression (e.g., H.264 at 500 Kbps.).
      - D/A, A/D, RF and IF transmission, channel combination, re-sampling, pitch change, pitch preserving time scaling, data reduction coding, amplitude compression, etc..

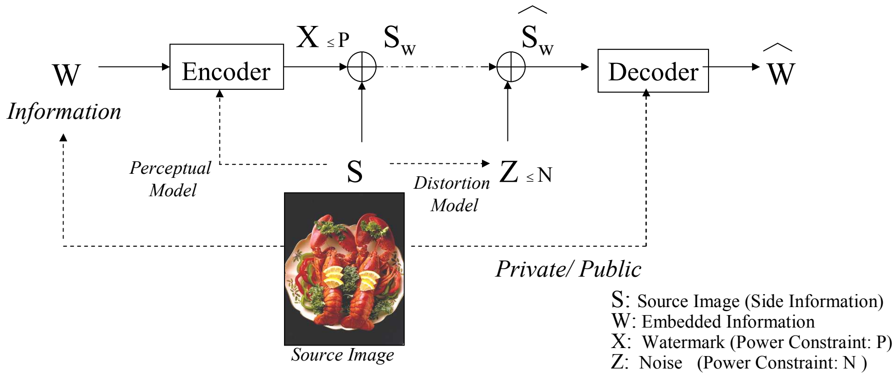
Security in Next-Generation DVD discs

- Advanced Access Content System (AACS):
  - Formed by Disney, IBM, Intel, Matsushita, Microsoft, Sony, Toshiba and Warner Bros in July 2004.
  - Based on Broadcast Encryption with a subset-difference tree using device keys and a media key block.
  - Allows unlimted, precise revocation without danger of collateral damage to innocent devices.
  - Designed to exclude clones or compromised devices.
  - Once the attacker has been detected, newly released content incorporates new media key blocks which exclude the keys known to the attackers.
  - A forensic media key block is fed into the device.

Outline

- ❑ Security in Digital Cinema and Next-Generation DVD Digital Rights Management
- ❑ Information Hiding Capacity and Human Vision System
- ❑ Enterprise Digital Rights Management

Watermarking -- Multimedia as Communication Channel



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

- Encoder may include two stages: *Coding* and *Modulation*.
- Coding: Error Correction Codes, Scrambling (use cryptographic keys).
- 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.

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

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.

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

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).

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

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

---

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

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.

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 $w_{ij} = 0.7$

Chou and Li's JND Model

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

where

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

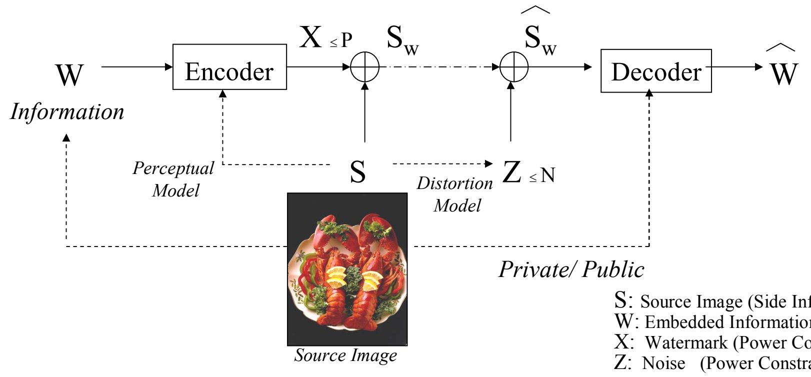
$$f_2(bg(x,y)) = \begin{cases} T_0 \cdot (1 - (bg(x,y)/127)^{0.5}) + 3 & for\ bg(x,y) \leq 127 \\ \gamma \cdot (bg(x,y) - 127) + 3 & for\ bg(x,y) > 127 \end{cases}$$

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

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

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.

Watermarking -- Multimedia as Communication Channel



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

Watermarking Capacity based on Legend Works

- Assumptions:
  - Uniform Power Constraints on Watermark and Noise
  - An image is a channel
- Channel Capacity:

Shannon (1948) (for private watermarking) , Costa (1983) (for public watermarking)

$$C = \frac{1}{2} \log_2 (1+ P/N) \quad \text{bit/sample}$$

Why Costa got the same hiding capacity regardless of the existence of the source signal?

➔ Information is shifted from the modulation coefficients to the content-dependent modulation bases.

Watermarking Capacity based on Non-uniform Power Constraints

Previous Propositions:

- Image as parallel channels?
  - Parallel Gaussian Channels – Akansu (1999), Servetto (1998), Kundur

    -- Possible Drawback: A channel needs infinite codeword length !!

Image as one channel

- Arbitrary Varying Channel (AVC, *Csiszar 1989*) – Possible Drawback: arbitrary varying

Our proposition:

- Image as a variant-state channel
- Image coefficient values are discrete

If not power-constraint, but amplitude constraints on noises,

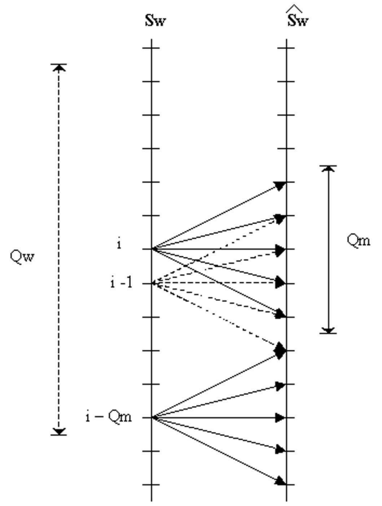
➔ Zero-Error Watermarking Capacity

Image as Communication Channel(s)

An M×N digital image can be considered as

- *Case 1*: a *variant-state discrete memoryless channel* (DMC). Transmission utilizes this channel for *M×N times*.
- *Case 2*: a mixture of Case 1 and 3. If an image is divided into B blocks with K coefficients in each block, then this image can be considered as *B parallel channels with K transmissions* in each channel.
- *Case 3*: a product of M×N *static-state* DMCs, in which each coefficient forms a DMC. Each channel can be at most transmitted *once*.

Adjacency-Reducing Mapping of Discrete Values given Bounded Noises



Adjacency-reducing mapping

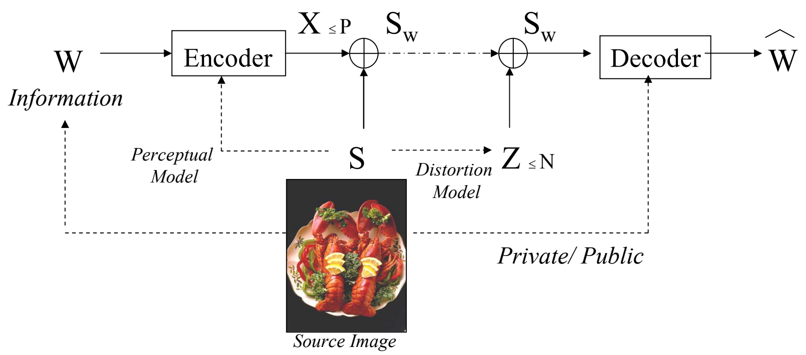
two input nodes are adjacent if there is a common output node which can be caused by either of these two.

-- Shannon *The zero-error capacity of a noisy channel*, Trans. on IT, 1956)

$$C(Q_w, Q_m) = \log_2 (\lfloor Q_w / Q_m \rfloor + 1) \text{ bits}$$

➔ *A bound for private/public watermarking*

Private Watermarking Capacity



- Image as a variant state, power-constrained discrete-value channel

Define: $\boldsymbol{X} = [X_1, X_2, \dots, X_n]^T$, $\boldsymbol{S} = [S_1, S_2, \dots, S_n]^T$

$$\boldsymbol{Y} = \boldsymbol{S_W} - \mathbf{S} = \boldsymbol{X} + \boldsymbol{Z}$$

masking function $f(.)$: $E(\boldsymbol{XX}^T) \le f(\boldsymbol{S})$

Then,

$$C = \max \quad \boldsymbol{I(X;\,Y)} \quad \text{given} \quad p(\boldsymbol{Z})$$

Private Watermarking Capacity

- Assume watermark is independent of the noise: the capacity function of a variant state, power-constrained discrete-value channel

$$C = \tfrac{1}{2} \log_2 (2\pi e)^n |f(\mathbf{S}) + E(\mathbf{ZZ}^T)| - h(\mathbf{Z})$$

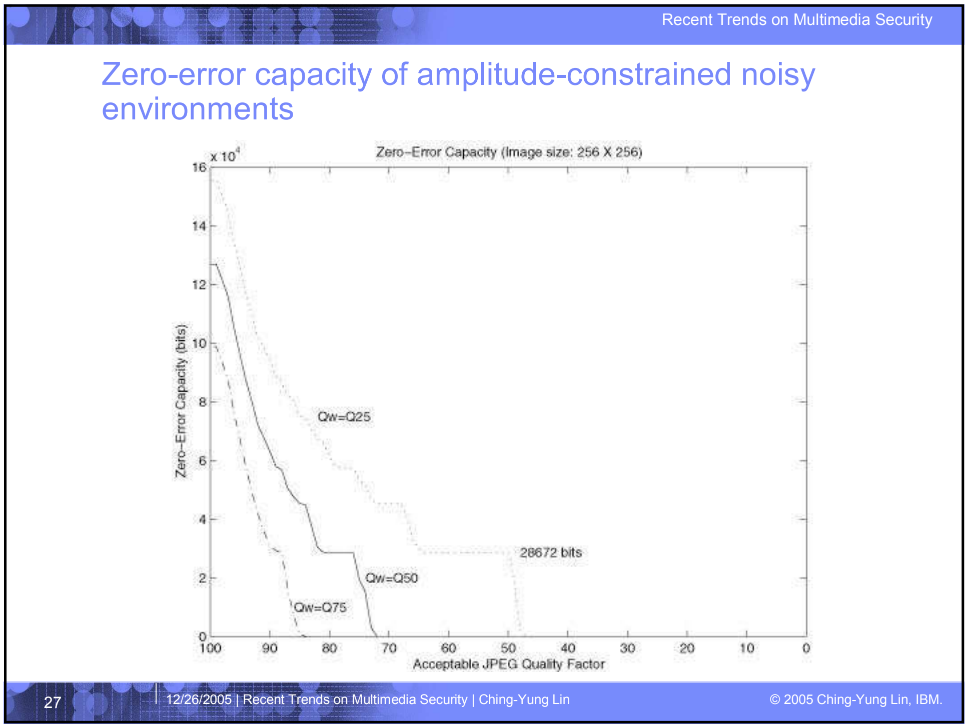
- If the noises are Gaussian distributed:

$$C_{min} = \tfrac{1}{2} |f(\mathbf{S}) + E(\mathbf{ZZ}^T)^{-1} + \mathbf{I}\,|$$

- Further, if f(**S**) is diagonal and Noise are independent of Source,

$$C = \Sigma \tfrac{1}{2} \log_2 (\, 1 + P_i/N_i) \text{ bits}$$

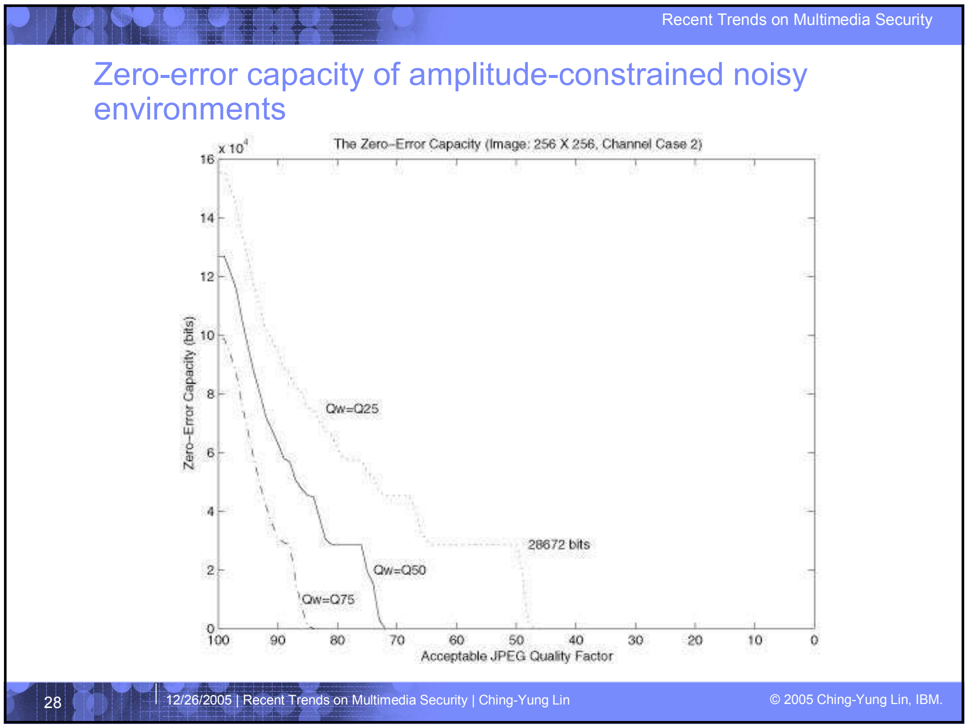
$E(\boldsymbol{XX}^T) \le f(\boldsymbol{S})$: Power constraint of watermark
$E(\boldsymbol{ZZ}^T)$: Power of noises



Recent Trends on Multimedia Security

Zero-error capacity of amplitude-constrained noisy environments

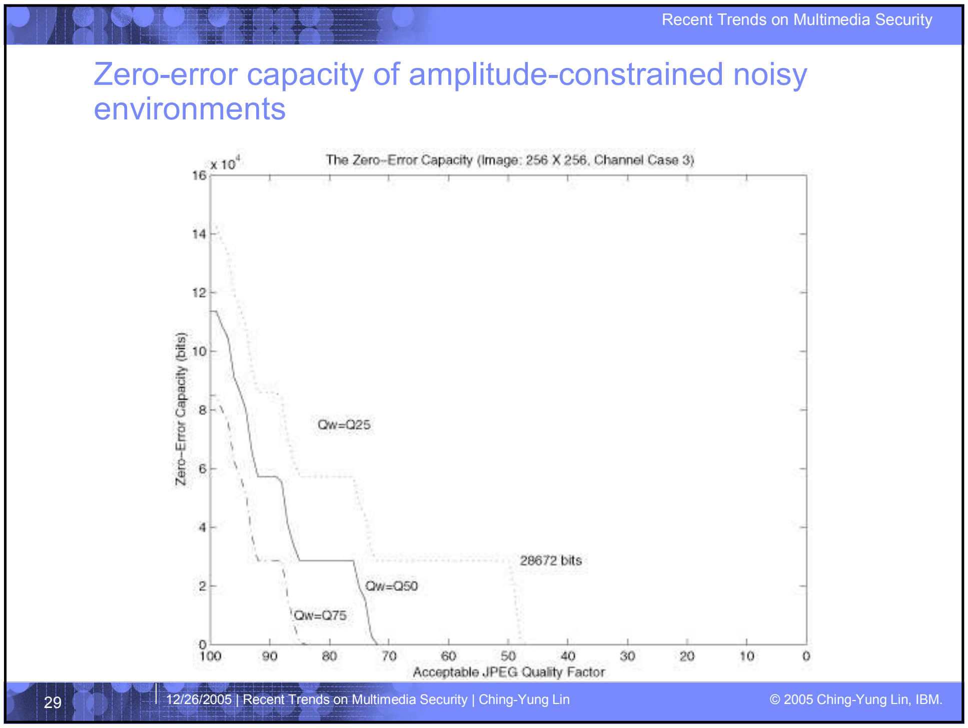
27 12/26/2005 | Recent Trends on Multimedia Security | Ching-Yung Lin © 2005 Ching-Yung Lin, IBM.



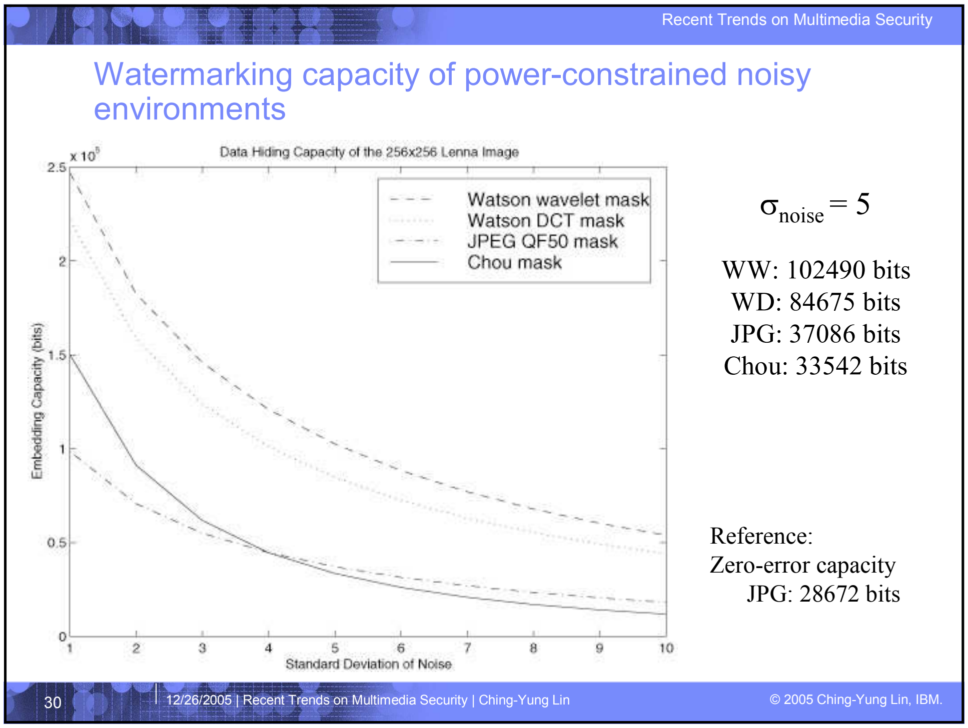
Recent Trends on Multimedia Security

Zero-error capacity of amplitude-constrained noisy environments

28 12/26/2005 | Recent Trends on Multimedia Security | Ching-Yung Lin © 2005 Ching-Yung Lin, IBM.



Zero-error capacity of amplitude-constrained noisy environments

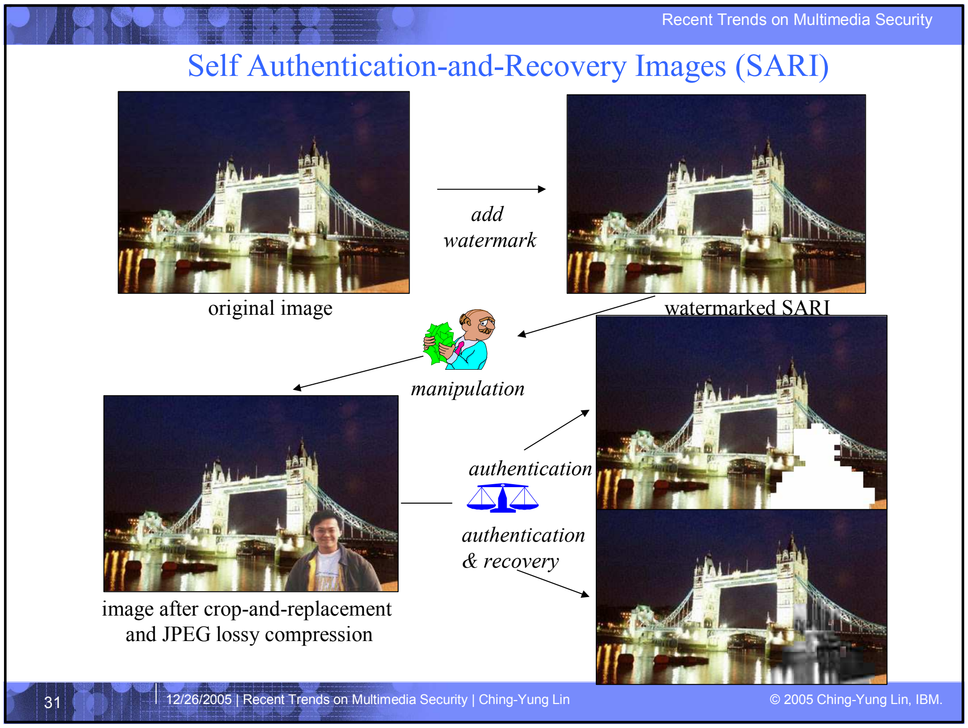


Watermarking capacity of power-constrained noisy environments

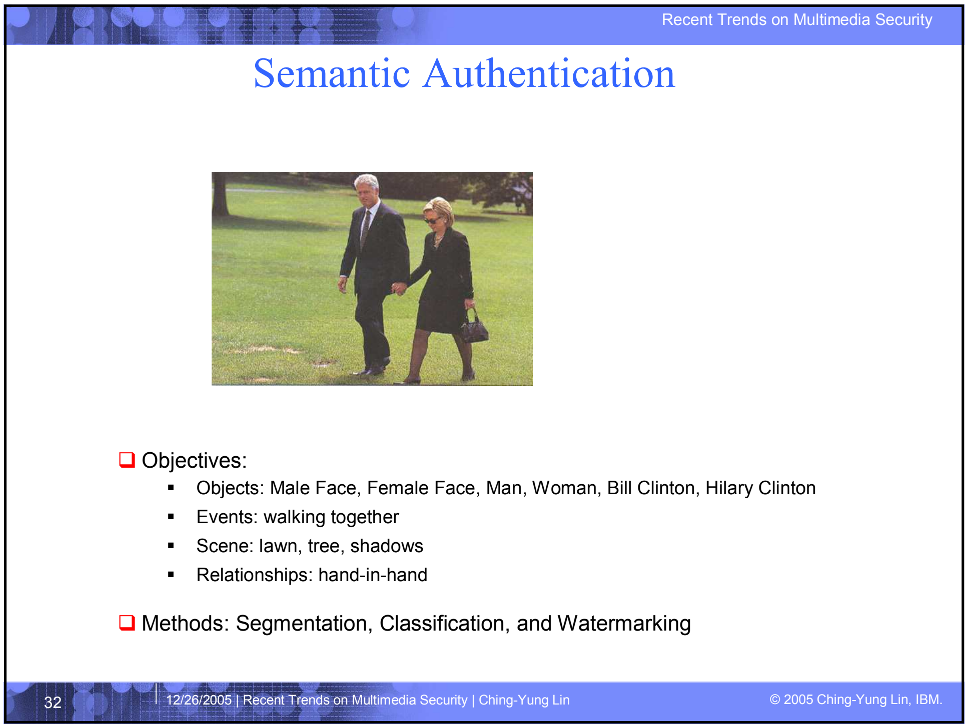
$\sigma_{\text{noise}} = 5$

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

Reference:
Zero-error capacity
JPG: 28672 bits

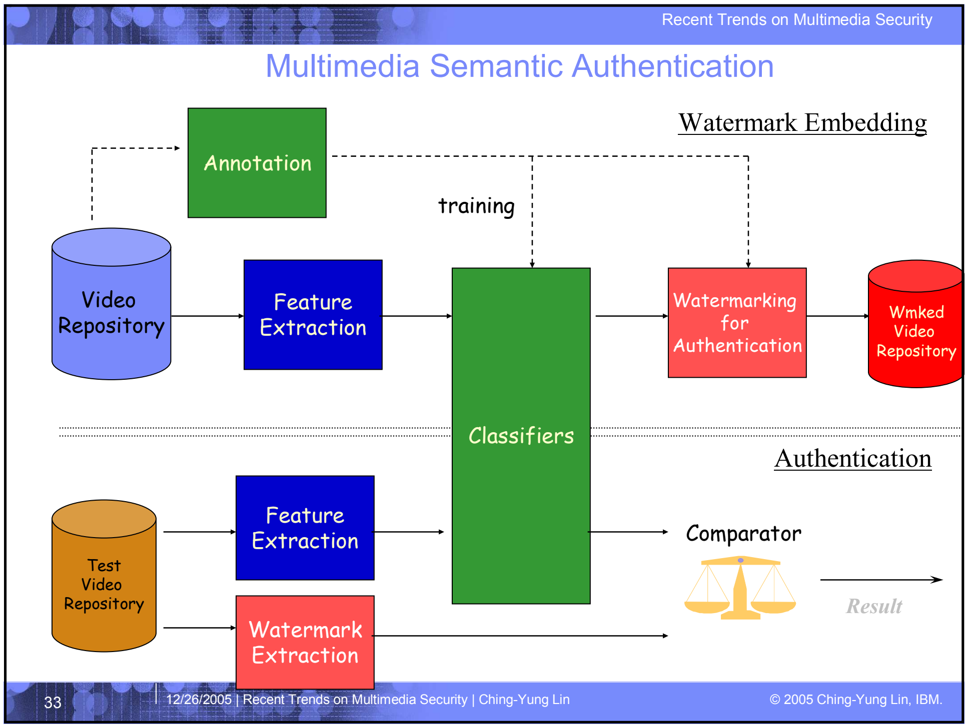


Self Authentication-and-Recovery Images (SARI)

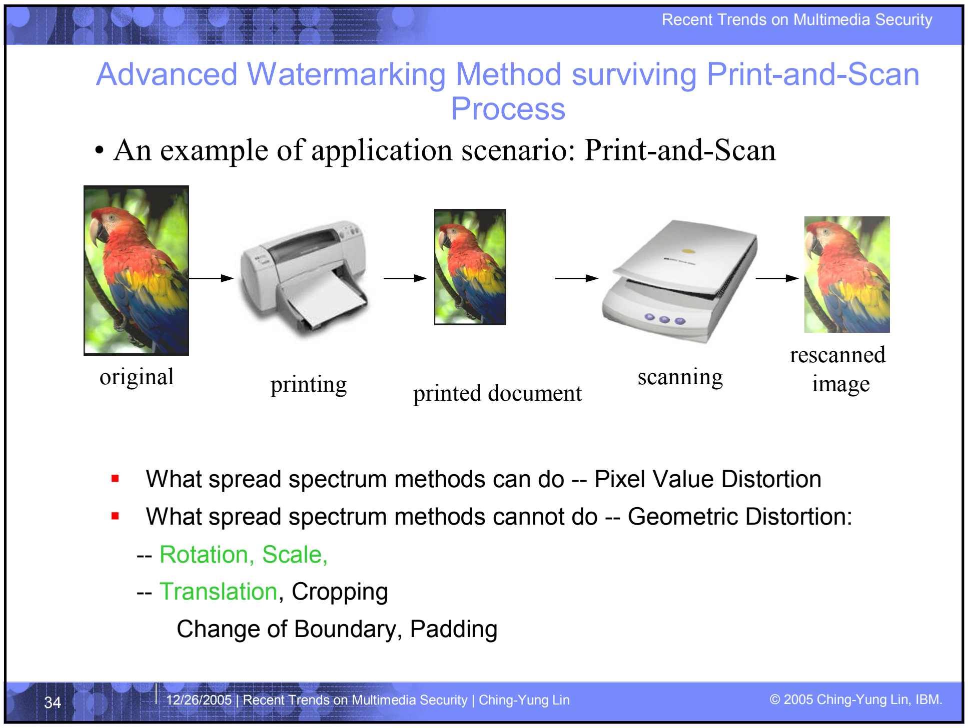


Semantic Authentication

- ❑ Objectives:
  - Objects: Male Face, Female Face, Man, Woman, Bill Clinton, Hilary Clinton
  - Events: walking together
  - Scene: lawn, tree, shadows
  - Relationships: hand-in-hand
- ❑ Methods: Segmentation, Classification, and Watermarking



Multimedia Semantic Authentication



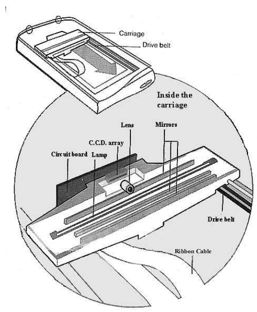
Advanced Watermarking Method surviving Print-and-Scan Process

- An example of application scenario: Print-and-Scan

- What spread spectrum methods can do -- Pixel Value Distortion
- What spread spectrum methods cannot do -- Geometric Distortion:
  - -- Rotation, Scale,
  - -- Translation, Cropping

    Change of Boundary, Padding

Pixel Value Distortion



Properties:

- Blurring
- Intensity, contrast, gamma variation
- Power of noise increases at
  - edges
  - moving direction of carriage in scanner

Model:

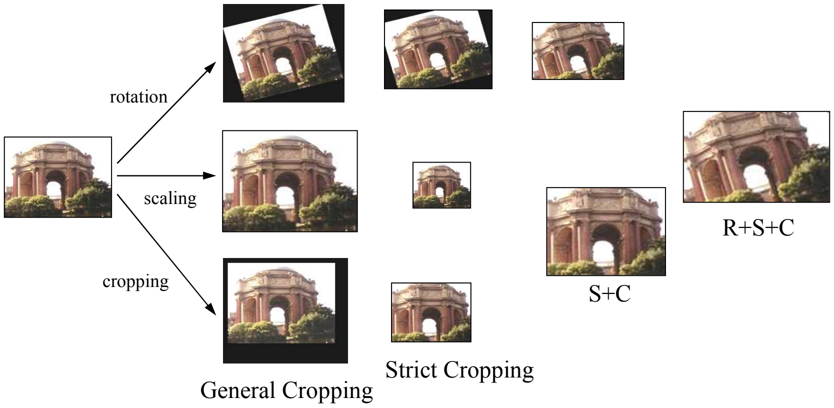
$$x'(t_1,t_2) = K\cdot[x*\tau_1+(x*\tau_2)\cdot N_1]$$

K: detector responsivity, τ_1: Low pass filter, τ_2 : High pass filter, N_1: Gaussian Noise

$$K(x)=\alpha\cdot(x-\beta_x)^\gamma+\beta_K+N_2(x)$$

Designing Robust Watermarking against Geometric Distortion

- Example of Rotation, Scaling, and Cropping



- Some solutions:
  - 2nd watermark (self-registration template): Univ. of Geneva, 1998.
  - Recognizable structure: Kutter, 1998.
  - Invariant coefficients: O'Ruanaidh, 1998; Lin et. al., 2000

Continuous Fourier coefficients of continuous images after RSC

- Rotation in time => Rotation in frequency

$$x_R(t_1,t_2) = x(t_1\cos\theta - t_2\sin\theta, t_1\sin\theta + t_2\cos\theta) \xleftrightarrow{F}$$
$$X(f_1\cos\theta - f_2\sin\theta, f_1\sin\theta + f_2\cos\theta) = X_R(f_1,f_2)$$

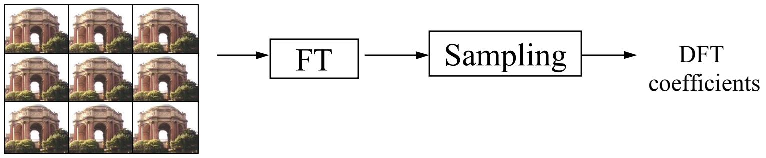
- Scaling in time => Scaling in frequency

$$x_S(t_1,t_2) = x(\tfrac{t_1}{\lambda_1}, \tfrac{t_2}{\lambda_2}) \xleftrightarrow{F} X(\lambda_1 f_1, \lambda_2 f_2) = X_S(f_1,f_2)$$

- Translation in time => Phase shift in frequency
- Information Loss in time => Noise in frequency
- Change of Image Size in time => No definition in frequency

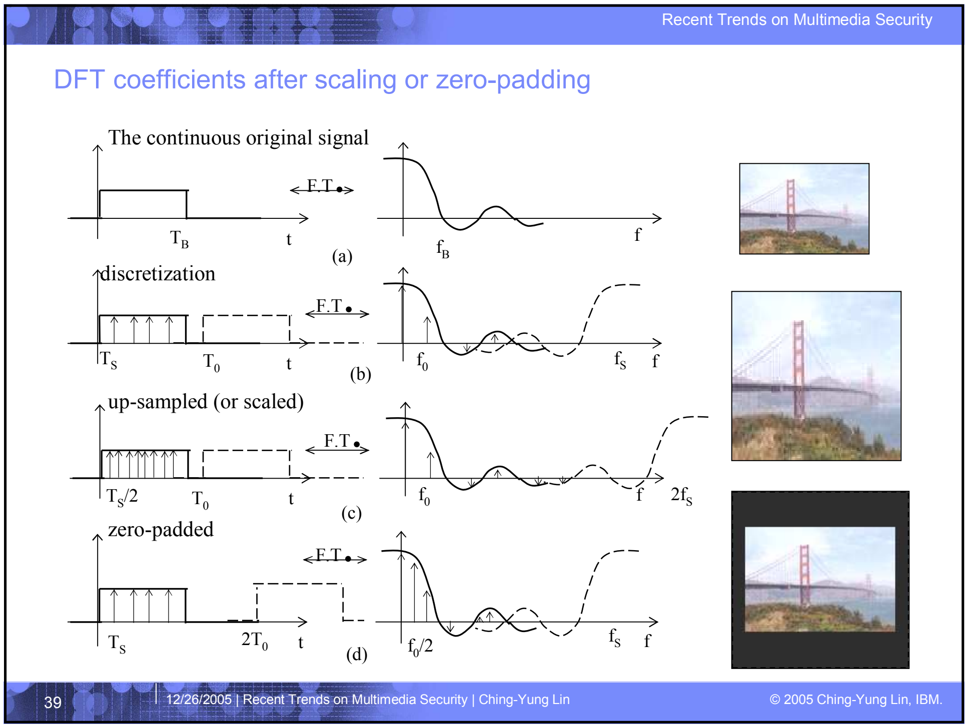
Difference between continuous Fourier Transform and Discrete Fourier Transform

- DFT: Samples of the Fourier coefficients of the repeated discrete image.



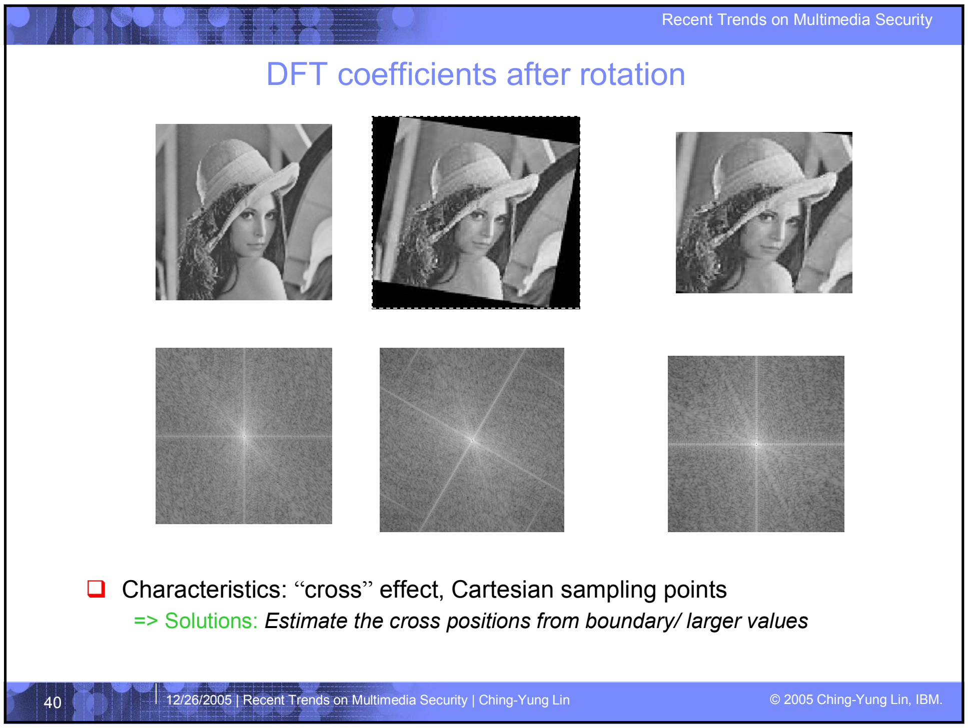
◆ Compare to the continuous domain

	Operations in the discrete image domain		
DFT Size	**Scaling**	**Cropping**	**Rotation**
Image size	Almost no effect*	Scaling + Phase shift + (Information loss)	Rotation
Fixed large size	Scaling	Phase shift + (Information loss)	Rotation
Smallest rectangle with radix-2 width/height	Scaling	Phase shift + (Information loss) + (Scaling)	Rotation
Smallest square including the whole image	Scaling in one dimension and no effect* in the other dimension	Scaling + Phase shift + (Information loss)	Rotation



Recent Trends on Multimedia Security

DFT coefficients after scaling or zero-padding



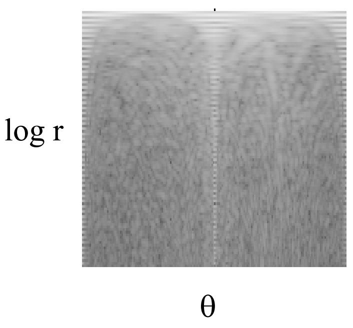
Recent Trends on Multimedia Security

DFT coefficients after rotation

- Characteristics: “cross” effect, Cartesian sampling points
  - => Solutions: *Estimate the cross positions from boundary/ larger values*

The Log-Polar Map of Fourier Coefficients

❑ Log-Polar Map



For RST (uniform scaling)

- Rotation: shift in the θ axis
- Scale without boundary change: shift in the log r axis.
- Translation: no effect on the magnitudes.
- Scale with boundary change, cropping: noise.

Projection along the log r axis:

- Cyclic shift for rotation,
- Invariant to scaling.

Algorithm for generating feature vector

Zero-padded to double image size

↓

Calculate the magnitudes of log-polar coefficients, |*Fm*|, from DFT magnitudes

↓

Summation of the log of the Fourier-Mellin magnitudes along log r axis

↓

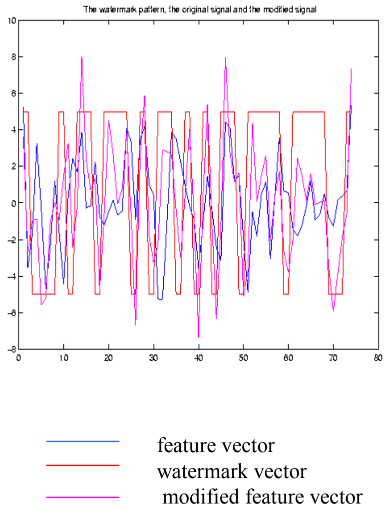
Combine values in orthogonal directions $g_1(\theta) = g_0(\theta) + g_0(\theta+90°)$

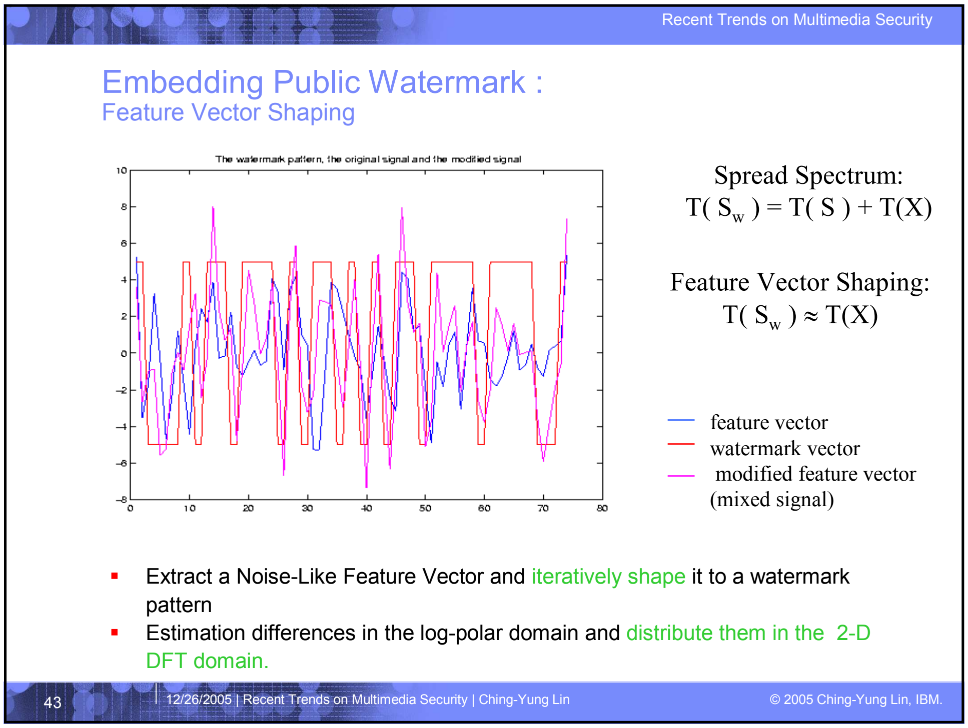
↓

Subtract $g(\theta)$ by its global mean, (whitening filter)

↓

The Feature Vector $fv = g(\theta_1, \ldots, \theta_n)$





Embedding Public Watermark :
Feature Vector Shaping

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

Feature Vector Shaping:
$T(S_w) \approx T(X)$

feature vector
watermark vector
modified feature vector (mixed signal)

- Extract a Noise-Like Feature Vector and iteratively shape it to a watermark pattern
- Estimation differences in the log-polar domain and distribute them in the 2-D DFT domain.

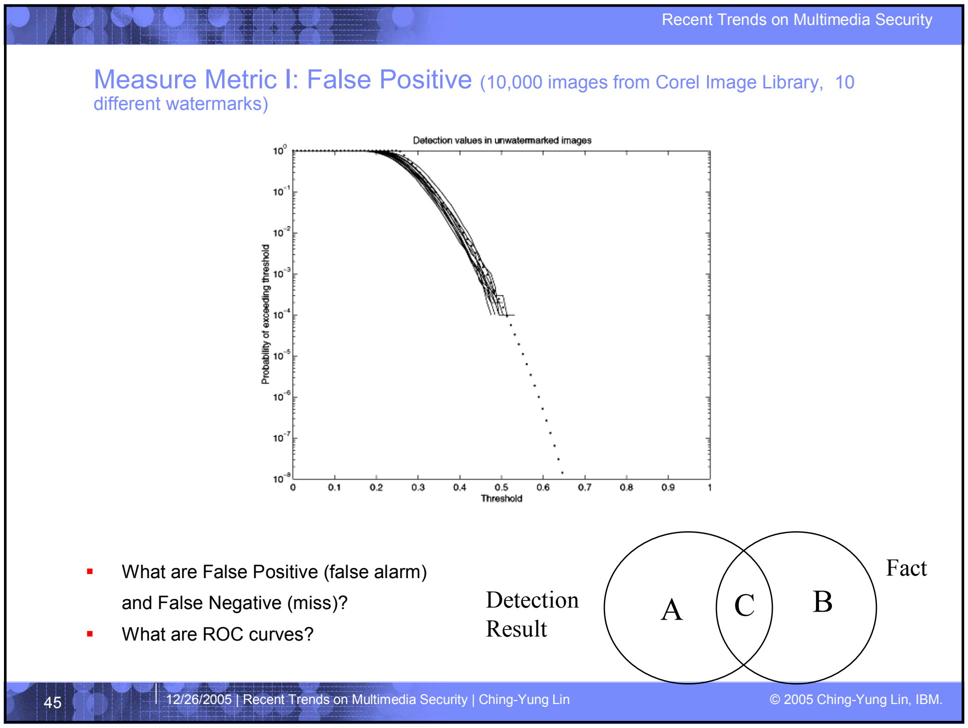
Test Example -- Print-and-Scan

Original Image [384x256]

Watermarked Image, PSNR 43.8dB, $\rho=0.84$, Z=7.02

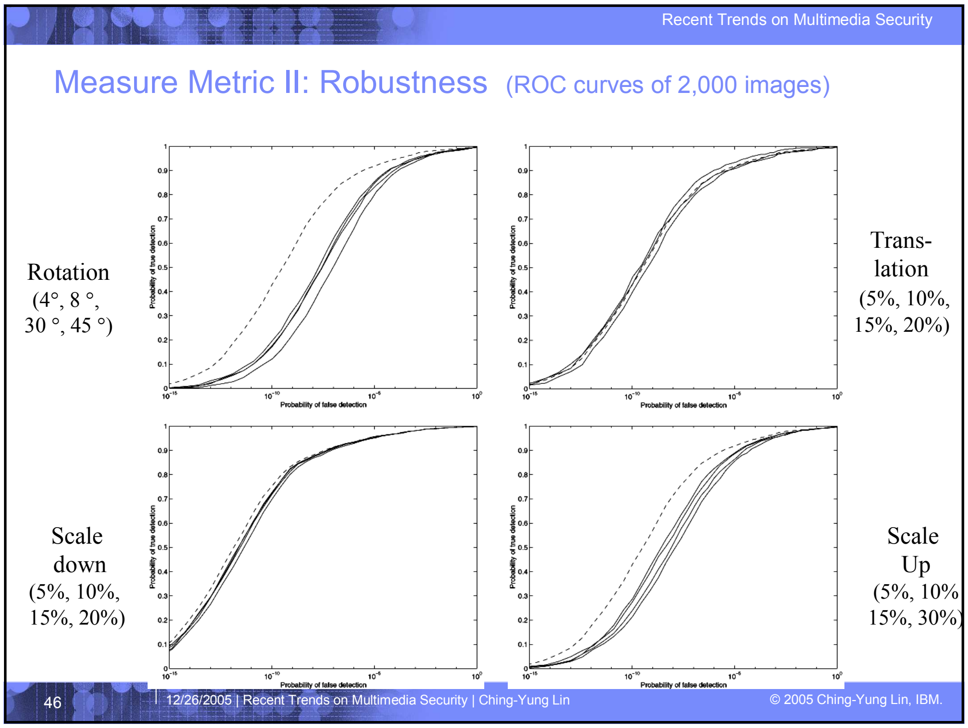
After Print & Scan, Crop to
402x266 => $\rho=0.80$, Z=6.46

After PS, Crop to 360x240 &
JPEG CR: 95:1 => $\rho=0.64$, Z=4.30



Measure Metric I: False Positive (10,000 images from Corel Image Library, 10 different watermarks)

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



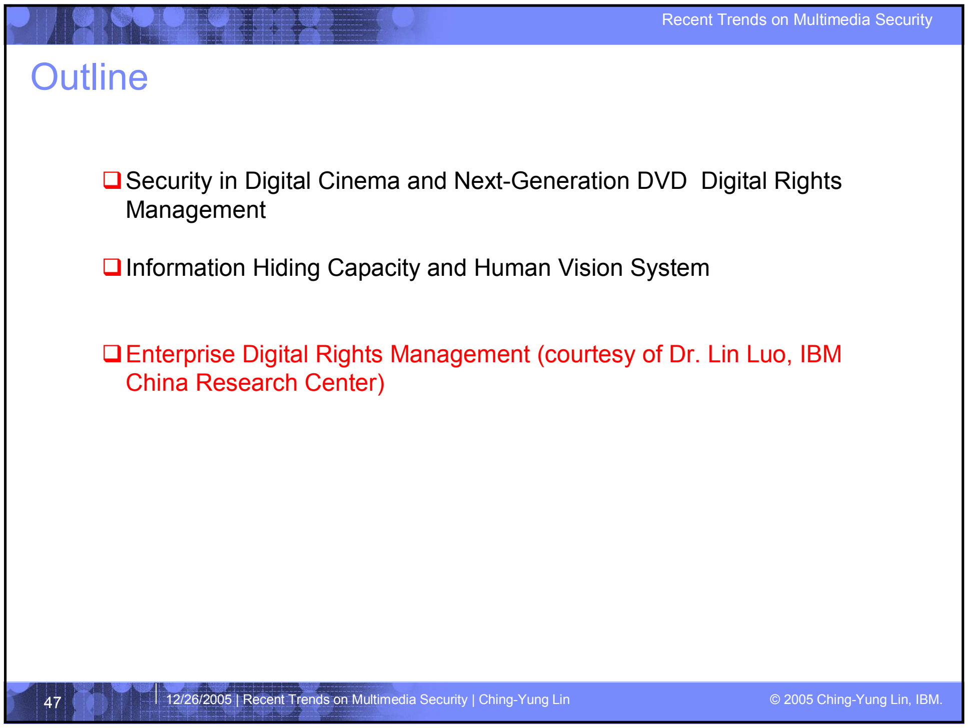
Measure Metric II: Robustness (ROC curves of 2,000 images)

Rotation
(4°, 8 °,
30 °, 45 °)

Trans-
lation
(5%, 10%,
15%, 20%)

Scale
down
(5%, 10%,
15%, 20%)

Scale
Up
(5%, 10%
15%, 30%)

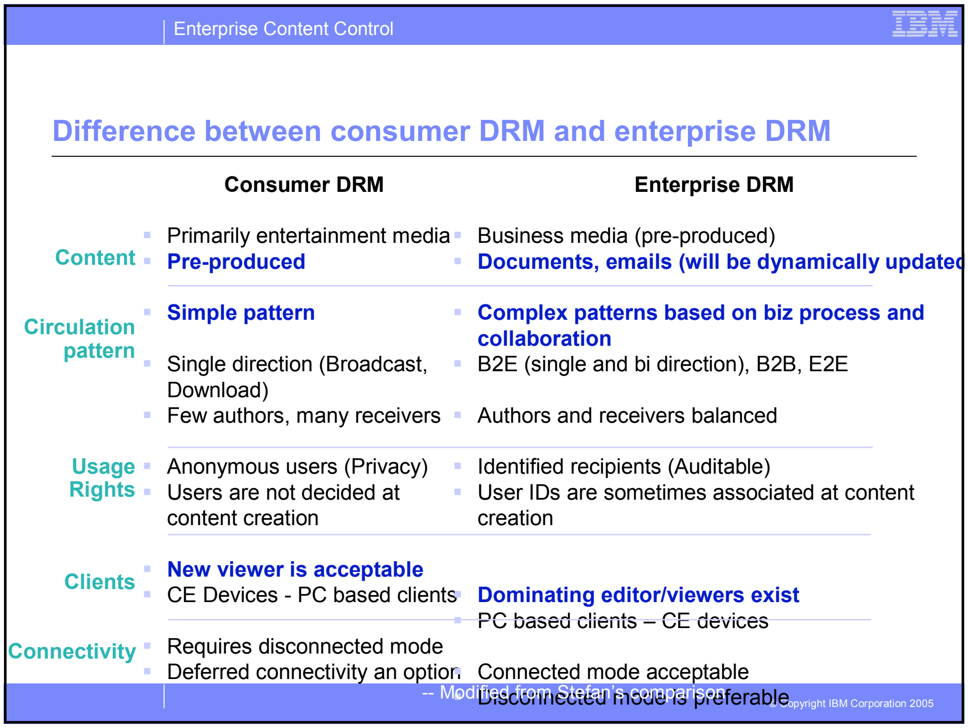


Recent Trends on Multimedia Security

Outline

- ❑ Security in Digital Cinema and Next-Generation DVD Digital Rights Management
- ❑ Information Hiding Capacity and Human Vision System
- ❑ Enterprise Digital Rights Management (courtesy of Dr. Lin Luo, IBM China Research Center)

47 | 12/26/2005 | Recent Trends on Multimedia Security | Ching-Yung Lin © 2005 Ching-Yung Lin, IBM.



Enterprise Content Control IBM

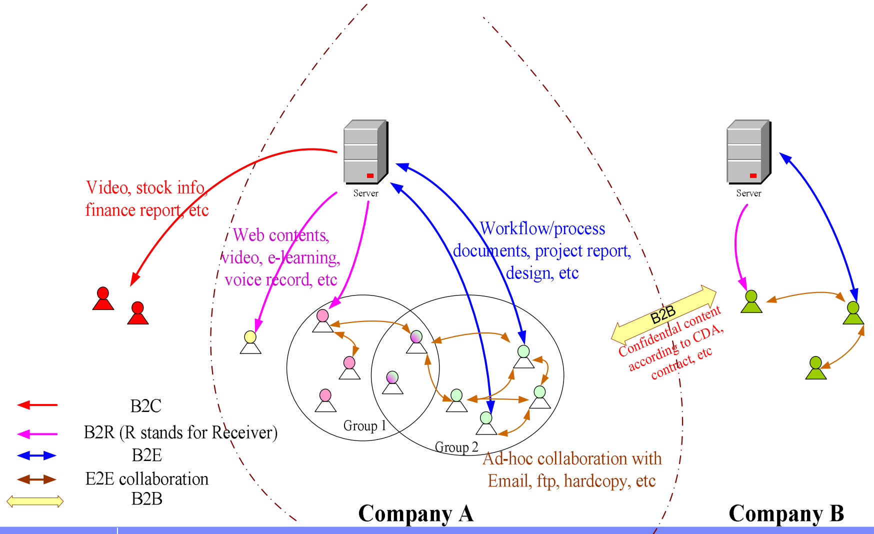
Difference between consumer DRM and enterprise DRM

	Consumer DRM	Enterprise DRM
Content	Primarily entertainment media **Pre-produced**	Business media (pre-produced) **Documents, emails (will be dynamically updated**
Circulation pattern	**Simple pattern** Single direction (Broadcast, Download) Few authors, many receivers	**Complex patterns based on biz process and collaboration** B2E (single and bi direction), B2B, E2E Authors and receivers balanced
Usage Rights	Anonymous users (Privacy) Users are not decided at content creation	Identified recipients (Auditable) User IDs are sometimes associated at content creation
Clients	**New viewer is acceptable** CE Devices - PC based clients	**Dominating editor/viewers exist** PC based clients – CE devices
Connectivity	Requires disconnected mode Deferred connectivity an option	Connected mode acceptable Disconnected mode is preferable

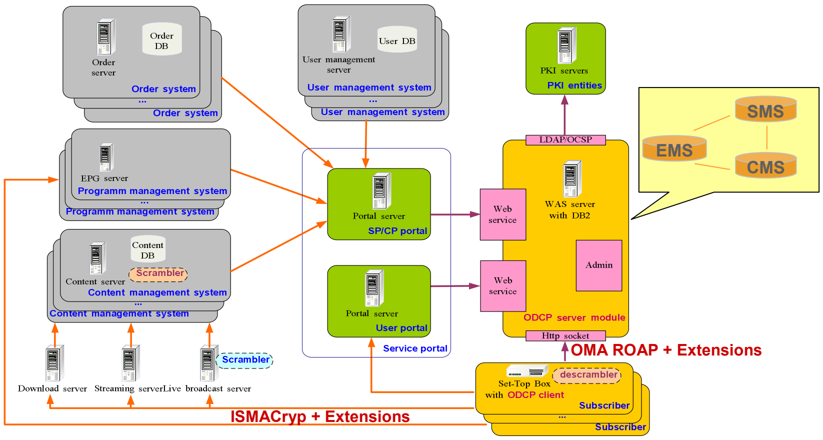
-- Modified from Stefan's comparison

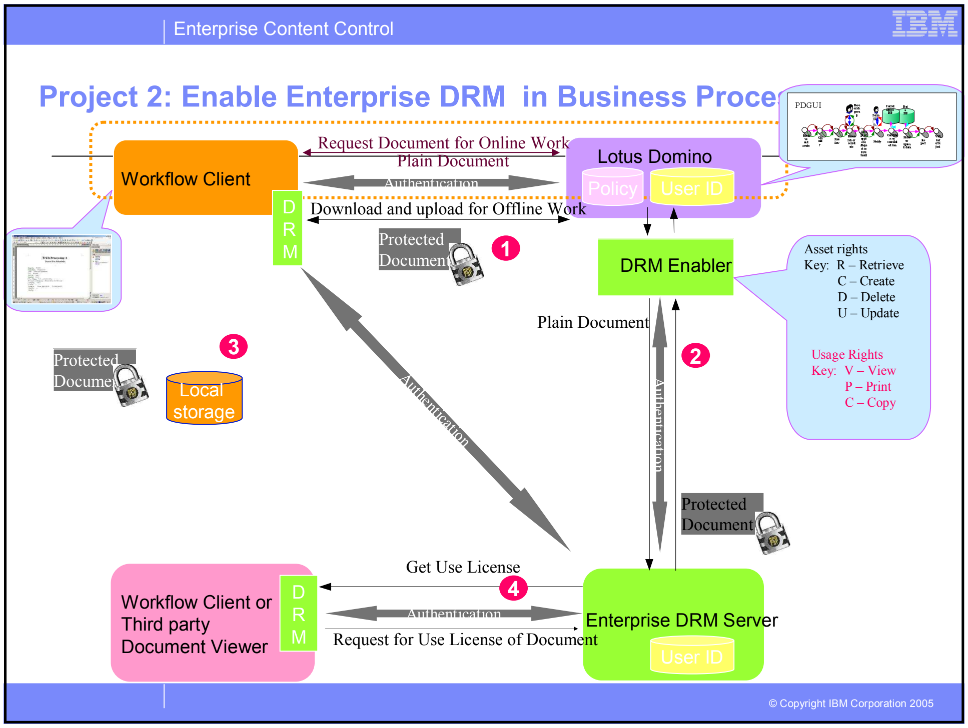
© Copyright IBM Corporation 2005

Enterprise DRM according to content circulation patterns



Project 1: DRM for IPTV (OMA-DRM based)





Enterprise Content Control

Project 2: Enable Enterprise DRM in Business Proce

PDGUI

Workflow Client

Request Document for Online Work

Plain Document

Authentication

Download and upload for Offline Work

Lotus Domino

Policy

User ID

D R M

Protected Document

1

DRM Enabler

Asset rights
Key: R – Retrieve
C – Create
D – Delete
U – Update

Usage Rights
Key: V – View
P – Print
C – Copy

Plain Document

2

Authentication

3

Protected Docume

Local storage

Authentication

Protected Document

Get Use License

4

Workflow Client or Third party Document Viewer

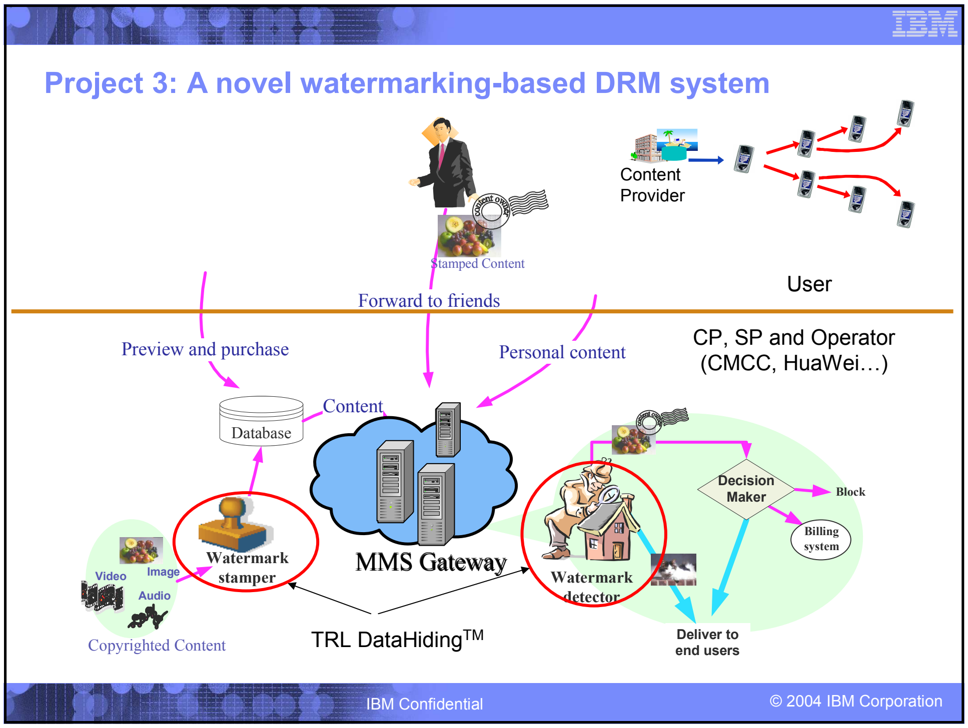
D R M

Authentication

Request for Use License of Document

Enterprise DRM Server

User ID



Project 3: A novel watermarking-based DRM system

Content Provider

Stamped Content

User

Forward to friends

Preview and purchase

Personal content

CP, SP and Operator (CMCC, HuaWei…)

Content

Database

MMS Gateway

Decision Maker

Block

Billing system

Video

Image

Audio

Watermark stamper

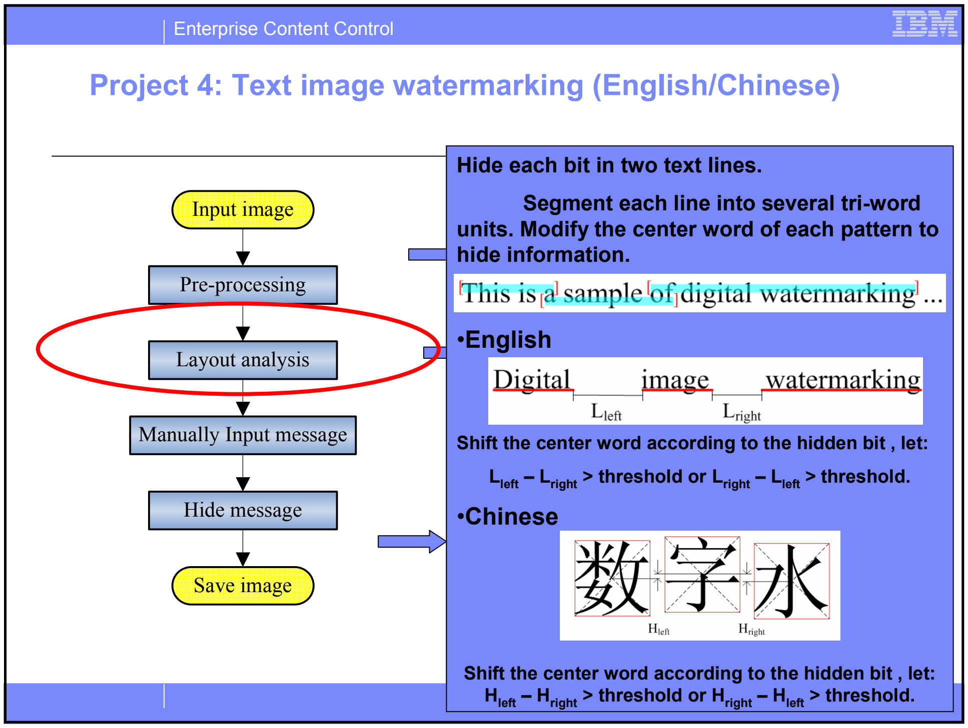
Watermark detector

Copyrighted Content

TRL DataHiding^{TM}

Deliver to end users

IBM Confidential



Enterprise Content Control

IBM

Project 4: Text image watermarking (English/Chinese)

Hide each bit in two text lines.

Segment each line into several tri-word units. Modify the center word of each pattern to hide information.

•English

Shift the center word according to the hidden bit , let:

$L_{left} – L_{right} >$ threshold or $L_{right} – L_{left} >$ threshold.

•Chinese

Shift the center word according to the hidden bit , let:
$H_{left} – H_{right} >$ threshold or $H_{right} – H_{left} >$ threshold.

Enterprise Content Control

IBM

Enterprise Asset Rights Management – what's new

- A combination of IP mgmt, Access control, Rights Mgmt and usage model analysis
- Dependent on asset formats and types
  - Sales asset, delivery asset, data asset
- Usage model is key to decide the rights mgmt pattern
  - Centralized B/S
  - Distributed assets rights enforcement
  - Heart-beat pattern
- Key mgmt
- The CRL effort in Banking industry would be the entry point
- What can ARM change the asset taxonomy

Outline

- Security in Digital Cinema and Next-Generation DVD Digital Rights Management
- Information Hiding Capacity and Human Vision System
- Enterprise Digital Rights Management
- Resources

Multimedia Security Technologies for Digital Rights Management (Elsvier, April 2006)

- **Part A Overview**
  - Chapter 1 Introduction – Multimedia security technologies past, present, and future (Scott Moskowitz, Bluespike)
  - Chapter 2 Digital Rights Management Systems (Marina Bosi, MPEG-LA)
  - Chapter 3 Putting Digital Rights Management in Context (Leonardo Chiariglione, Digital Media Project)
- **Part B Fundamentals of multimedia security**
  - Chapter 4 Multimedia encryption (Bin Zhu, Microsoft Research Asia)
  - Chapter 5 Key management for multimedia access and distribution (Amhed M. Eskicioglu, City Univ. of NY)
  - Chapter 6 Digital watermarking (Koduvayuri P. Subbalakshmi & Rajarathnam Chandramouli, Steven Institute of Technology)
  - Chapter 7 Multimedia authentication (Qibin Sun, IIR)
  - Chapter 8 Biometric based media security techniques (Anil K. Jain, Michigan State U.)
  - Chapter 9 Authorization: from access control to rights granting (Xin Wang, Content Guard)

Multimedia Security Technologies for Digital Rights Management (Elsvier, April 2006)

- **Part C Advanced topics**
  - Chapter 10 Format compliant encryption (Wenjun Zeng , Univ. of Missouri)
  - Chapter 11 Streaming media encryption (Susie Wee & John Apostolopoulos, HP Labs)
  - Chapter 12 Broadcast encryption (Jeff Lotspiech, IBM Research)
  - Chapter 13 Proxy encryption and signing (Xin Wang, Content Guard)
  - Chapter 14 3D mesh watermarking (Ryutarou Ohbuchi, University of Yamanashi)
  - Chapter 15 Steganalysis (Jessica Fridrich, (SUNY) Binhamton Univ.)
  - Chapter 16 Security in Digital Cinema (Jeffrey Bloom, Thmoson)
  - Chapter 17 Digital media forensics (Shih-Fu Chang, Columbia)
  - Chapter 18 Traitor Tracing (Hongxia Jun, IBM Research)

- **Part D Standards and Legal Issues**
  - Chapter 19 Standard activities (Xin Wang, Content Guard)
  - Chapter 20 Legal issues (Greg Stobbs, HDP)
  - Chapter 21 Conclusion and future directions (Editors)