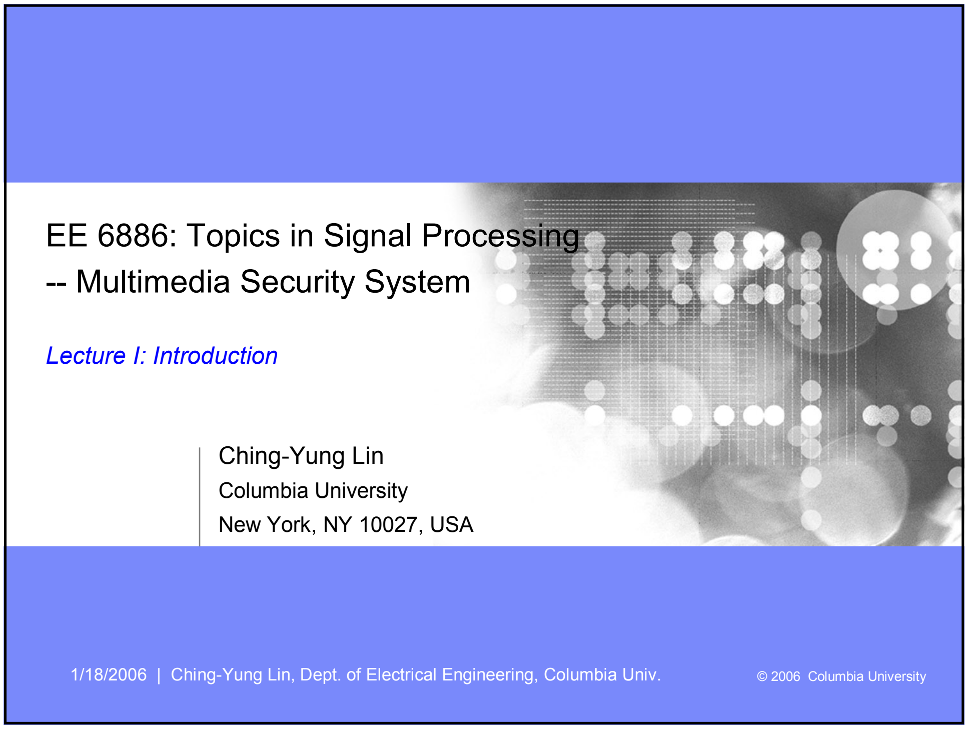
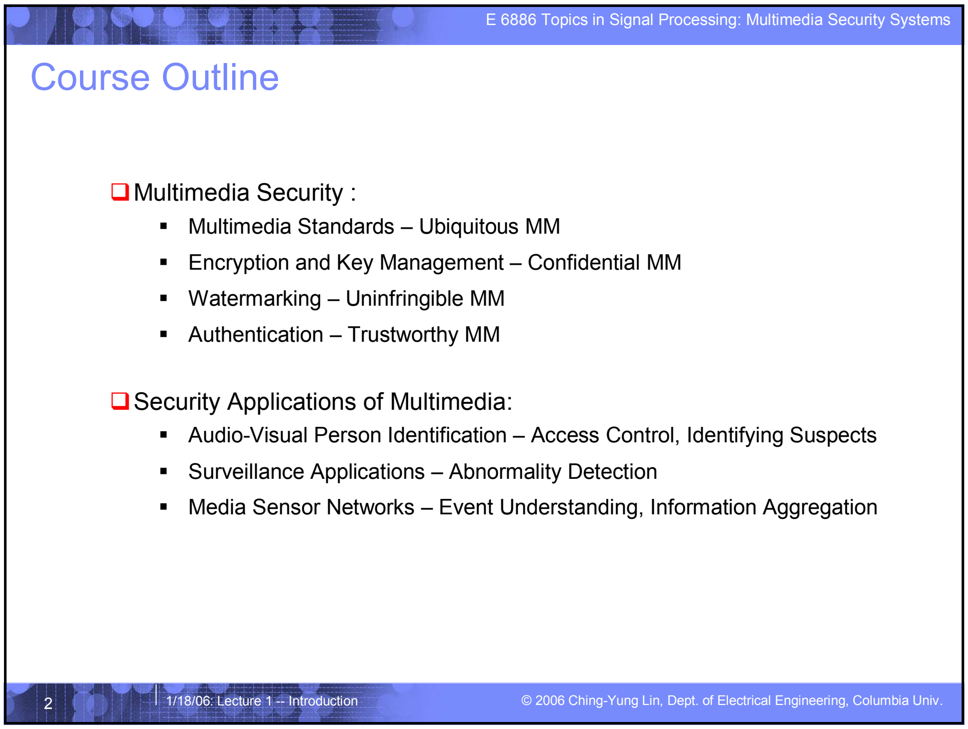


EE 6886: Topics in Signal Processing -- Multimedia Security System

Lecture I: Introduction

Ching-Yung Lin
Columbia University
New York, NY 10027, USA

1/18/2006 | Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.



Course Outline

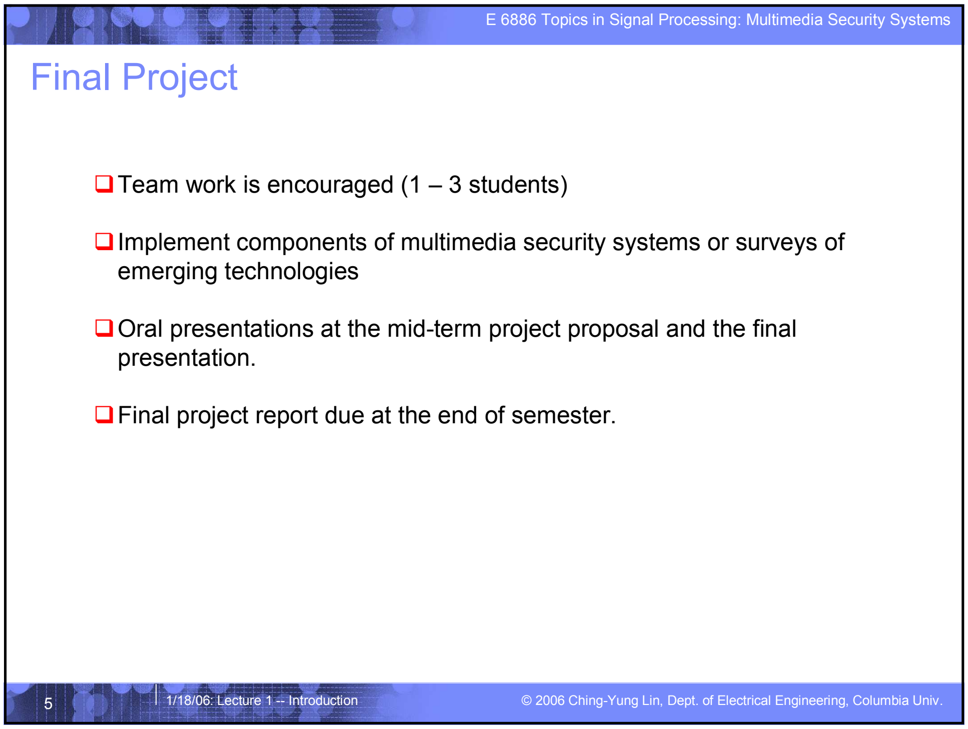
- ❑ Multimedia Security :
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – Confidential MM
  - Watermarking – Uninfringible MM
  - Authentication – Trustworthy MM
- ❑ Security Applications of Multimedia:
  - Audio-Visual Person Identification – Access Control, Identifying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

About this course

- Instructor: Ching-Yung Lin
- Email: cylin@ee.columbia.edu
- Office Hour: Wednesday 6:40 – 7:10 pm, Mudd 1312, or by appointment
- Course Webpage: http://www.ee.columbia.edu/~cylin/course/mss/
- Course Time: Wednesday 4:10 – 6:40 pm
- Course Format: Lecture 100 – 120 mins + Presentation/Discussion 20 – 40 mins
- Location: Mudd 535
- TA: TBD
- TA Office Hour: TBD
- Grading: 3 homeworks: 50%, final project: 50%

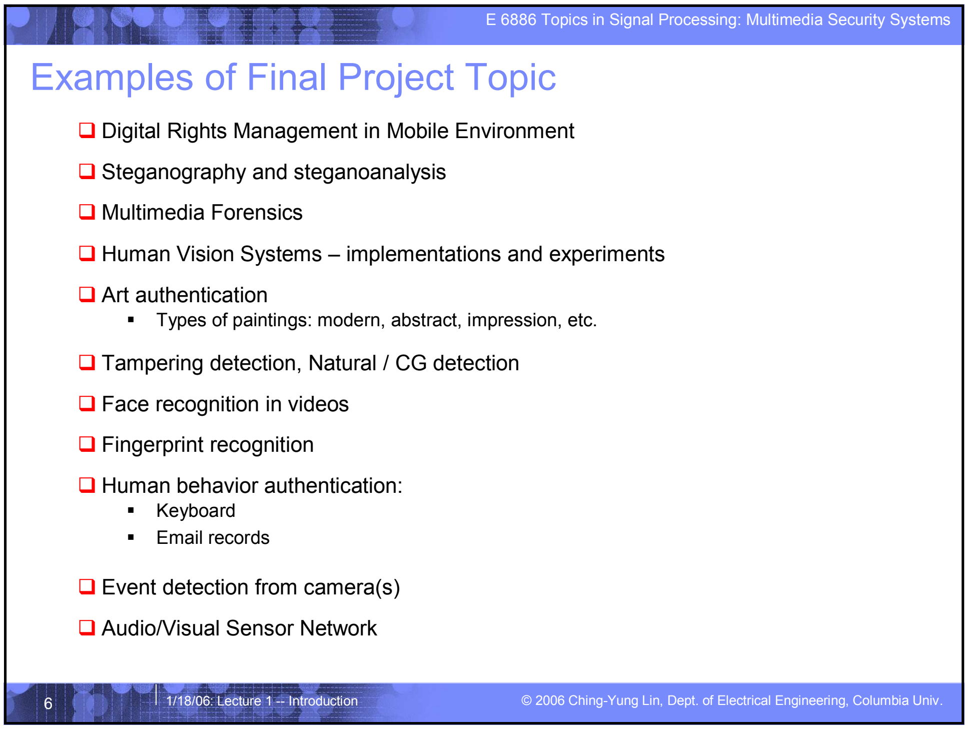
Homeworks

- HW #1: Image compression and encryption experiments.
- HW #2: Video watermarking experiments
- HW #3: Audio speaker authentication experiments
- Software Requirements: C, C++, Java, Matlab, or others
- Hardware Requirements: Windows, Unix/Linux or Mac



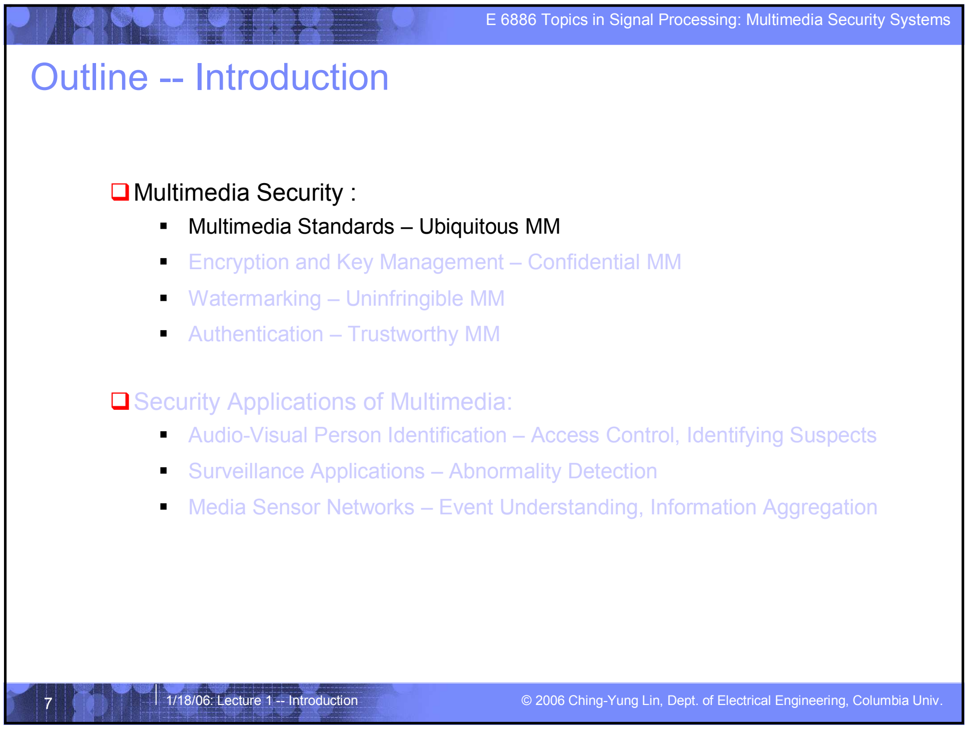
Final Project

- ❑ Team work is encouraged (1 – 3 students)
- ❑ Implement components of multimedia security systems or surveys of emerging technologies
- ❑ Oral presentations at the mid-term project proposal and the final presentation.
- ❑ Final project report due at the end of semester.



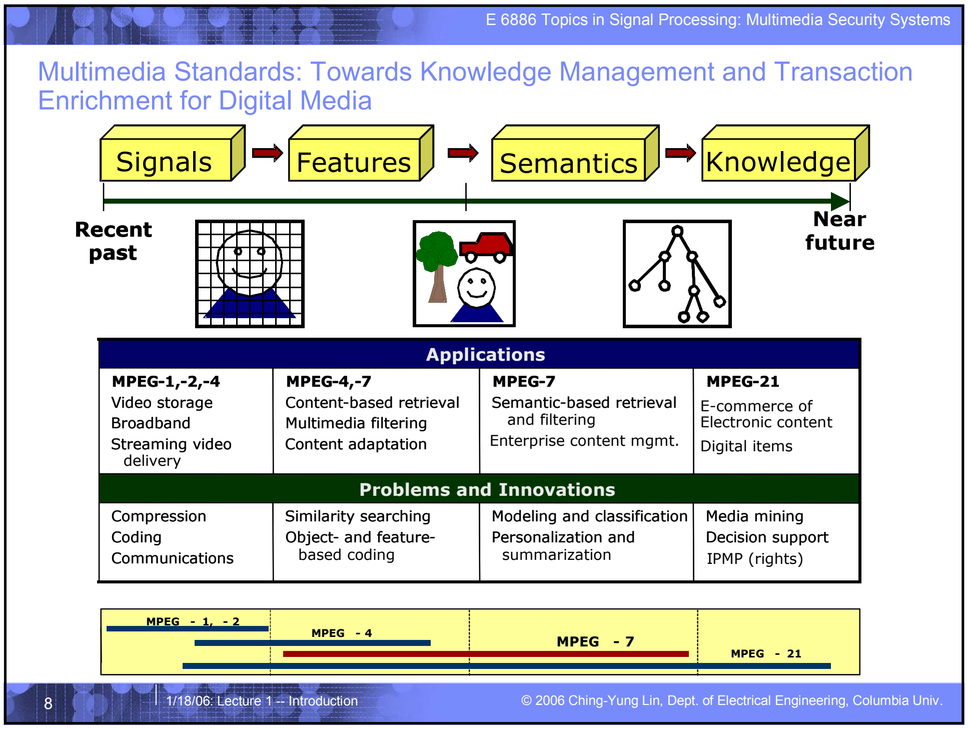
Examples of Final Project Topic

- ❑ Digital Rights Management in Mobile Environment
- ❑ Steganography and steganoanalysis
- ❑ Multimedia Forensics
- ❑ Human Vision Systems – implementations and experiments
- ❑ Art authentication
  - Types of paintings: modern, abstract, impression, etc.
- ❑ Tampering detection, Natural / CG detection
- ❑ Face recognition in videos
- ❑ Fingerprint recognition
- ❑ Human behavior authentication:
  - Keyboard
  - Email records
- ❑ Event detection from camera(s)
- ❑ Audio/Visual Sensor Network



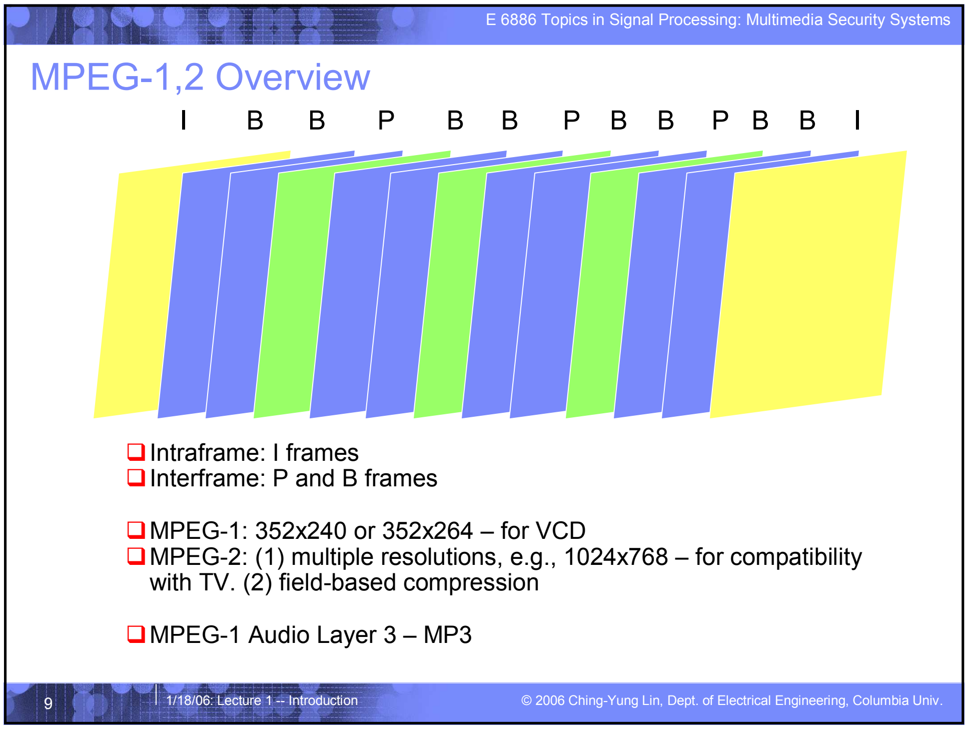
Outline -- Introduction

- ❑ Multimedia Security :
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – 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



Multimedia Standards: Towards Knowledge Management and Transaction Enrichment for Digital Media

Applications			
MPEG-1,-2,-4 Video storage Broadband Streaming video delivery	**MPEG-4,-7** Content-based retrieval Multimedia filtering Content adaptation	**MPEG-7** Semantic-based retrieval and filtering Enterprise content mgmt.	**MPEG-21** E-commerce of Electronic content Digital items
Problems and Innovations			
Compression Coding Communications	Similarity searching Object- and feature-based coding	Modeling and classification Personalization and summarization	Media mining Decision support IPMP (rights)



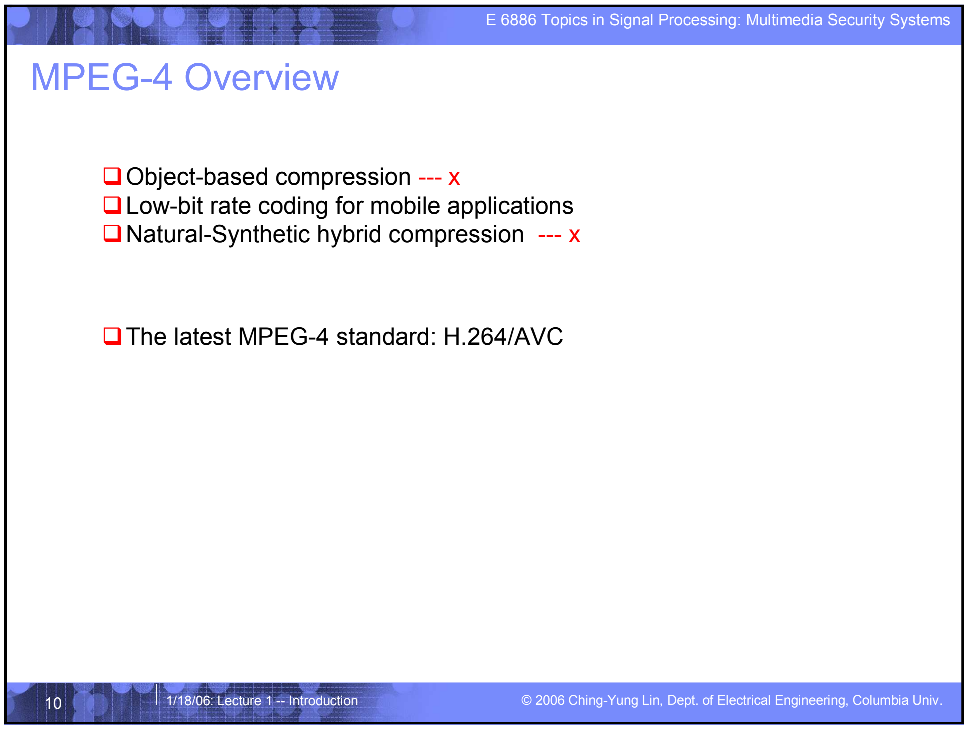
MPEG-1,2 Overview

I
B
B
P
B
B
P
B
B
P
B
B
I

- Intraframe: I frames
- Interframe: P and B frames

- MPEG-1: 352x240 or 352x264 – for VCD
- MPEG-2: (1) multiple resolutions, e.g., 1024x768 – for compatibility with TV. (2) field-based compression

- MPEG-1 Audio Layer 3 – MP3



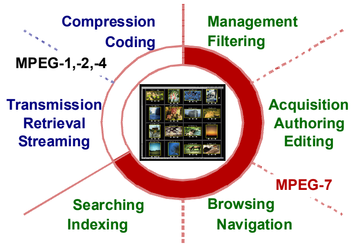
MPEG-4 Overview

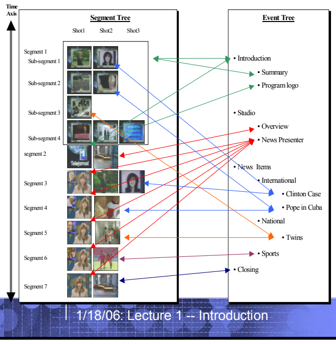
- Object-based compression --- x
- Low-bit rate coding for mobile applications
- Natural-Synthetic hybrid compression --- x

- The latest MPEG-4 standard: H.264/AVC

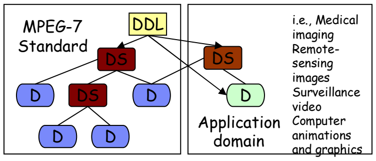
MPEG-7 Overview

XML Metadata for Multimedia Content Description

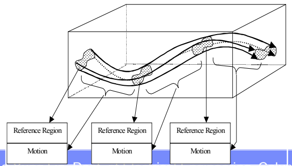




- ❑ MPEG-7 Normative elements:
  - Descriptors and Description Schemes
  - DDL for defining Description Schemes
  - Extensible for application domains



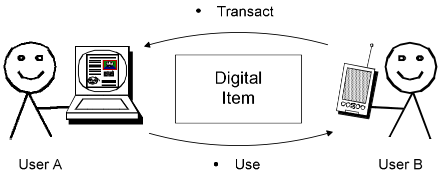
- ❑ Rich, highly granular descriptions:
  - Video segments, moving regions, shots, frames, …
  - Audio-visual features: color, texture, shape, …
  - Semantics: people, events, objects, scenes, …



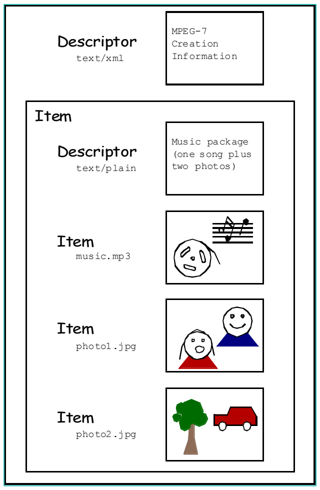
MPEG-21 Multimedia Framework

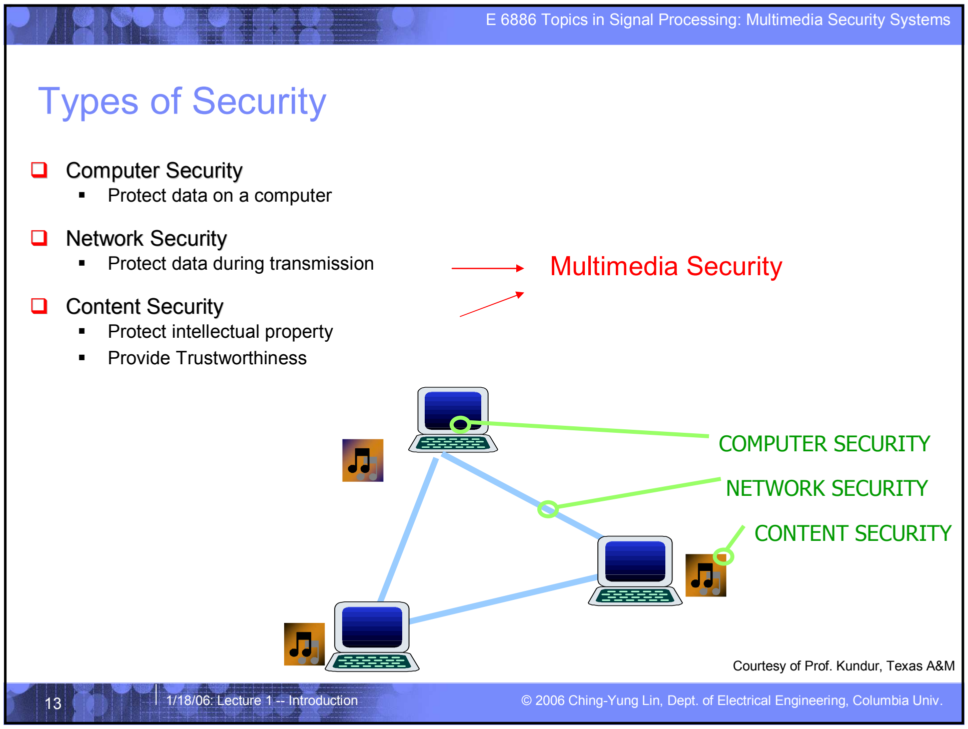
“Transactions of Digital Items”

- ❑ Users and participants in the content value chain seamlessly exchange content in form of “digital items” across networks and devices
- ❑ Framework supporting all forms of electronic content/intellectual property (video, music, learning objects, on-line reports, etc.)
- ❑ Digital Item = bundling of:
  - Essence (i.e., media resources)
  - Metadata
  - Rights expressions
  - Identifiers



Example: Digital music package





Types of Security

- ❑ Computer Security
  - Protect data on a computer
- ❑ Network Security
  - Protect data during transmission
- ❑ Content Security
  - Protect intellectual property
  - Provide Trustworthiness

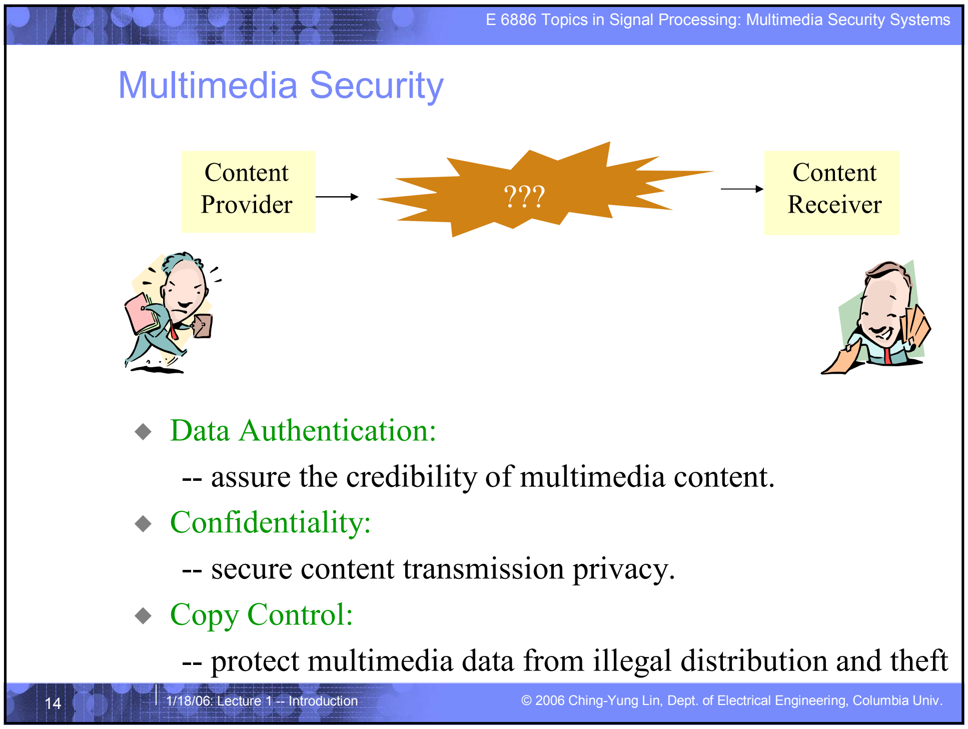
→ Multimedia Security

COMPUTER SECURITY

NETWORK SECURITY

CONTENT SECURITY

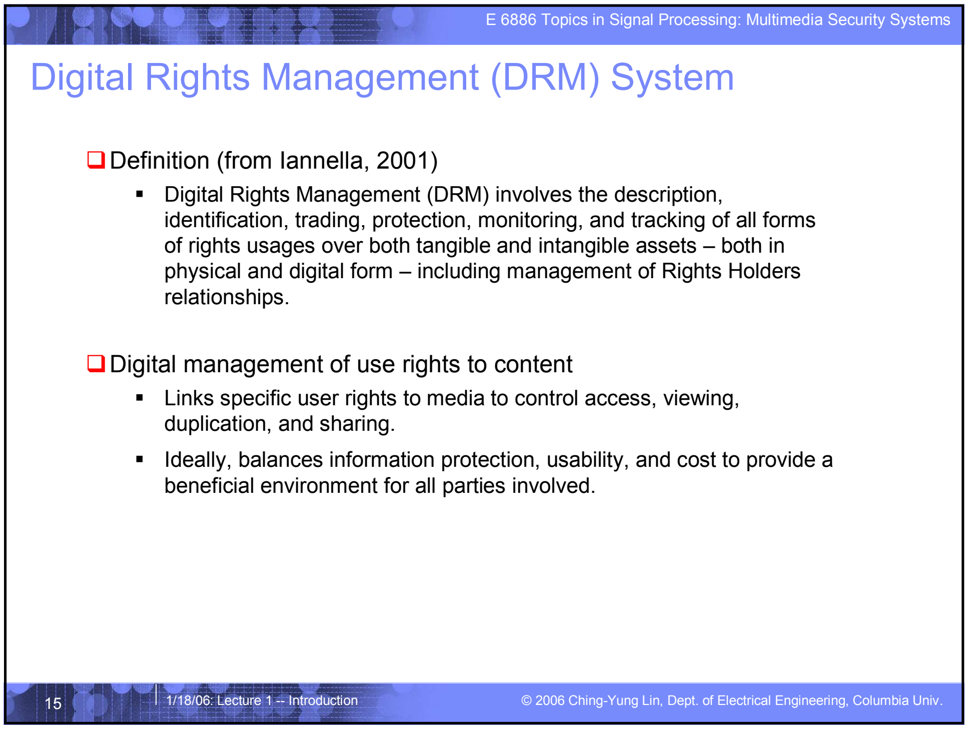
Courtesy of Prof. Kundur, Texas A&M



Multimedia Security

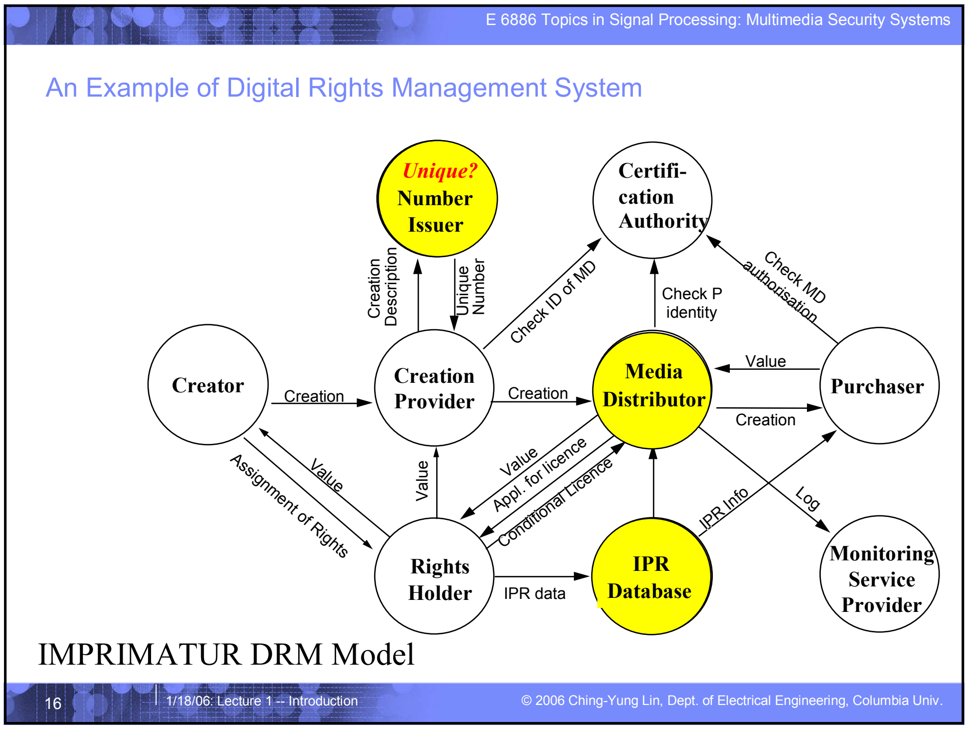
Content Provider → ??? → Content Receiver

- ◆ Data Authentication:
  -- assure the credibility of multimedia content.
- ◆ Confidentiality:
  -- secure content transmission privacy.
- ◆ Copy Control:
  -- protect multimedia data from illegal distribution and theft



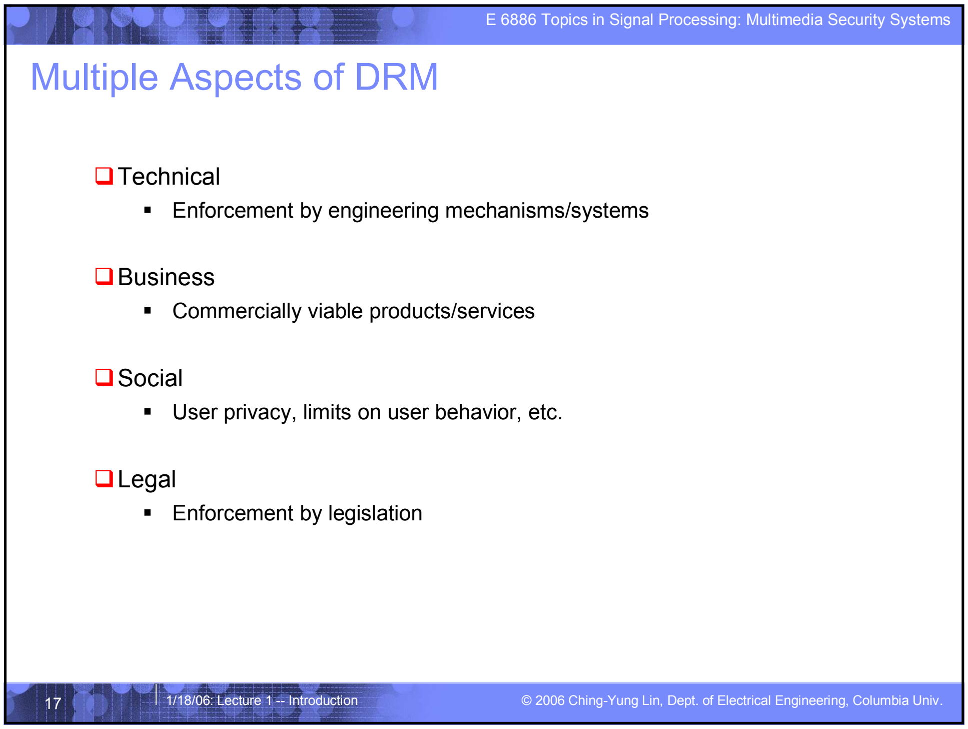
Digital Rights Management (DRM) System

- Definition (from Iannella, 2001)
  - Digital Rights Management (DRM) involves the description, identification, trading, protection, monitoring, and tracking of all forms of rights usages over both tangible and intangible assets – both in physical and digital form – including management of Rights Holders relationships.
- Digital management of use rights to content
  - Links specific user rights to media to control access, viewing, duplication, and sharing.
  - Ideally, balances information protection, usability, and cost to provide a beneficial environment for all parties involved.



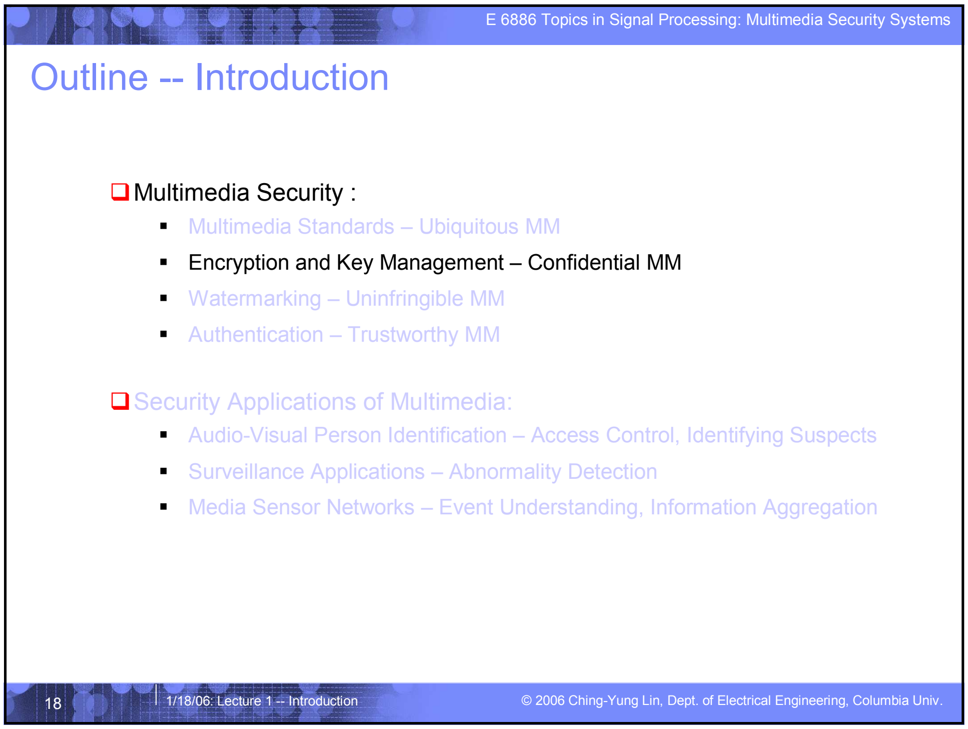
An Example of Digital Rights Management System

IMPRIMATUR DRM Model



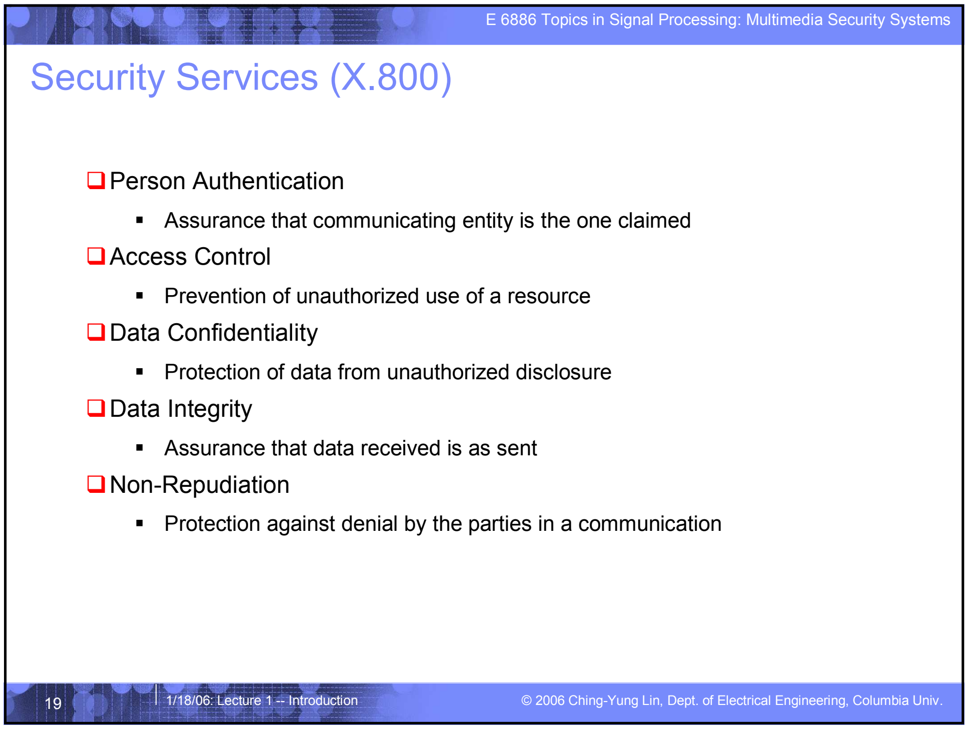
Multiple Aspects of DRM

- ❑ Technical
  - Enforcement by engineering mechanisms/systems
- ❑ Business
  - Commercially viable products/services
- ❑ Social
  - User privacy, limits on user behavior, etc.
- ❑ Legal
  - Enforcement by legislation



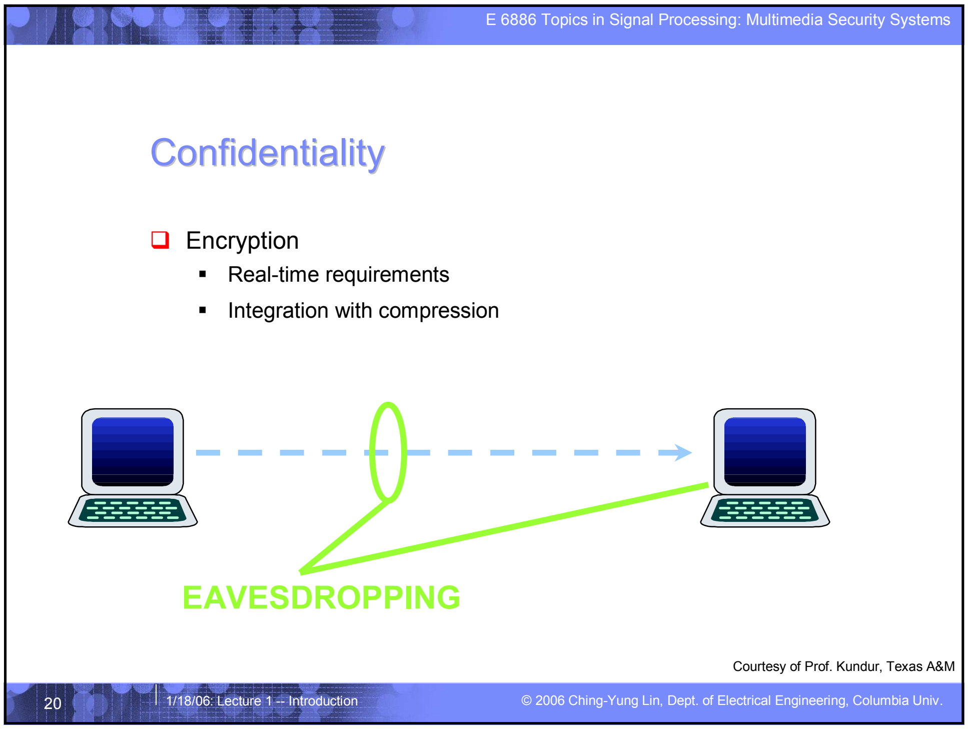
Outline -- Introduction

- ❑ Multimedia Security :
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – 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



Security Services (X.800)

- ❑ Person Authentication
  - Assurance that communicating entity is the one claimed
- ❑ Access Control
  - Prevention of unauthorized use of a resource
- ❑ Data Confidentiality
  - Protection of data from unauthorized disclosure
- ❑ Data Integrity
  - Assurance that data received is as sent
- ❑ Non-Repudiation
  - Protection against denial by the parties in a communication



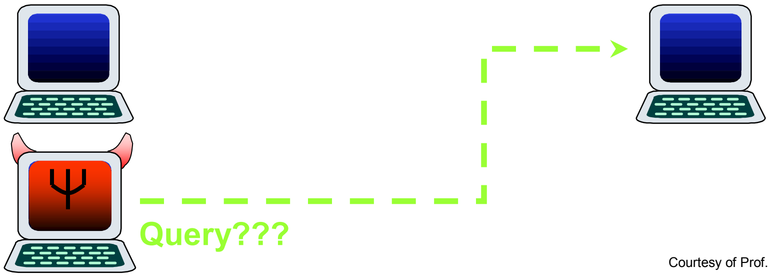
Confidentiality

- ❑ Encryption
  - Real-time requirements
  - Integration with compression

Courtesy of Prof. Kundur, Texas A&M

Access Control

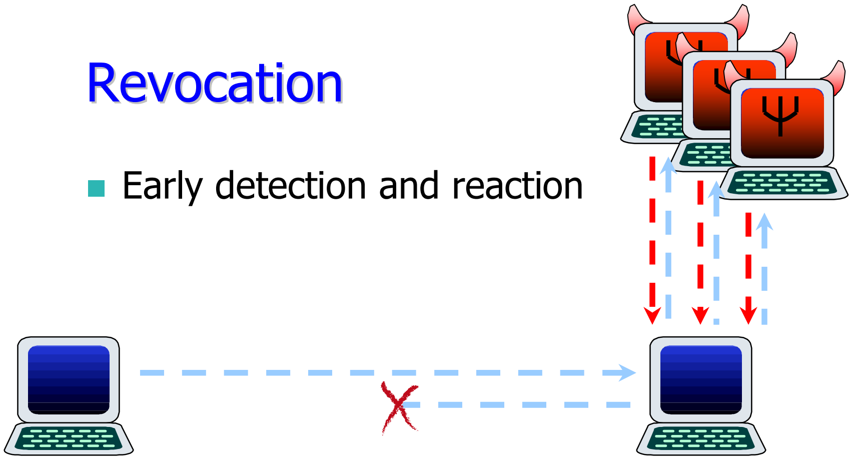
- Encryption
- Authentication



Courtesy of Prof. Kundur, Texas A&M

Revocation

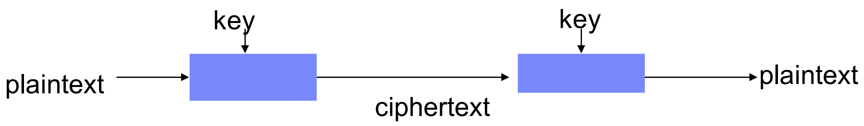
- Early detection and reaction



Courtesy of Prof. Kundur, Texas A&M

Conventional Encryption Algorithms

- ❑ Data Encryption Standard (DES)
  - The most widely used encryption scheme
  - DES is a block cipher – the plaintext is processed in 64-bit blocks
  - The key is 56-bits in length
  - Based on Feistel Cipher Structure
- ❑ Triple DES
  - Effective key length of 112/168 bits
- ❑ Advanced Encryption Standard (AES)
  - 128-bit data, 128/192/256-bit keys
  - Stronger & faster than Triple-DES
- ❑ Public key encryption: asymmetric key

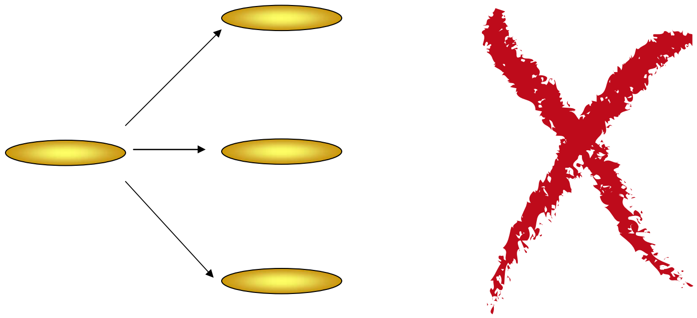


Outline -- Introduction

- ❑ Multimedia Security :
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – 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

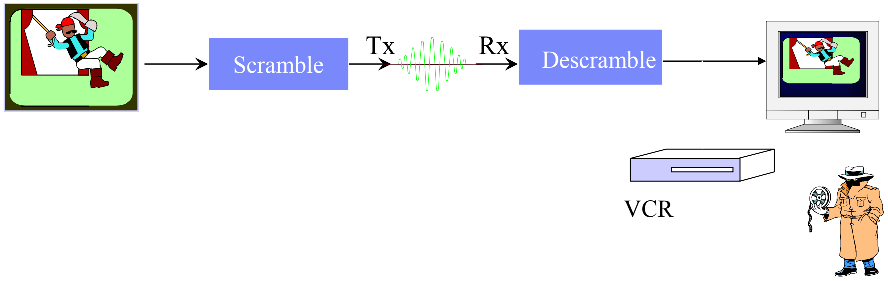
Piracy Protection

- Compliant Players



Courtesy of Prof. Kundur, Texas A&M

Copyright Protection and Copy Control



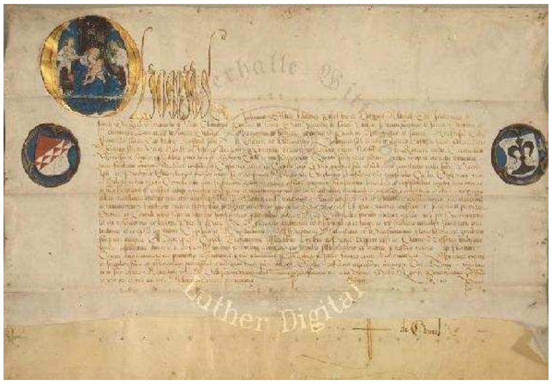
content-preserving transcoding:

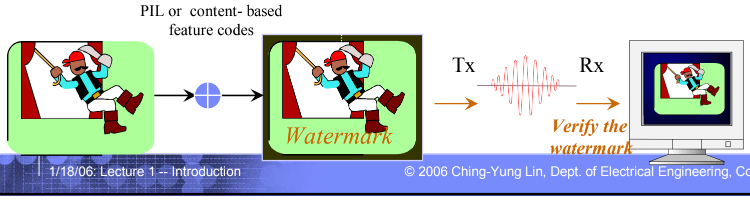
- Ownership Identification, Copy Control have to survive multi-stage transcoding

➔ Use *robust watermarking*

Watermarking

- Embedding Visible/Invisible Codes in Multimedia Data for (or not for) Security Purpose





Visible Watermark

- Purpose:
  - Claim the ownership and prevent content piracy.
- Properties:
  - Robust: *Watermarks must be very difficult, if not impossible, to be removed.*
  - Non-obtrusive: *Watermarks must not affect the audiovisual contents too much.*
  - Visible: *It must be visible, but it had better to be insensible.*

Visible Watermark Example

❑ **Description:**

- **Pixel brightness were altered pixel by pixel. Depending on the brightness of each mask pixel, if it is larger than a threshold, then we add a value to the corresponding pixel of the original image to make it brighter. Otherwise, if it is smaller than a threshold, then we subtract a value to make the corresponding pixel darker.**

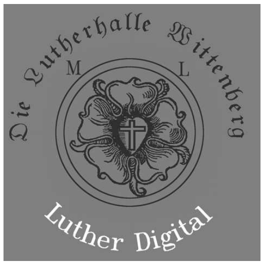
❑ **Alternation Function:**

$$\hat{Y}_{i,j} = Y_{i,j} + \frac{(m_{i,j} - T)}{|m_{i,j} - \mu_A|} \cdot \frac{Y_w}{38.667} \cdot (\frac{Y_{i,j}}{Y_w})^{\frac{2}{3}} \cdot \Delta$$

♦ **Robustness:**

- **Randomly set the adjustment factor.**
- **Randomly locate the mask.**
- **The mask pixels may depend on the image contents.**

Watermark mask



HIC SCHEVRLINA SIMVL TVCHERINAQ SIGNA REFVLGENT
QVE DOCTOR GEMINI SCHEVRLE PARENTIS HABES

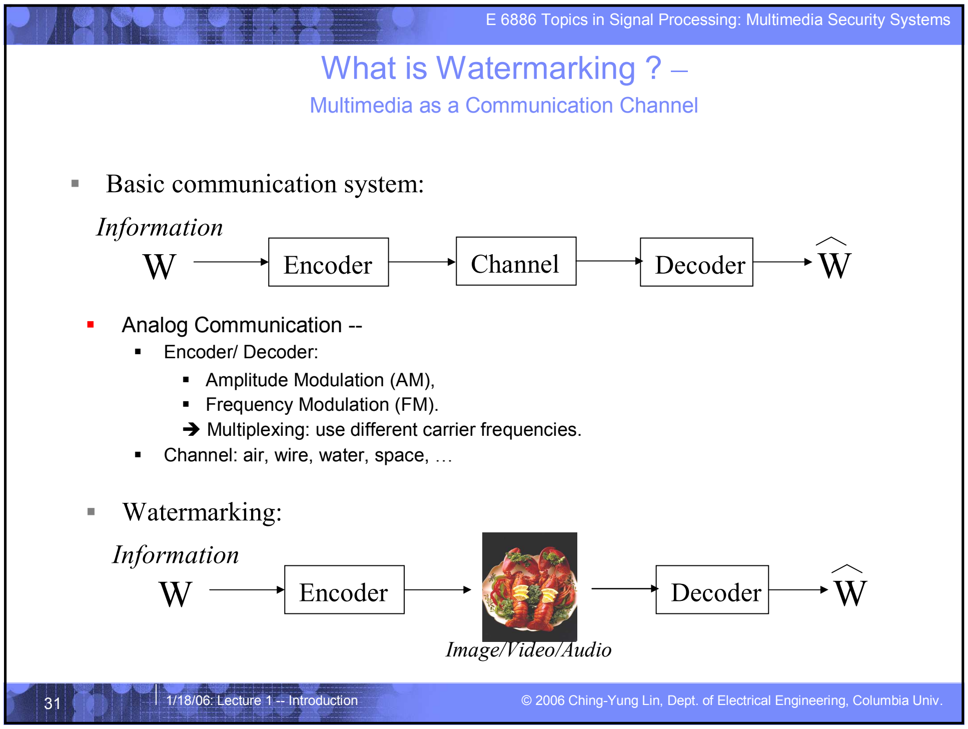
Invisible Watermark

❑ Purpose:

- Protect ownership and trace illegal use.

❑ 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.



What is Watermarking ? –

Multimedia as a Communication Channel

- Basic communication system:

Information

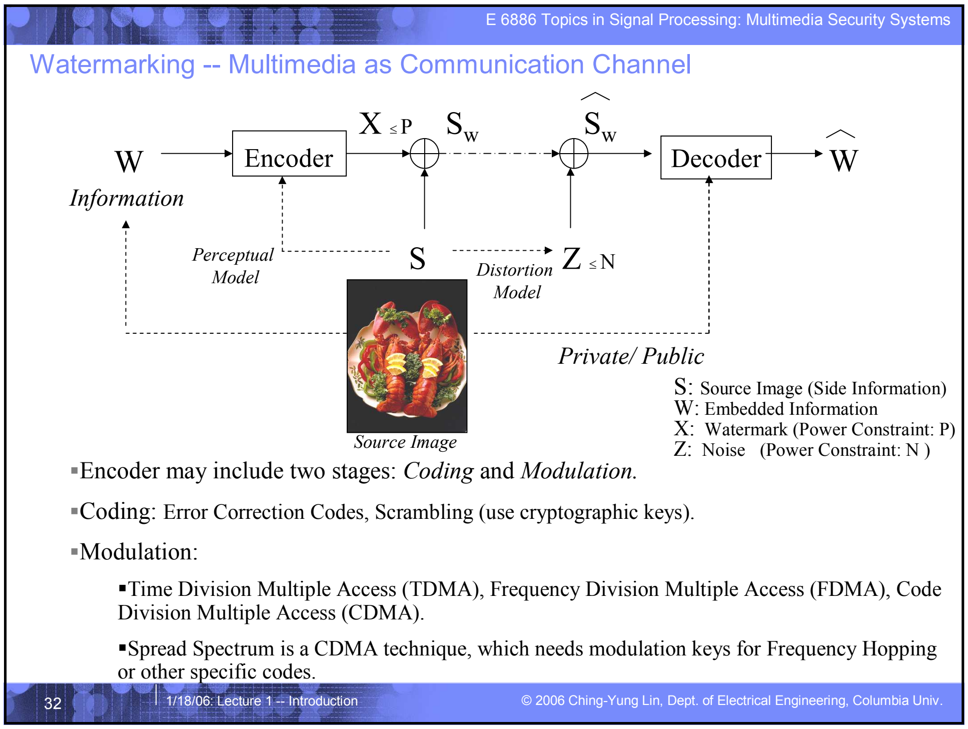
W → Encoder → Channel → Decoder → $\hat{W}$

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

- Watermarking:

Information

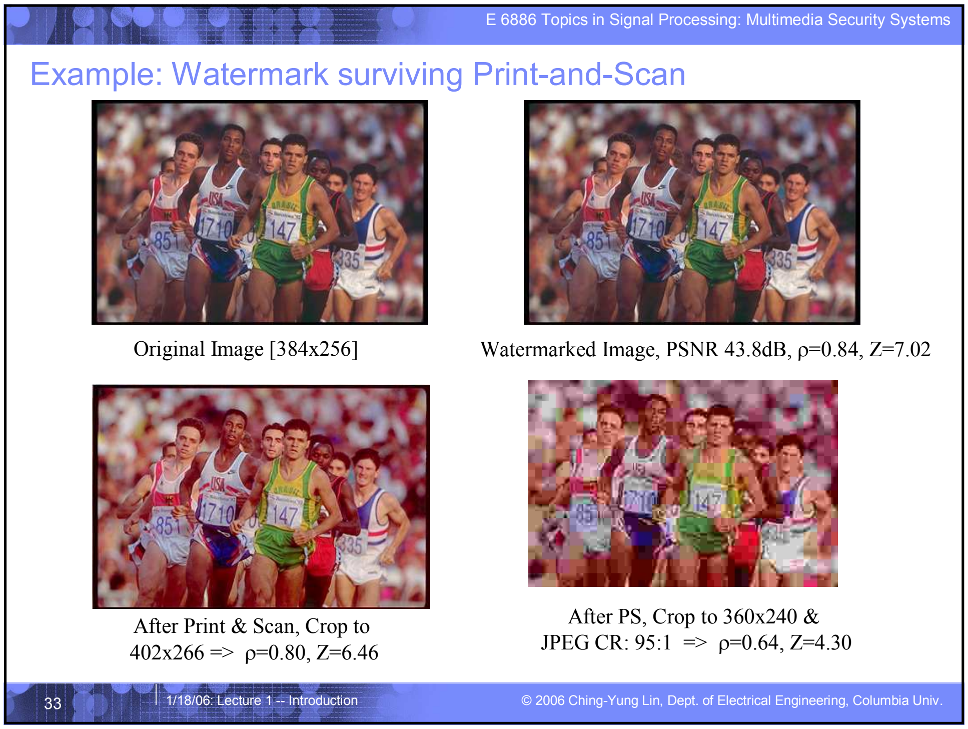
W → Encoder → *Image/Video/Audio* → Decoder → $\hat{W}$



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.



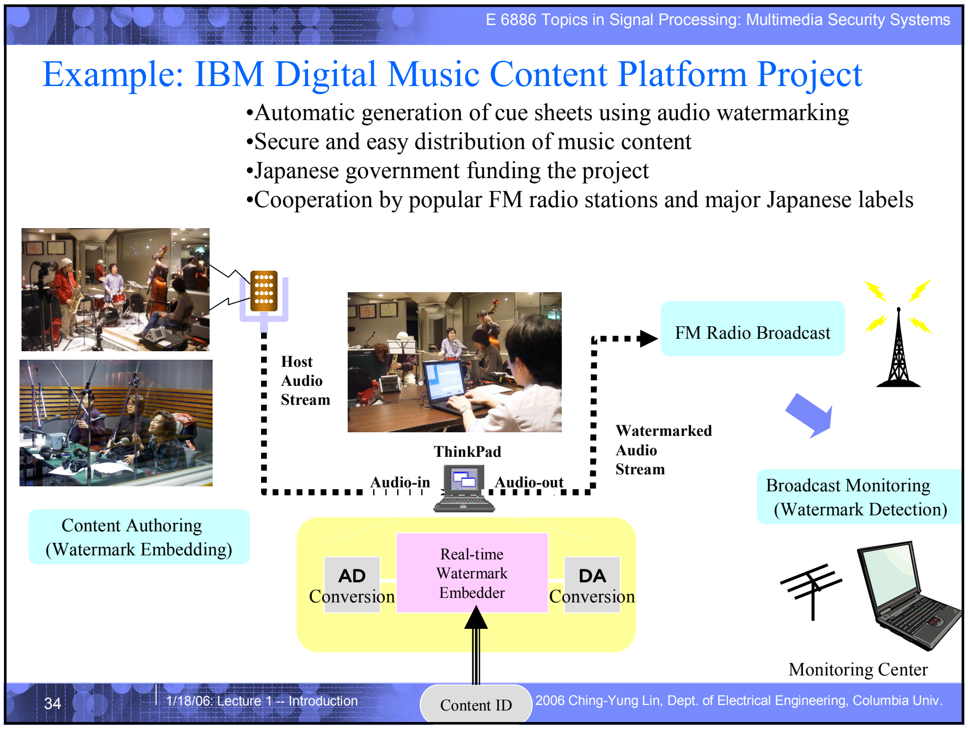
Example: Watermark surviving Print-and-Scan

Original Image [384x256]

Watermarked Image, PSNR 43.8dB, ρ=0.84, Z=7.02

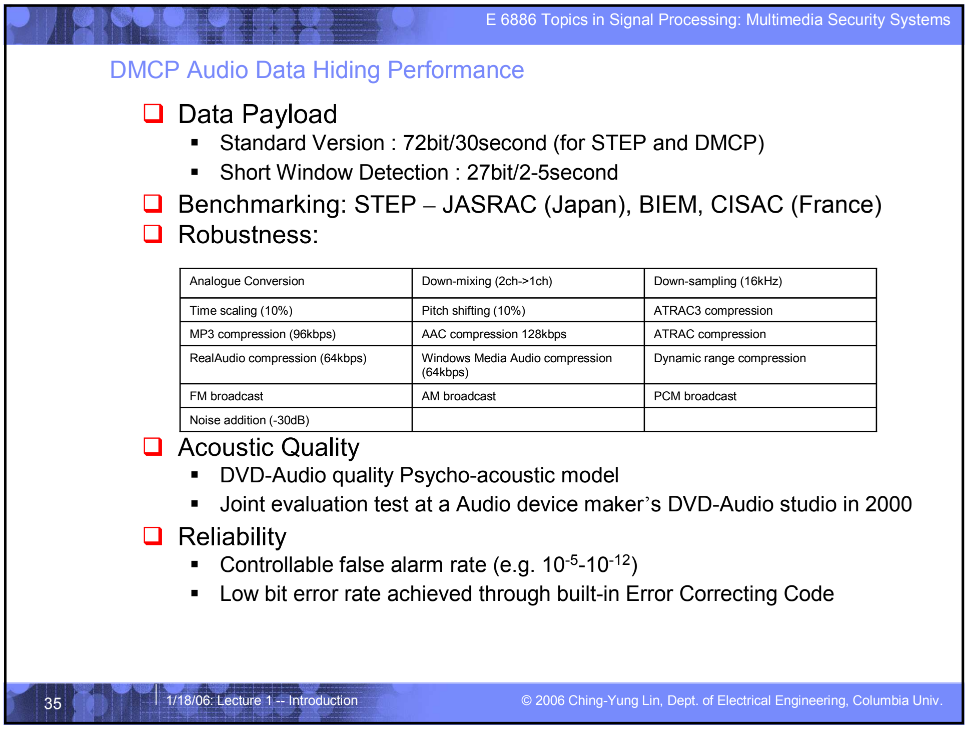
After Print & Scan, Crop to 402x266 => ρ=0.80, Z=6.46

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



Example: IBM Digital Music Content Platform Project

- Automatic generation of cue sheets using audio watermarking
- Secure and easy distribution of music content
- Japanese government funding the project
- Cooperation by popular FM radio stations and major Japanese labels

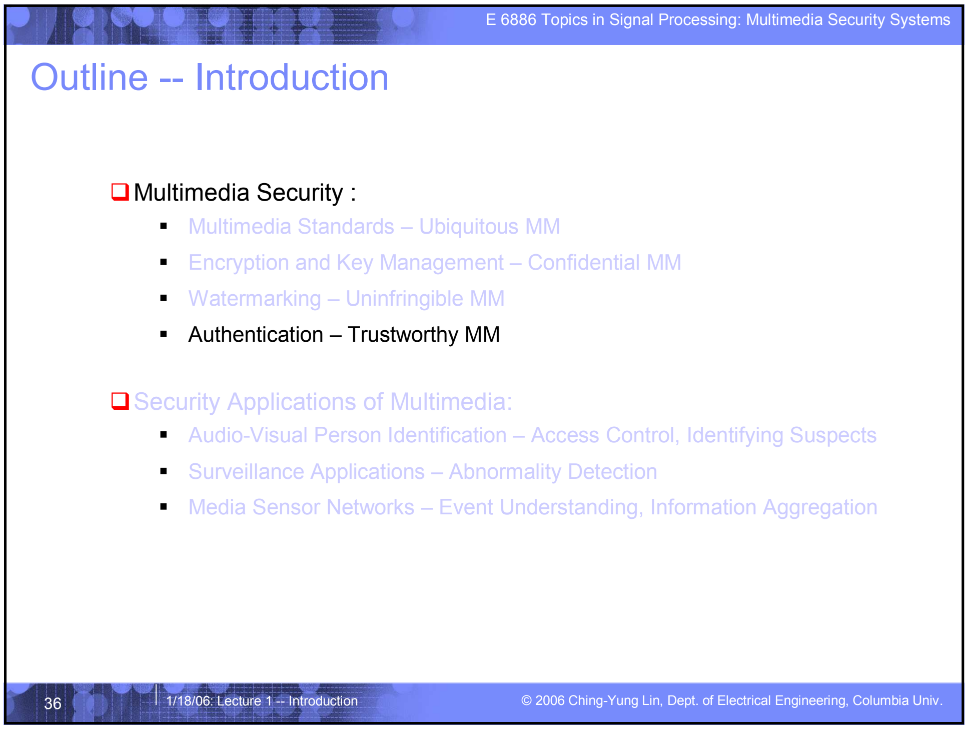


DMCP Audio Data Hiding Performance

- ❑ Data Payload
  - Standard Version : 72bit/30second (for STEP and DMCP)
  - Short Window Detection : 27bit/2-5second
- ❑ Benchmarking: STEP – JASRAC (Japan), BIEM, CISAC (France)
- ❑ Robustness:

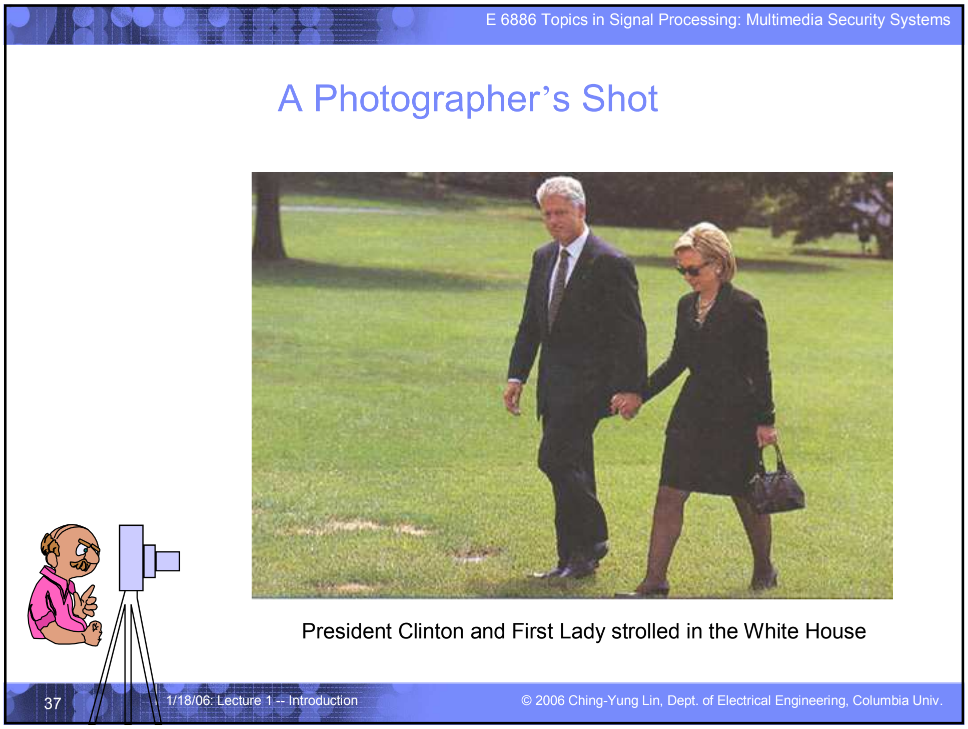
Analogue Conversion	Down-mixing (2ch->1ch)	Down-sampling (16kHz)
Time scaling (10%)	Pitch shifting (10%)	ATRAC3 compression
MP3 compression (96kbps)	AAC compression 128kbps	ATRAC compression
RealAudio compression (64kbps)	Windows Media Audio compression (64kbps)	Dynamic range compression
FM broadcast	AM broadcast	PCM broadcast
Noise addition (-30dB)		

- ❑ Acoustic Quality
  - DVD-Audio quality Psycho-acoustic model
  - Joint evaluation test at a Audio device maker's DVD-Audio studio in 2000
- ❑ Reliability
  - Controllable false alarm rate (e.g. 10^{-5}-10^{-12})
  - Low bit error rate achieved through built-in Error Correcting Code



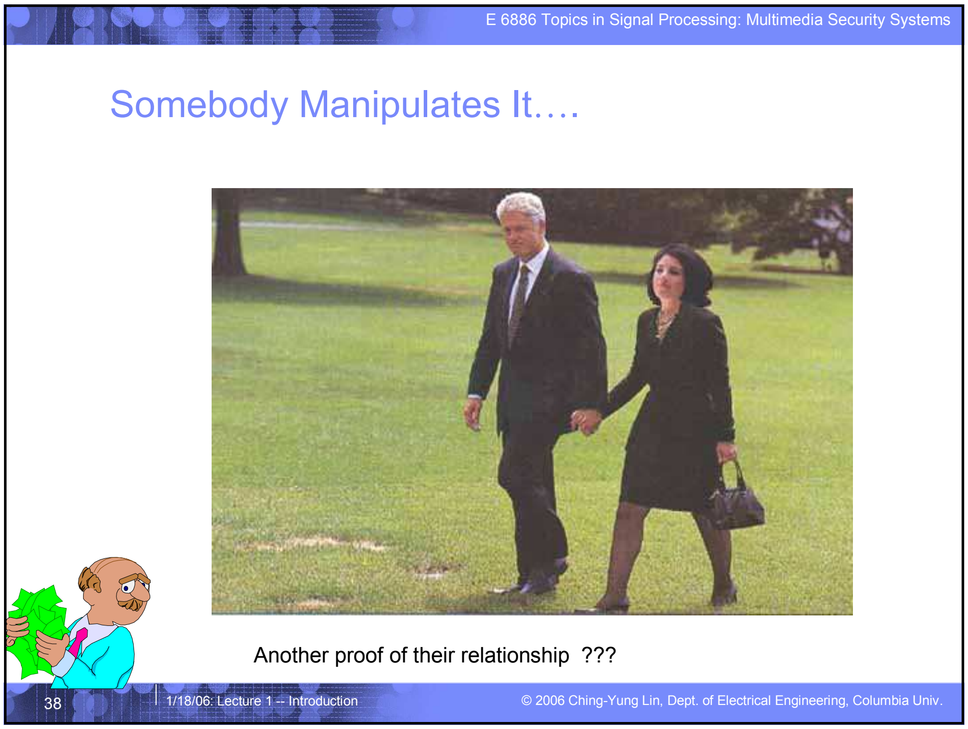
Outline -- Introduction

- ❑ Multimedia Security :
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – 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



A Photographer’s Shot

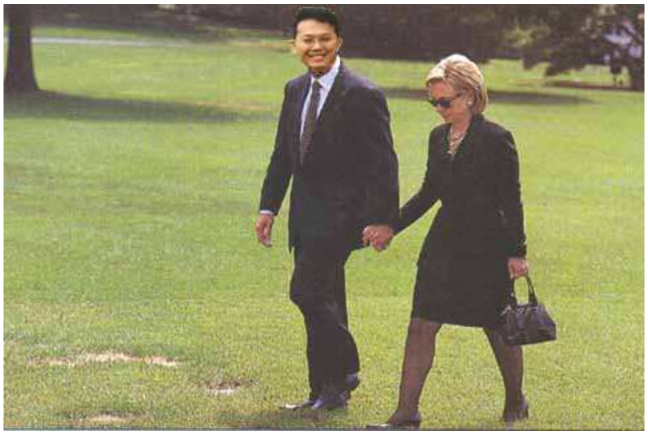
President Clinton and First Lady strolled in the White House



Somebody Manipulates It….

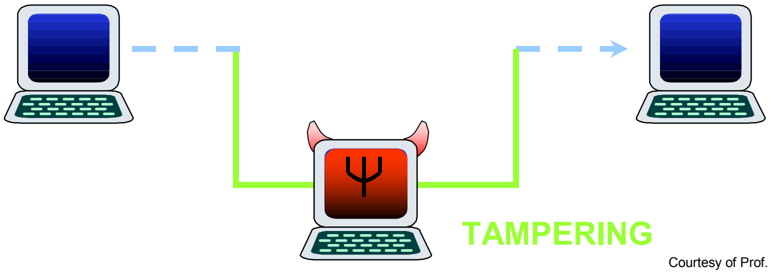
Another proof of their relationship ???

Hillary's Revenge???

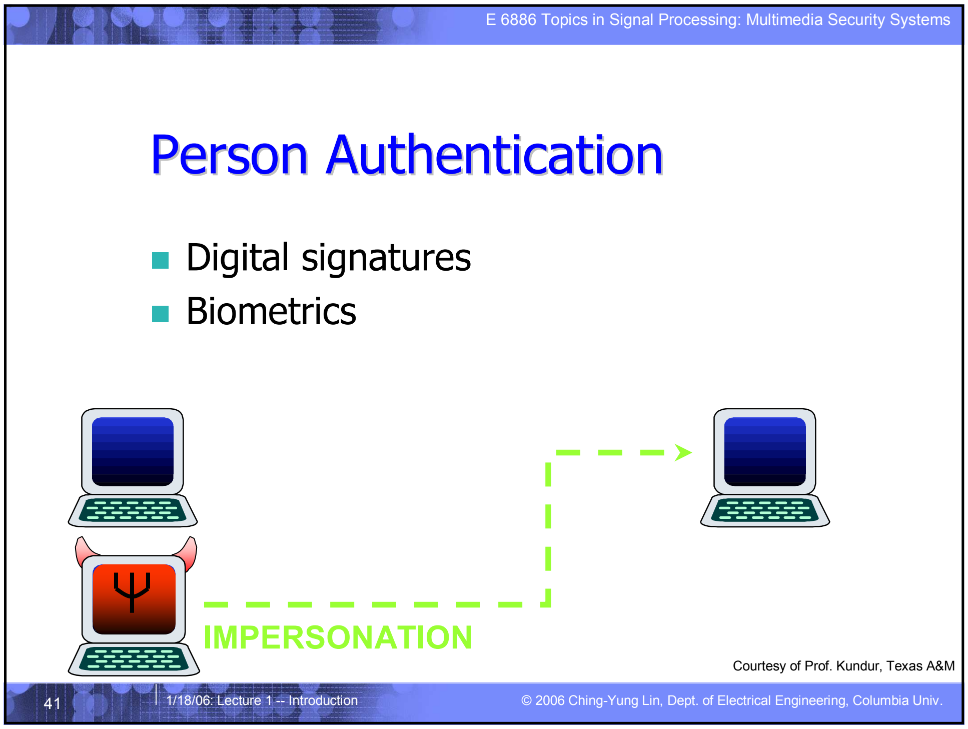


Integrity

❑ Hash Functions
- Traditional approaches sensitive to format conversion and minor bit changes
- Existing software tools enable seamless tampering



Courtesy of Prof. Kundur, Texas A&M

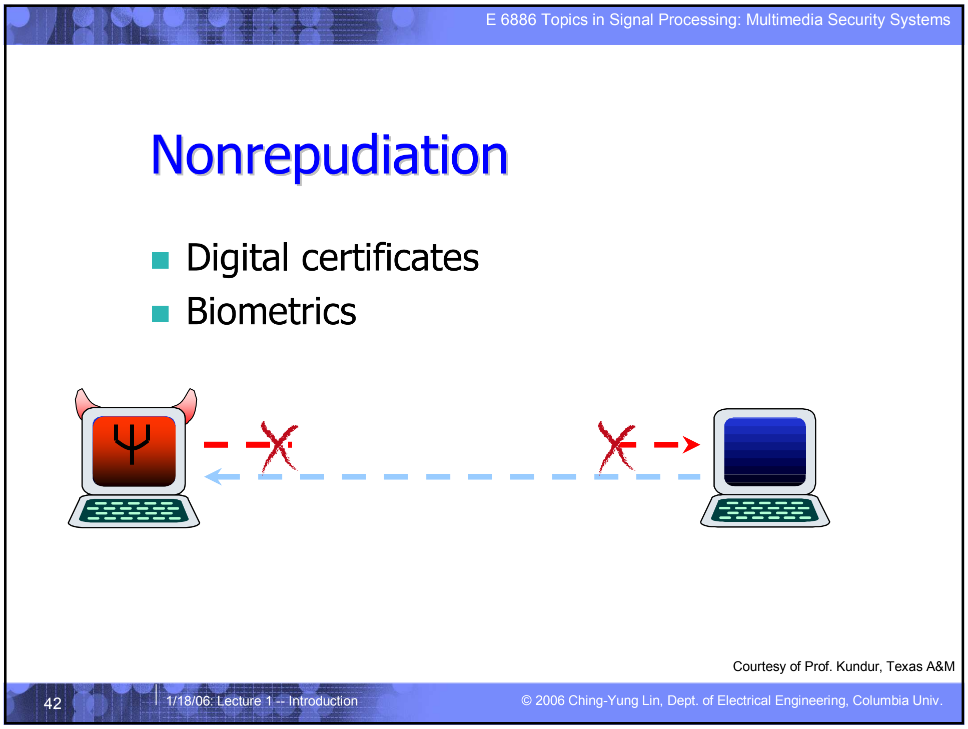


Person Authentication

- Digital signatures
- Biometrics

IMPERSONATION

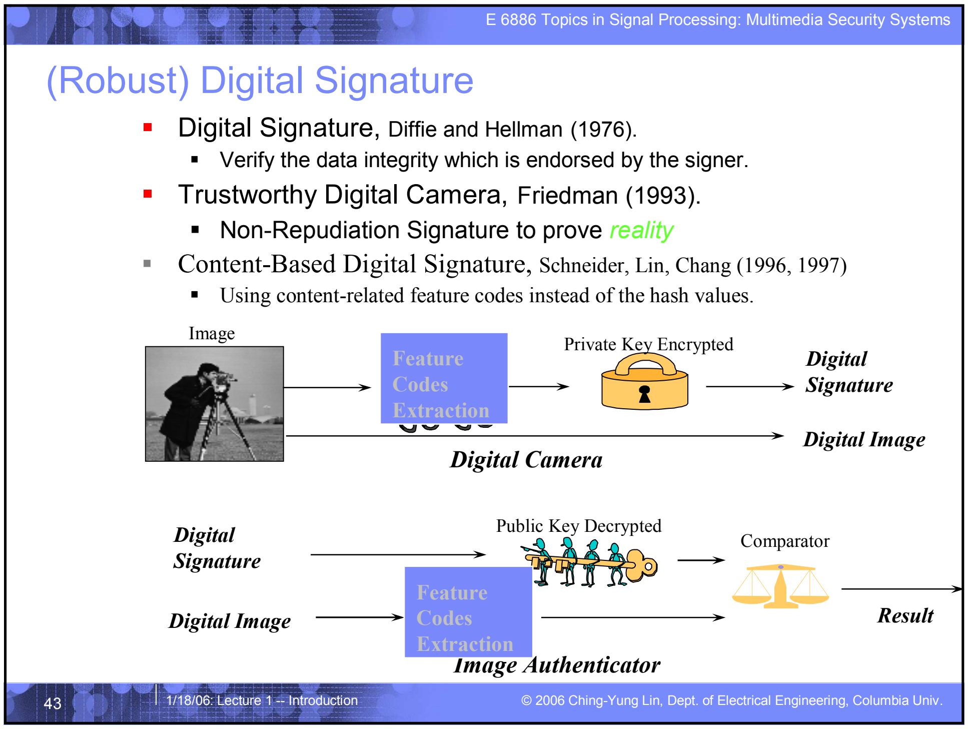
Courtesy of Prof. Kundur, Texas A&M



Nonrepudiation

- Digital certificates
- Biometrics

Courtesy of Prof. Kundur, Texas A&M



(Robust) Digital Signature

- Digital Signature, Diffie and Hellman (1976).
  - Verify the data integrity which is endorsed by the signer.
- Trustworthy Digital Camera, Friedman (1993).
  - Non-Repudiation Signature to prove *reality*
- Content-Based Digital Signature, Schneider, Lin, Chang (1996, 1997)
  - Using content-related feature codes instead of the hash values.

Image

Feature Codes Extraction

Private Key Encrypted

Digital Signature

Digital Image

Digital Camera

Digital Signature

Public Key Decrypted

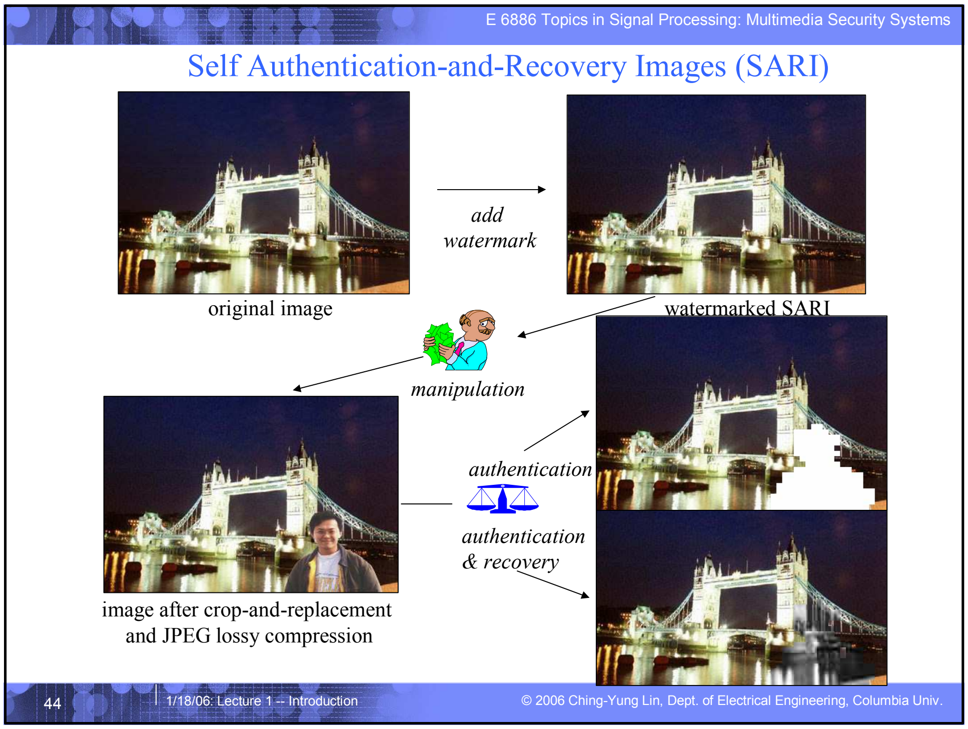
Comparator

Digital Image

Feature Codes Extraction

Result

Image Authenticator



Self Authentication-and-Recovery Images (SARI)

add watermark

original image

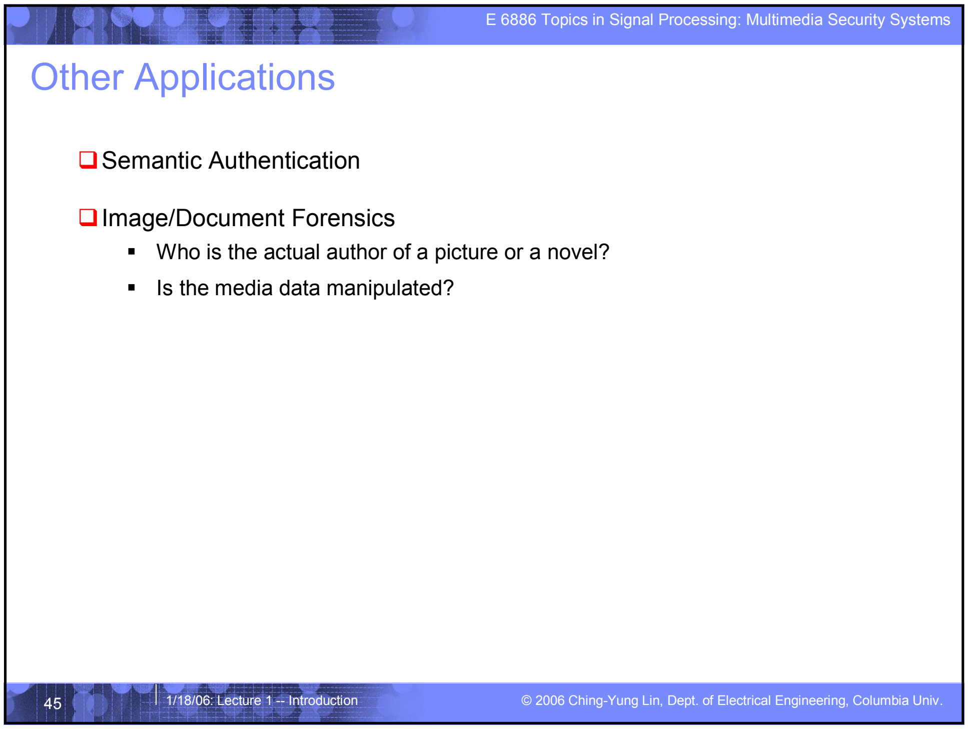
watermarked SARI

manipulation

authentication

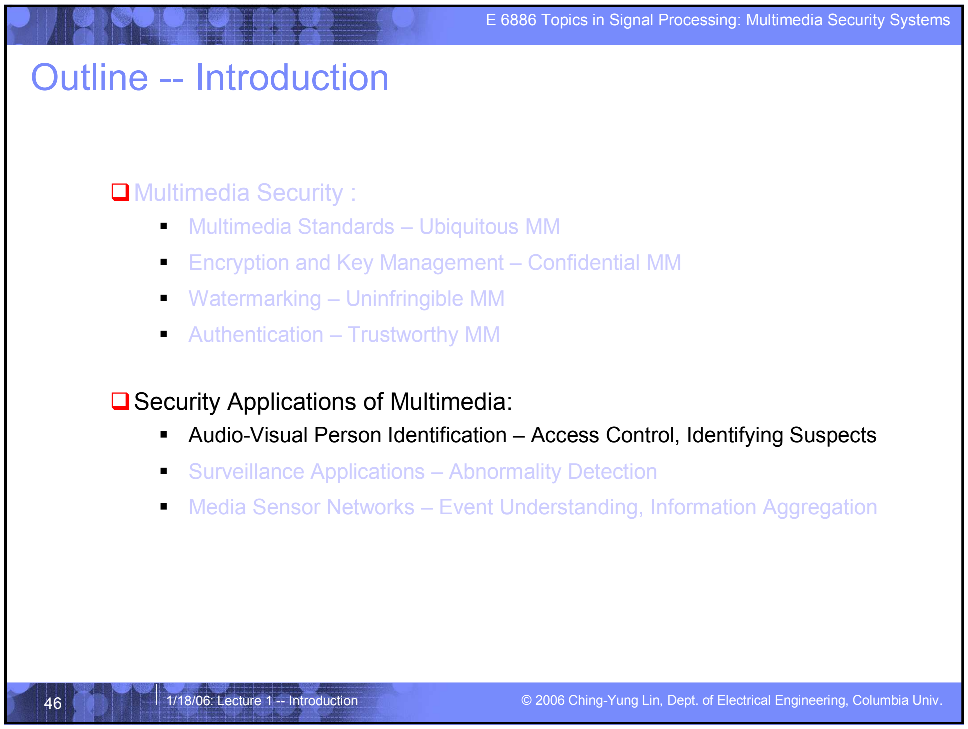
authentication & recovery

image after crop-and-replacement and JPEG lossy compression



Other Applications

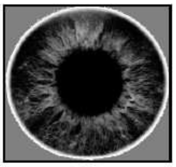
- ❑ Semantic Authentication
- ❑ Image/Document Forensics
  - Who is the actual author of a picture or a novel?
  - Is the media data manipulated?

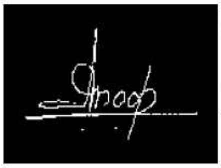


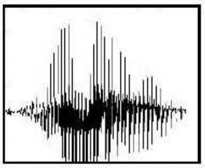
Outline -- Introduction

- ❑ Multimedia Security :
  - Multimedia Standards – Ubiquitous MM
  - Encryption and Key Management – 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

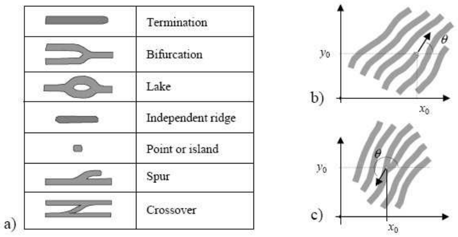
Biometric Features for Person Authentication





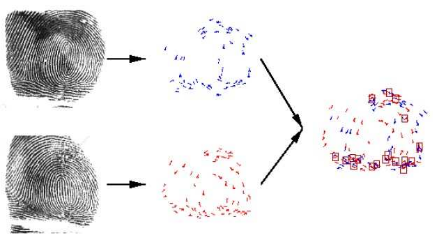


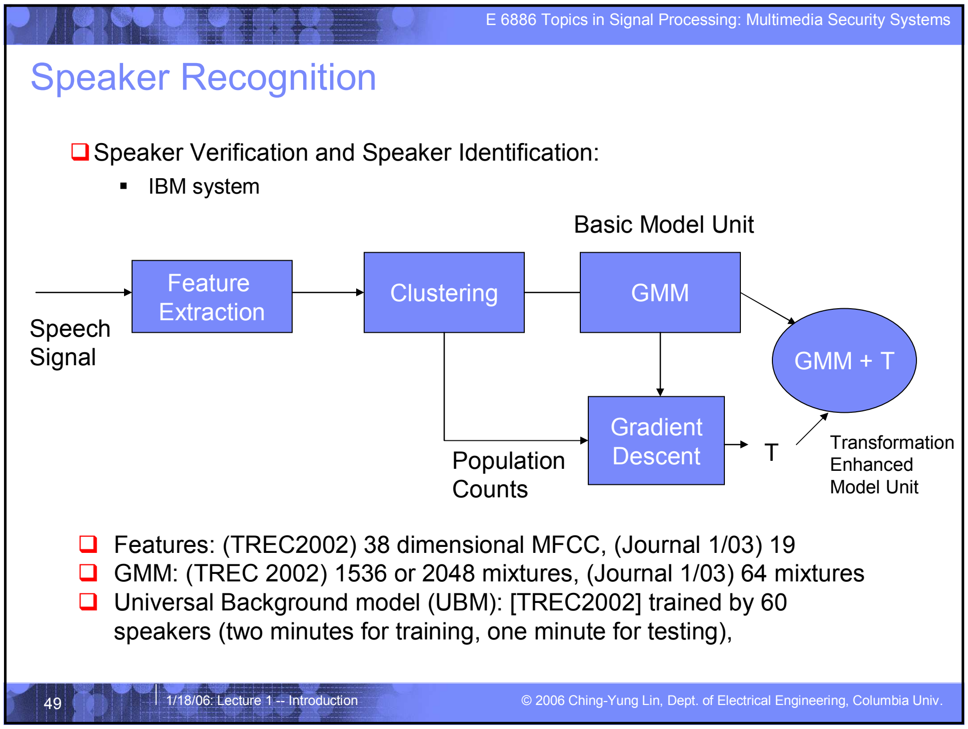
Example: Fingerprint-based Authentication



Fingerprint minutiae

Fingerprint Match





Speaker Recognition

❑ Speaker Verification and Speaker Identification:
- IBM system

Basic Model Unit

Speech Signal

Feature Extraction

Clustering

GMM

GMM + T

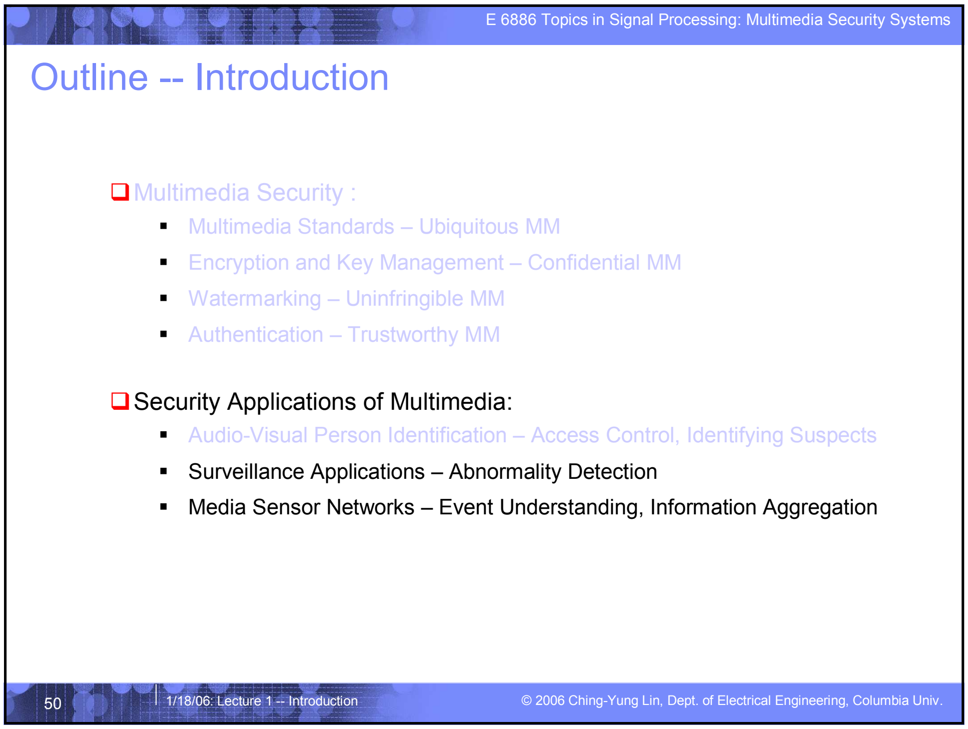
Gradient Descent

T

Population Counts

Transformation Enhanced Model Unit

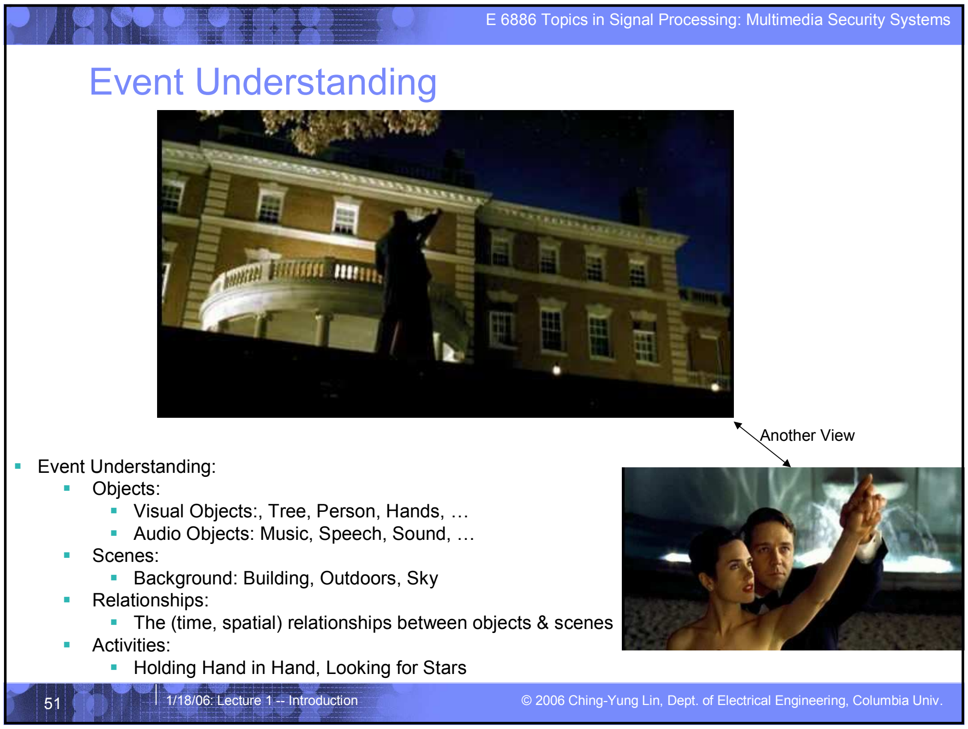
❑ Features: (TREC2002) 38 dimensional MFCC, (Journal 1/03) 19
❑ GMM: (TREC 2002) 1536 or 2048 mixtures, (Journal 1/03) 64 mixtures
❑ Universal Background model (UBM): [TREC2002] trained by 60 speakers (two minutes for training, one minute for testing),



Outline -- Introduction

❑ Multimedia Security :
- Multimedia Standards – Ubiquitous MM
- Encryption and Key Management – 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



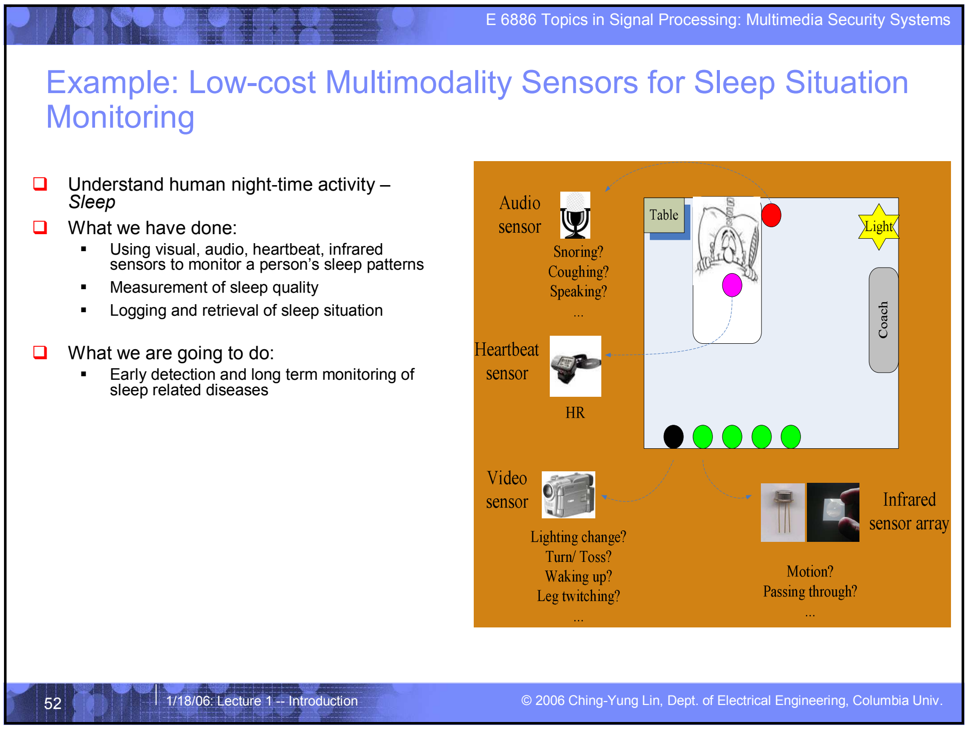
E 6886 Topics in Signal Processing: Multimedia Security Systems

Event Understanding

Another View

- Event Understanding:
  - Objects:
    - Visual Objects:, Tree, Person, Hands, …
    - Audio Objects: Music, Speech, Sound, …
  - Scenes:
    - Background: Building, Outdoors, Sky
  - Relationships:
    - The (time, spatial) relationships between objects & scenes
  - Activities:
    - Holding Hand in Hand, Looking for Stars

51 | 1/18/06: Lecture 1 -- Introduction © 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.



E 6886 Topics in Signal Processing: Multimedia Security Systems

Example: Low-cost Multimodality Sensors for Sleep Situation Monitoring

- ❑ Understand human night-time activity – *Sleep*
- ❑ What we have done:
  - Using visual, audio, heartbeat, infrared sensors to monitor a person's sleep patterns
  - Measurement of sleep quality
  - Logging and retrieval of sleep situation
- ❑ What we are going to do:
  - Early detection and long term monitoring of sleep related diseases

Audio sensor

Snoring?
Coughing?
Speaking?
…

Table

Light

Coach

Heartbeat sensor

HR

Video sensor

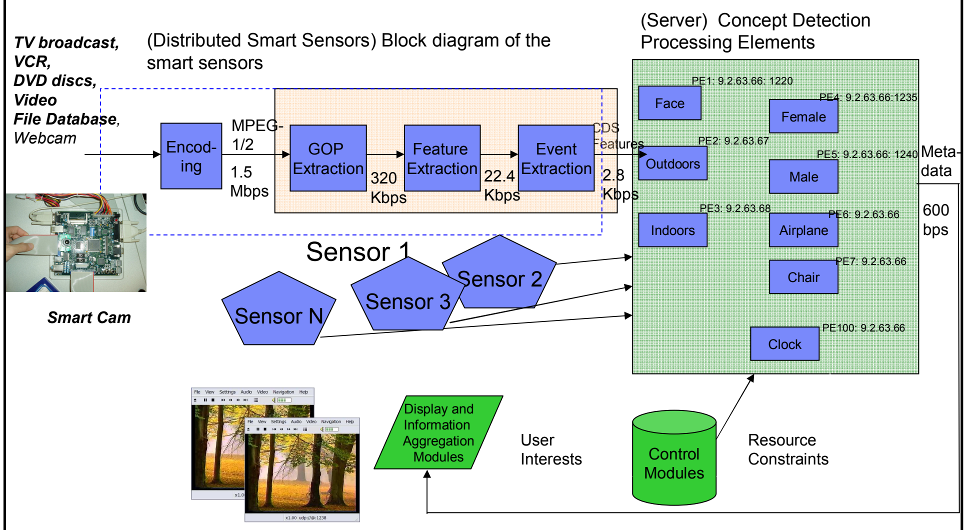
Lighting change?
Turn/ Toss?
Waking up?
Leg twitching?
…

Infrared sensor array

Motion?
Passing through?
…

52 | 1/18/06: Lecture 1 -- Introduction © 2006 Ching-Yung Lin, Dept. of Electrical Engineering, Columbia Univ.

Distributed Video Signal Understanding

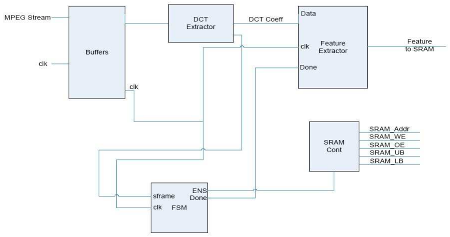


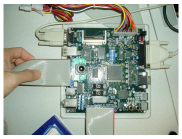
References

- K. Hill, “Imprimatur Business Model,” *MCPS 2nd Consensus Forum*, Stockholm, May 1997.
- ISO/IEC JTC 1/SC 29/WG 11 N4269, “Information Technology – Multimedia Framework (MPEG-21) – Part 4: Intellectual Property Management and Protection,” July 2001.
- G. Kesden, “Introduction on Content Scrambling System,” Lecture on Operating Systems: Design and Implementation, CMU, Dec. 2000.
- R. Tachibana, “Audio Watermarking for Live Performance,” *SPIE Security and Watermarking of Multimedia Contents V*, San Jose, January 2003.
- J. A. Bloom, I. J. Cox, T. Kalker, J.-P. Linnartz, M. L. Miller and B. Traw, “Copy Protection for DVD Video,” *Proceedings of the IEEE*, July 1999.
- J. A. Bloom, M. L. Miller and I. J. Cox, “Digital Watermarking”, Morgan Kaufmann Publishers, 2001.
- C.-Y. Lin and S.-F. Chang, “Semi-Fragile Watermarking for Authenticating JPEG Visual Content,” *SPIE Security and Watermarking in Multimedia Contents II*, Vol. 3971, Jan. 2000.
- U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, “Biometric Cryptosystems: Issues and Challenges,” Prof. of the IEEE, June 2004.

M.S. Research Projects Available (Spring 2006, 3Pts)

- ❑ Developing Distributed Smart Video Cameras (Phase II):





- ❑ Large-Scale Data Mining, Community Modeling, Human Behavior Modeling

Other Related Research Issues

- ❑ Issues in multimedia security
  - copyright protection, authentication, fingerprinting: system, theory and techniques
  - public watermarking techniques, watermarking attacks, quality evaluations and benchmarks
  - perceptual models, noise models, information theoretical models
  - conditional access
  - Traitor tracing
  - legal aspects
  - watermarking protocols
  - security in JPEG2000, MPEG-4, MPEG-7 or MPEG21
  - biometrics and multimedia security
  - watermarking/ information hiding applications

http://www.research.ibm.com/people/c/cylin

Acknowledgment: Thanks for Prof. Deepa Kundur's (Texas A&M U.) assistance on the graphical examples of MM security objectives.

Columbia and IBM

- T. J. Watson Research Center

1945-1953
(612 W116th St.)

1953-1970
(612 W115th St.)

- The first computer science course (1947)
- The founding of ACM (1947)
- The first “personal” computer (1948)

- The first supercomputer (1954)

1970 –
(Yorktown Heights)

Open Discussion