INT 307
Multimedia Security System

Introduction

Sichen.Liu@xjtlu.edu.cn

XJTLU | SCHOOL OF FILM AND TV ARTS

Xi’an Jiaotong-Liverpool University
西交利物浦大学

Lecturer - Sichen Liu

- Graduated from Institute of Acoustics, Chinese Academy of Sciences

- Worked as an audio algorithm researcher at Tencent Video (Beijing)

- Research focus: Machine Listening

- Tuesday, 2 - 4 pm @ SD 557 room. E-mail me before coming

Welcome to INT307

This is a year 4 module, which means that you are expected to

- Be able to learn by yourself with little guidance provided
- Set your own learning outcome and select the most proper way to learn
- Learn how to learn

Official learning outcomes

- Demonstrate practical knowledge of multimedia systems and security technologies
- Demonstrate knowledge of multimedia compression technologies and standards
- Evaluate algorithms, theories and tools developed for multimedia security issues, including digital rights management, copyright protection, and authenticity verification
- Demonstrate an awareness of theories, research issues and recent developments of multimedia-based security systems such as multimedia surveillance and biometric applications
- Recognise the security risks that may be involved in the operation of computing and information systems

Lecture Overview

- Overview: Week 1
- Multi-media Representation and Compression: Week 2-4
- Watermarking: Week 5
- Presentation for CW1: Week 6
- Multimedia Encryption: Week 8-9
- Presentation for CW2: Week10
- Neural Network and Adversarial Attack: Week 11-12
- Review: Week 14

Tutorials

There are 6 Tutorials in this module

- Week 2: Q&A
- Week 3: Q&A
- Week 4: Q&A
- Week 5: Q&A
- Week 6: CW1 Presentation
- Week 10: CW2 Presentation

Module Assessment

Coursework 1

There are three assessments in this module

Coursework 1	15%
Coursework 2	15%
Final exam (Closed Book)	70%

Module Assessment

Coursework 1

Write an one-page essay reviewing the advances in ***one*** of the following fields:

- Robust Face Recognition
- Media Sensor Network
- Cloud Computing for Multimedia Services

For more marks

You should suggest a possible future research direction of the techniques you have chosen, according to the papers you have reviewed

Module Assessment

Coursework 1

- 15% of the final mark
- Must have more than 10 academic references (website does not count)
- No more than 20% similarity in Turnitin report (reference list excluded)
- 3-min Presentation on Week 6 (50 Marks)
- Report Submission DDL: 29th Oct 2023 (50 Marks)

Note

Remember to include a title!

Module Assessment

Coursework 2

Write an one-page essay to review the most up-to-date works in the one of the following fields

- Speaker Recognition
- Audio Fingerprinting
- Audio Watermarking

For more marks

You should suggest a possible future research direction of the techniques you have chosen, according to the papers you have reviewed

Module Assessment

Coursework 2

- 15% of the final mark
- Must have more than 10 academic references (website does not count)
- No more than 20% similarity in Turnitin report (reference list excluded)
- 3-min Presentation on week 10 (50 Marks)
- Report submission DDL: 26th Dec 2023 (50 Marks)

Note

Remember to include a title!

Module Assessment

Final Exam

- 70% of the final mark
- Closed book exam (2 hours)

Aims of exam

- Makes sure you have mastered enough knowledge to meet the learning outcomes
- You can only pass a module (towards graduation) by participating an exam

Teaching Assistants

- yuxuan.liu2204@student.xjtlu.edu.cn
- siyue.yao2302@student.xjtlu.edu.cn
- zihan.ye22@student.xjtlu.edu.cn
- yue.dong22@student.xjtlu.edu.cn

Note

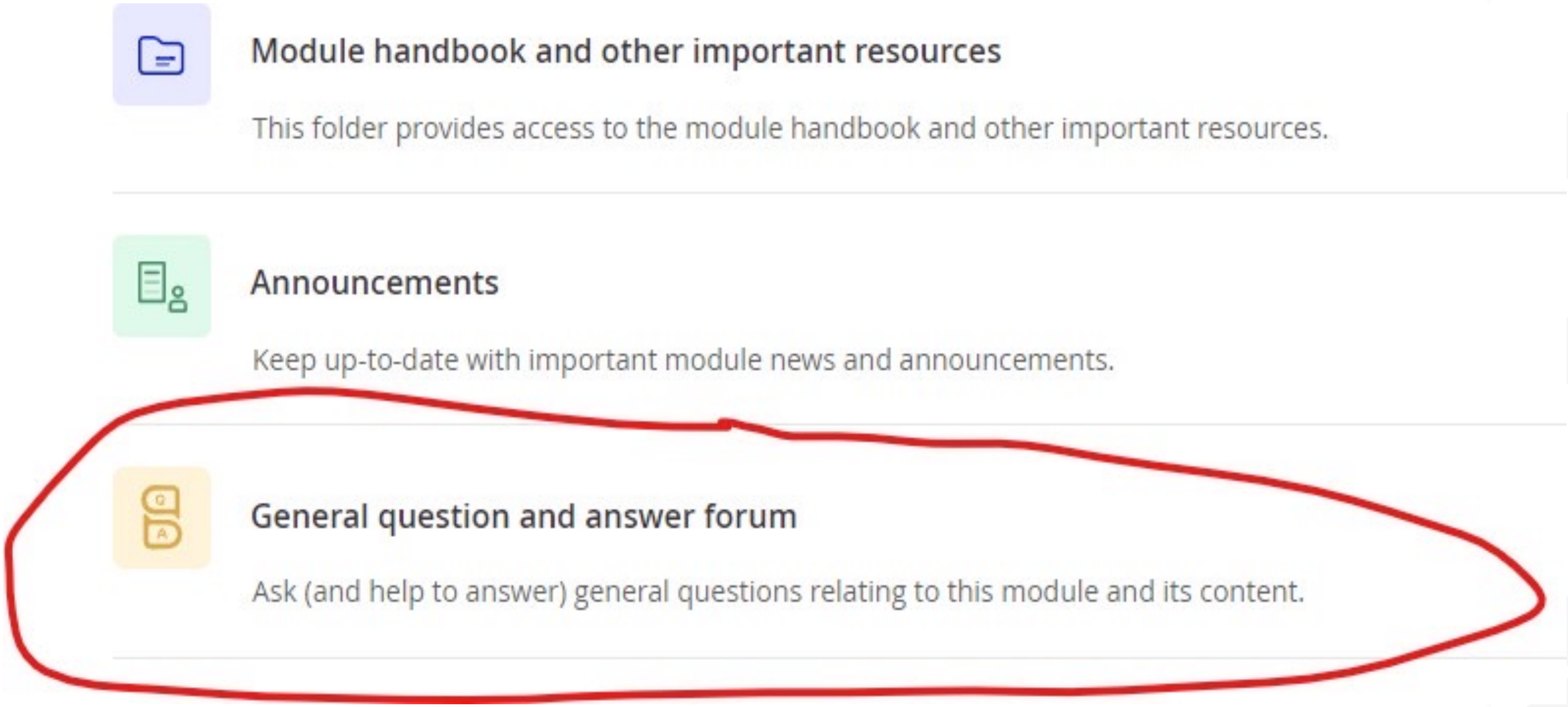
Your TA has their own works. You cannot rely on TA to finish your coursework

Lecture Recording

- Will be released on week 6 and week 12
- In-class discussion will not be recorded
- Recordings are an additional resource and should not be seen as a substitute for attendance

Raise a Question

Please use Learning Mall to raise your question (with a good title)



Module handbook and other important resources

This folder provides access to the module handbook and other important resources.

Announcements

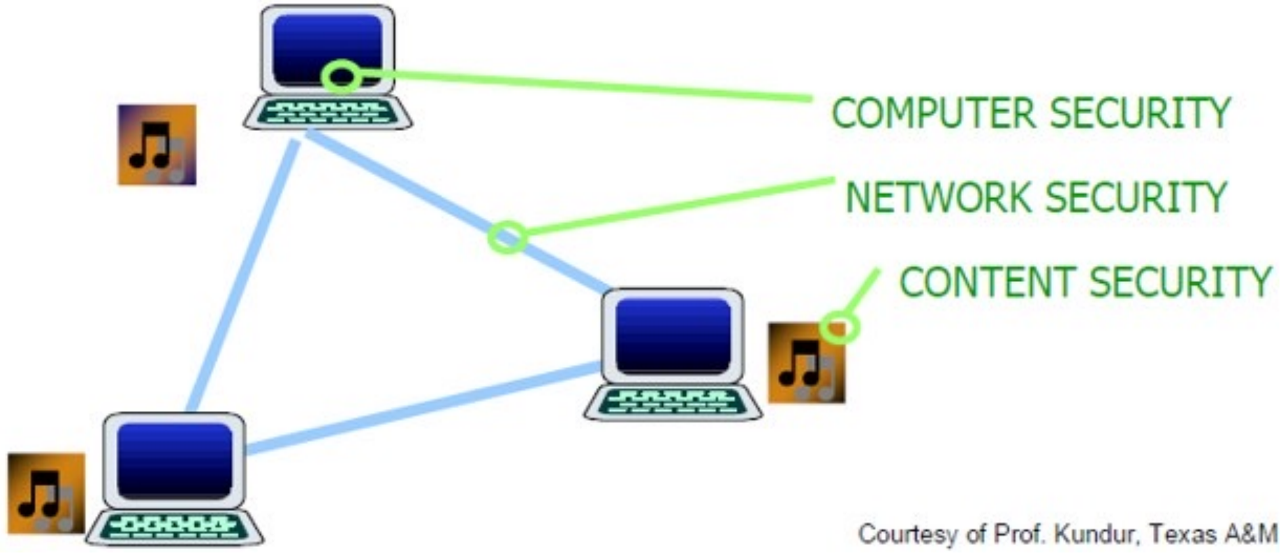
Keep up-to-date with important module news and announcements.

General question and answer forum

Ask (and help to answer) general questions relating to this module and its content.

Types of Security

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



Courtesy of Prof. Kundur, Texas A&M

Multimedia Security

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

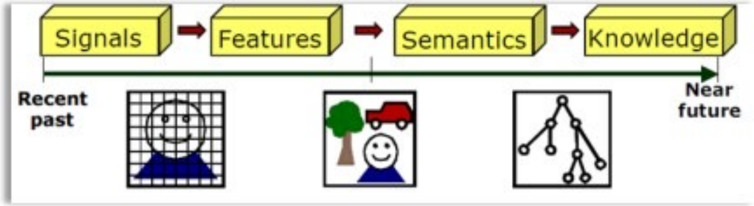
Digital Rights Management (DRM) System

- 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.

Multiple Aspects of DRM

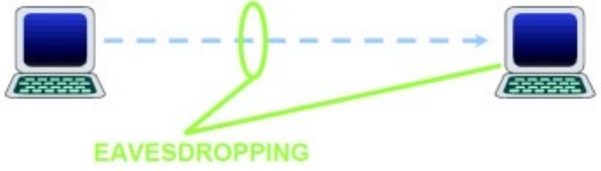
- Technical: Enforcement by engineering mechanisms/systems
- Business: Commercially viable products/services
- Social: User privacy, limits on user behavior, etc.
- Legal: Enforcement by legislation
- Error resilience to enable robust transmission

Full-view of Course



Multimedia Standards:

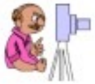
How to represent Multimedia

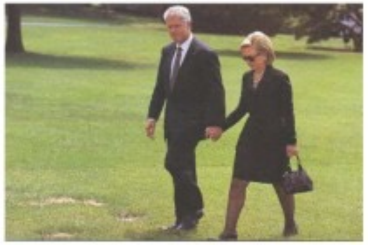


Courtesy of Prof. Kundur, Texas A&M

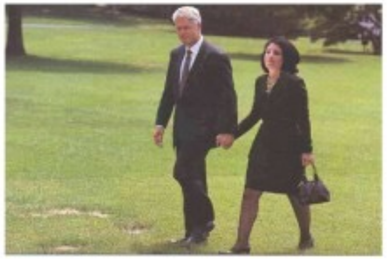
Multimedia Encryption :

How to make confidential multimedia





President Clinton and First Lady strolled in the White House



Another proof of their relationship ???

Multimedia Authetication:

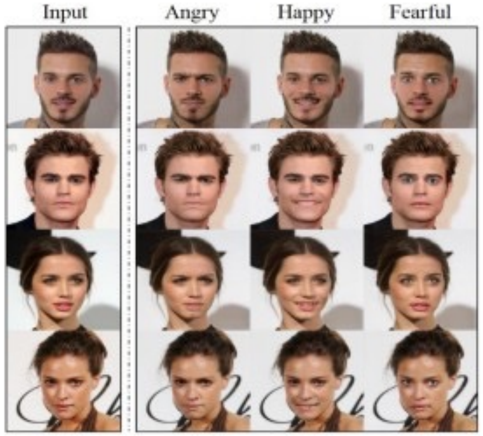
How to authenticate multimedia

Die Lutherhalle Wittenberg
M L
Luther Digital

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

Water Marking:

How to control copyright of Multimedia



Adversarial attack:

How to attack or protect Multimedia

Outline of the Introduction

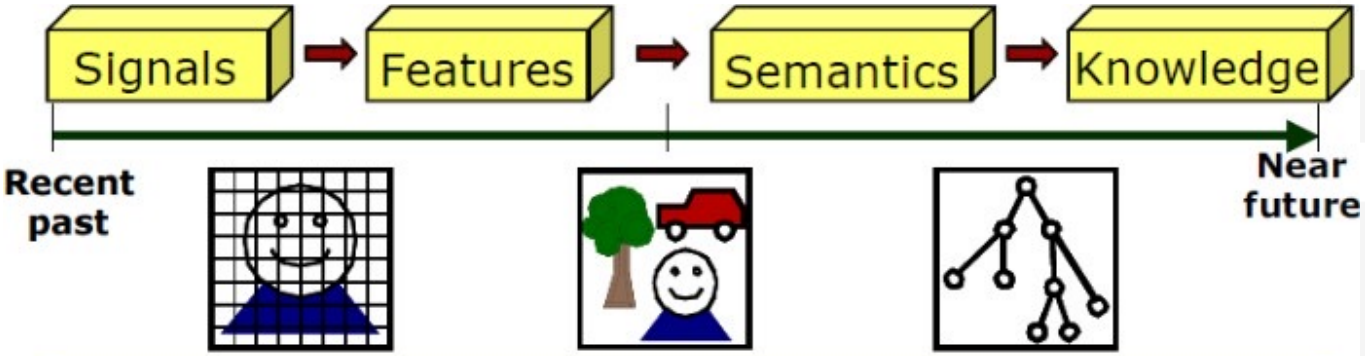
- Multimedia Security
  - Multimedia Standards - Ubiquitous MM
  - Encryption and Key Management - Confidential MM
  - Watermarking - Uninfringible MM
  - Authentication - Trustworthy MM
  - Adversarial Example and Adversarial Network (Deep Learning)
- Security Applications of Multimedia
  - Audio-Visual Person Identification - Access Control, Identifying Suspects
  - Surveillance Applications - Abnormality Detection

Applications…

- Digital Rights Management in Mobile Environment
- Steganography and steganoanalysis (encryption)
- 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 images/videos
- Fingerprint recognition
- Human behavior authentication: Keyboard and Email records
- Event detection from camera(s)
- Audio/Visual Sensor Network

Multimedia Standards - Ubiquitous M M

- Multimedia Standards: Towards Knowledge Management and Transaction
- MPEG: Moving Picture Experts Group

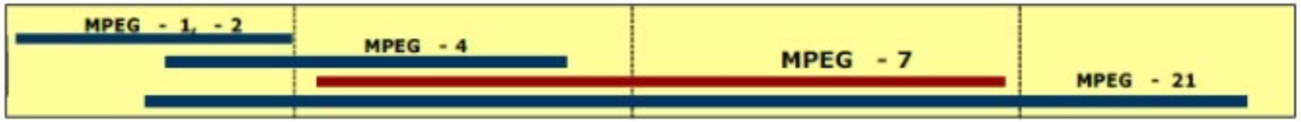


Signals → Features → Semantics → Knowledge

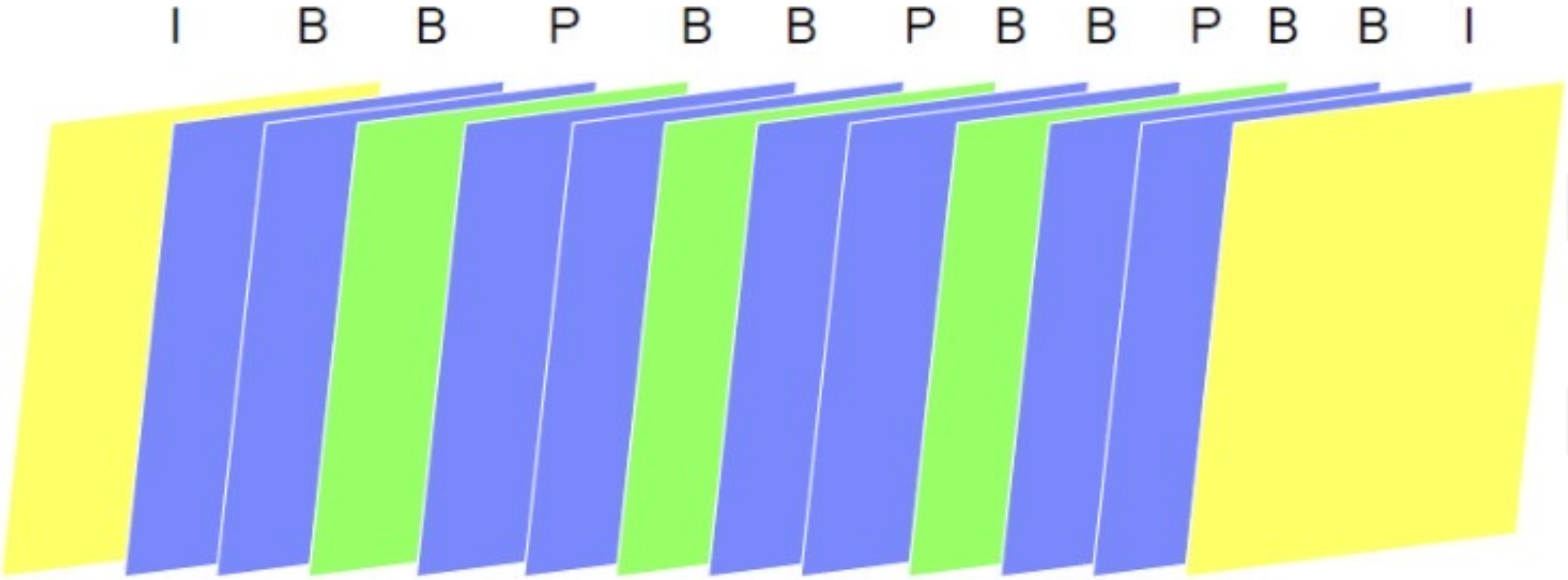
Recent past

Near future

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



- 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

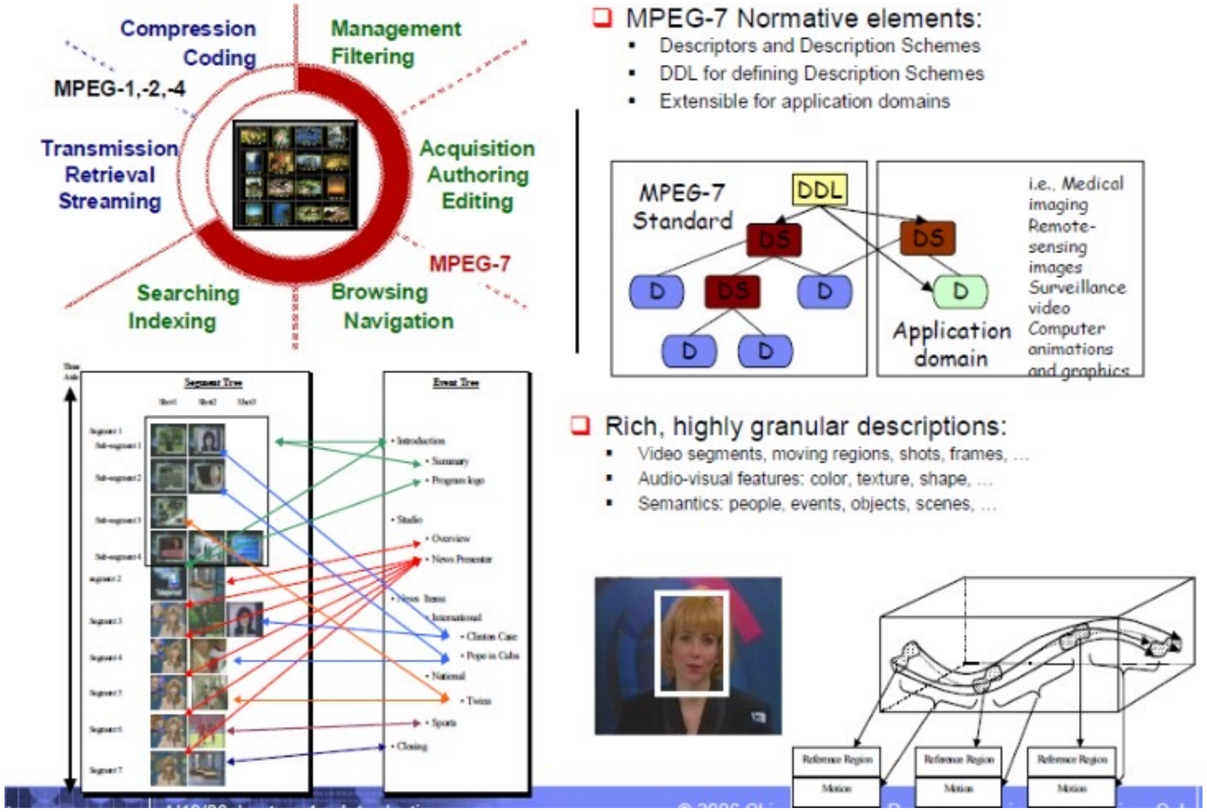
- MPEG-1 Audio Layer 3 – MP3

MPEG-4 Overview

- Object-based compression
- Low-bit rate coding for mobile applications
- Natural-Synthetic hybrid compression
- The latest MPEG-4 standard: H.264/AVC

MPEG-7 Overview

- XML Metadata for Multimedia Content Description
  - A set of description schemes (DS): semantic relations between its components
  - A language to specify these schemes: Description Definition Language (DDL): the structural relations between the descriptors.
  - A scheme for coding the description



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

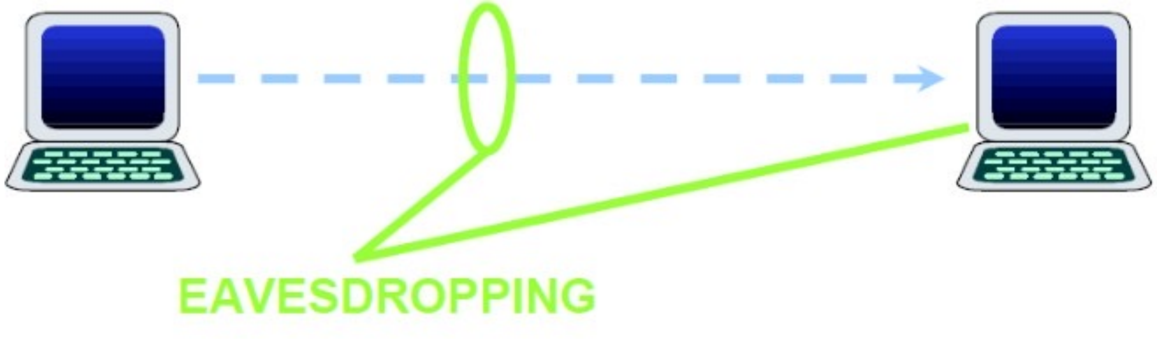
❑ Rich, highly granular descriptions:
- Video segments, moving regions, shots, frames, …
- Audio-visual features: color, texture, shape, …
- Semantics: people, events, objects, scenes, …

Confidential MM: Security Services (X.800)

- Person Authentication: Assurance that communicating user 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

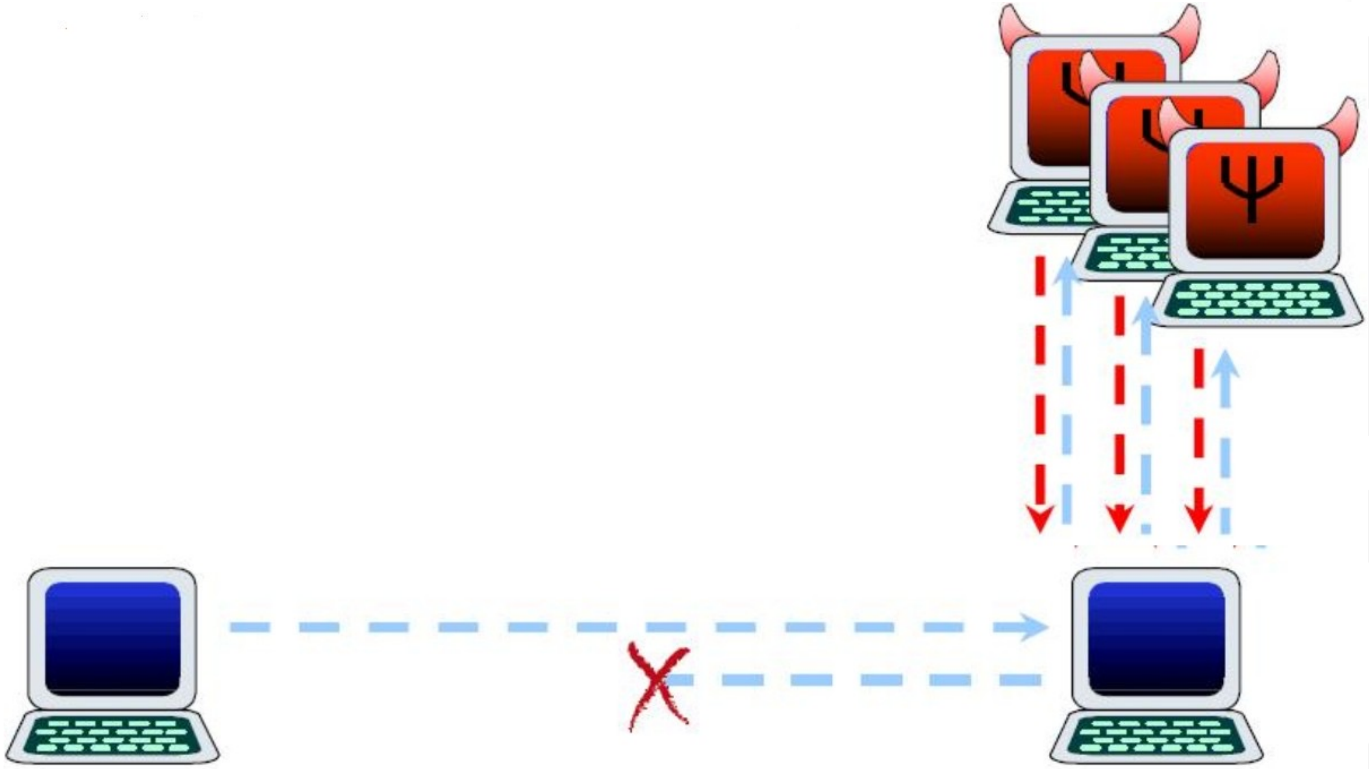
- Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
  - Printing, displaying and other forms of disclosure



Courtesy of Prof. Kundur, Texas A&M

Revocation

- Early detection and reaction

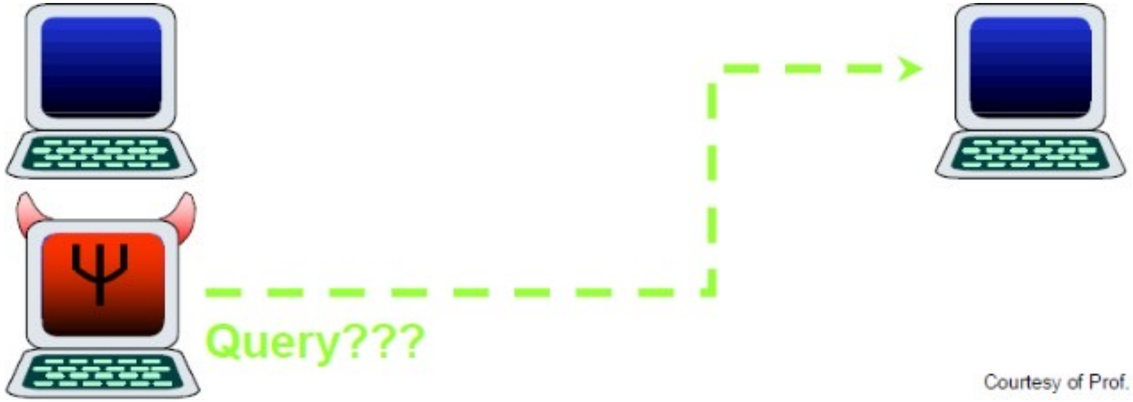


Authentication and Integrity

- Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
- Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information.
- Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

Access Control

- Access control: Requires that access to information resources should be controlled by the target system



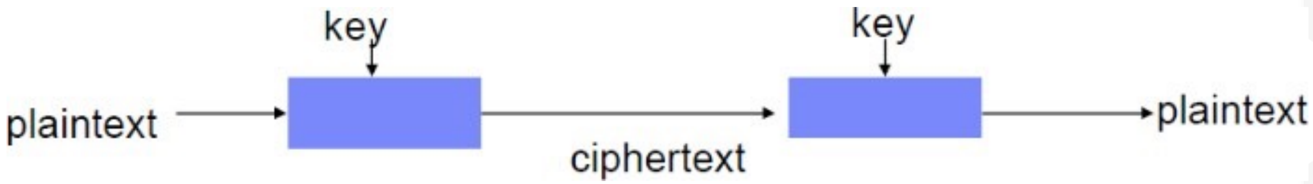
Courtesy of Prof. Kundur, Texas A&M

Non repudiation and Availability

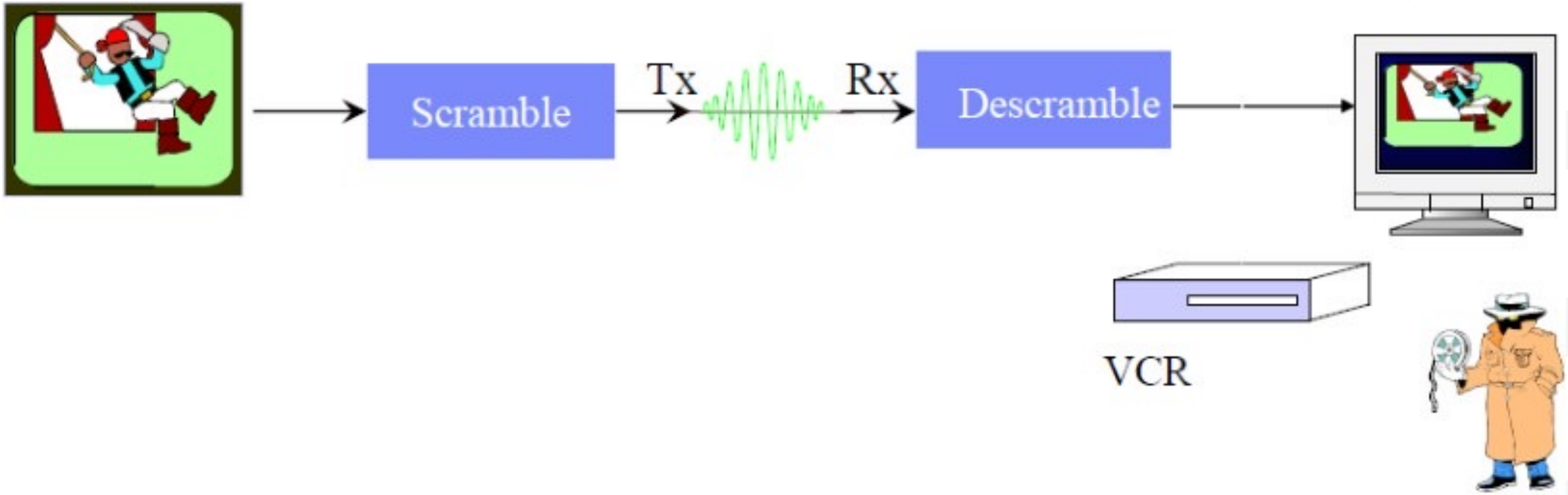
- Non-repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
- Availability: Requires that computer system assets be available to authorized parties when needed

Encryption

- Cryptography: The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form
- Plaintext: The original intelligible message
- Cipher text: The transformed message
- Cipher: An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- Key: Some critical information used by the cipher, known only to the sender& receiver
- Encipher (encode): The process of converting plaintext to cipher text using a cipher and a key
- Decipher (decode): the process of converting cipher text back into plaintext using a cipher and a key



Uninfringible MM: Copyright Protection and Copy Control



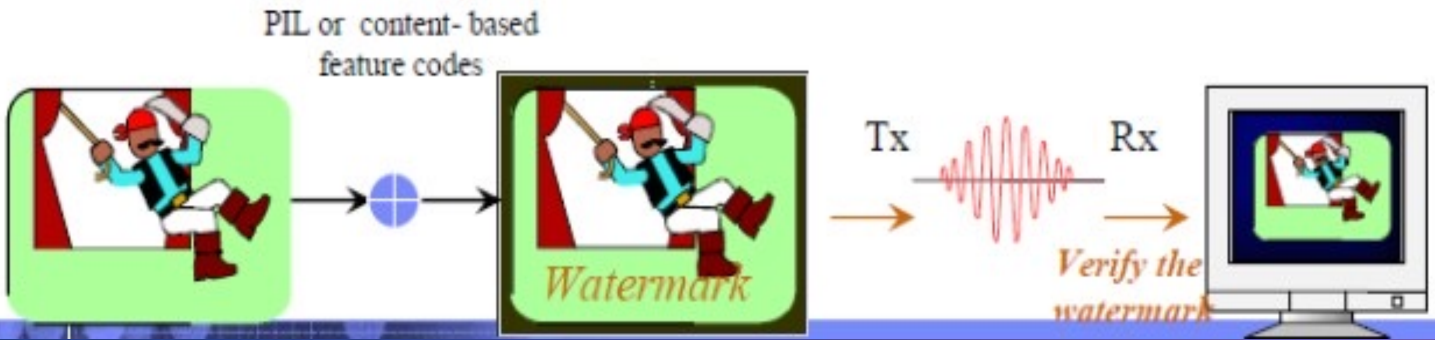
content-preserving transcoding:

- 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 audio-visual contents too much.
    - Visible: It must be visible, but it had better to be insensible.

Invisible Watermark

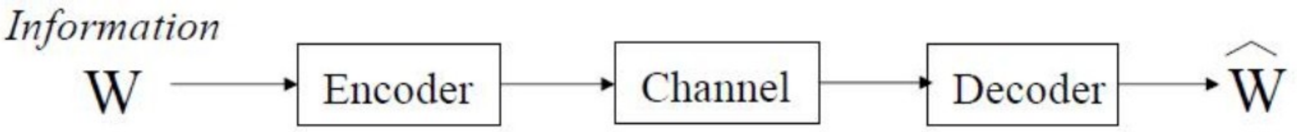
- Purpose
  - Protect ownership and trace illegal use.

- 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.

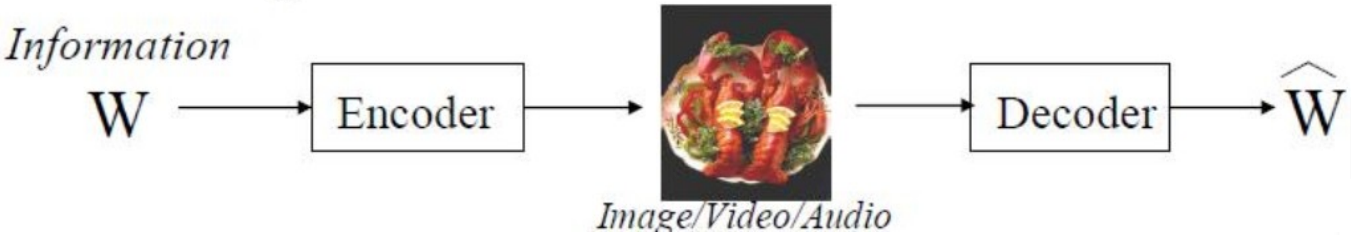
  - Invisible: The watermark should not visually affect the image/video content.

What is Watermarking?
Multimedia as a Communication Channel

- Basic communication system:

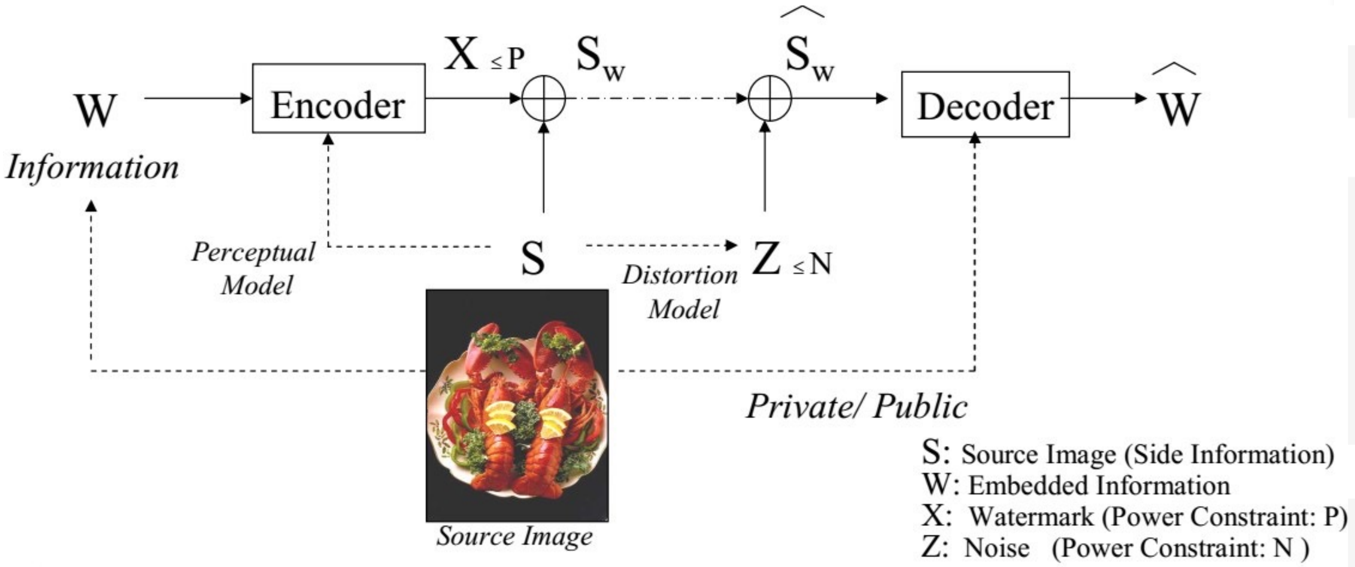


- Analog Communication – Encoder/ Decoder:
  - Amplitude Modulation (AM),
  - Frequency Modulation (FM).
  - Multiplexing: use different carrier frequencies.
  - Channel: air, wire, water, space,
- Watermarking:



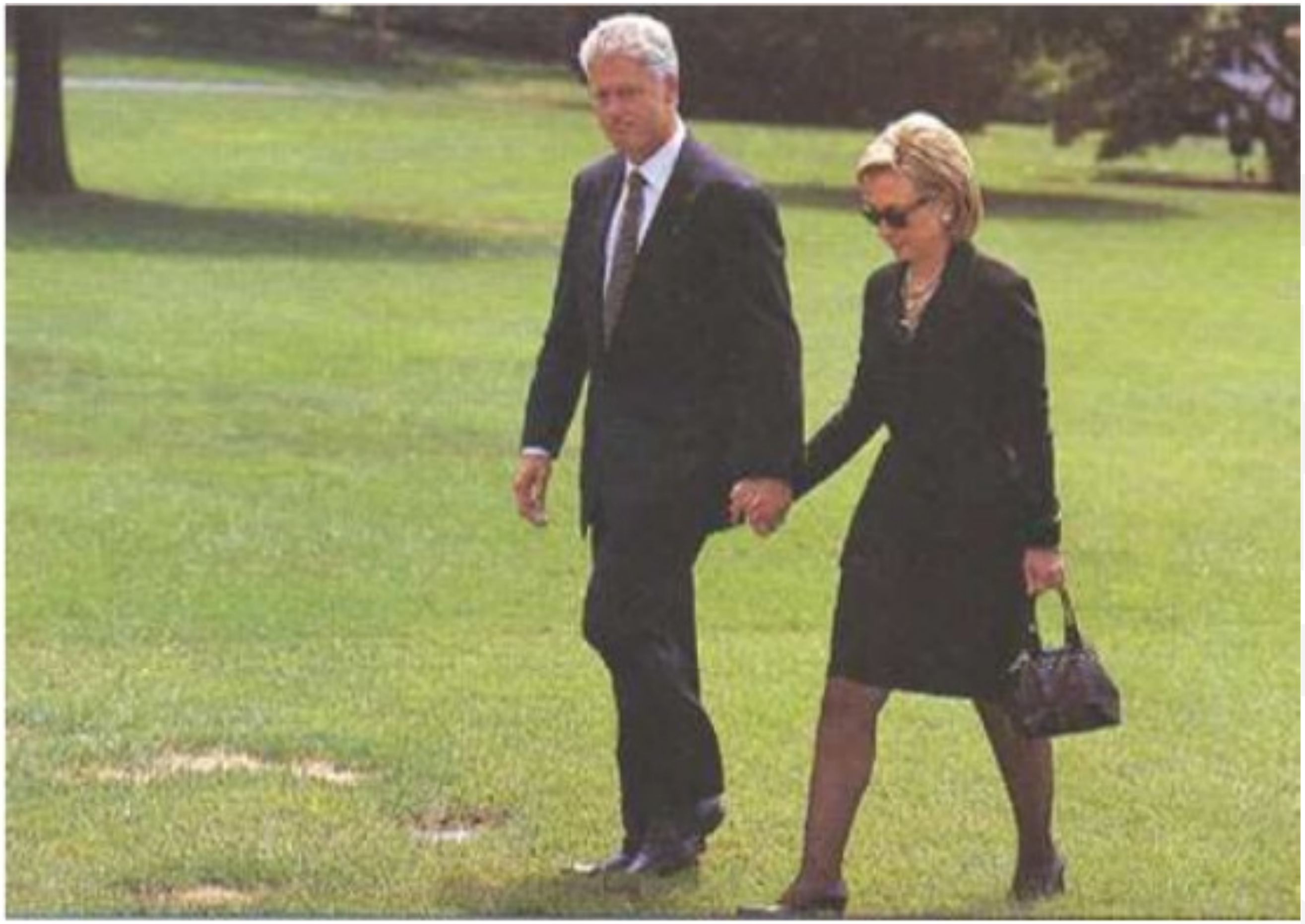
Watermarking-Multimedia as Communication Channel

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

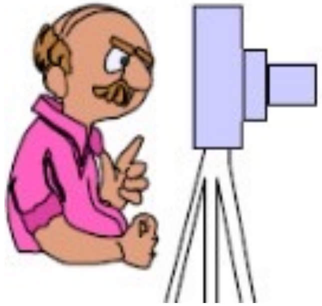


- Modulation
  - Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA).
  - Spread Spectrum is a CDMA technique, which needs modulation keys for Frequency Hopping or other specific codes.

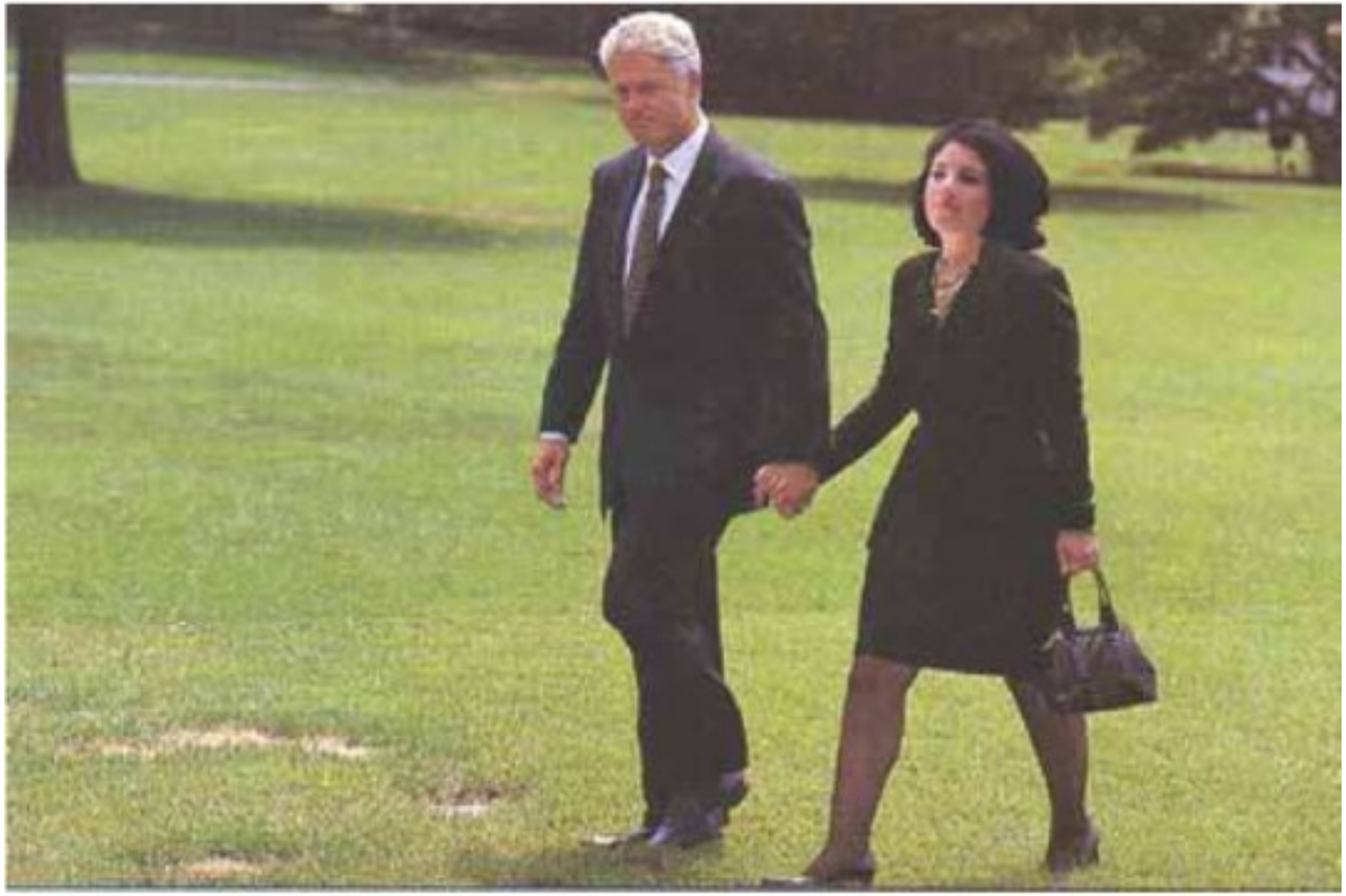
Authentication - Trustworthy MM



President Clinton and First Lady strolled in the White House



Somebody Manipulate …

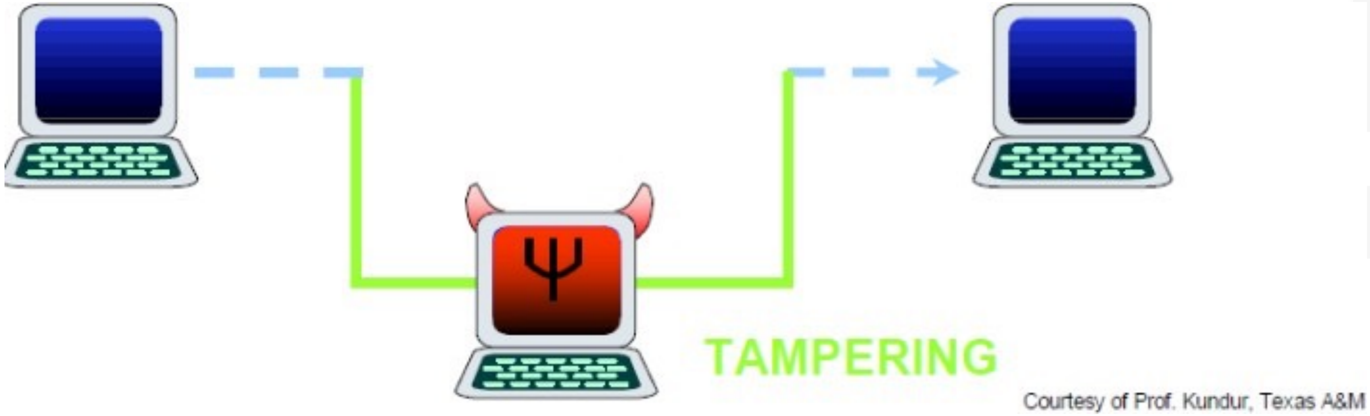


Another proof of their relationship ???

Hillary's Revenge???

Integrity

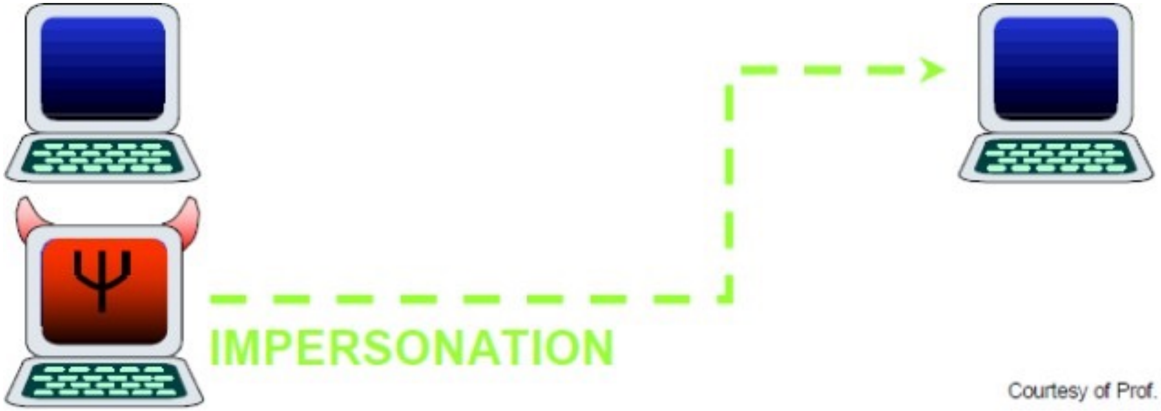
- Hash Functions
  - Traditional approaches sensitive to format conversion and minor bit changes
  - Existing software tools enable seamless tampering



Courtesy of Prof. Kundur, Texas A&M

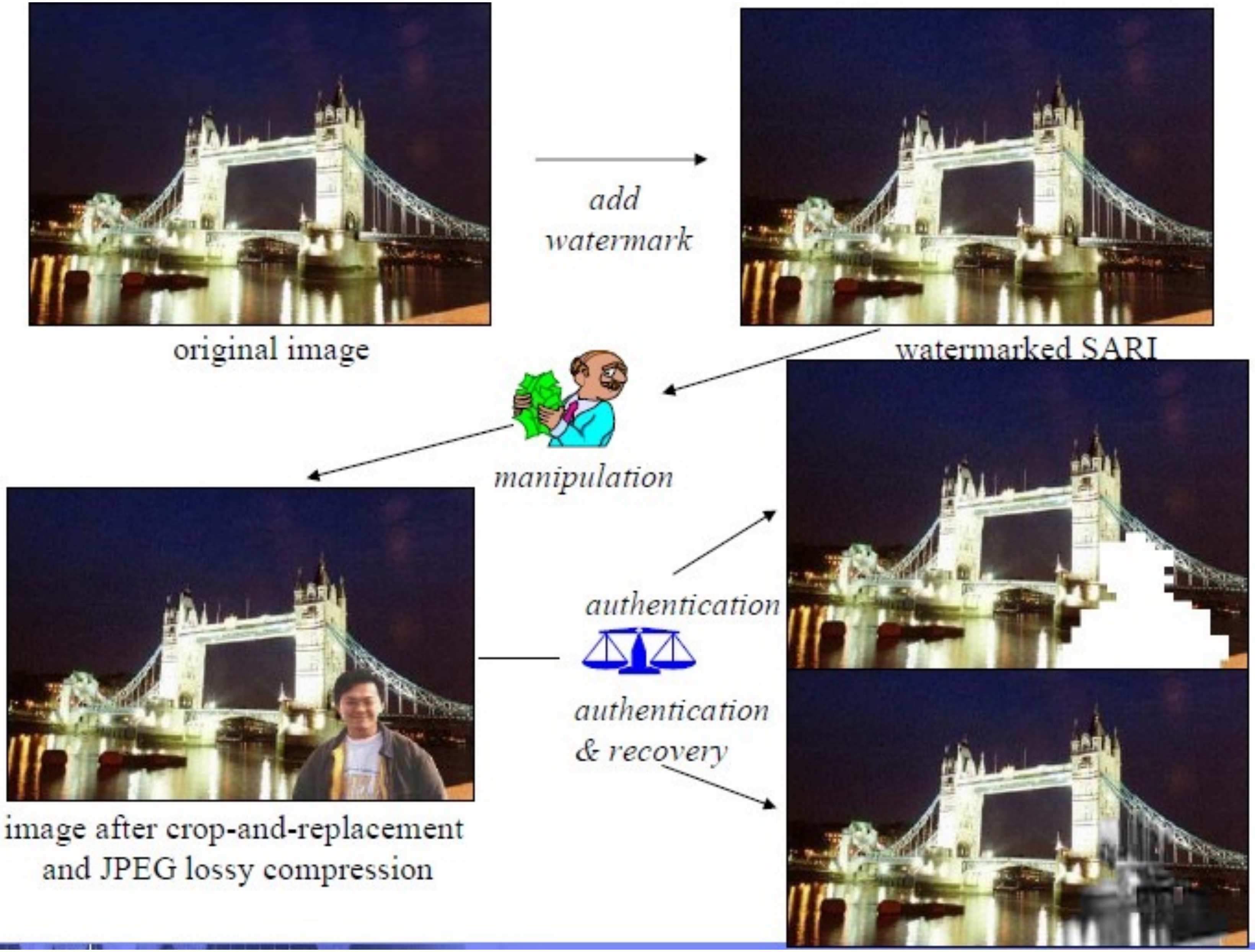
Person Authentication

- Digital signatures
- Biometrics

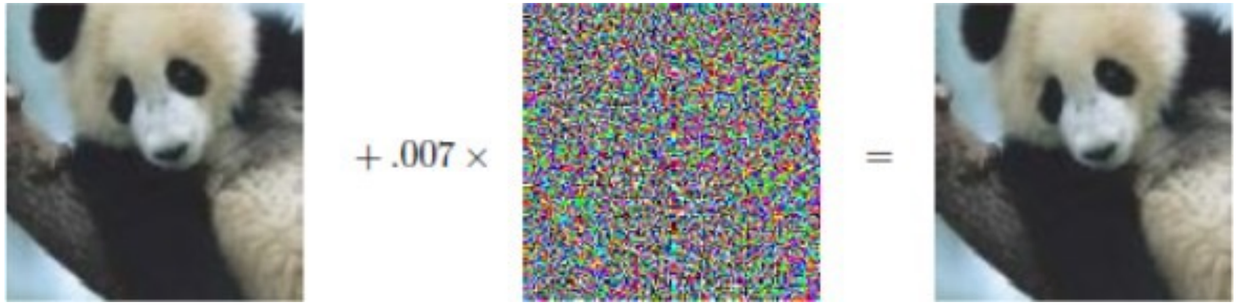


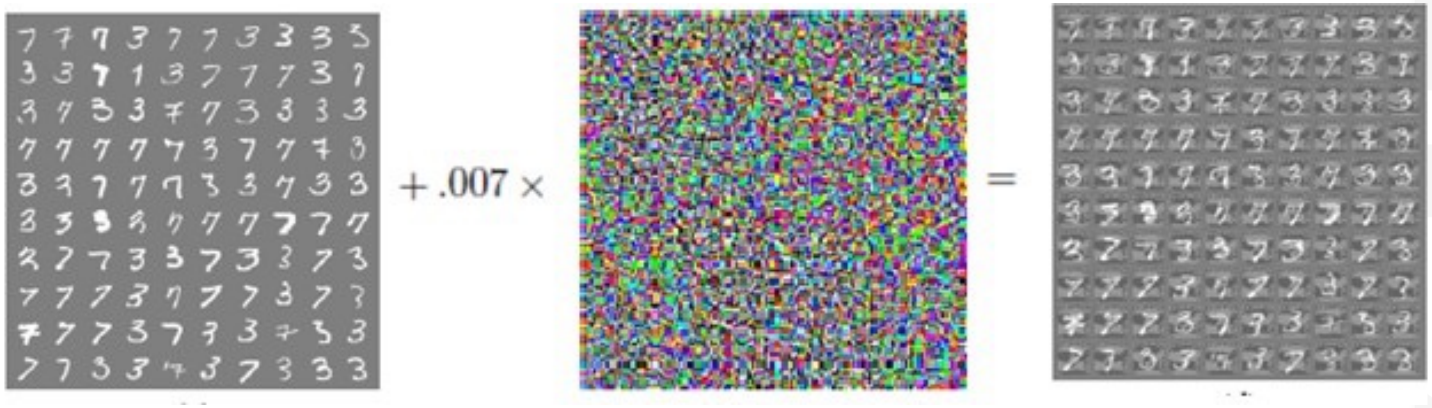
Courtesy of Prof. Kundur, Texas A&M

Self Authentication and Recovery Images


original image
add watermark
watermarked SARI
manipulation
image after crop-and-replacement and JPEG lossy compression
authentication
authentication & recovery

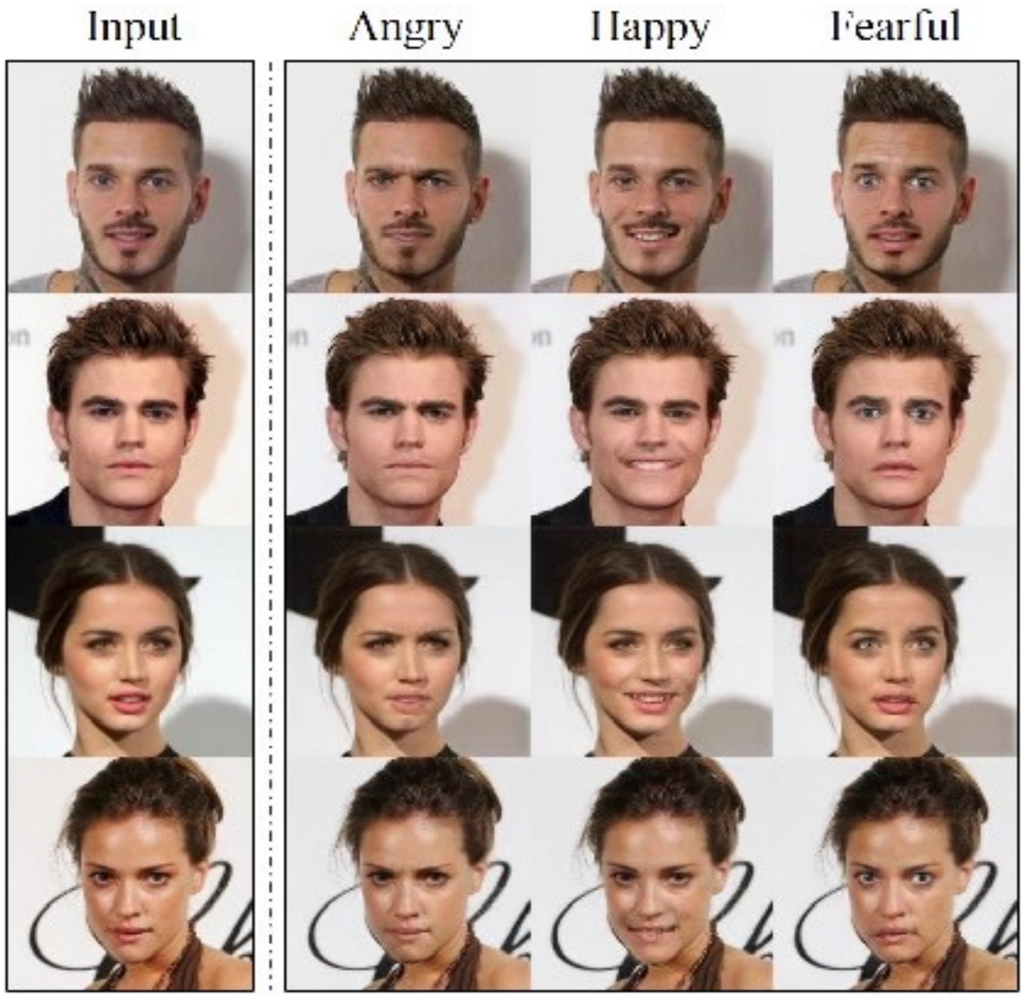
Adversarial Example and Adversarial Network



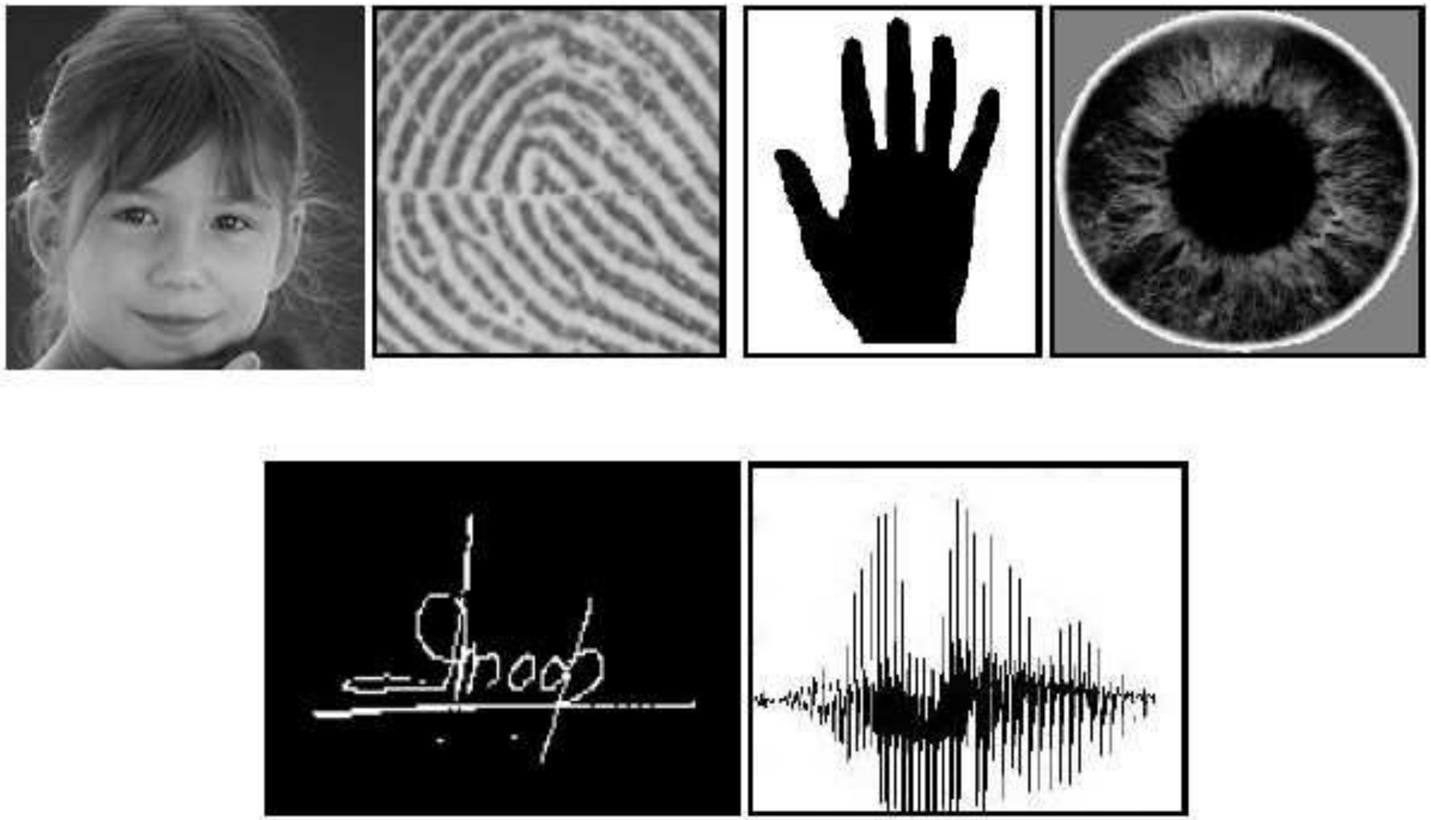


Adversarial Networks

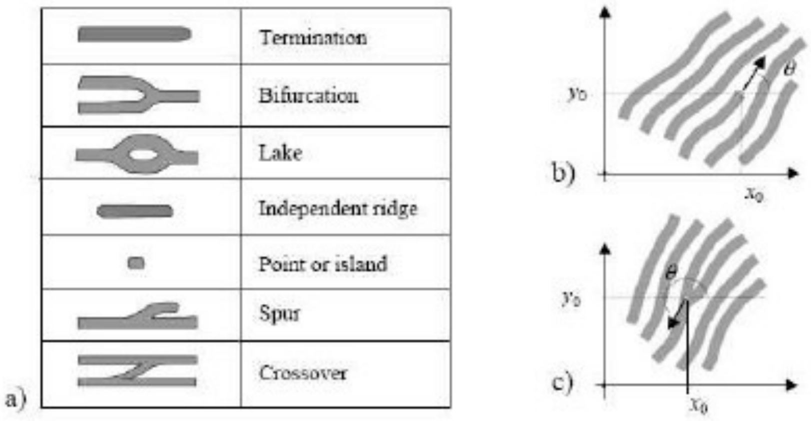
- All the images in the right columns are generated from input...



Biometric Features for Person Authentication

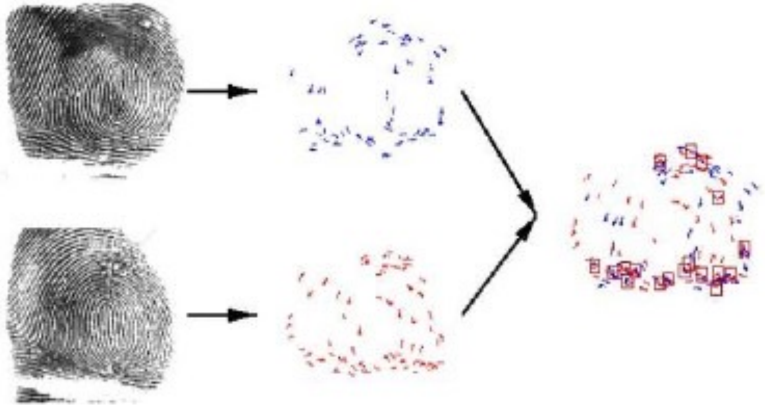


Example: Fingerprint-based Authentication



Fingerprint minutiae

Fingerprint Match



Other Related Research Issues

- 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

THANK YOU

VISIT US

WWW.XJTLU.EDU.CN

FOLLOW US

@XJTLU

Xi'an Jiaotong-Liverpool University
西交利物浦大学

XJTLU | SCHOOL OF FILM AND TV ARTS