INT307 Multimedia Security System

Overview

Shengchen Li

Xi'an Jiaotong-Liverpool University

17th Aug 2022

Lecturer - Shengchen Li

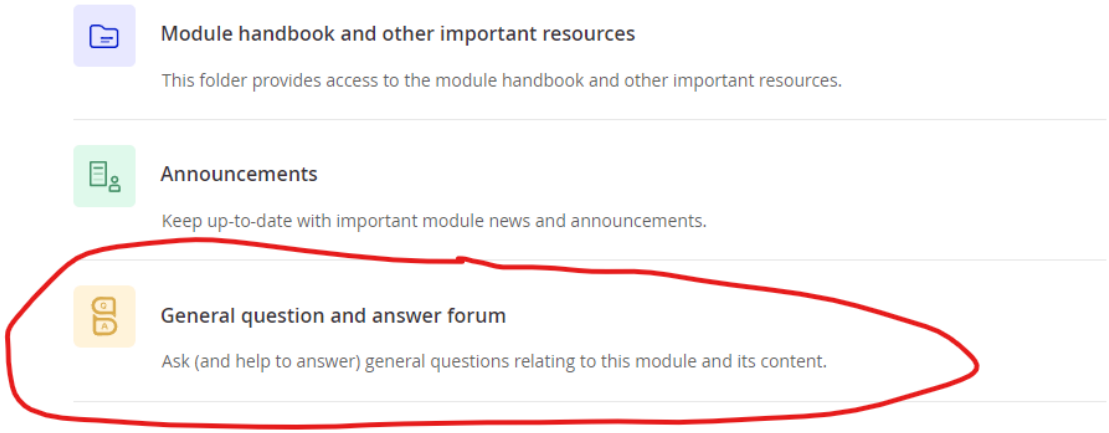
- Graduated from Queen Mary University of London
- Was a lecturer in Beijing University of Posts and Telecommunications
- Research focus: machine listening

Office Hours

TBD

Raise a Question

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



Teaching Assistants

TBA

NOTE

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

Lecture Recording

- Not an alternative to attending lectures
- Will be released one week later than lectures to allow editing and double check
- In-class discussion will not be recorded

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

Module Assessment

Overview

There are three assessments in this module

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

Module Assessment

Coursework 1

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

- Encryption (Cipher)
- Digital Signature
- Digital Forensics
- Steganography
- Blockchain

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 24th Oct 2022 (50 Marks)
- Report Submission Deadline: 20th Oct 2022 (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

- Robust face recognition system
- Evaluation of robustness for a deep learning algorithm
- Attacks on audio fingerprinting system

For more marks

You should propose a possible future research direction for the topic

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 10-13 (along with lectures) (50 Marks)
- Formal report submission DDL: 15th Dec 2022 (50 Marks)

Two round submission

A draft report should be handed in before the presentation for feedbacks

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

Lecture Overview

- Overview: Week 2
- Multi-media Compression: Week 3-4
- Media Security: Week 5-6
- Presentation for CW1: Week 7
- Deep Learning Basics: Week 9-10
- Algorithm Security: Week 11-13
- Review: Week 14

Attendance

You will not be punished for low attendance rate

Attendance

Attend all lectures would help to prevent module failure

Multi-media Compression

- Introduction of human perception
- Introduction of multimedia representation
- Basics of encoding
- Commonly used industry standards

Media Security

- Cipher / Encryption
- Digital Forensics
- Digital Signature
- Steganography
- Blockchain

Deep Learning

- Neural Network
  - Fully Connected Network
  - Convolutional Neural Network
  - Recurrent Neural Network
  - Transformer

- Generative Learning
  - Sequence to Sequence
  - Variational Auto-Encoder
  - Generative Adversarial Network

Algorithm Security

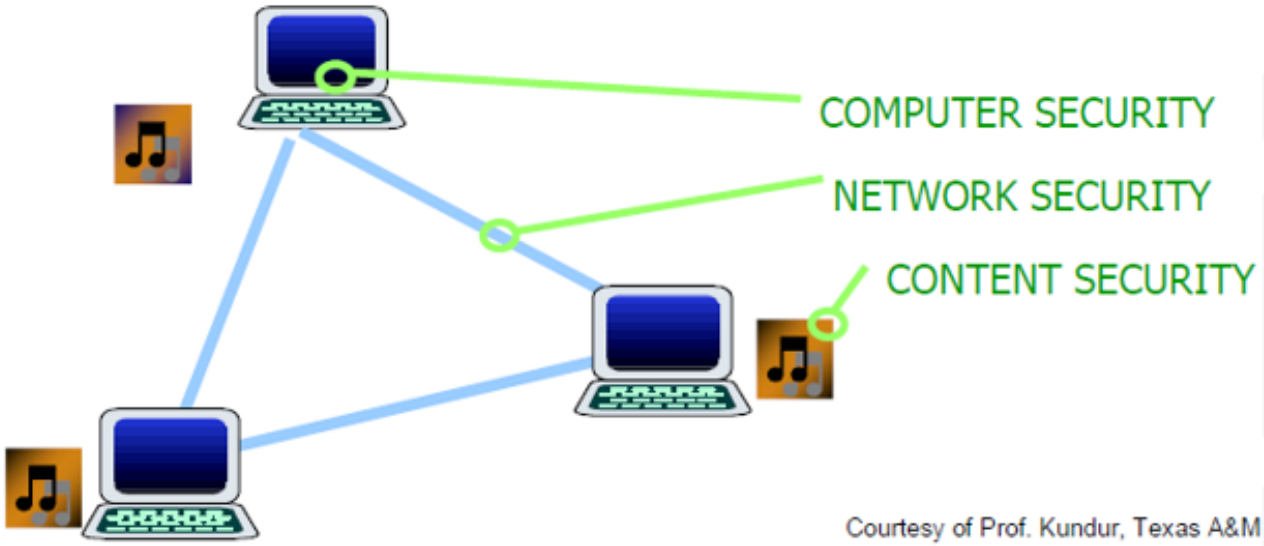
- Adversarial Attack
- Evaluation of deep learning systems
- Improve the robustness of deep learning systems
- Deepfake and identification of deepfake

Tutorials

There are 6 Tutorials in this module

- Week 3: Reference Hunting
- Week 5: Academic Writing
- Week 7: CW1 Presentation
- Week 9: Feedback for CW1
- Week 11: CW2 Presentation
- Week 13: Feedback for CW2

Type of Security



- Network Security
- Software Security
- Content Security

Network Security

- Authentication over transmission
- Protection over transmission
- Discussion
  - How can we prevent unexpected media modification
  - How can we demonstrate a media file has been modified over transmission

Content Security

- Content Protection
  - Encryption
  - Modification Detection
- Machine Generation Detection
  - ASVspoof
  - Deepfake
- Discussion
  - What new challenge has been brought to us by deep learning?

Multimedia Security

- Data Security / Media Security
  - Encryption
  - Watermarking
- Algorithm Security
  - Robust Information Retrieval
  - Fake Multimedia Detection

Applications

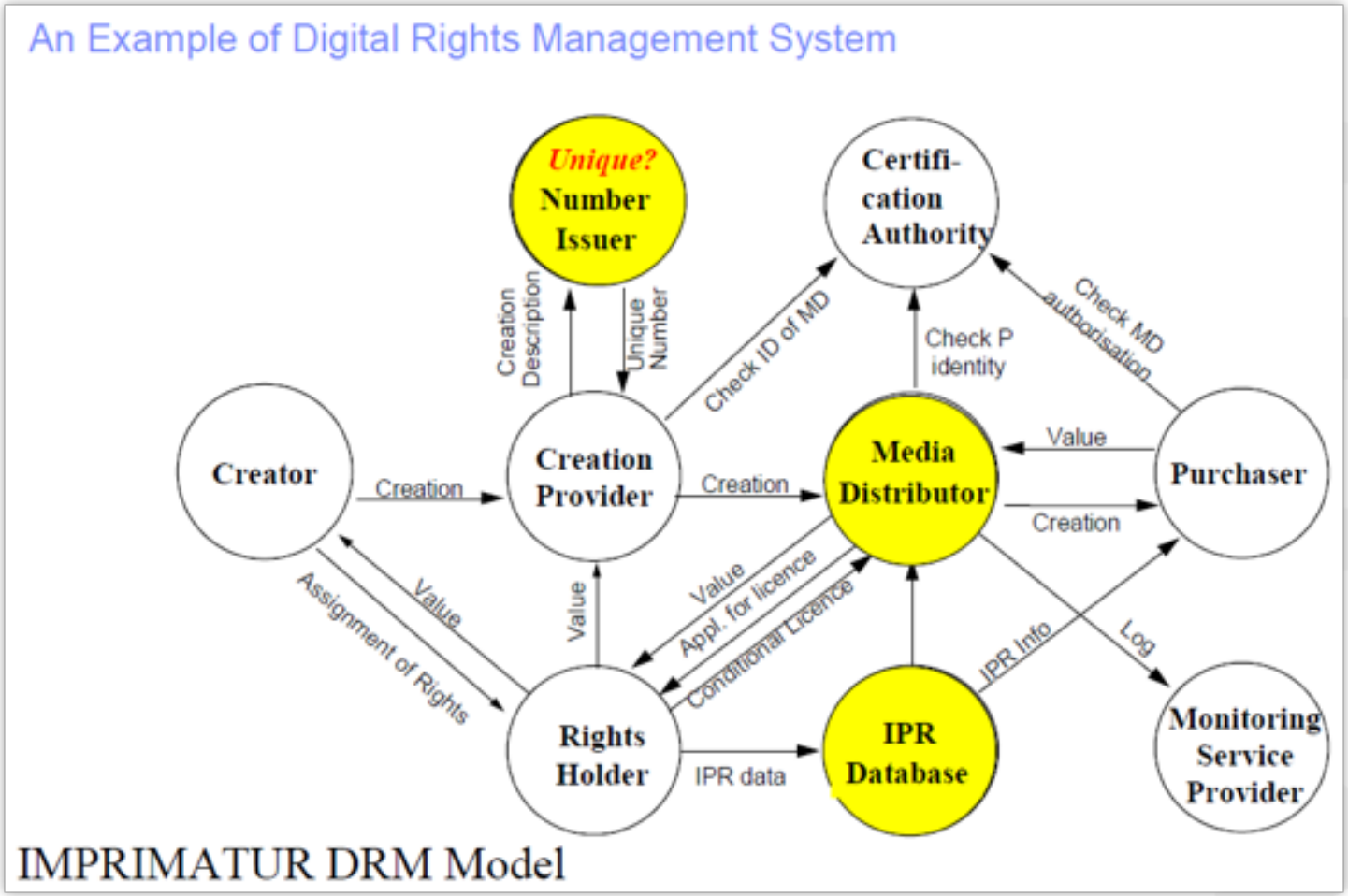
- Authentication
- Copy Protection
- Automatic Surveillance
- Synthesised Media Detection
- Digital Forensics

Authentication

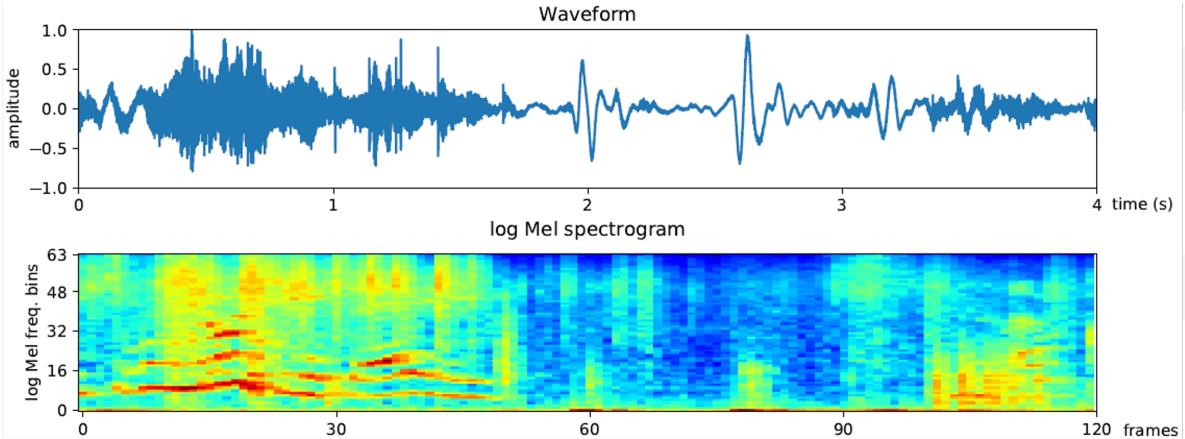
Possible Factors

- Audio: Audio Fingerprint
- Fingerprint
- Password / Passcode
- Face Recognition

Copyright Protection

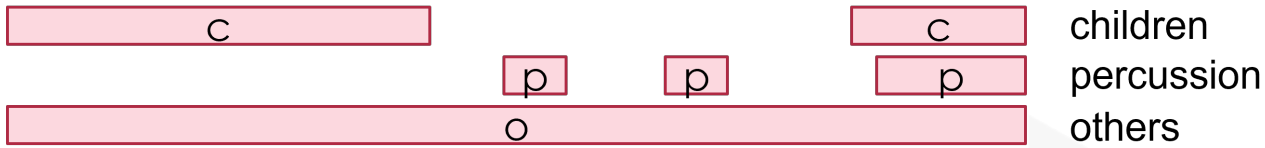


Digital Surveillance

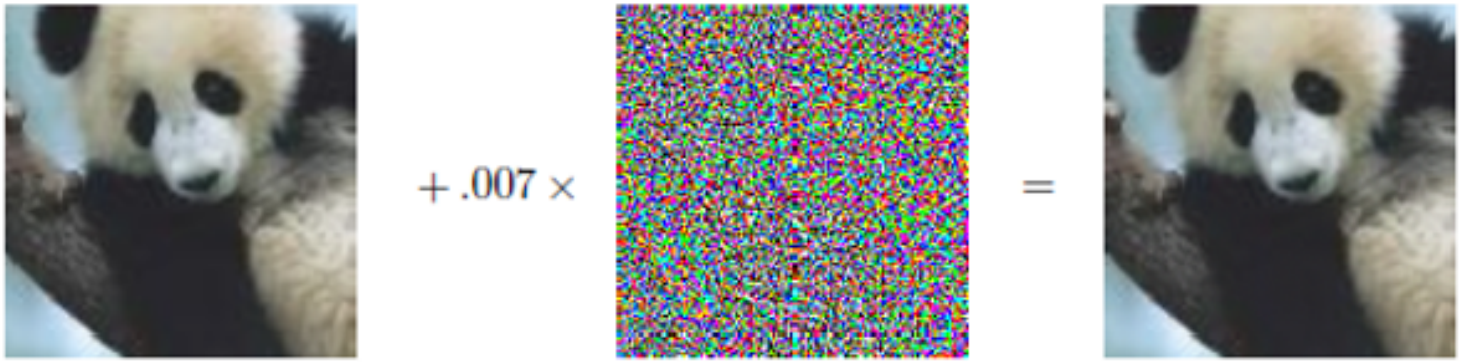


Audio tagging: children (c), percussion (p), other sounds (o).

Sound event detection:



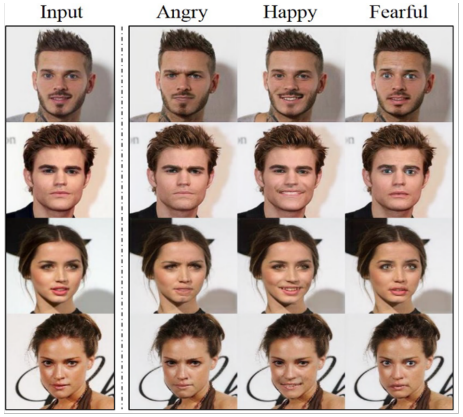
Adversarial Attack



Synthesised Media Detection

Multimedia Authentication:

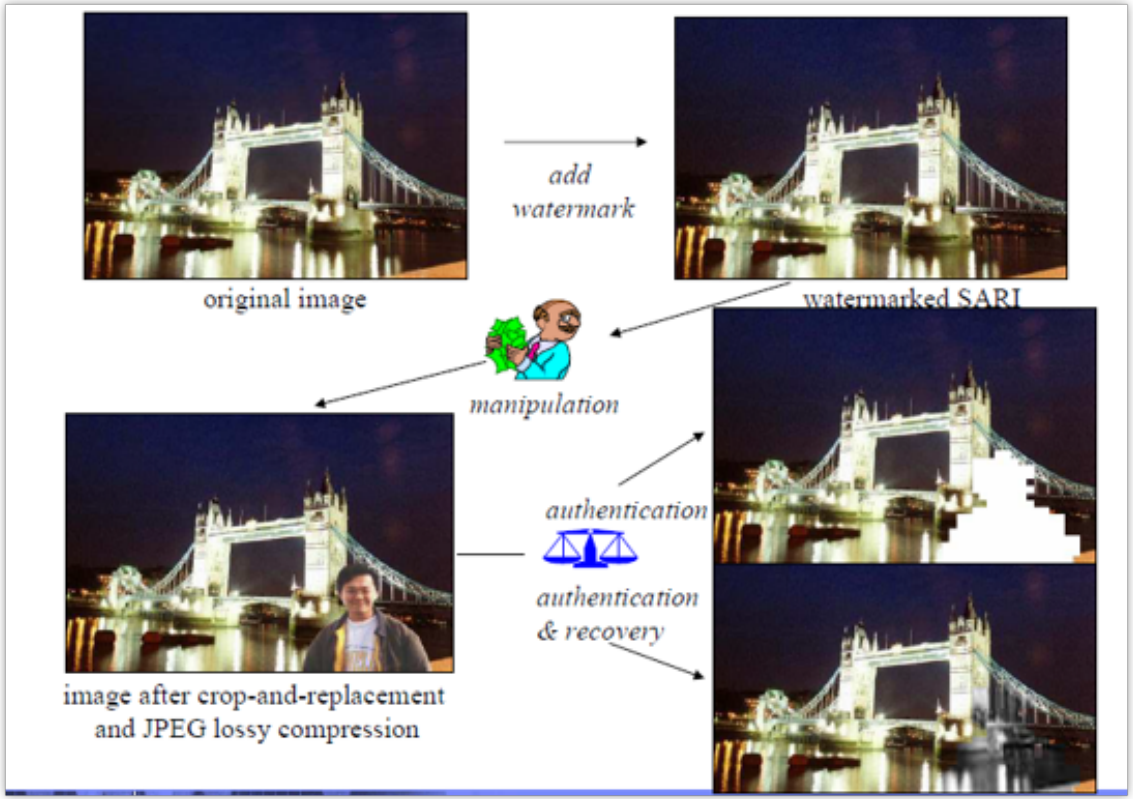
How to authenticate multimedia



Adversarial attack:

How to attack or protect Multimedia

Digital Forensics



- Identify the source of images
- Identify possible modifications

Methodologies

- Advanced Algebra Methods
  - Encryption
  - Blockchain (HASH function)
- Probability Methods
  - Multimedia Surveillance
  - Robust Detection
  - Fake Multimedia Detection

More Recent Development

- The development of deep learning methods
- New Problems:
  - Media synthesis
  - Media modification
- This introduces a new topic of algorithm security