CS355-15 Digital Forensics

23/24

Department
Computer Science
Level
Undergraduate Level 3
Module leader
Yu Guan
Credit value
15
Module duration
10 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

In this module, you will learn about the scientific techniques used to collect probative facts from digital data often in relation to cyberphysical crime.

Module aims

The module will focus on a subfield of digital forensics that involves analysing image and video data for forensic purposes. This subfield (digital image forensics) is getting increasingly important since digital cameras and sophisticated photo editing softwares have become commonplace. Advanced machine learning methods are now capable of generating fake images and videos that can easily fool humans. Image forensic experts develop and use computational techniques to identify photo forgery, detect image sources and collect crime-related evidences from image data.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The module will deal with core concepts and enabling methodologies in multimedia-based digital forensics. It will also examine current applications, and address theoretical and practical challenges. More specifically the syllabus will cover:

- Methodologies and standards for acquisition and processing in digital forensics
- Modalities of device fingerprints
- Extraction and representation of device fingerprints
- Enhancement of device fingerprints
- Source device identification based on device fingerprints
- Content/device linking based on device fingerprints
- Content integrity verification based on device fingerprints
- Source-oriented image/video clustering based on device fingerprints
- Digital content hashing
- Data hiding
- Digital watermarking for copyright protection
- Digital watermarking for content authentication
- Steganography
- Steganalysis
- Counter-forensics and counter-counter-forensics

Learning outcomes

By the end of the module, students should be able to:

- Understand the basics of image and video data acquisition and analysis, and computational methods to detect image or video forgery.
- Identify and/or design a suitable computational technique to establish or revoke authenticity of a given image/video.
- Apply the identified computational techniques to detect authenticity of image and video data.

Research element

The 'Sensor based forensics' section in the syllabus is based on recent research advances on this topic. The students will be reading from research papers instead of textbooks. They will also implement the techniques described in the research paper.

Subject specific skills

Knowledge of types of image forgery
State-of-the-art forensics methods
Forensics algorithms
Forensics practices.

Transferable skills

Programming
Knowledge of image and video processing
Knowledge of basic probability, linear algebra and transforms
Report writing
Analytical thinking.

Study

Study time

Type	Required
Lectures	20 sessions of 1 hour (13%)
Practical classes	9 sessions of 1 hour (6%)
Private study	121 hours (81%)
Total	150 hours

Private study description

Studying textbook, lecture notes, other resources provided
Solving the exercise questions and practice problems, given during the lectures
Coursework preparation including programming and report preparation.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Students can register for this module without taking any assessment.

Assessment group D4

	Weighting	Study time
Individual practical assignment 1 Individual practical assignment.	15%	
Individual practical assignment 2 Individual practical assignment.	15%	
In-person Examination Exam	70%	

- Answerbook Pink (12 page)
- Students may use a calculator

Assessment group R3

	Weighting	Study time
In-person Examination - Resit resit examination	100%	

- Answerbook Pink (12 page)
- Students may use a calculator

Feedback on assessment

Written feedback on coursework will be provided to the students.

Past exam papers for CS355

Availability

Pre-requisites

Students must have studied the content of CS131 Mathematics for Computer Scientists II or CS137 Discrete Mathematics II or ES193 Engineering Mathematics or have studied equivalent material.

Courses

This module is Optional for:

- UCSA-G4G1 Undergraduate Discrete Mathematics
  - Year 3 of G4G1 Discrete Mathematics
  - Year 3 of G4G1 Discrete Mathematics
- Year 3 of UCSA-G4G3 Undergraduate Discrete Mathematics
- Year 4 of UCSA-G4G4 Undergraduate Discrete Mathematics (with Intercalated Year)
- Year 4 of UCSA-G4G2 Undergraduate Discrete Mathematics with Intercalated Year

This module is Option list A for:

- Year 4 of UCSA-G504 MEng Computer Science (with intercalated year)
- UCSA-G500 Undergraduate Computer Science
  - Year 3 of G500 Computer Science
  - Year 3 of G500 Computer Science
- UCSA-G502 Undergraduate Computer Science (with Intercalated Year)
  - Year 4 of G502 Computer Science with Intercalated Year

    - Year 4 of G502 Computer Science with Intercalated Year
- UCSA-G503 Undergraduate Computer Science MEng
    - Year 3 of G500 Computer Science
    - Year 3 of G503 Computer Science MEng
    - Year 3 of G503 Computer Science MEng
- USTA-G302 Undergraduate Data Science
    - Year 3 of G302 Data Science
    - Year 3 of G302 Data Science
- Year 3 of USTA-G304 Undergraduate Data Science (MSci)
- Year 4 of USTA-G303 Undergraduate Data Science (with Intercalated Year)