CS355-15 Digital Forensics

26/27

Department
Computer Science
Level
Undergraduate Level 3
Module leader
Yu Guan
Credit value
15
Module duration
9 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, preserve, and analyse digital evidence, often in the context of cybercrime and cyber-physical incidents.

Module web page

Module aims

The module focuses on a subfield of digital forensics concerned with the forensic analysis of image and video data. Digital image forensics has become increasingly important as digital cameras, sophisticated editing software, and AI-based image generation tools have become widely accessible. Modern machine learning methods are now capable of generating highly realistic fake images and videos that can be difficult for humans to detect. This module explores the computational techniques used to identify image manipulation, determine image provenance, and extract evidential information from digital image data for forensic and investigative purposes.

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
- Image enhancement for forensic applications
- Digital watermarking
- Image forgery detection
- Image Compression and compression-based forensic approaches
- Visual computing and pattern matching
- Source camera identification based on device fingerprints
- Deepfake detection

Learning outcomes

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

- Demonstrate a systematic understanding of how image and video data are acquired and analysed, including established methods for detecting image and video forgery.
- Evaluate and justify appropriate computational techniques for determining whether image and video data are authentic, taking into account the nature of the data and the context of the problem.
- Apply established computational techniques to analyse image and video data, determine their authenticity, and interpret and communicate the results appropriately.

Research element

The 'source camera identification' and 'deepfake detection' sections in the syllabus are 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 D5

	Weighting	Study time	Eligible for self-certification
Individual practical assignment.	30%		No
In-person Examination	70%		No
Exam			

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

Assessment group R4

	Weighting	Study time	Eligible for self-certification
In-person Examination - Resit resit examination	100%		No

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

Feedback on assessment

Written feedback on coursework will be provided to the students.

Past exam papers for CS355

Availability

Pre-requisites

Basic skills in linear algebra and programming are required.

Courses

This module is Optional for:

- 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)

This module is Core option list A for:

- Year 5 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
  - 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 G503 Computer Science MEng
  - Year 3 of G503 Computer Science MEng

This module is Core option list B for:

- UCSA-G4G1 Undergraduate Discrete Mathematics
    - Year 3 of G4G1 Discrete Mathematics
    - Year 3 of G4G1 Discrete Mathematics
- UCSA-G4G3 Undergraduate Discrete Mathematics
    - Year 3 of G4G1 Discrete Mathematics
    - Year 3 of G4G3 Discrete Mathematics
- Year 5 of UCSA-G4G4 Undergraduate Discrete Mathematics (with Intercalated Year)
- Year 4 of UCSA-G4G2 Undergraduate Discrete Mathematics with Intercalated Year