CS955-15 Digital Forensics

26/27

Department
Computer Science
Level
Taught Postgraduate Level
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 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 critical understanding of how image and video data are acquired and analysed, including advanced and emerging methods for detecting image and video forgery, informed by current research in digital forensics.
- Critically evaluate, select, and adapt computational techniques for determining whether image and video data are authentic, taking into account assumptions, limitations, and incomplete or ambiguous evidence.
- Apply and adapt advanced computational techniques to analyse complex image and video data, working autonomously to design investigations and critically interpret and communicate the results.
- Critically evaluate existing approaches to image and video forensics and propose justified improvements or alternative approaches informed by current research and professional practice.

Indicative reading list

Reading lists can be found in Talis

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 papers.

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.

Assessment group D

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

	Weighting	Study time	Eligible for self-certification

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

Assessment group R

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

- 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 CS955

Availability

Courses

This module is Optional for:

- TCSA-G5PD Postgraduate Taught Computer Science
  - Year 1 of G5PD Computer Science
  - Year 1 of G5PG Computer Science with specialism in Artificial Intelligence and Machine Learning
  - Year 1 of G5PH Computer Science with specialism in Cyber Security
  - Year 1 of G5PI Computer Science with specialism in Data Analytics

This module is Core option list A for:

- Year 1 of TCSA-G5PD Postgraduate Taught Computer Science

This module is Core option list B for:

- TCSA-G5PD Postgraduate Taught Computer Science
  - Year 1 of G5PG Computer Science with specialism in Artificial Intelligence and Machine Learning
  - Year 1 of G5PI Computer Science with specialism in Data Analytics