MPhil in Advanced Computer Science
Topics in Security: Forensic Signal Analysis

Leader:	Dr Markus Kuhn
Term:	Michaelmas 2009
Prerequisites:	Linear Algebra, Probability or Statistics, Digital Signal Processing, Information Theory and Coding, Security
Structure:	8 × 2-hour seminar sessions

AIMS

This module looks at recent research literature on security applications of digital signal processing techniques.

SYLLABUS

A particular focus will be algorithms for the forensic analysis of digital signals, such as identifying origin, processing history, manipulation, information leakage, or steganographic content in radio signals, images, audio or video recordings. Related topics that may be touched upon include advanced eavesdropping and side-channel analysis techniques that are of concern in the design of secure and privacy-preserving digital devices. Example topics are

- Digital photography: processing pipeline and sensor characteristics, sensor identification.
- Anomaly detection: statistics of natural images, inconsistencies in lighting and chromatic abberation, duplication detection.
- Image and video processing: resampling algorithms (rotation, scaling) and their identification via linear dependency patterns among adjacent pixels, compression history identification, super-resolution.
- Document printer/scanner identification.

with possible excursions into

- Steganography, watermarking, and fingerprinting: algorithms for hiding, recovering, detecting and distorting embedded signals, invariant properties
- Side-channel attacks: timing analysis on cipher implementations, power analysis, electromagnetic analysis, compromising emanations

OBJECTIVES

On completion of this module students should:

- have gained an overview of the existing literature in forensic signal analysis and some other security applications of signal processing algorithms,

- appreciate the theoretical fundations, prerequisites and skills needed for doing research in this area,
- have gained experience in critically reviewing papers (like in conference program committees).

COURSEWORK

This seminar will be dominated by student presentations of papers and their discussion. Each student is expected to

- prepare and give a 40-minute presentation on 2–3 related papers on the reading list (15 hours);
- prepare an essay on the subject of the presentation (15 hours);
- write single-page reviews for eight of the papers on the reading list (8×2 hours);
- prepare and present a research proposal for a project related to the topic of this seminar (3 hours).

Students can pick papers from the reading list depending on their interest, but there must be no overlap between the papers presented. (All these numbers may change depending on the number of students actually taking the course.)

PRACTICAL WORK

Each student is expected to implement as a prototype and demonstrate one or two of the signal processing techniques described in the paper that they present (e.g., in MATLAB), depending on their complexity (15 hours).

ASSESSMENT

The final grade will be the average of five subgrades given for the presentation, the essay, the practical experiment, the reviews, and participation in the discussions (the latter including credit for the project proposal and attendance).

READING LIST

`http://www.cl.cam.ac.uk/teaching/0910/R08/`
(students are welcome to suggest additions to the reading list,
see `http://www.cl.cam.ac.uk/~abl26/bibliography/` for further suggestions)

Last updated: October 2009