Topics in Security:
Forensic Signal Analysis

Markus Kuhn, Andrew Lewis

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

http://www.cl.cam.ac.uk/teaching/0910/R08/

Michaelmas 2009 – MPhil ACS

Introductory examples:

manipulation of photographs

Fact or fiction?

Hans D. Baumann, DOCMA

Real

Hans D. Baumann, DOCMA

or fantasy

Hans D. Baumann, DOCMA

Political photos may suddenly lack past company ...

Stalin, 1930

`http://www.cs.dartmouth.edu/farid/research/digitaltampering/`

... unreliable government hardware ...

Iranian missile test, July 2008

`http://www.cs.dartmouth.edu/farid/research/digitaltampering/`

... or even body parts.

President Nicolas Sarkozy. *Paris Match*, August 2007

`http://www.cs.dartmouth.edu/farid/research/digitaltampering/` ... with many more

Forensic Signal Analysis

This course looks at the use of digital signal processing techniques in a security context, to uncover hidden information from image, video, audio, electromagnetic, etc. signals, in particular to

- ⟶ identify manipulation;
- ⟶ identify/verify processing history;
- ⟶ identify/verify type or instance of the acquiring sensor;
- ⟶ eavesdrop on persons or computer systems;
- ⟶ communicate covertly (steganography).

This is a "reading class", i.e. the "lecture notes" are selected recent original research publications and the material is mostly presented by the students.

Prerequisites

A background in digital signal processing, image processing, linear algebra, probability, statistics, data compression, communication technology (modulation and detection) will be useful.

Some background reading beyond the presented papers will be helpful, in particular on

- ⟶ Fourier transform, linear time-invariant systems, filters
  `http://www.cl.cam.ac.uk/teaching/0809/DSP/`
- ⟶ Discrete Cosine Transform, JPEG, MPEG
  `http://www.w3.org/Graphics/JPEG/itu-t81.pdf`
  Pennebaker, Mitchell: JPEG still image data compression standard. (Moore Library)
- ⟶ Digital photography
  CCD/CMOS sensors, Bayer pattern and interpolation, "raw" formats, noise reduction algorithms, . . .

Presentation + Essay

Each student has to choose and lead a 1-hour slot of the course, each of which covers typically 2–3 related papers. This student will

- ⟶ implement small experiments inspired by a presented paper;
- ⟶ prepare an essay of up to 2500 words that summarizes and discusses the experiment and the main contributions of the chosen papers;
- ⟶ prepare and present a $\approx$ 40 minute talk on the same.

The remaining time is for questions, discussion of the presented papers and the reviews, discussion of related research ideas, as well as for brief tutorials on related background knowledge.

Each student should meet the lecturer one week before *their* presentation slot and must hand in their essay (PDF email to mgk25) by **Wednesday 12:00** after the day of their presentation.

Reviews

Each week, all other students (excluding those presenting in the next session) will write an about 300–500 word long review of *one or two* of the papers that are going be presented at the next session. These reviews must be handed in by **Wednesday 12:00** before the session (plain-text email to mgk25, no Word or PDF please). Only eight reviews have to be submitted in total.

Reviews should be similar in style to those expected from journal reviewers and members of conference programme committees, i.e.

- ⟶ concisely summarize the contribution of the paper;
- ⟶ identify particular strengths and weaknesses of the paper;
- ⟶ suggest possible improvements;
- ⟶ assign and justify a grade on a 1–10 scale
  0=hopeless, 10=brilliant, where 5/6 is is the dividing line between recommending acceptance and rejection at a selective conference.

Slides, essays and reviews will be made available to all course participants via the course web page.

Project proposal

Each student is also asked to prepare a research project proposal (e.g. for an MPhil or PhD thesis), consisting of a brief handout and a 10-minute "sales-pitch".

Such a proposal should

- ⟶ outline a problem area;
- ⟶ state a research question;
- ⟶ list potentially applicable research methods and tools;
- ⟶ identify the most relevant related literature;
- ⟶ identify risks;
- ⟶ identify success criteria and milestones.

These are due for the last session of the course. No slides are expected for the oral presentation.

Evaluation

The lecturer will assess each of the following contributions on a 0–100% scale, and the overall course mark will be formed out of an arithmetic average, weighted as follows:

- ⟶ presentation: 20%
- ⟶ essay: 20%
- ⟶ experiment: 20%
- ⟶ top-8 reviews: 20%
- ⟶ participation in discussions, attendance, project proposal: 20%

A good average contribution will receive a 75% grade, leaving room above for extensions that go beyond.

Each missed session will reduce by 5% the participation score!

The 80-hour time budget for the course consists of 16 hours for the sessions, 8×2 hours for the reviews, 15 hours each for preparing the experiment, the essay and the presentation, and 3 hours for preparing the project proposal.

Topics

Students are most welcome to suggest additional or alternative papers within each topic.

For additional references and URLs, see
Andrew Lewis: Multimedia forensics bibliography
`http://www.cl.cam.ac.uk/~abl26/bibliography/`

Resampling detection in images

- ⟶ Popescu, Farid: Statistical tools for digital forensics (part)
- ⟶ Kirchner: Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue
- ⟶ Gloe, Kirchner, et al.: Can we trust digital image forensics? (part)

Recompression history

- ⟶ Neelamani et al.: JPEG compression history estimation for color images
- ⟶ Hany Farid: Exposing digital forgeries from JPEG ghosts
- ⟶ Tjoa, Lin, Liu: Transform coder classification for digital image forensics

Image characteristics

- ⟶ Fu, et al: A generalized Benford's law for JPEG coefficients and its applications in image forensics
- ⟶ Wang, Weihong: Detecting re-projected video

Image sensor identification

- ⟶ Chen, Fridrich, Goljan: Digital imaging sensor identification (further study)
- ⟶ Goljan, Fridrich, Filler: Large scale test of sensor fingerprint camera identification

CFA interpolation detectors

- ⟶ Popescu, Farid: Exposing digital forgeries in color filter array interpolated images
- ⟶ Gallagher, Chen: Image authentication by detecting traces of demosaicing
- ⟶ Kirchner, Böhme: Synthesis of color filter array patters in digital images

Macroscopic features

→ Johnson, Farid: Exposing digital forgeries by detecting inconsistencies in lighting

→ Popescu, Farid: Exposing digital forgeries by detecting duplicated image regions

Printers and scanners

→ Kee, Farid: Printer profiling for forensics and ballistics

→ Khanna, Chiu, Allebach, Delp: Scanner identification with extension to forgery detection

Display eavesdropping I

→ van Eck: Electromagnetic radiation from video display units: an eavesdropping risk? Computers & Security 4(269–286)

→ Kuhn, Anderson: Soft Tempest: hidden data transmission using electromagnetic emanations. IHW 1998, LNCS 1525

→ Kuhn: Compromising emanations: eavesdropping risks of computer displays, Chapter 3: Analog video displays. UCAM-CL-TR-577

Display eavesdropping II

→ Kuhn: Electromagnetic Eavesdropping Risks of Flat-Panel Displays. PET 2004, LNCS 3424

→ Kuhn: Optical time-domain eavesdropping risks of CRT displays. IEEE S&P 2002

→ Backes et al.: Tempest in a Teapot: compromising reflections revisited. IEEE S&P 2009

Keyboard eavesdropping

→ Asonov, Agrawal: Keyboard acoustic emanations. IEEE S&P 2004

→ Zhang, Zhou, Tygar: Keyboard acoustic emanations revisited. ACM CCS 2005

→ Song, Wagner, Tian: Timing analysis of keystrokes and timing attacks on SSH. USENIX Security 2001

→ Vuagnoux, Pasini: Compromising electromagnetic emanations of wired and wireless keyboards. USENIX Security 2009

Microcontroller power analysis

- ⟶ Kocher, Jaffe, Jun: Differential power analysis. CRYPTO '99, LNCS 1666
- ⟶ Chari, Rao, Rohatgi: Template attacks. CHES 2002, LNCS 2523

Steganography

- ⟶ Cox, Miller, Brown, Fridrich, Kalker: Digital Watermarking and Steganography (one book chapter). [K.6 74]

Schedule

8 October: Preparation meeting / JPEG tutorial
15 October: Video TEMPEST demo / slot 1
22 October: slot 2 / slot 3
29 October: slot 4 / slot 5
5 November: slot 6 / slot 7
12 November: slot 8 / slot 9
19 November: slot 10 / slot 11
26 November: Project proposals + wrap up

The final schedule will be announced and updated as necessary on the course web page.