



MM&Sec

# Multimedia & Security

Summer Term 2009

Lecture: Wednesday, 11:15-12:45 (Building 29, Room 335)

**Exercise:** Monday, 13:15-14:45 (Building 29, Room K058)

***April 6th, 2009***

Multimedia and  
Security

**Lecture:**

**Prof. Dr.-Ing. Jana Dittmann**

With support from

**Prof. Dr.-Ing. Claus Vielhauer**

(AMSL, FH Brandenburg)

**Exercise:**

**Christian Krätzer**

[kraetzer@iti.cs.uni-magdeburg.de](mailto:kraetzer@iti.cs.uni-magdeburg.de)

With support from:

Tobias Hoppe and Stefan Kiltz

# MM&Sec Concept

## Multimedia and Security

### Assessment and grading:

- Registration for a task within the exercise
- Exercise Points
  - 6x10 points for exercise sheets
  - 20 points for the poster & presentation
    - A) Scientific Presentation: Layout & Design, Images, Visualisation of test results and/or processes, work with references, identification of the authors, etc - 8 points
    - B) Content: Completeness and correctness of the content presented - 8 points
    - C) Test results and adherence to the submission deadlines: Delivering the material (test material collection, poster, report) at the corresponding deadlines - 4 points
  - Sum: 80 points
  - For **Schein**: 64 points (80%) required
- Exams:
  - **Prerequisite** is the presentation of a poster
  - Points gathered in the exercise act as bonus points in the exam; question to the exercise topic during oral examination and additional to the overall course topic

# MM&Sec Topics - Summary

## Multimedia and Security

- Topic 1: Watermarking classification
- Topic 2: Microphone Forensics: Intra Microphone Class Classification
- Topic 3: Microphone Forensics: Inter Microphone Class Classification
- Topic 4: Features for Audio Forensics
- Topic 5: Entropy Analysis for Steganalysis
- Topic 6: Automotive Security
- Topic 7: RS-Analysis for Audio
- Topic 8: Hypersonic Audio
- Topic 9: Survey on audio steganography tools

# MM&Sec Topic 1: Watermarking classification

- Goal: Update an existing watermark classification framework:
  - Make yourself familiar with the watermark classification approach presented in [Dit2000]
  - Perform a survey on current research directions concerning digital watermarking
  - Update the watermark classification framework
- Literature:
  - [Dit2000] Jana Dittmann: Digitale Wasserzeichen. Springer Verlag, ISBN 3-540-66661-3, 2000.
  - ECYPT D.WVL.1: First Summary Report on Fundamentals, 2004.
  - Cox et al: Digital Watermarking and Steganography. Morgan Kaufmann, 2007.

## Topic 2 - Microphone Forensics: Intra Microphone Class Classification

- Test plan: Generate a set of audio recordings for microphone forensics and perform a first analysis on the potential [intra microphone class statistical discrimination](#) of the recorded material
- Test setup:
  - Test hardware, software and reference signals: A set of reference signals and hardware (2x4 identical microphones, loudspeaker, notebook, soundcard) for the recordings will be provided
  - Test data: Use your recoded material from 10 different locations to perform a first analysis on the potential statistical intra microphone class discrimination
  - Test results: Results are the set of recordings generated (on CD/DVD) with a description of the used parameters/hardware/locations/etc. and the results of the performed analysis on the discrimination as classification accuracies
- Literature:
  - C. Kraetzer, A. Oermann, J. Dittmann and A. Lang: Digital Audio Forensics: A First Practical Evaluation on Microphone and Environment Classification; Proceedings of the ACM Multimedia and Security Workshop 2007, Dallas, Texas, September 20th-21st, 2007, ISBN: 978-1-59593-857-2
- Task-Coach: Christian Kraetzer

## Topic 3 - Microphone Forensics: Inter Microphone Class Classification

- Test plan: Generate a set of audio recordings for microphone forensics and perform two analyses on the potential [inter microphone class statistical discrimination](#) of the recorded material
- Test setup:
  - Test hardware, software and reference signals: A set of reference signals and hardware (8 different microphones, loudspeaker, notebook, soundcard) for the recordings will be provided
  - Test data: Use your recoded material (with and without the usage of reference signals) from 10 different locations to perform a first analysis on the potential statistical intra microphone class discrimination
  - Test results: Results are the set of recordings generated (on CD/DVD) with a description of the used parameters/hardware/locations/etc. and the results of the performed analysis on the discrimination as classification accuracies
- Literature:
  - C. Kraetzer, A. Oermann, J. Dittmann and A. Lang: Digital Audio Forensics: A First Practical Evaluation on Microphone and Environment Classification; Proceedings of the ACM Multimedia and Security Workshop 2007, Dallas, Texas, September 20th-21st, 2007, ISBN: 978-1-59593-857-2
- Task-Coach: Christian Kraetzer

# MM&Sec Topic 4 – Features for Audio Forensics

MFCCs and LFCCs are widely used in speaker and speech recognition and are currently gaining importance also in audio forensic domains.

Goals:

- Integrate LFCC computation into AAST
- Compare the results achieved in steganalysis using LFCCs with the results achieved with MFCCs for three given data hiding algorithms (time-, freq.- and wavelet-domain) to show the impact to accuracy

Provided material / References / Literature:

- Christophe Charbuillet, Bruno Gas, Mohamed Chetouani, Jean Luc Zarader: Multi filter bank approach for speaker verification based on genetic algorithm. NOLISP 2007.
- AAST source
- A test set containing material marked by three steganographic algorithms for non-blind testing

# MM&Sec Topic 5 – Entropy Analysis for Steganalysis

Since entropy (in information theory) is a measure of the uncertainty associated with a random variable it can for example be used to evaluate whether data was encrypted or compressed.

Goals:

- Implement a segmental entropy analysis for PCM coded WAV files
- Use it to show the impact of steganographic embedding by different algorithms to the entropy of audio files

Provided material / References / Literature:

- A test set containing material marked by four steganographic algorithms for non-blind testing
- Task-Coach: Christian Kraetzer

# MM&Sec Topic 6: Automotive Security

- Similar to today's desktop IT, automotive security becomes an increasing issue. The risks involved rise dramatically with the ever increasing number of interconnected electronic devices in current vehicles.
- We already see a rising number of mischievous manipulations to these electronic systems, mostly to modify the performance of the car or to get access to specific functionalities. Also indications for an increasing threat to the automotive IT can be found in literature.
- Task: Perform an survey on possible techniques for the manipulation of automotive IT-components to evaluate the realistic threat level to selected components/systems.
- Present the results of your survey in the following form:
  - Reference to the source of information,
  - Short description of the source of information,
  - Source of information addresses: protection mechanisms and/or attacks (manipulations)
  - Car manufacturers/car types/components (HW/SW) involved
  - Aim of the protection mechanisms (protection goal) and/or attacks (manipulations) – if possible using CERT-taxonomy
  - Security aspects involved (direct and indirect)
  - Other (if necessary)
- Relevant research project and web pages (as a starting point for your survey) are:
  - eSecurity Working Group; SeVeCom <http://www.sevecom.org>;  
[http://www.esafetysupport.org/en/esafety\\_activities/esafety\\_working\\_groups/esecurity.htm](http://www.esafetysupport.org/en/esafety_activities/esafety_working_groups/esecurity.htm); CarNet  
<http://www.sichere-identitaet.de/zukunftsthemen/kommunikation/carnet>; Evita <http://www.evita-project.org>; COMO <http://www.uni-magdeburg.de/automotive/>
  - <http://www.canhack.de/>; <http://www.navi-projekt.de/>; <http://www.canhack.org/>; <http://www.car-pc.info/phpBB2/index.php>; <http://www.smart-roadster-board.de/board/thread.php?threadid=6886>
- Task coaches: Tobias Hoppe and Stefan Kiltz

# MM&Sec Topic 7: RS-Analysis for Audio

Regular-Singular analysis is a global feature extraction method applied in image steganalysis to estimate the amount data embedded into images.

Goals:

- Make yourself familiar with the concept of RS-Analysis
- Transfer the concept to audio signal analysis (PCM coded WAV)
- Implement it prototypically and test it with audio files

Provided material / References / Literature:

- Digital Invisible Ink Toolkit: <http://diit.sourceforge.net/>
- [JGD2001] J. Fridrich, M. Goljan and R. Du: Reliable detection of LSB steganography in color and grayscale images, Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5, 2001.

## MM&Sec Topic 8: Hypersonic Audio

Hypersonic audio is a technique presented by American Technology Corp. (HSS) for focussed sound projection.

Goals:

- Analyse the technological approach used
- Identify security risks involved
- Devise for a museum application scenario with a basic assumption of 20 people per room the necessary technical realisation of individual sound projection

Provided material / References / Literature:

- [Spot] [http://www.audiospotlights.com/directional\\_sound\\_intro.html](http://www.audiospotlights.com/directional_sound_intro.html)

Multimedia and  
Security

# MM&Sec Topic 9: Survey on audio steganography tools

To successfully counter steganography requires a knowledge of existing techniques.

Goals:

- Perform a survey of existing audio steganography tools
- Classify them by:
  - Execution environment (Windows, Linux, ...)
  - Working domain (frequency, wavelet, time, ...)
  - Embedding strategy (substitution, addition, etc.)
  - Proposed capacity
  - etc)
- Use N. F. Johnsons website as a starting point

Provided material / References / Literature:

- <http://www.jjtc.com/Steganography/>

# MM&Sec Topics - Summary

## Multimedia and Security

- Topic 1: Watermarking classification
- Topic 2: Microphone Forensics: Intra Microphone Class Classification
- Topic 3: Microphone Forensics: Inter Microphone Class Classification
- Topic 4: Features for Audio Forensics
- Topic 5: Entropy Analysis for Steganalysis
- Topic 6: Automotive Security
- Topic 7: RS-Analysis for Audio
- Topic 8: Hypersonic Audio
- Topic 9: Survey on audio steganography tools

- Next week no exercise – see you on Monday 20th!