WTP “Praktikum IT-Security” (P-ITSEC)
[WTP] or [P-ITSEC]

Summer term 2025

PD Dr.-Ing. habil. Christian Krätzer - kraetzer@iti.cs.uni-magdeburg.de

supported by:
Dennis Siegel, Stefan Seidlitz, Andrey Makrushin

Module responsible / examiner:
Prof. Dr.-Ing. Jana Dittmann

Options / classifications

„Scientific team project“ / „Wissenschaftliches Teamprojekt“ [WTP]
(in „Schlüssel- und Methodenkompetenz“)

OR / XOR

Digital Engineering Project / Interdisziplinäres Teamprojekt (6 ETCS)

OR / XOR

Module „Praktikum IT Sicherheit“ [P-ITSEC]

Zuordnung zum Curriculum:	FIN: M.Sc. CV - Bereich Informatik; FIN: M.Sc. DIGIENG - Methoden der Informatik; FIN: M.Sc. DKE - Applied Data Science; FIN: M.Sc. DKE (alt) - Bereich Applications; FIN: M.Sc. INF - Bereich Informatik; FIN: M.Sc. INGINF - Bereich Informatik; FIN: M.Sc. WIF - Bereich Informatik

Options / classifications

- Lehrveranstaltungen nach Studiengängen (LSF)

Strukturbaum

Die Veranstaltung wurde **11** mal im Vorlesungsverzeichnis SoSe 2023 gefunden:

- Vorlesungsverzeichnis
- Fakultät für Informatik
- Lehrveranstaltungen nach Studiengängen
- Ingenieurinformatik - Master (IngINF;M)
- Schlüssel- und Methodenkompetenz
- Wissenschaftliches Teamprojekt --- 1
- Bereich Informatik --- 2
- Informatik - Master (INF;M)
- Schlüssel- und Methodenkompetenz
- Wissenschaftliches Teamprojekt --- 3
- Informatik --- 4
- Wirtschaftsinformatik - Master (WIF;M)
- Schwerpunkt Schlüssel- und Methodenkompetenz
- Wissenschaftliches Teamprojekt --- 5
- Katalog INF --- 6
- Computervisualistik - Master (CV;M)
- Schlüssel- und Methodenkompetenz
- Wissenschaftliches Teamprojekt --- 7
- Informatik --- 8
- Data & Knowledge Engineering - Master (DKE;M - alt)
- Applications --- 9
- Digital Engineering - Master (DigiEng;M)
- Methoden der Informatik --- 10
- Interdisziplinäres Teamprojekt --- 11

Module:

[WTP] or [P-ITSEC] or DE

[P-ITSEC]: Organisation & concept

- Practical course: Working on a practical topic as a programming task in a group and preparing a presentation and a scientific report for submission
- The topics are usually designed for groups of 2-4 students

- 6 credit points (Master) = 180h:
  - Attendance time: Project discussion, presentations
  - Independent work: Individual work on the practice-related topic (approx. 142h), coordination, documentation of the results into the final report as well as preparation and realisation of an interim and final presentation (approx. 20h)
- Exam: The submitted scientific report („Hausarbeit“)

- AG Multimedia and Security - Webseite:
  `http://omen.cs.uni-magdeburg.de/itiamsl/`

Milestones

- 15.04.2025: Administratives, Themenvorstellung und -vergabe an Teams / Topic presentation and distribution
- 13.05.2025: Zwischenpräsentation durch das Team und Prüfungsanmeldung / Interim presentation by the team and exam registration
- 24.06.2025: Abschlusspräsentation / Final presentation
- Bis Ende August: Abgabe der Hausarbeit / Submission of the final report

Referenzierung der Aufgabenstellung in Hausarbeit:
Dittmann, Krätzer, <supervisor>: WTP/P-ITSEC Sommersemester 2025, Aufgabenstellung, April 2025.

Referencing of the task in the term paper:
Dittmann, Krätzer, <supervisor>: WTP/P-ITSEC Summer Semester 2025, Task assignment, April 2025.

Topics

Topic 1: Brute Force Attacks against Steghide WAV Audio

Motivation:

- Steganographic communication is one possible approach to secure the message exchange between communicating parties. In contrast to cryptography, where only the content of a message is protected, in steganography the existence of the communication itself is hidden by embedding the message into innocent looking cover objects.

Practical tasks:

- Necessary precondition: Implement for WAV files a brute force attack framework against the steganography tool Steghide (https://wiki.ubuntuusers.de/Steghide/)

```
kraetzer@T495:~/DOCUMENT_WORKSPACE/LECTURE/SS25/P-ITSEC$ steghide embed -cf ZZYU75146067475021.wav -ef message.txt --passphrase mypassword
Bette "message.txt" in "ZZYU75146067475021.wav" ein... fertig
kraetzer@T495:~/DOCUMENT_WORKSPACE/LECTURE/SS25/P-ITSEC$ steghide --info ZZYU75146067475021.wav --passphrase mypassword
"ZZYU75146067475021.wav":
  Format: wave audio, PCM encoding
  Kapazit[illegible]: 2,1 KB
  Eingebettete Datei "message.txt":
    Gr[illegible]: 13,0 Byte
    verschl[illegible]selt: rijndael-128, cbc
    komprimiert: ja
kraetzer@T495:~/DOCUMENT_WORKSPACE/LECTURE/SS25/P-ITSEC$ steghide --info ZZYU75146067475021.wav --passphrase mypassword2
"ZZYU75146067475021.wav":
  Format: wave audio, PCM encoding
  Kapazit[illegible]: 2,1 KB
steghide: Mit diesem Passwort konnten keine Daten extrahiert werden!
```

- After the precondition has been met:
  - Practically evaluate different approaches to compose the password list(s) required for such brute force attacks, starting with established lists (incl. Rockyou.txt; https://github.com/dw0rsec/rockyou.txt) and considering the methods for password list generation offered by HashCat (https://hashcat.net/hashcat/).
  - Try to perfom a password cracking on Steghide with HashCat.
  - Document your solution concept, implementation, evaluation plan and evaluation results in a scientific report

Task coach: Christian Krätzer (2-3 students)

Topic 2: AudiostegoÆ

Detection and removal of audio steganography using AutoEncoder(s) with Open Source

Tasks:

- Familiarisation with literature and, if necessary, further research to understand the task and selection of open source - see references and supplementary sheet for the task [AMSL25])
- Per person:
  - Training and testing of a DeepLearning approach for the detection and removal of AudioStego in WAV files
- Training configuration:
  - Train network based on open source (references see below or in the supplement) with provided data, viewing the audio stream as a 1D vector
- Evaluation (for details see supplement [AMSL25]):
  - Detection of the audio stego by selecting the approaches in the supplementary sheet
  - Introduction of methods of explainability in all steps of the procedure (cf. [AMSL25]) considering the data as an image (converter is provided by AMSL) using open source
  - Removal of the audio stego incl. comparison of the native data with the cleaned data

Topic 2: AudiostegoÆ

Detection and removal of audio steganography using AutoEncoder(s) with Open Source

Expected result:

- Executable open source instance of the AI architecture under consideration (as source code), including all successfully trained models or approaches for explainability (executable on the AMSL GPU computer, possibly as a Docker instance)
- Scientific elaboration, including process-accompanying documentation of all steps, well-founded selection of a concept taking into account and naming alternatives
- Basic knowledge: Programming skills (e.g. Python); basics of image processing; basic understanding of machine learning; motivation to familiarise yourself with new topics
- Supervisors: Stefan Seidlitz (AI), Dennis Siegel (XAI)
- Team: 2-4 (one tool per participant)

References (starting point):

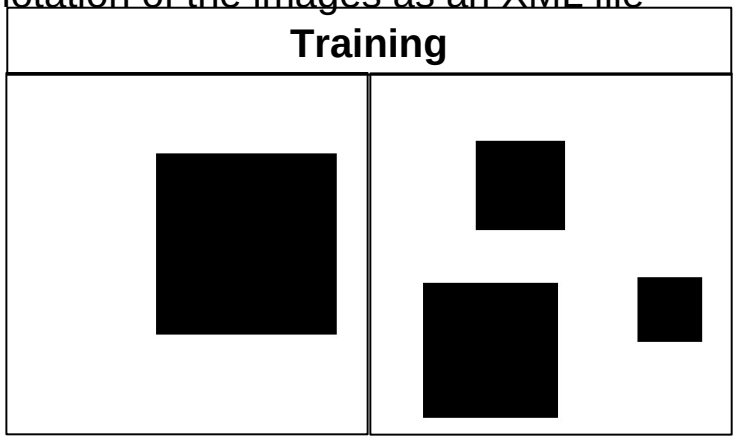
- [LAH19] Yin-Jyun Luo, Kat Agres, & Dorien Herremans. (2019). Learning Disentangled Representations of Timbre and Pitch for Musical Instrument Sounds Using Gaussian Mixture Variational Autoencoders. (GitHub: https://github.com/yjlolo/vae-audio)
- [GSM21] Gal Greshler, Tamar Rott Shaham, & Tomer Michaeli (2021). Catch-A-Waveform: Learning to Generate Audio from a Single Short Example. In Advances in Neural Information Processing Systems. (GitHub: https://github.com/galgreshler/Catch-A-Waveform)
- [PLF24] Marco Pasini, Stefan Lattner, & George Fazekas. (2024). Music2Latent: Consistency Autoencoders for Latent Audio Compression. (GitHub: https://github.com/SonyCSLParis/music2latent)
- [AMSL25] Stefan Seidlitz, Dennis Siegel, Christian Krätzer und Jana Dittmann; AudiostegoÆ: Detektion und Entfernung von Audiostego über AutoEncoder; Otto-von-Guericke Universität Magdeburg, Sommersemester 2025
- The provided dataset should be referenced as: Dittmann, Krätzer, Seidlitz, Siegel: WTP/P-ITSEC Summer Semester 2025, Provided data sets, April 2025.

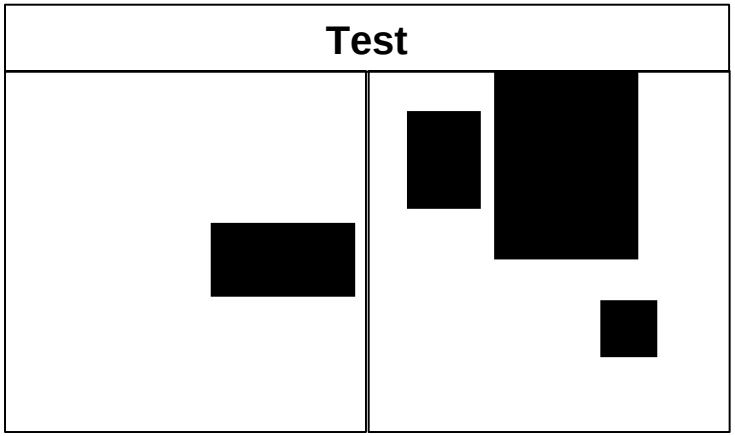
Topic 3: Understand AI: Finding traces in KI with geometric objects with Open Source

Introduction/Motivation: AI in the form of deep learning is being used more and more frequently. However, such approaches are mostly ‘black box’ approaches as it is often unclear how the algorithms work internally. In order to gain a better understanding, a simplified data set of geometric objects is to be used for training and testing both generative and predictive AI - see preliminary work in [SD24].

Information on the AMSL dataset:

- Resolution: 512x512 pixels
- Format: PNG
- Training: Images with squares of different sizes (8, 16, 32, 64, 128 pixels)
- Test: Images with rectangles of different sizes (varying based on {8, 16, 32, 64, 128} pixels)
- Annotation of the images as an XML file





Topic 3: Understand AI: Finding traces in KI with geometric objects with Open Source – Generative AI

Tasks:

- Literature review and, if necessary, further research on task understanding and selection of open source of different generative AI architectures
- Per person: Training and testing of a simplified open source autoencoder for the generation of quadrilaterals based on the AMSL dataset. Selection of possible autoencoder architectures based on open source (e.g. based on the pythae library, see [CVA22]):
    - Disentangling Variational Autoencoder [DKL+19]
    - Conditional Variational Autoencoder [KW14]
- Variation of the training configuration by means of:
    - Variation of the training duration (number of epochs)
    - Variation of the training data (size of the quadrilaterals, 1 vs. several quadrilaterals per image, amount of data)
    - Consideration of different sizes of the latent vector
- Evaluation of training and test images in comparison with the images reconstructed by the autoencoder
    - manual/visual comparison on a smaller test set of at least 10 images (per person)
    - Automated comparison, e.g. by means of a difference image, checking the shape and size of the quadrilaterals and the internal angle of the quadrilateral, performed on at least 1000 images
- XAI / explainability on the basis of the latent vector:
    - Visualise changes in the latent vector
    - Visualise the latent space with tSNE

Topic 3: Understand AI: Finding traces in KI with geometric objects with Open Source – Predictive AI

Tasks:

- Literature review and, if necessary, further research on task understanding and selection of open source of various generative AI architectures
- Per person: Training and testing of a simplified open source deep learning approach for object recognition of quadrilaterals, trained on the basis of the AMSL dataset. Selection of possible architectures based on open source:
    - SSD300, ResNet50, etc.
- Variation of the training configuration by means of:
    - Variation of the training data (size of the quadrilaterals, 1 vs multiple quadrilaterals per image, amount of data)
    - Variation of the classification target (detection of quadrilaterals, classification of size)
    - Consideration of different sizes of the latent vector
- Evaluation of training and test images in comparison with the images reconstructed by the autoencoder
    - manual/visual comparison on a smaller test set of at least 10 images (per person)
    - Automated comparison (e.g. using overlapping areas between detected bounding box and annotation or confusion matrix for classification of variables) on at least 1000 images
- Strengthening explainability using existing open source tools:
    - Consideration of layer-based XAI methods (cf. e.g. LRP, Grad-Cam, Captum https://github.com/pytorch/captum)
    - Consideration of counterfactual explanations (e.g. DiCE https://github.com/interpretml/DiCE)

Topic 3: Understand AI: Finding traces in KI with geometric objects with Open Source – both teams

Tasks:

- Literature review and, if necessary, further research on task understanding and selection of open source of various generative AI architectures
- Per person: Training and testing of a simplified open source deep learning approach for object recognition of quadrilaterals, trained on the basis of the AMSL dataset. Selection of possible architectures based on open source:
    - SSD300, ResNet50, etc.
- Variation of the training configuration by means of:
    - Variation of the training data (size of the quadrilaterals, 1 vs multiple quadrilaterals per image, amount of data)
    - Variation of the classification target (detection of quadrilaterals, classification of size)
    - Consideration of different sizes of the latent vector
- Evaluation of training and test images in comparison with the images reconstructed by the autoencoder
    - manual/visual comparison on a smaller test set of at least 10 images (per person)
    - Automated comparison (e.g. using overlapping areas between detected bounding box and annotation or confusion matrix for classification of variables) on at least 1000 images
- Strengthening explainability using existing open source tools:
    - Consideration of layer-based XAI methods (cf. e.g. LRP, Grad-Cam, Captum https://github.com/pytorch/captum)
    - Consideration of counterfactual explanations (e.g. DiCE https://github.com/interpretml/DiCE)

Topic 3: Understand AI: Spurensuche in KI mit geometrischen Objekten mit Open Source

Expected result:

- Executable open source instance of the AI architecture under consideration (as source code), including all successfully trained models or approaches for explainability (executable on the AMSL GPU computer, possibly as a Docker instance)
- Scientific elaboration into a presenation and a scientific report, including process-accompanying documentation of all steps, well-founded selection of a concept taking into account and naming alternatives

Basic knowledge:

Programming skills (e.g. Python); basics of image processing; basic understanding of machine learning; motivation to familiarise yourself with new topics

Supervisors: Stefan Seidlitz (AI), Dennis Siegel (XAI)

Team: 4-8 (2-4 per subtask)

References:

[SD24] Stefan Seidlitz, Jana Dittmann: ‘Forensic Analysis of GAN Training and Generation: Output Artifacts Assessment of Circles and Lines’. Proceedings of the SECURWARE 2024, The Eighteenth International Conference on Emerging Security Information, Systems and Technologies, IARIA, 2024

[DKL+19] Yann Dubois, Alexandros Kastanos, Dave Lines, Bart Melman: ‘Disentangling VAE’. Online https://github.com/YannDubs/disentangling-vae 2019.

[CVA22] Clément Chadebec, Louis J. Vincent, Stéphanie Allassonnière: ‘Pythae: Unifying Generative Autoencoders in Python - A Benchmarking Use Case’. In Advances in Neural Information Processing Systems, vol 35, 2022

[KW14] Diederik P. Kingma, Max Welling: Auto-Encoding Variational Bayes. ICLR 2014, or the online source https://github.com/unnir/cVAE

Topic 4: Analysing Alexa network traffic after ‚Cloud only‘ move

Motivation:

- In March 2025 Amazon finally disabled an option that allows Alexa voice conversations to be processed locally instead of in the cloud. This does not only have privacy implications but assumedly also influences the network traffic behavior of Alexa devices.

Practical tasks:

- Necessary precondition: Use existing publications such as [Janak2021], [Barceló-Armada2022] and [Ford2019] to summarize how the network traffic behavior of Alexa devices was before this policy shift.
- After the precondition has been met:
  - Use our Alexa devices to design and implement a network traffic evaluation setup mimicking the experiments described in the papers mentioned above
  - Perform network traffic analysis experiments documenting Alexas behaviour in your setup and compare it to the previously reported behaviour.
  - Design and implement additional network and privacy analyses on Alexa traffic (including SSLKEYLOGFILE environment variable attacks (https://my.f5.com/manage/s/article/K50557518), if possible
  - Document your solution concept, implementation, evaluation plan and evaluation results in a scientific report

- Literature (starting points):
  - [Janak2021] Jan Janak, Teresa Tseng, Aliza Isaacs, Henning Schulzrinne: An Analysis of Amazon Echo's Network. CoRR, abs/2105.13500, 2021. https://arxiv.org/abs/2105.13500
  - [Barceló-Armada2022] Rubén Barceló-Armada, Ismael Castell-Uroz, Pere Barlet-Ros: Amazon Alexa traffic traces. Computer Networks, Volume 205, 108782, ISSN 1389-1286, 2022. https://doi.org/10.1016/j.comnet.2022.108782
  - [Ford2019] M. Ford, W. Palmer: Alexa, are you listening to me? An analysis of Alexa voice service network traffic. Pers Ubiquit Comput 23, 67–79, 2019. https://doi.org/10.1007/s00779-018-1174-x

Task coach: Christian Krätzer (2-4 students)

Topic 5: FaceGenAI - Identity-preserving face generation

Motivation:

- The students are to investigate which GenAI techniques are suitable for generating several different facial images **of the same person** from one facial image.

Practical tasks:

- Necessary precondition: Install and test ComfyUI – focus exclusively on the Open-Source Stable diffusion models (SD1.5, SD2.1, SDXL etc.) or their derivatives (RealisticVision, Azovya, FormulaXL, RealisticVisionXL usw.) in combination with InstantID/IDAdaptor and ControlNet.
- After the precondition has been met:
  - Create a public dataset of facial images suitable for training facial recognition systems. This set has to contain for multiple virtual/generated ID sets of at least 10 images per ID.
  - Test a pseudo-random generation first.
  - Secondly, an attribute check should be carried out using both prompts (CLIP) and the ControlNet.
  - In a third test, a complex set of facial attributes (head position, facial expression, age, etc.) and also environmental parameters (such as position of light sources, image quality, image production artefacts, etc.) should be controlled.
  - Evaluate the generated images / image sets (here, as reference the GAN-based inversion using DiscoGAN or SD-based inversion with Arc2Face should be used). **You coordinate the evaluation framework with Andrey.**
  - If possible Flux and Janus-Pro should be considered in this evaluation context.
  - Document your solution concept, implementation, evaluation plan and evaluation results in a scientific report

• Literature:

  - ComfyUI (https://www.comfy.org/), more references will be provided by Andrey

Task coach: Andey Makrushin (2-3 students)

Topic Overview

- Topic 1: Brute Force Attacks against Steghide WAV Audio - Task coach: Christian Krätzer (2-3 students)
- Topic 2: AudiostegoÆ - Task coaches: Stefan Seidlitz, Dennis Siegel (2-4 students)
- Topic 3: Understand AI - Task coaches: Stefan Seidlitz, Dennis Siegel (2-4 students)
- Topic 4: Analysing Alexa network traffic - Task coach: Christian Krätzer (2-4 students)
- Topic 5: FaceGenAI - Identity-preserving face generation – Task coach: Andrey Makrushin (2-3 students)

Milestones

- 15.04.2025: Administratives, Themenvorstellung und -vergabe an Teams / Topic presentation and distribution
- 13.05.2025: Zwischenpräsentation durch das Team und Prüfungsanmeldung / Interim presentation by the team and exam registration
- 24.06.2025: Abschlusspräsentation / Final presentation
- Bis Ende August: Abgabe der Ausarbeitung / Submission of the final report

Referenzierung der Aufgabenstellung in Hausarbeit:
Dittmann, Krätzer, <supervisor>: WTP/P-ITSEC Sommersemester 2025, Aufgabenstellung, April 2025.

Referencing of the task in the term paper:
Dittmann, Krätzer, <supervisor>: WTP/P-ITSEC Summer Semester 2025, Task assignment, April 2025.