netidee

STIPENDIEN

Empowering Data Ownership and Intellectual Property

Zwischenbericht | Call 20 | Stipendium ID 7859

Inhalt

1 Einleitung

This interim report summarises the progress of the netidee stipend project *"Empowering Data Ownership and Intellectual Property Protection in Open Data Sharing"* (*ID 7859*) during the reporting period. The project investigates methods for protecting ownership and accountability of structured data through data fingerprinting and related intellectual property protection mechanisms.

The work during this reporting period focused on three main directions:

- conducting and analysing a large-scale adversarial study on realistic attacks against data fingerprinting systems,
- developing and refining the *NCorr-FP* fingerprinting methodology for structured data,
- and integrating the resulting scientific contributions into dissertation chapters and peer-reviewed publications.

The project progressed largely according to the planned timeline and resulted in several significant scientific outcomes, including:

- the successful completion of the adversarial user study,
- the preparation of a scientific publication currently under peer review at ACSAC,
- and the advancement of the journal publication at IEEE Transactions on Information Forensics and Security (TIFS) to *accept with mandatory minor revision* status.

In addition to the scientific outputs, the project continued to emphasise open-science and dissemination activities through public blog posts, open-source tooling, and openly available study infrastructure and documentation.

2 Status

2.1 **Meilenstein 1** – Blog Post

The objective of this milestone was to initiate the public dissemination activities of the project by publishing an introductory blog post on the netidee platform. The blog post aimed to communicate the motivation behind the research, outline the challenges of intellectual property (IP) protection in data sharing, and present the broader goals of the dissertation project to both technical and non-technical audiences.

netidee blog post #1: Intellectual Property Protection in Open Data Sharing

No deviations from the original project plan occurred during this milestone. The dissemination activity was completed as scheduled in November 2025.

2.2 **Meilenstein 2 –** Adversarial Study Conducted

Kurzbeschreibung der Haupttätigkeiten

The objective of this milestone was to conduct a structured adversarial study investigating how real users attack fingerprint-protected datasets under realistic conditions. The study aimed to evaluate the robustness, interpretability, and practical security of data fingerprinting schemes beyond conventional algorithmic robustness evaluations typically considered in the literature.

Erkenntnisse zur Vorgangsweise

A comprehensive adversarial user study was designed and conducted in the form of a **hackathon-style competition** integrated into the university course *Security, Privacy and Explainability in Machine Learning* at TU Wien. Participants consisted of master's students with technical backgrounds in machine learning, privacy, and security.

The study infrastructure included:

- preparation of fingerprint-protected datasets,
- implementation and deployment of attack environments,
- development of attack tasks and evaluation workflows,
- creation of supporting documentation and tutorials,
- deployment of automated scoring and leaderboard systems,
- collection of qualitative and quantitative study data.

Participants were tasked with attacking fingerprinted datasets under realistic constraints while preserving data utility. The competition format encouraged iterative experimentation and exploration of diverse attack strategies. Participants received feedback in the form of success scores and rankings through a leaderboard mechanism.

The collected material included:

- attack implementations and workflows,
- structured questionnaires,
- participant self-assessments,
- qualitative explanations of attack reasoning,
- quantitative robustness and fidelity measurements,
- observations from moderated study interactions.

The conducted study directly contributed to the research publication *"Data Fingerprints in the Wild: An Adversarial Study of Behavior Beyond Standard Attack Models and Implications for Robustness Evaluation"*, which analyses how human adversaries attack data fingerprinting systems in practice and highlights important gaps between theoretical robustness evaluations and real-world adversarial behaviour (described more in detailed in the next section*).*

Open-Source Artefacts and Documentation

To ensure transparency and reproducibility, the study infrastructure, exercise descriptions, and fingerprinting documentation were released openly:

- Study documentation and exercise materials
- Open-source repository for the study infrastructure

For ethical and privacy reasons, the original participant submissions are not publicly released. All participating students provided informed consent allowing their solutions and interactions to be analysed anonymously for research purposes.

Kurzbeschreibung der erreichten Ergebnisse

The milestone was successfully completed through:

- the design and execution of a large-scale adversarial study,
- systematic collection of empirical attack data,
- creation of reusable open-source study infrastructure and documentation.

The study produced a unique empirical dataset on human adversarial behaviour against fingerprint-protected data and forms a central contribution of the ongoing dissertation work.

Gab es große Abweichungen zum Plan? Warum?

No major deviations from the original project plan occurred. The study was successfully conducted within the planned timeframe by January 2026 and produced results exceeding the initial scope in terms of diversity of observed attack strategies and qualitative insights.

2.3 **Meilenstein 3** – Analysis and Results of Adversarial Study

Kurzbeschreibung der Haupttätigkeiten

The objective of this milestone was to systematically analyse the qualitative and quantitative results collected during the adversarial user study from the previous milestone and derive insights into real-world attacker behaviour against fingerprint-protected datasets.

Erkenntnisse zur Vorgangsweise

The analysis adopted a **mixed-methods approach** combining technical robustness evaluation with qualitative methodologies commonly used in usable security research. Rather than evaluating attack success rates in isolation, the study investigated how participant assumptions, intuitions, uncertainty, and understanding of the fingerprinting mechanisms influenced their attack choices and outcomes.

The analysis activities were performed in close collaboration with an expert researcher from CISPA Helmholtz Center for Information Security[1] specialising in qualitative research methods and usable security. This collaboration supported rigorous coding procedures, validation of thematic interpretations, and alignment with established qualitative research practices.

[1] https://cispa.de

Kurzbeschreibung der erreichten Ergebnisse

The analysis identified several recurring attack behaviours and decision-making patterns that substantially influenced adversarial outcomes.

Interestingly for a scientific contribution, the study further revealed that many participants employed attack classes that are underrepresented or absent in conventional robustness evaluations.

Overall, the analysis demonstrated that human-centred adversarial evaluations reveal robustness limitations, attacker behaviours, and usability considerations that are not captured through purely automated benchmarking approaches.

Scientific Output

The findings of the analysis phase resulted in scientific publication:

Šarčević, T., Gerhardt, D., Rauber, A., Mayer, R. "Data Fingerprints in the Wild: An Adversarial Study of Behavior Beyond Standard Attack Models and Implications for Robustness Evaluation (2026).",

currently prepared for peer-review at ACSAC[2], a highly ranked international security conference.

Besondere Erfolge/ Probleme

A major success of this milestone was the successful integration of technical robustness evaluation with qualitative usable-security methodologies, i.e. the **interdisciplinary perspective**.
Another significant success was the **collaboration** with CISPA, which strengthened the methodological quality and scientific rigor of the qualitative analysis process. The interdisciplinary exchange substantially improved the interpretation and validation of participant behaviour and thematic findings.
The study also produced a **unique empirical dataset** on realistic human adversarial behaviour against fingerprint-protected datasets, representing a novel contribution to the field of data intellectual property protection.

A primary challenge of this milestone was the time-intensive nature of qualitative coding and thematic analysis. Achieving consistent interpretation of participant behaviour required multiple iterative review, discussion, and validation cycles between collaborators. Additionally, coordinating analysis activities and interpretation sessions with external collaborators introduced scheduling and organisational complexity that extended the analysis timeline beyond the initial estimate. However, this additional effort significantly improved the depth and scientific quality of the resulting findings and publication.

[2] https://www.acsac.org/

Gab es große Abweichungen zum Plan? Warum?

The overall objectives and scope of the adversarial study analysis remained fully aligned with the original project plan.

However, the analysis phase required additional time due to the interdisciplinary collaboration with CISPA, incorporation of rigorous qualitative analysis methodologies and preparation of a high-quality scientific publication. The milestone was thus reached in April 2026. This deviation was considered beneficial for the overall project quality, as it substantially strengthened both the scientific contribution and methodological rigor of the study.

2.4 Meilensteine 5, 6, 7 – Literature review, methodology and toolbox

Kurzbeschreibung der Haupttätigkeiten

This milestone combined the planned activities related to:

- the completion of the literature review on data intellectual property protection,
- the development of the dissertation methodology chapters,
- and the finalisation of the fingerprinting toolbox and core fingerprinting method *NCorr-FP*:

Šarčević, T., Rauber, A., Mayer, R. "NCorr-FP: A Neighbourhood-based Correlation-preserving Fingerprinting Scheme for Intellectual Property Protection of Structured Data." arXiv preprint arXiv:2505.06379 (2025).

The work focused on advancing the methodological and technical foundations of the dissertation through the development, evaluation, and refinement of a robust fingerprinting scheme.

Erkenntnisse zur Vorgangsweise

The main activities during this phase concentrated on the of the *NCorr-FP* fingerprinting scheme for structured data. This included:

- conducting an extensive literature review on data watermarking, fingerprinting, robustness, and ownership protection mechanisms,
- formalising the methodological foundations of the dissertation,
- designing and implementing the *NCorr-FP* embedding and detection algorithms,
- performing extensive experimental evaluation and parameter analysis,
- refining the open-source fingerprinting toolbox and associated evaluation infrastructure.

A major focus of the work involved responding to the major revision process of the *NCorr-FP* journal submission to IEEE Transactions on Information Forensics and Security (TIFS)[3], Q1-ranked journal[4].

[3] https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
[4] https://www.scimagojr.com/journalsearch.php?q=4000149002&tip=sid

The revision process required additional robustness evaluations, extended parameter analyses and refinement of theoretical explanations. The resulting work directly contributed to several dissertation chapters.

In parallel, the associated open-source toolbox and evaluation framework were finalised, documented, and refined to support reproducibility and future experimentation:

Toolbox and NCorr-FP open-source

Kurzbeschreibung der erreichten Ergebnisse

The *NCorr-FP* method was successfully developed, refined, and validated through extensive empirical evaluation.

A major outcome of this milestone was the **successful progression of the journal publication through the peer-review process at IEEE Transactions on Information Forensics and Security (TIFS)**. During the reporting period, the submission advanced from *major revision* status to *accept with mandatory minor revision*, representing a substantial scientific achievement and external validation of the developed methodology.

The work additionally resulted in:

- finalised dissertation methodology chapters,
- a completed literature review foundation,
- a refined open-source toolbox and evaluation framework,
- and improved reproducibility and documentation of the implemented methods.

The results and methodological contributions of NCorr-FP were additionally disseminated through a **netidee blog post (blog #2):**

netidee blog post #2: Data Fingerprinting

Besondere Erfolge/ Probleme

A major success of this milestone was the development of the *NCorr-FP* fingerprinting method that extends state-of-the-art approaches.
Another significant success was the positive outcome of the highly competitive TIFS review process.
The finalisation of the toolbox and supporting infrastructure further strengthened the project's reproducibility and open-science contributions.

The primary challenge during this milestone was the highly demanding and partly unpredictable journal revision process. In particular, the major revision required substantial additional experimentation and methodological refinement, one reviewer became unavailable during the

follow-up review cycle, and the extended review coordination increased the overall duration of the revision process.

Gab es große Abweichungen zum Plan? Warum?
The overall objectives of the planned milestones (literature review (M5), methodology development (M6), and toolbox finalisation (M7)) remained fully aligned with the original project plan and were successfully completed.
However, the originally planned standalone interim report **(Zwischenbericht) milestone (M4)** was effectively absorbed into the substantially expanded revision activities surrounding the *NCorr-FP* journal publication. The major revision process at TIFS coincided temporally with the planned reporting period in February/March 2026 and required significantly more effort than initially anticipated.
This deviation was considered scientifically beneficial for the project because the revision process substantially improved the quality of the work and the accepted journal publication represents a major milestone exceeding the originally planned outcomes for this phase.

Consequently, the reporting, methodology, literature review, and toolbox finalisation activities became tightly interconnected within the broader *NCorr-FP* development and revision process rather than progressing as fully independent milestones.

2.5 Meilenstein 8 – Thesis Submission

Kurzbeschreibung der Haupttätigkeiten & Erkenntnisse zur Vorgangsweise
During this milestone, the dissertation manuscript was prepared for submission. This included integrating the results from the conducted research activities, refining dissertation chapters, harmonising methodological and evaluation sections, and incorporating the latest outcomes from the adversarial study and the *NCorr-FP* journal revision process.

Kurzbeschreibung der erreichten Ergebnisse
At the end of the reporting period, the **dissertation entered the pre-submission phase in April 2026** and is currently undergoing final supervisory review and feedback prior to formal submission planned in May 2026.

The dissertation integrates the core scientific contributions of the project, including the preceding milestones:

- the *NCorr-FP* fingerprinting methodology,
- robustness and fidelity evaluations,
- adversarial user study findings,
- and the broader analysis of data intellectual property protection mechanisms.

Besondere Erfolge/ Probleme

A major success of this phase was the successful integration of multiple interconnected research outputs into a unified dissertation framework. The positive outcome of the *NCorr-FP* journal review process additionally strengthened the scientific quality of the dissertation content.
Minor scheduling dependencies emerged due to ongoing supervisory review and feedback cycles, which are part of the standard dissertation submission process.

Gab es große Abweichungen zum Plan? Warum?
A minor deviation from the planned timeline occurred: while the dissertation has not yet been formally submitted at the time of reporting, it is currently in the planned pre-submission review stage awaiting final supervisory feedback, hence the submission is moved from the planned April 2026 to May 2026.
The revision period (M9) is consequently adjusted to May 2026 – September 2026.
The subsequent final submission schedule remains consistent with the original project plan.

3 Zusammenfassung Planaktualisierung

Alle Anpassungen des Planungsdokuments kurz zusammengefasst

We make three minor adjustments to the project timeline, while the planned project content and scientific objectives remained unchanged.

The main adjustment to the original planning document concerns the interim report (Zwischenbericht) timeline, which shifted:

- from February 2026 to May 2026. (C1)

The reason for this change was the extended analysis and revision activities related to the adversarial study publication and the NCorr-FP journal revision process at IEEE Transactions on Information Forensics and Security (TIFS).
A further change is regarding the submission plan:

- Thesis submission is moved from April 2026 to May 2026 (C2)
- Thesis revision is consequently adjusted to last from May 2026-September 2026 (C3)

I would like to note that the milestones originally planned after the interim report (Zwischenbericht), including literature review (M5), methodology development (M6), toolbox finalisation (M7) were successfully completed during this reporting period.

The overall dissertation and project completion timeline remains unchanged and on track.