UNCOVER

Development of an efficient steganalysis framework for uncovering hidden data in digital media

www.uncoverproject.eu

@UNCOVER_EU

ABSTRACT

Criminals and terrorists use more and more data hiding methods (steganography) for concealing incriminating information in innocent-looking digital media files such as images, video, audio, and text files. The main objective of UNCOVER is to fill existing gaps in the ability of Law Enforcement Agencies (LEAs) for detecting the presence of such hidden information (i.e., steganalysis). The partners of UNCOVER are committed to substantially increase the technological autonomy of LEAs in the field of digital media steganalysis. With its consortium of 22 partners including LEAs, forensic institutes, leading researchers working at universities and research institutions, as well as industrial companies, UNCOVER sets out to outperform available steganalysis solutions in terms of performance, usability, operational needs, privacy protection, and chain-of-custody considerations.

PROJECT **OBJECTIVES**

CONDUCT a detailed analysis about the various aspects of the needs and requirements of LEAs for detecting and investigating steganography.

CONSOLIDATE relevant information about existing steganographic tools and centralise this information in an intuitive database for LEAs.

IMPROVE existing methods for operational steganalysis in digital media workflows.

IMPLEMENT a flexible and interoperable platform for the integration of steganalysis detection tools.

DEMONSTRATE the steganographic detection capabilities with realistic test cases and scenarios.

ENSURE the obtained results are admisible in European court rules.

PROVIDE a comprehensive training program for LEAs and forensic institutes by providing in-house training.

DISSEMINATE outcomes, communicate the project and prepare an exploitation and sustainability plan.

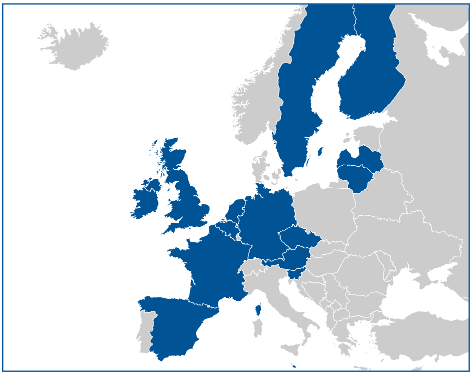
SUMMER SCHOOL AND CAPTURE THE FLAG:

From the 4th to the 8th of September 2023 the UNCOVER partners organized a successful Summer School and Capture the Flag Event in Prague, Czech Republic. The event attracted Law Enforcement Agents (LEAs) and PhD students (with information technology background) who wanted to develop their skills in steganography and steganalysis, and learn how to uncover hidden data in digital media.

The Summer School had 53 participants from 15 different countries within Europe. The majority of the participants were Law Enforcement Agents, 21 were from outside the consortium, 7 from within the project consortium, and the other 25 participants were distributed among Forensic Institute, Security Practitioners, Project Experts, and Academics and researchers.

The vast majority of participants rated the training as satisfactory and reported that the content met their expectations and they improved their knowledge in steganography and steganalysis. Almost 100% of participants would recommend the training to others.

SUMMER SCHOOL ATTENDEES



SUMMER SCHOOL LECTURES

- Steganography Principles and Practices : Hiding data into media
- JPEG Images for Steganography and Steganalysis
- First step into Steganalysis : Visual inspections and simple detectors
- Sample Pair Steganalysis for LSB Substitution
- Digital Forensics: Methods and Tools for Extracting Information from Digital Media
- File Formats: An Overview of Audio, Text, and Video Formats
- Coding in Steganography
- Steganography with Public Keys
- Robust Steganography
- Audio Steganography & Steganalysis
- Text Steganography & Steganalysis
- Password Recovery and Other Topics in Digital Media Security
- Operational Challenges: Steganography in Malware

UNCOVER TOOLS

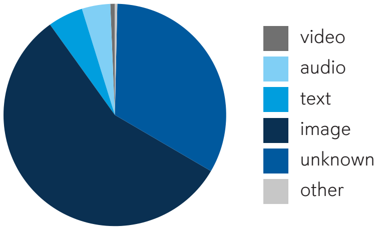
The three graphs show the results of the UNCOVER project's analysis of available steganography tools.

The first chart reveals how many steganography tools use images, videos, audio files, text files, unknown media types, or other media types as cover.

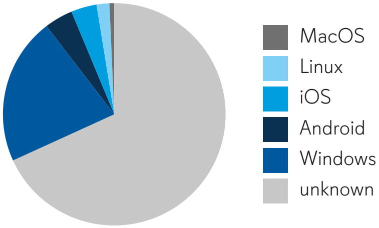
The second graph indicates which operating systems are used by the steganography tools, including Windows, Linux, Android, MacOS, iOS, and other unknown systems.

The third chart shows which programming languages are most popular for steganography tools, including C, C++, C#, Java and Python.

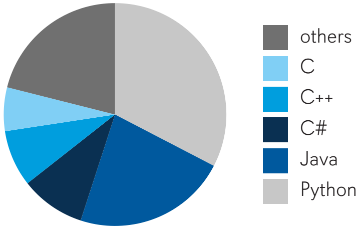
1.



2.

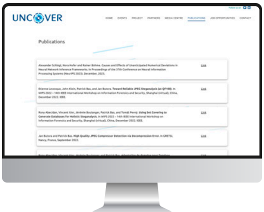


3.



PUBLICATIONS:

UNCOVER Project has produced a number of scientific publications and reports that provides insights about steganography and steganalysis.



Publications

Alexander Schlögl, Nora Hofer and Rainer Böhme. Causes and Effects of Unanticipated Numerical Deviations in Neural Network Inference Frameworks. In Proceedings of the 37th Conference on Neural Information Processing Systems (NeurIPS 2023). December, 2023. Link

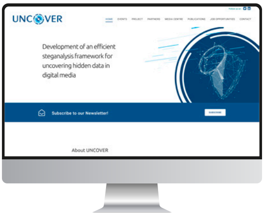
Etienne Levecque, John Klein, Patrick Bas, and Jan Butora. **Toward Reliable JPEG Steganalysis (at QF100).** In WIFS 2022 – 14th IEEE International Workshop on Information Forensics and Security, Shanghai (virtual), China, December 2022. IEEE. Link

Rony Abecidan, Vincent Itier, Jérémie Boulanger, Patrick Bas, and Tomáš Pevný. **Using Set Covering to Generate Databases for Holistic Steganalysis.** In WIFS 2022 – 14th IEEE International Workshop on Information Forensics and Security, Shanghai (virtual), China, December 2022. IEEE. Link

Jan Butora and Patrick Bas. **High Quality JPEG Compressor Detection via Decompression Error.** In GRETSI, Nancy, France, September 2022. Link

UNCOVER Project Website

www.uncoverproject.eu



Development of an efficient steganalysis framework for uncovering hidden data in digital media

Subscribe to our Newsletter!

About UNCOVER

PROJECT FACTS

Duration
36 Months

Reference
101021687

Horizon 2020
SU-FCT02-2020
Research and
Innovation Action

Coordinator
ROYAL MILITARY ACADEMY
(Belgium)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021687.

FOLLOW US &
FIND OUT MORE

CONTACT **US**

@UNCOVER_EU

office@uncoverproject.eu