UNCOVER

In recent years, the criminal use of information hiding techniques (i.e., steganography) in digital media such as images, video, audio and text files has been increasing rapidly. An important reason for this is that many steganographic tools have been made available as program source code packages. Consequently, perpetrators can easily selectively pick, adapt and combine information hiding tools for their criminal activities.

Due to the availability of tools, we are observing a significant increase in the use of steganographic methods in typical areas such as cybercrime and malware attacks and campaigns as well as beyond.

In preparation of UNCOVER, an initial survey of the Criminal Use of Information Hiding (CUIng) initiative on the Europol Platform for Experts (EPE) reveals that evidence of steganography and related principles has been found in a wide variety of types of crime including child pornography, industrial espionage, criminal attacks on enterprises, credit card fraud and skimming, system intrusion, and backdoor injection and delivery methods.

However, steganographic methods and technologies are a major challenge for Law Enforcement Agencies (LEAs) due to a lack of resources and procedures for investigations or structured operations. These problems are amplified by the increasing amount of digital evidence that LEAs and judicial partners have to handle.

UNCOVER therefore aims to address these issues and to further develop steganographic tools in order to establish a tailored toolkit for LEAs.

UNCOVER OBJECTIVES

1. **Conduct** a detailed analysis about the various aspects of the needs and requirements of LEAs for detecting and investigating steganography.
2. **Consolidate** relevant information about existing steganographic tools and centralise this information in an intuitive database for LEAs.
3. **Improve** existing methods for operational steganalysis in digital media workflows.
4. **Implement** a flexible online-platform by combining the micro-service architecture with REST- APIs for supporting interoperability.
5. **Demonstrate** the steganographic detection capabilities with realistic test cases and scenarios delivered by the LEAs.
6. **Analyse** the requirements in order to make the obtained results admissible in European court rules.
7. **Provide** a comprehensive training program for LEAs and forensic institutes by providing in-house training.
8. **Validate** the project results with practitioners, disseminate the outcomes, and prepare an exploitation plan.

UNCOVER IMPACTS

UNCOVER's objectives are aligned with the expected impacts based on each work program. The first impact that UNCOVER will have is to provide LEAs and forensic institutes with the ability to detect and extract information hidden in different types of digital media. In addition to making their work more efficient, speeding-up processing time and reliability (detection error rate).

UNCOVER will also establish a network for cooperation, raising awareness, tracking progress, sharing information, working jointly and training the staff. Contributing to the

reduction or prevention of threats from criminals and terrorists using steganography.

In conclusion, UNCOVER will work towards an international harmonization of information formats, improved cross-border acceptance and an exchange of court-proof evidence.

NEWS

Image Detectives

The University of Vigo (UVIGO) has participated in talks/events addressed to high school students and also to the general public as a means to bring UNCOVER research closer to society. Under the title of "Image Detectives", members of the UVIGO team have given several talks in high schools of the four Galician provinces and also in "Expo fairs" (i.e., open-house events) at Vigo, covering the science behind UVIGO's research work in UNCOVER.

Either in a funny/entertaining way: dressing up as Sherlock Holmes and posing enigmas and puzzle games to children or in a more formal manner to adult audiences: showcasing illustrative examples and explaining how math can help sort out different research problems; the final aim of these talks is first to raise awareness about possible misuses of innocent-looking images (that could be exploited to conduct criminal activities containing forged contents or conveying incriminating information as a steganographic message) and then point out current image-forensics and steganalysis techniques that enable the detection of such hidden information.

UNCOVER Events

The UNCOVER project has already been presented at various public events, like SICUR in Madrid or at the 21st Annual Conference of the European Society of Criminology in order to familiarise stakeholders, like law enforcement agencies, on the outcomes and potential of the project.
In the upcoming month UNCOVER will be once more providing updates and insights to interested parties, for instance at the CEPOL European Research & Science Conference in Vilnius, which will take place on 08 – 10 June; or at the European Academy of Forensic Science Conference in Stockholm from May 30th to June 3rd.

TEAM INVOLVED

The Royal Military Academy is a Belgian federal institution of university education and research. It is responsible for the academic, military and physical training of future officers, and for the continuing advanced training of officers during their career. RMA has already coordinated several European projects and has been active in international research projects for over 30 years. All research activities funded by external sources are run by the RMA with its own legal personality, different from that of the Belgian State.The research conducted by RMA is primarily aimed at increasing the security and safety in Belgium and Europe. This is achieved by collaboration with research institutes, industry and end-users active in these fields. The entities of RMA participating in the UNCOVER proposal are the Research Unit "Cryptography and Steganography" of the Department of Mathematics and the Staff Department of Scientific Research (RSWO).

The University of Vigo (UVIGO) is a public University located in Galicia (Northwest of Spain). It has 3 campus: the main one located in Vigo, and 2 more in Pontevedra (30 Km from Vigo) and Ourense (95 Km). UVIGO has placed a considerable emphasis on R&D activities by way of numerous funded projects, as well as through its various services and research centres.

UVIGO has about 22,000 students and 200 research groups, whose activity has resulted in significant scientific production in the form of doctoral theses, publications, conference communications and patents. Over the last 3 years more than 950 projects confirm the cooperation of the University with the enterprises and economic associations. In the same way, more than 25 patent requests have been submitted by UVIGO over the last years. Moreover, more than 60 European Projects has been developed over the last 10 years with a total of more than 30 million euros get.

With 3500 students, 200 faculty members, Troyes University of Technology (UTT) in one of the largest Engineer School in France. It was created in 1996 with research, with a strong emphasis on research, especially on statistical system modeling and security.

The UTT created a cyber-security workgroup in 2011 backed with a platform (https://www.cybersec.utt.fr/) that gather all resources to foster its research on cyber-security. The researchers of this team have a well-recognized expertise in the development of accurate statistical models of complex signals and in hypothesis testing theory.Those together allows the designing of statistical tests that can take into account nuisance parameter and whose performances are warranted which is crucial for reliable detection of weak signals.

Located in the heart of the Alps, the University of Innsbruck (UIBK) is home for over 27,000 students and 5,000 staff members. UIBK's Security and Privacy Lab is a leading research hub for interdisciplinary research in the fields of information forensics and security.

Key members of the lab have a strong background in steganography and steganalysis. Current and completed projects span topics such as the economic impacts of cybercrime, game-theoretic approaches to content-adaptive, information-theoretic approaches to signal forensic, prosecution and prevention of organized financial crime, development of data-driven tools for the forensic investigation of transactions in underground markets and second-generation cryptocurrencies, as well as the design of compliant forensic toolchains. UIBK's role in the project is to advance fundamental research in the automatic analysis of traces left by steganographic tools.

AVAST is a global leader in digital security and privacy, headquartered in Prague, Czech Republic. With over 435 million users online, Avast offers products under the Avast and AVG brands that protect people from threats on the internet and the evolving IoT threat landscape. The company's threat detection network is among the most advanced in the world, using machine learning and artificial intelligence technologies to detect and stop threats in real time. Avast digital security products for Mobile, PC or Mac are top-ranked and certified by VB100, AV-Comparatives, AV-Test, SE Labs and others. Avast is a member of Coalition Against Stalkerware, No More Ransom and Internet Watch Foundation. Visit: www.avast.com.

Centre National De La Recherche Scientifique (CNRS) is located in Lille, France, within the Lab called CRISTAL. Main CRISTAL Research activities involve topics related to major scientific and social issues such as Big Data, software, image and its uses, human-computer interaction, robotics, control and supervision of large systems, intelligent vehicle systems, bio-informatics ... with applications in retails, technologies for health, smart grids. The laboratory is composed of about 470 members (230 permanent employees and more than 240 non-permanent employees) among whom 28 permanent employees of the CNRS and 23 of Inria

The Otto-von-Guericke-University Magdeburg (OvGU) is one of Germany's youngest universities having been founded in 1993 in a merger of three older institutions of higher education. Representing OvGU within UNVOVER is the Advanced Multimedia and Security Lab (AMSL) as part of the Department of Computer Science.

Since being founded in 2002 this lab, led by Prof. Dr.-Ing. Jana Dittmann, has been conducting more than 40 research projects funded by EU, German national funding or industry. The lab has gathered close to 20 years of experience both in Data Hiding and in Forensic Methodologies and Techniques. In terms of research outcomes, AMSL members have published multiple books and book chapters as well as more than 250 papers in peer-reviewed international journals and conference proceedings.

Ertzaintza (ERTZ) is the police force of the Basque Country. It is a comprehensive police that assumes the bulk of the remits in matter of security, coexisting with the Local Police Forces and the State Security Forces.

The structure of Ertzaintza is based on three pillars: the Citizen Protection Division, the Criminal Investigation Division and the Central Intelligence Office. In this framework, the different specialized units are grouped in all areas of police activity: citizen security, traffic, institutional security, tactical support, criminal investigation, command and control center, games and spectacles, scientific police and private security. All these units have highly qualified staff and advanced technical means. Ertzaintza also develops judicial police functions and it currently has an R+D+I service.

SYNYO is an applied-research company focusing on security, social science, and technology, and it is based in Vienna, Austria. SYNYO explores, develops and implements novel methods, approaches, technologies and solutions in various domains for tackling societal, political, ecological and economical challenges.

SYNYO analyses the impact of emerging technologies from different angles and from an interdisciplinary perspective. The team at SYNYO consists of high-skilled researchers and developers, which are specialized in domains such as Security, Education, Social Science, Migration and Smart Technologies. The +25 employees of SYNYO are working on national and international projects, where the them is collaborating with a broad variety of European and international partners.

The Czech Technical University in Prague (CTU) is one of the largest and oldest technical universities in Europe. CTU occupies first place in the rankings for technical universities in the Czech Republic. CTU currently has eight faculties and more than 17,800 students.

The AI Center (AIC) is an excellent research institution covering a wide range of artificial intelligence research with strong emphasis on applications. We are located in the heart of Prague at the Faculty of Electrical Engineering, Czech Technical University in Prague (CTU).

Founded in 2001 by Michal Pěchouček, AIC has grown to become a world-class research center employing over 70 researchers from all over the world who work on over 30 projects supported by national, EU and US funding agencies as well as industry partners.

Together, we cover the following research areas and application domains: game theory, robotics, automated planning, machine learning, optimization, cybersecurity and smart mobility.

Gradiant is a Research and Technology Organization (RTO) focused on connectivity, intelligence and security technologies. Gradiant is an innovation provider, with over 10 years of experience on technology incubation and more than 100 engineers, Gradiant has a footprint in 30 countries and over 370 customers.

Gradiant is backed by a board that includes representatives of the three Galician universities (Vigo, Santiago and A Coruña) and seven companies from the telecommunications industry: Abanca, Altia, Arteixo Telecom, Egatel, Indra, Plexus, R, Telefónica, Televés; and INEO business association, which represents most of ICT Galician companies. In the last 2 years, Gradiant has

Resorting under the Ministry of Justice, and acting as the Belgian central authority on forensic research, the National Institute for Criminalistics and Criminology (NICC) has three main missions. First, it realizes forensic analyses on demand of the judicial authorities, in the criminalistics domains of genetics, biology, analytical chemistry, drugs, toxicology, ballistics, and digital information.

Second, it conducts scientific studies on crime phenomena to inform criminal policy. Finally, the third main branch of activities, revolves around the organization of and participation to research projects ranging from both smaller in-house projects to ameliorate or update existing technologies, to full-

quintupled the license agreements of its innovation projectss, which already reach 150 licenses in 18 countries. Some recent public international references include Telefónica, Vodafone, Samsung, PSA Peugeot Citroën, NATO, Indra, Everis, Babcock international and Boeing. Gradiant track record in EU projects includes participation in 27 FP7 and H2020 projects, 4 of them as Project Coordinator.

scale European projects (e.g., FP7/H2020, ISEC funding, etc.) carried out in collaboration with academic and commercial partners. The NICC is a full member of, and has been actively participating and contributing to various projects and activities within the European Network of Forensic Science Institutes (http://enfsi.eu/).

SUNERIS
a Thales company

SUNERIS is part of the THALES Group and is located in France. The company delivers solutions for the supervision and control of telecommunication network traffic.

Federal
Criminal Police Office

Bundeskriminalamt (BKA) - Federal Criminal Police Office in Germany

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

The CTA (Centre for Technical Assistance) is a law enforcement agency of the French Minister of Interior. The CTA helps both judicial authorities and investigative services when they are facing, during investigation, seized digital media which plain content cannot be accessed (encrypted data, locked devices ...).

Polisen
Swedish Police

The Swedish National Forensic Centre, NFC, is an expert organization within the Swedish Police Authority with an overall responsibility for forensics. NFC conducts forensic investigations and analyses on behalf of the judicial authorities. Our mission is to integrate, consolidate and streamline the national forensic services to meet society's need. An important part of NFCs operation is to conduct R&D within the field of forensic science. NFC conducts R&D to ensure forensic capabilities both now and in the future.

Plus ethics

Plus Ethics is a private start-up founded in partnership with the University Miguel Hernández of Elche (Spain), aimed at supporting and solving ethical and legal issues in research and innovation projects.
Our expertise is grounded in: 1) outlining the international, national and institutional legal frameworks to set out governing principles for ensuring the project's compliance with the existing legal framework, 2) monitoring the fulfilment of legal and ethical standards for addressing challenges arising during project implementation, advising on protocols and training for their solution, 3) assessing social desirability and research impact by undertaking evidence-based ethical studies with a view to obtaining knowledge and information capable of contributing to the establishment of a new set of moral requirements and the social and professional acceptance, 4) elaborating of codes of best practices tailored to different stakeholders and projects, and 5) applying Responsible Research Innovation (RRI) by using of different dimensions of the nexus between research and innovation and society: citizen participation, open access, gender equality, science education, ethics and governance.

THALES
Building a future we can all trust

THALES SIX GTS FRANCE SAS (TSG) revenues exceed 1 billion Euro with 6.900 employees. TSG addresses every activity related to telecommunications: wireless communications, IP networks, satellite communication, network administration and security.
TSG has a long experience in very large Information systems and secure infrastructures for systems and networks, including Internet and Intranets. TSG also develops a full range of telecommunication and cloud platforms and components, a range of high performance security products and has a deep skill in secure telecommunications and information systems for public and governmental organizations, or emergency services. Advance studies of TSG is made of a set of applied research laboratories working conjointly and involved in cutting-edge projects.

POLITIE

ZITiS

The Central Office for Information Technology in the Security Sector (ZITiS) is a research and development organization within the portfolio of the German Federal Ministry for the Interior. As part of the Cyber security strategy of Germany, ZITiS takes on a central role in the research and development of solutions, methods, tools and comprehensive strategies for improving domestic security.
ZITiS pools expertise in cyber-related technology and provides support to law enforcement agencies with regard to effective threat prevention and criminal prosecution. ZITiS has no powers of enforcement and has no external administrative powers. The work of ZITiS is tailored to the needs of German security organizations and covers the fields of digital forensics, lawful interception, cryptanalysis and big data analysis. ZITiS carries out research in collaboration with research institutions, security agencies and enterprises and takes part in the scientific discourse worldwide. ZITiS is an active partner in several national and international research projects, such as different Horizon 2020 projects.

The National Police of the Netherlands consists of Regional Units, the Central Unit and the Police Services Centre. Each Unit include Frontline Teams, which answer calls for emergency assistance, patrol the streets, advise on crime prevention, resolve traffic-related issues, conduct basic investigative activities, assist the public, process official reports and share information within their networks.
The Central Unit carries out specialist tasks. The Central Units tasks include: monitoring, supporting and coordinating major operations; combating serious organized crime; providing security support in the fight against crime; deploying mounted police, forensic expertise; carrying out and supporting police work in infrastructure, etcetera. The Police Services Centre (PDC) provides operational management services, such as finance, ICT, communications and human resources. NPN will be responsible for Law Enforcement expertise and advisory in relation to the targets, ambition and goals of the project.

Netherlands Forensic Institute
Ministry of Justice and Security

The Netherlands Forensic Institute (NFI) is a part of the Ministry of Justice and Security provides products and services to a wide range of national and international clients.
Using its expertise in over thirty forensic disciplines, the NFI not only performs analyses in actual and potential criminal cases, but also provides assistance and advice to governments, government agencies (e.g., law enforcement, customs, inspectorates, foreign justice authorities, and special investigative services) and forensic laboratories or institutes. The digital and biometric traces department does have over 100 persons employed and digital forensics around 50 persons, whereas we have experience with images, PRNU and many other techniques also related to data hiding.

POLIISI
NATIONAL BUREAU OF INVESTIGATION

The National Bureau of Investigation (NBI) is one of the national police units under the Finnish National Police Board, which is the administrative central agency of the Finnish Police. NBI carries out sophisticated, large-scale measures to combat crime.
The tasks of NBI also includes improvement of crime investigation procedures and forensic investigation methods in national level. Forensic Laboratory of the NBI is the national forensic laboratory in Finland. Its main duties are i) producing expert reports for law enforcement authorities, ii) forensic methods development, iii) training of police and other interest groups, and iv) controlling the quality of technical crime scene investigation in Finland. The laboratory is also responsible for the national DNA, fingerprint, shoeprint and voice registers. The main responsibilities of the digital forensics group are producing expert reports for law enforcement authorities and development of forensic methods. The group is focused on imaging and analyzing data from unknown, unsupported or damaged devices. IT-forensics team also analyses functionality of unknown electronic devices.

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