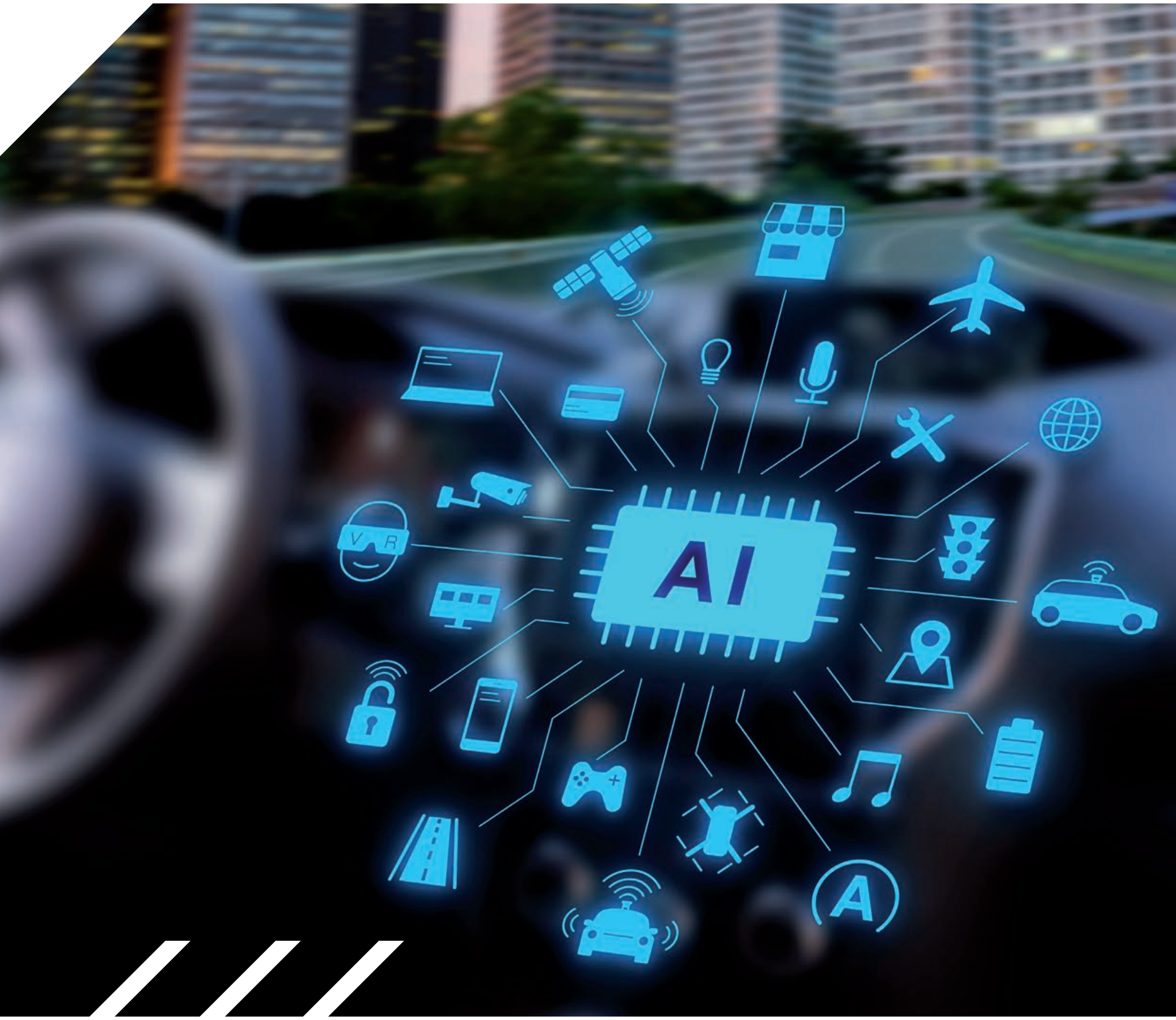
CENTER FOR DIGITAL
SAFETY & SECURITY

AUSTRIAN INSTITUTE
OF TECHNOLOGY



ARTIFICIAL INTELLIGENCE (AI)

Applications, Services and Solutions

APPLICATIONS, SERVICES AND SOLUTIONS

INTRODUCTION

Headquarter of AIT Austrian Institute of Technology in Vienna, Austria.

Today, AIT has established an internationally leading position in the field of Data Science & Artificial Intelligence. A multidisciplinary team in the Center for Digital Safety & Security provides data science solutions and consulting for making informed decisions based on large, heterogeneous, and real-time data under strict conditions of IT security and data protection.

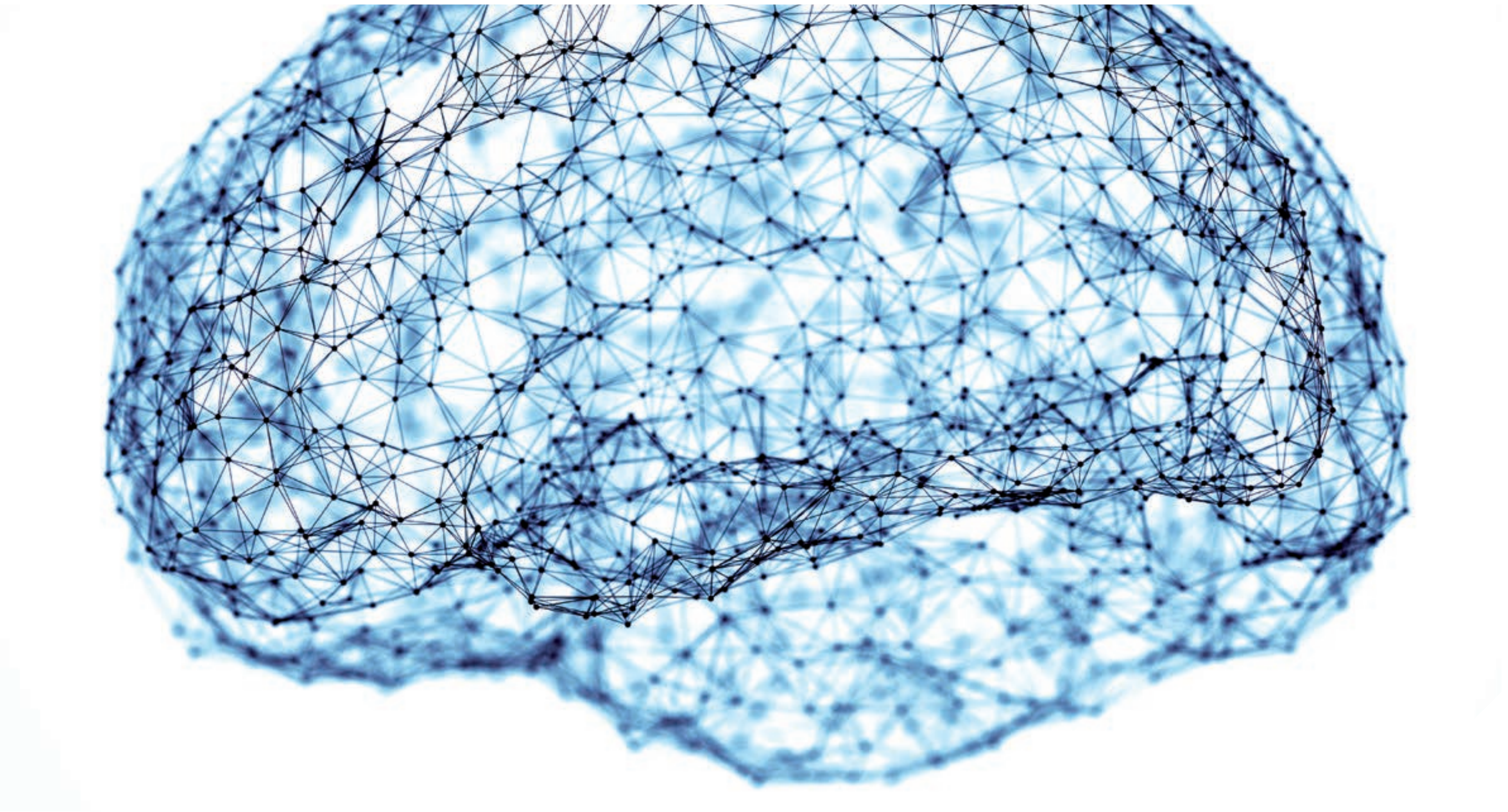
The strategic key areas for new AI technologies lie in dedicated application areas such as monitoring (e.g. cyber security), allowing large data volumes to be analysed in real time and identifying patterns as well as deviations. By using self-learning models, AI systems are also suitable for finding and extracting relevant information from large volumes of data (data mining), and interpreting the abstract patterns that have been identified.

Another key function of AI lies in the ability to make predictions, such as forecasting future trends. The interpretation capability of AI systems is the most significant factor. This allows AI systems to analyse and interpret complex, unstructured data deriving from images, videos, audio and text files, as well as sensor data.

Perhaps the most important function of AI is, however, interaction with the physical environment, such as with robots or sensors for the efficient control and navigation of highly automated systems, with both human interaction (e.g. via gestures, speech, facial expressions) and interaction between machines within M2M constellations.

Nevertheless, AI is a complex and diverse research field, ranging from technical to ethical and legal aspects. Applying AI solutions responsibly in a socio-technological environment requires comprehensive understanding and control of all components and technologies. That is why experts at AIT also focus on responsibility aspects when applying AI solutions. This also includes explainability in AI systems developed at AIT to improve safety & security of applications, increase the performance and also detect biases in the data.

The following pages provide an overview of leading-edge AI-based services and solutions developed at AIT Center for Digital Safety & Security together with and for partners in business and industry.



AI4NETS – AI FOR COMPLEX NETWORK ANALYSIS

Data communication networks, including data center networks, are among the largest and most intricate data carriers in society today, operating as complex systems with trillions of events occurring every second, even in medium-sized networks. These networks generate massive amounts of data, making AI-enabled and learning-based approaches crucial for building more efficient, reliable, and secure communication systems. Applying deep learning to such complex systems presents significant challenges, including the handling of the 4 Vs of big data: the sheer volume and variety of heterogeneous data (Volume and Variety), the fast-paced and dynamic nature of data streams (Velocity), and the uncertainty of data quality and lack of ground truth (Veracity).

Leveraging deep learning and AI in these networks can help organizations unlock new potential in managing and optimizing communication networks and similar complex systems, particularly within data center environments, where efficiency and performance are critical.

NETWORK SECURITY (AI4NETSEC)

AI can significantly enhance the detection accuracy of attacks and other threats flowing through communication and data center networks, without compromising the robustness of the analysis (i.e., false alarms). It can rapidly identify complex threats and detect previously unseen attacks, including sophisticated forms of web-phishing—one of the most prevalent and rapidly growing cyber-crimes today. The frequency and scale of phishing attacks have surged, making them a critical focus for AI-based detection. AI can not only detect phishing patterns hidden in vast volumes of network traffic but also manage obfuscated and adversarial learning environments, where attackers attempt to evade detection through various deceptive techniques.

NETWORK ANOMALY DETECTION & DIAGNOSIS (AI4NETADD)

The automatic detection and diagnosis of the ever-growing number of anomalies faced by network operators is a paramount challenge. By enabling the analysis of highly dimensional time-series data with both real-time and large-scale requirements, AI and big data principles and platforms can significantly improve the visibility and understanding of such complex and rare events, empowering a quick troubleshooting process.

NETWORK MONITORING AND ANALYSIS (AI4NETMON)

Network monitoring and analysis is crucial for managing large-scale and complex networks, enabling real-time performance monitoring, traffic classification, and network policing. Monitoring systems must be scalable, capable of processing millions of heterogeneous events, and able to quickly detect and respond to anomalies or security threats. At AIT, we design AI-capable platforms that integrate scalable monitoring techniques with AI-driven insights, ensuring that the network's performance aligns with end-user needs and expectations, even under the challenges posed by encryption.

INTERNET QUALITY OF EXPERIENCE (AI4NETQOE)

Quality of Experience (QoE) is a well-known concept that permits operators to understand and assess the functioning of networks and services from the standpoint of the end user or service customer. QoE development has been traditionally limited to small-scale controlled environments, but today QoE-based network measurements represent a paramount source of information for Internet service and content providers. Here at AIT, we are experts in QoE for networks at scale, incorporating the QoE paradigm into the design, analysis and operation of real-world networks, services, and distributed systems. AI-based Internet-QoE relies on big data analytics to generate useful user-centric insights from large-scale network measurements, even under the increasing prevalence of end-to-end encryption.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Pedro Casas
Tel. +43(0) 50550 4104
Giefinggasse 4, 1210 Vienna
pedro.casas@ait.ac.at
www.ait.ac.at/cybersecurity

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Dr. Florian Skopik
Tel. +43(0) 50550 3116
Giefinggasse 4, 1210 Vienna
florian.skopik@ait.ac.at
www.ait.ac.at/cybersecurity

References (excerpt)

ÆCID - Automatic Event Correlation for Incident Detection; aecid.ait.ac.a

BIG-DAMA – Big Data Analytics for Network Traffic Monitoring and Analysis; bigdama.ait.ac.at

MobiQoE – Monitoring and Analysis of Quality of Experience in Mobile Networks; mobiqoe.ait.ac.at

AI FOR NATURAL LANGUAGE PROCESSING (NLP)

Discovering valuable information within unstructured, heterogeneous text is a challenging task, given the vast amount of textual data that we must cope with in today's information society. AIT provides the expertise and support for a broad range of use cases by applying a variety of machine-learning techniques – including algorithmics, mathematics and statistics – to discover topics and semantic relationships, and to extract meaningful, structured information.

With the advent of more powerful computing hardware, deep learning has emerged as a new and promising machine-learning paradigm in natural language processing (NLP). The use of neural network-based machine learning is not new, but with the application of new approaches for learning vector representations of words in very large text collections, deep learning has been proven to deliver excellent results in machine-learning tasks such as classification or the detection of semantic relationships between words.

While deep learning has changed the manner in which NLP is carried out, it is only part of the solution. AIT offers advice on the many classic tasks that still play a fundamental role, such as corpus building and cleaning, pre-processing, tokenization and stemming. Classic information retrieval measures such as co-occurrence statistics, TF-IDF (term frequency–inverse document frequency), bag-of-words (BoW) representation, or part-of-speech tagging (PoS) are still important parts of the NLP toolset. Depending on the specific use case, these are individually applied as input for Deep Neural Networks (DNN), or in conjunction with other machine-learning algorithms such as Support Vector Machines (SVM).

AIT solutions enable the analysis and overview of new text document collections using unsupervised machine learning methods. Topic modelling allows us to reveal important concepts, terms and relationships that occur in a collection of documents.

Using pre-defined or manually assigned labels, classification algorithms support the structuring and filtering of large text collections into sub-groups. This is also important for building a domain-specific, cleaned corpus for use in a specific application domain. Once such a well-defined text corpus exists, it can be used to implement supervised machine learning tasks. These include, for example, Named Entity Recognition (NER) in which, based on external knowledge, words are assigned to abstract classes such as names of persons or organizations, events, machine parts in industry or medical terms in healthcare.

AIT´S ANNOTATION PLATFORM

One of our primary goals is to minimize the effort required for the manual annotation and labelling of text, because this task relies on manual work and domain knowledge. One method of achieving this goal is to provide efficient and user-friendly labelling tools. Recogito is our annotation platform which uses existing gazetteers and dictionaries to aid in the process of producing the high-quality ground-truth training data required for supervised machine-learning tasks. This task can be supported by active learning, where the learning algorithm actively suggests significant terms to the user who is then able to confirm, reject or refine effectively, and by transfer learning, which allows us to leverage generic language models which can then be tailored to domain-specific languages and document types with significantly less effort.

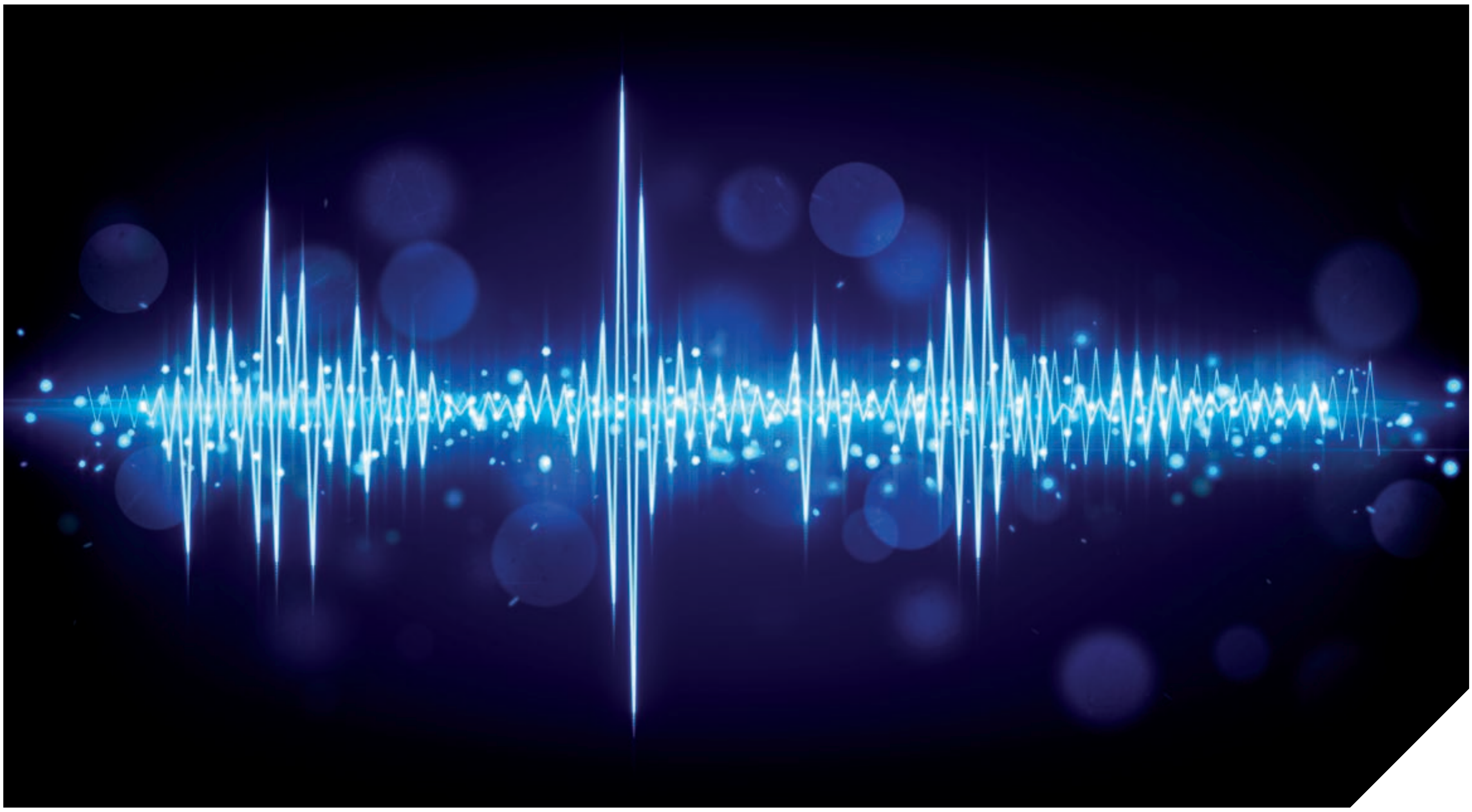
References (excerpt)

COPKIT (H2020) – Intelligence-led Early Warning and Early Action system for Law Enforcement Agencies; https://copkit.eu/

TRAVELOGUES (FWF) – Perceptions of the Other 1500–1876; http://www.travelogues-project.info/

Pelagios Projects – a collection of multiple projects under which the Recogito platform was developed: http://commons.pelagios.org/ (Andrew. W. Mellon Foundation), https://pelagios.org/

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Alexander Schindler
Tel. +43(0) 50550 2902
Giefinggasse 4, 1210 Vienna
alexander.schindler@ait.ac.at
www.ait.ac.at/dsai



MULTI-MODAL AI FOR SECURITY APPLICATIONS

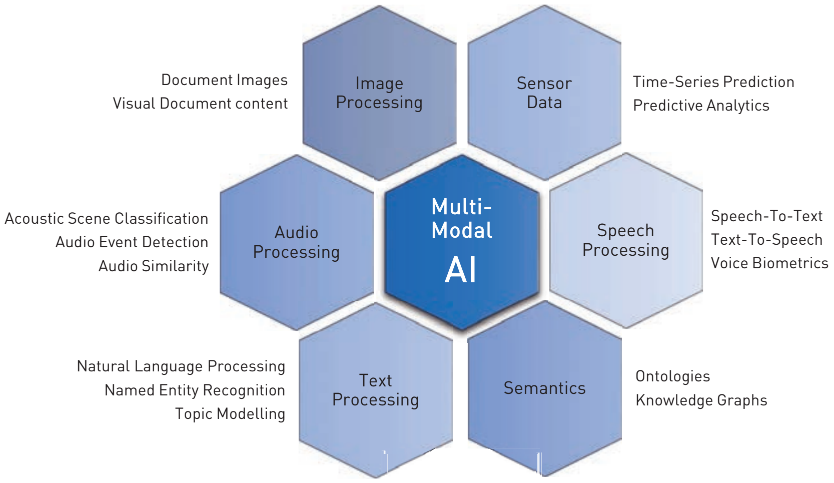
AIT has expertise in scalable security platforms designed for implementing multi-modal AI at a level suitable for a wide range of real-world applications. The platform addresses the needs of various end users, including service providers and stakeholders such as law enforcement agencies (LEAs). One application of such a platform is to analyse and prioritize large volumes of audio and video content provided by the public, especially in the aftermath of critical incidents. Experience shows that such events generate extensive amounts of visual and audio material, requiring efficient processing and analysis.

This development relies on several areas of AIT expertise:

Video and Image Analysis: Videos are searched for visual features. Designated objects can be detected and tracked. A flexible analysis component plug-in layer allows for the simple inclusion of additional algorithms such as the extraction of text from images or the detection of symbols or logos. Images can be localized based on intrinsic visual features alone, in the absence of any geospatial metadata. Manipulated images, AI-generated images, and Deepfake videos can be detected.

Audio Analysis: The platform can integrate various audio algorithms such as audio event detection, audio scene recognition, and speech-to-text transcription. Non-visual events such as gunshots and explosions are indexed to facilitate search, using methods based on deep neural networks to detect relevant acoustic events. Additionally, relevant video sequences can be selected to identify other sequences with similar audio content. This is useful as an aid in personal identification, for example. Videos with similar audio will be recorded at the same place and at the same time, possibly providing a different angle on the same person. We also offer audio fingerprinting techniques that allow the system to synchronize multiple data sources based on audio events.

Text Analysis: Natural Language Processing (NLP) and Large Language Models (LLMs) have become critical tools in the security domain, enabling more efficient and accurate analysis of vast amounts of textual data. By processing unstructured information from open-source intelligence (OSINT) sources, our models can detect potential threats, analyse trends, and prioritise material for investigations. These technologies also aid law enforcement agencies in identifying risks, assessing public sentiment, and responding to crises quickly and effectively.



Scalable Data Processing: Scalable data processing is essential in the security domain for efficiently handling large volumes of multimedia and text data. We have experience in scalable architectures making use of High-Performance Computing (HPC) clusters of Graphics Processing Units (GPUs), which are used to efficiently deploy our machine learning algorithms. We specialize in local solutions that do not depend on third-party services or hardware. By leveraging distributed computing and our advanced algorithms, law enforcement agencies can rapidly analyse and prioritize data and manage the challenge of constantly increasing volumes of digital information.

References (excerpt)

VICTORIA – Video analysis for Investigation of Criminal and TerrORIst Activi¬ties; https://www.victoria-project.eu/ (EU H2020)

FLORIDA; https://www.kiras.at/gefoerderte-projekte/detail/d/florida/ (funded under the Austrian KIRAS security programme of the Federal Ministry of Transport, Innovation and Technology)

STARLIGHT; https://starlight-h2020.eu/ (EU H2020)

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Ross King
Tel. +43(0) 50550 4271
Giefinggasse 4, 1210 Vienna
ross.king@ait.ac.at
www.ait.ac.at/dsai

MULTI-MODAL AI FOR DOCUMENT MANAGEMENT

Document management systems need to be able to store, archive, process, and extract information from digital-born as well as scanned, image-based documents. Documents and their relevant parts need to be searchable and to be presented appropriately with respect to their context and document type. In recent times, AI in general, and machine learning in particular, has opened up new possibilities for better supporting users and providing more efficient tools for managing large collections of heterogeneous documents.

AIT offers a full range of software and expertise, from document acquisition to access. Its portfolio comprises modular and flexible components for creating domain-specific document processing workflows that are ready to scale up and work on very large document collections. Multi-modal AI is applied to this domain in three primary areas.

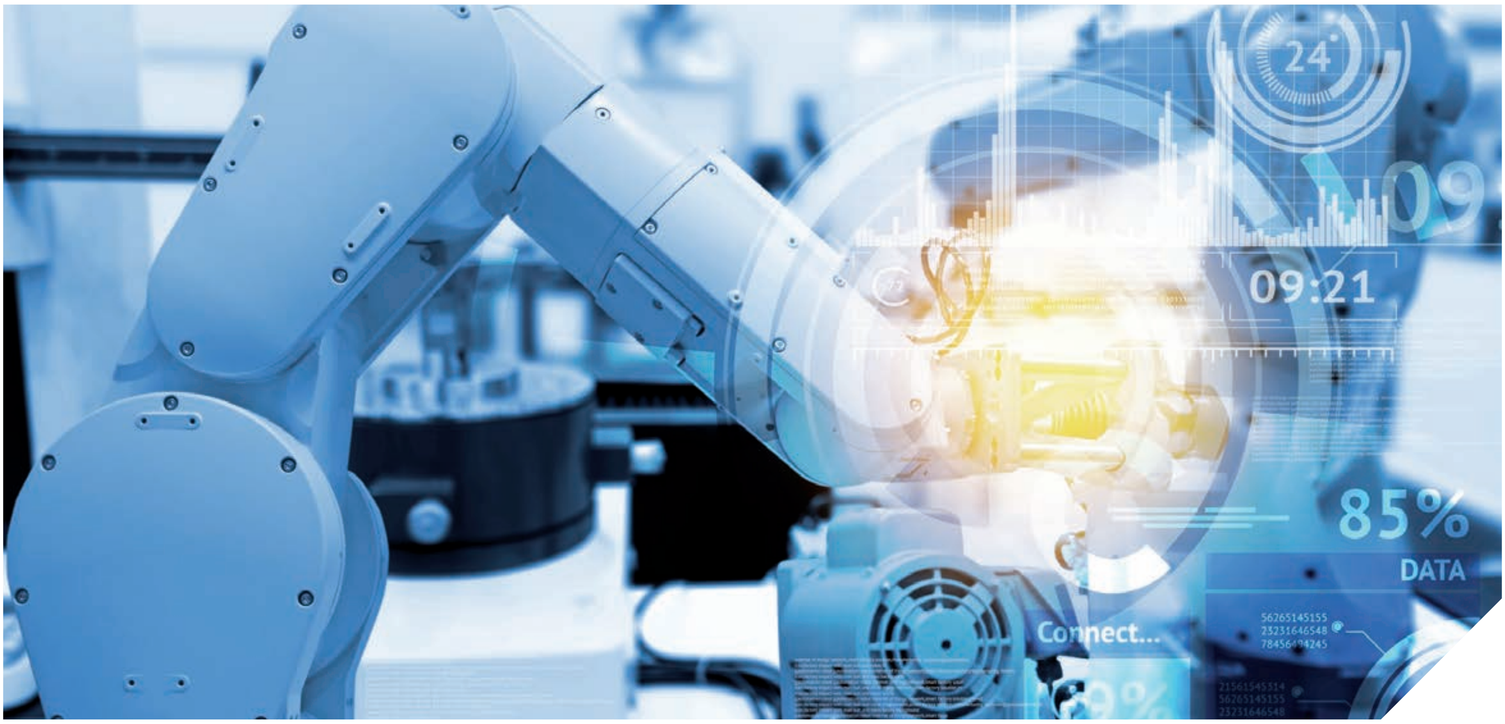
First, the quality of OCR (optical character recognition) has improved significantly in recent years, also with the help of AI. While digital-born and good quality scans can be reliably transformed into text, challenges remain for low quality scans or photographs taken from documents. Here multi-modal AI can help by using a combination of techniques (OCR and Image Analysis) to achieve better overall performance. At AIT, we use these techniques to address challenging tasks such as gaining structured information from tables contained in document images or extracting semantically meaningful blocks including the sender, addressee, and subject line of a scanned letter.

Second, AI is now at the heart of "document understanding". Domain-specific language and document structure and layout models are required to reach a good level of performance in document classification, clustering, information extraction, and natural language analytics tasks. This in turn requires the creation and management of adequate training data and, in many cases, a scalable storage and compute environment for pre-processing and for the creation of machine learning models. AIT can advise your organization on how to manage this new aspect of data and software maintenance.

Third, AI has become indispensable for advanced document access, retrieval and document understanding, and AIT can support the introduction of this new approach in your knowledge management landscape. Modern AI technologies, particularly those using Large Language Models (LLMs), provide the ability to perform semantic search while integrating with internal or external knowledge bases via APIs, vector databases, or other retrieval-augmented generation (RAG) mechanisms. This includes, for example, search technology that leverages Large Language Models (LLMs) for semantic search and to include information from internal or external knowledge bases via APIs or other retrieval mechanisms. AIT helps you applying AI-driven data science in specific application domains, such as the extraction of geospatial information from unstructured text, enabling the generation of map data and advanced spatial analysis, for example.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Sven Schlarb
Tel. +43(0) 50550 4179
Giefinggasse 4, 1210 Vienna
sven.schlarb@ait.ac.at
www.ait.ac.at/dsai

References (excerpt)
E-ARK – European Archival Records and Knowledge Preservation; www.eark-project.com (EU CIP), wwwe-ark4all.eu



AI4INDUSTRY – INTEGRATING AI IN INDUSTRIAL ENVIRONMENTS

With manufacturing industries on the verge of a data-driven revolution, there is an enormous potential to advance their analysis and optimization through data-driven solutions. AI4Industry combines data science and AI to address the unique challenges of deploying AI solutions in industrial settings. Our mission is to help organizations harness AI to optimize processes, increase operational efficiency, and drive business innovation. By applying data-driven approaches to industrial data, we help companies unlock insights into the technical and relational aspects of their complex value-creation processes. These AI-powered solutions aim to enhance business outcomes through increased automation, smarter decision-making, reduced costs, and improved overall performance.

At AIT, we focus on creating a tangible impact for industries, using AI to deliver higher revenues, lower operational costs, and sustainable competitive advantages.

1. TIME-SERIES ANOMALY DETECTION (AI4TSAD)

Industrial environments generate vast amounts of time-series data, making anomaly detection critical for identifying irregularities and potential failures. At AIT, we leverage advanced deep learning and AI foundation models to detect subtle anomalies in real time, predict system failures, and optimize performance. This proactive approach helps prevent costly downtime and supports the next generation of intelligent industrial production.

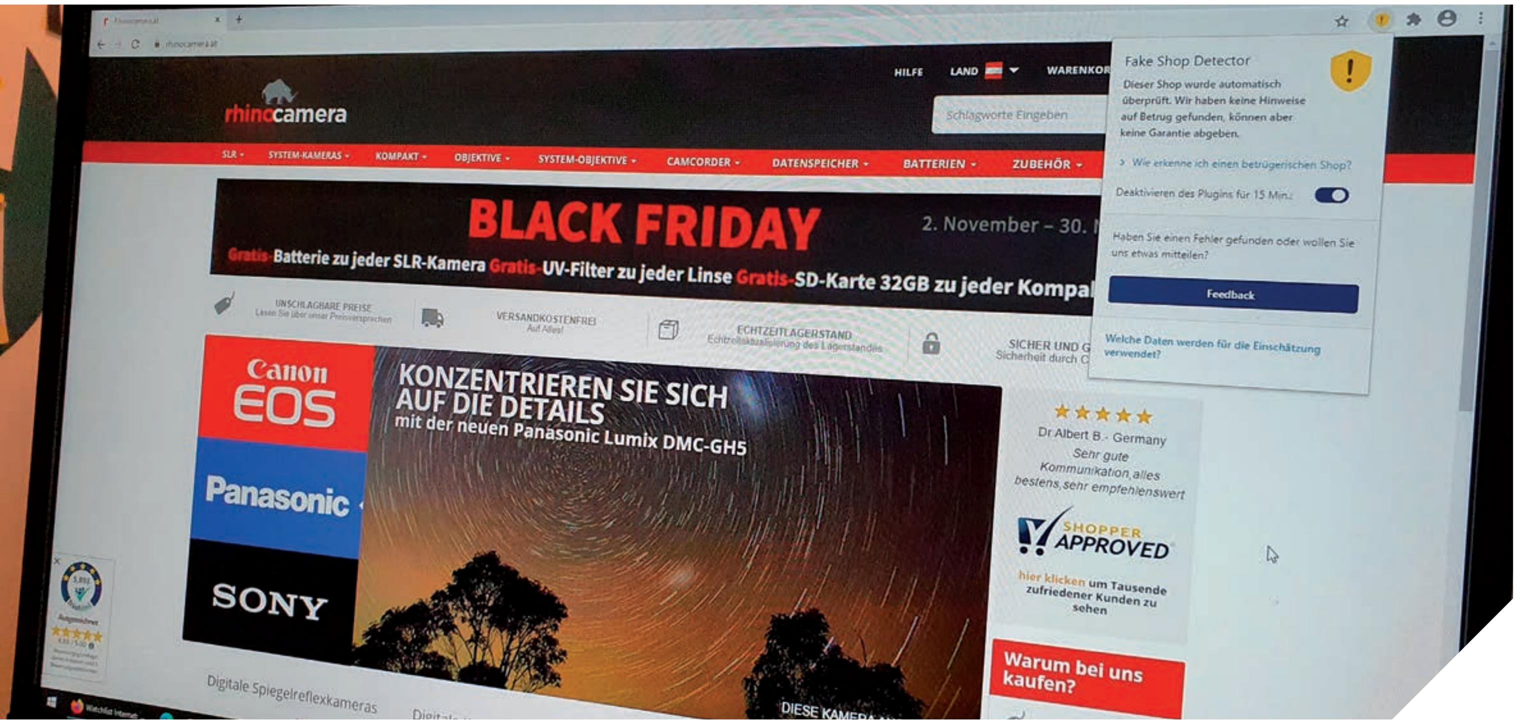
2. PREDICTIVE MAINTENANCE (AI4PHM)

Predictive maintenance (including Prognostics and Health Management) leverages AI to monitor the condition and history of industrial equipment, predicting when maintenance should be performed. This AI-driven approach enables industries to move from reactive or scheduled maintenance to a more efficient, condition-based strategy. At AIT, we develop models that detect equipment degradation early, allowing organizations to plan maintenance proactively, reduce unexpected breakdowns, and avoid unnecessary maintenance costs for healthy machines.

3. MANUFACTURING OPTIMIZATION (AI4PROD)

Manufacturing industries consume over half of the world's energy and are significant contributors to CO_2 emissions. By optimizing manufacturing processes, industries can reduce energy consumption and improve resource utilization. At AIT, we use AI-assisted modeling and optimization techniques to enhance the efficiency and sustainability of production processes, driving improvements in both energy consumption and production quality. Our AI-driven solutions empower manufacturers to make data-informed decisions, resulting in more efficient and eco-friendly operations.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Pedro Casas
Tel. +43(0) 50550 4104
Giefinggasse 4, 1210 Vienna
pedro.casas@ait.ac.at
www.ait.ac.at/cybersecurity



Fake Shop Detector

Dieser Shop wurde automatisch überprüft. Wir haben keine Hinweise auf Betrug gefunden, können aber keine Garantie abgeben.

› Wie erkenne ich einen betrügerischen Shop?

Deaktivieren des Plugins für 15 Min.:

Haben Sie einen Fehler gefunden oder wollen Sie uns etwas mitteilen?

Feedback

Welche Daten werden für die Einschätzung verwendet?

rhinocamera
HILFE
LAND
WARENKORB
Schlagworte Eingeben
BLACK FRIDAY
2. November – 30.
Gratis-Batterie zu jeder SLR-Kamera Gratis-UV-Filter zu jeder Linse Gratis-SD-Karte 32GB zu jeder Kompal
KONZENTRIEREN SIE SICH AUF DIE DETAILS
mit der neuen Panasonic Lumix DMC-GH5
Canon EOS
Panasonic
SONY
Dr Albert B.- Germany
Sehr gute Kommunikation,alles bestens,sehr empfehlenswert
SHOPPER APPROVED
hier klicken um Tausende zufriedener Kunden zu sehen
Warum bei uns kaufen?
Digitale Spiegelreflexkameras

AI BASED FAKE-SHOP DETECTION

Online shopping is booming like never before, but at the same time, the fake-shop trap is snapping shut more and more frequently. These shops lure unsuspecting buyers into their trap with advertising in search engines and social media, as well as with low prices. Products are ordered and paid for, but never arrive. Fake shops are becoming more and more professional and are therefore increasingly difficult to recognize as such. The damage caused by fake shops in Austria runs into the millions, with tens of thousands of reports being received by Watchlist Internet every year. Once paid, the money is often lost. By the time the fraud is discovered, the shops have usually already disappeared. This makes prevention all the more important.

For the first time in Austria, a tool has been developed that protects consumers from e-commerce fraud by cleverly combining expert knowledge and artificial intelligence (AI). This was achieved by combining the expertise of the Watchlist Internet Experts at ÖIAT, the top research team on machine learning at AIT and the IT professionals at X-Net. The AI models measure the similarity of web shops to already known fake shops and warn users in real time using a traffic light system. The Fake-Shop Detector is available as a plug-in for the Firefox, Edge and Chrome internet browsers. Users can check questionable online shops on their cell phones using the shop check at www.fakeshop.at or directly in the Watchlist Internet app.

The Fake-Shop Detector has become an Austrian flagship project for applied AI because it combines human expertise and machine efficiency: First, a database curated by experts, which provides a comprehensive "whitelist" of trustworthy web shops in Germany, Austria and Switzerland, is searched by well-known cooperation partners, along with a "blacklist" that includes over 20,000 fake shops. If a shop is not listed, it is checked by the AI in a real-time analysis. For this purpose, AIT has developed a unique method for classifying fake shops, in which features are extracted purely from the source code, instead of defining characteristics in advance as is usually the case. The robustness of the AI approach results from the fact that no single characteristic stands out on its own, but that the combination of a large number of different characteristics, each with a low weighting, is crucial for correct classification. There are currently 21,528 assessable features available to the models. The combination of a large number of features thus leads to a robust risk assessment and ensures that criminal actors cannot circumvent automated detection by making simple changes to their websites.

With over 10,000 active daily users, 1.8 million existing risk assessments, active protection against 20,000 fraudulent online shops, an AI accuracy rate of over 97% in the highest Detector warning level, and over 2,000 newly processed AI analyses daily, the Fake Shop Detector is highly effective in preventing fraud in online retail. In cooperation with Watchlist-Internet, the Detector's warnings are directly adopted on one of the most important fraud prevention platforms with an enormous reach. This contributes significantly to reducing the fraudulent window of opportunity. Through the Fake-Shop

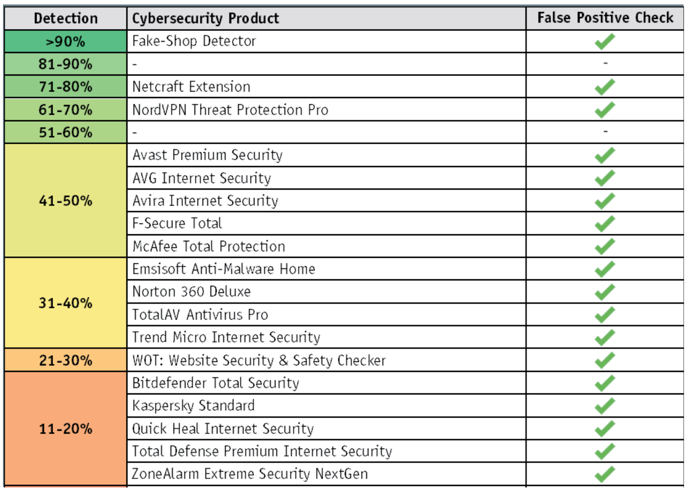
The development team of the Fake-Shop Detector has been awarded the Austrian State Prize for Digitalisation by the State Secretary for Digitalisation Claudia Plakolm in 2024.

Fake-Shop Detector

Detector and the community effect, it is possible to expose 450 domains per month with a fake-shop risk at the highest warning level of the AI and to confirm these manually by human quality assurance, by providing an integrated solution for support for expert organizations, within the shortest possible time.

This groundbreaking work of the Fake-Shop Detector, an AI-based technology in the fight against fraudulent online shops and cybercrime, was awarded the Austrian State Prize for Digitization in the category "Lifestyle, Youth and E-Sports" in 2024. AV Comparatives rated the Fake-Shop Detector as the most effective security product against internet fake shops in August 2024. In addition, the Fake-Shop Detector team is pleased to have won the Constantinus Award 2024 in the category of Digitization

The research work for the implementation of the Fake-Shop Detector was primarily funded by the KIRAS security research program of the Federal Ministry of Finance and the Austrian Research Promotion Agency FFG as part of the SINBAD and RIO projects.



Detection	Cybersecurity Product	False Positive Check
>90%	Fake-Shop Detector	✓
81-90%	-	-
71-80%	Netcraft Extension	✓
61-70%	NordVPN Threat Protection Pro	✓
51-60%	-	-
41-50%	Avast Premium Security	✓
	AVG Internet Security	✓
	Avira Internet Security	✓
	F-Secure Total	✓
	McAfee Total Protection	✓
31-40%	Emsisoft Anti-Malware Home	✓
	Norton 360 Deluxe	✓
	TotalAV Antivirus Pro	✓
	Trend Micro Internet Security	✓
21-30%	WOT: Website Security & Safety Checker	✓
11-20%	Bitdefender Total Security	✓
	Kaspersky Standard	✓
	Quick Heal Internet Security	✓
	Total Defense Premium Internet Security	✓
	ZoneAlarm Extreme Security NextGen	✓

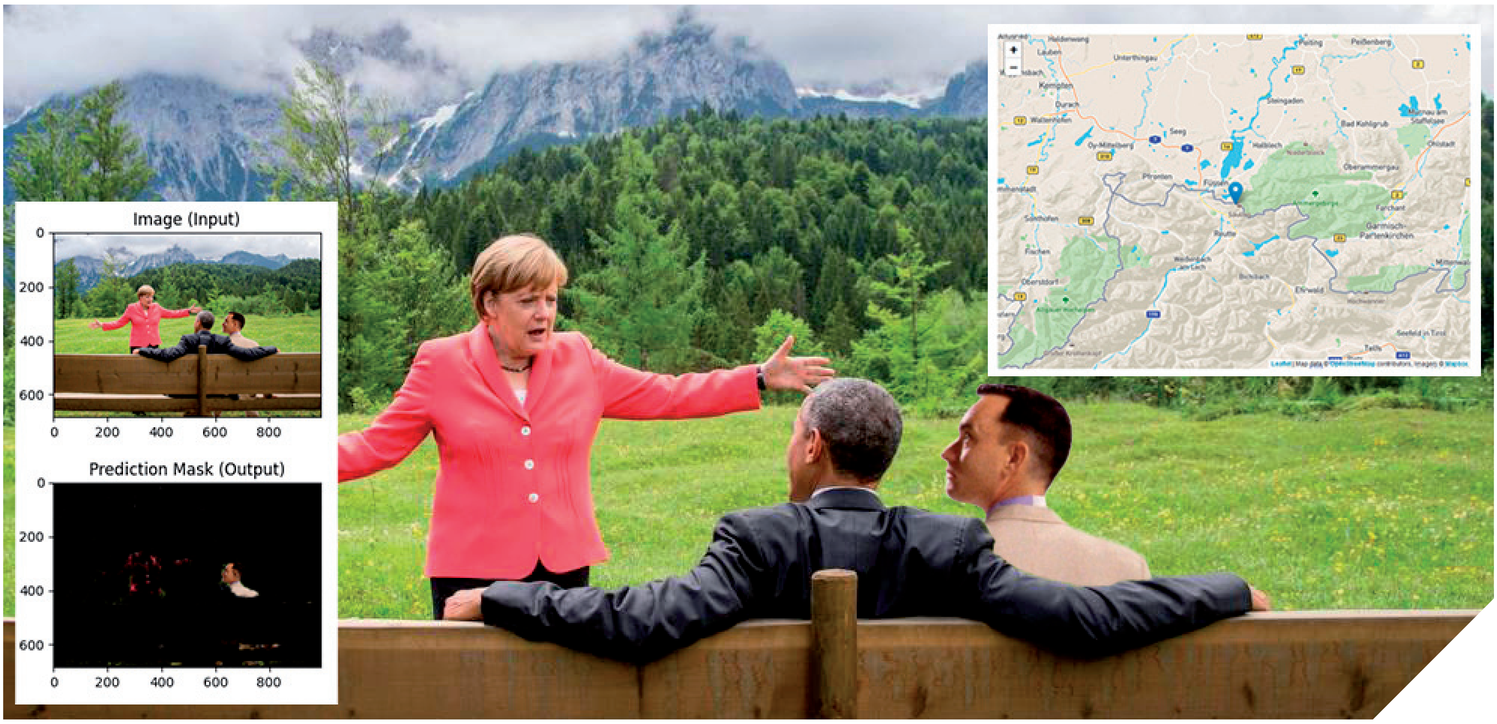
The Fake-Shop Detector is Austrian winner among 35 international cyber security products tested for their effectiveness against fake shops.

RIO
Resilience in online trading
Website: projekte.ffg.at/projekt/4489816
Duration: 2022-2024

SINBAD
SINBAD - Security and Prevention of Organized Internet Order Fraud for Users through Digital Forensics Measures
Website: projekte.ffg.at/projekt/3807747
Duration: 2020-2022

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Mag. Andrew Lindley
Tel. +43(0) 50550 4272
Giefinggasse 4, 1210 Vienna
andrew.lindley@ait.ac.at
www.fakeshop.at

Images: ÖIAT (left), BKA–Christoph Dunker (right), AV-Comparatives (bottom)



AI BASED DETECTION OF DISINFORMATION

At the AIT Austrian Institute of Technology, media forensic tools are being developed to support humans in better identifying DeepFakes and manipulated or generated media content. In the past and ongoing national research projects "defalsif-AI" (Detection of False Information by means of Artificial Intelligence) and "defame Fakes" (Detection of DeepFakes and manipulations in digital images and videos) – both funded by the KIRAS security research programme of the Austrian Federal Ministry of Finance (BMF) and coordinated by the AIT Center for Digital Safety & Security – a Media Intelligence platform is being developed that allows investigating authorities, public administrations, media organizations, the private sector – and in future also citizens – to assess the credibility of text, image, video or audio material on the Internet. Artificial Intelligence (AI) is used for this.

AIT is also a partner of the German-Austrian Digital Media Observatory (GADMO) – an alliance of fact-checkers, media literacy experts and scientists taking a coordinated approach to combating disinformation and misinformation.

AIT projects in this area revolve around 2 main goals:

a) the design and research of appropriate, human-understandable assessment-tools for the detection of DeepFakes and manipulations in large collections of digital image and video content – in order to hereby strengthen the technological capabilities enabling appropriate, reactive measures - as well as...
b) the initiation and design of awareness-raising activities in close cooperation with public authorities, media, SSH partners and relevant national and European stakeholders, with the ultimate aim of defining preventive measures and emphasizing knowledge and awareness building throughout the public security landscape.

Manipulating video, photos, and text is no longer the job of intelligence professionals. In theory, everyone has the tools on their computer – and smartphone – and instructions are easy to find on the Internet. Even the production of so-called deep fakes, videos in which people – often celebrities or politicians – are deceptively made to say things they never said, is no longer difficult. And unlike traditional media such as newspapers or radio, whose content goes through a rigorous verification process, such user-generated content can be distributed online very quickly with a single click.

The Media Intelligence platform is designed to help identify such fake content at an early stage. When a user searches for clues, the software gives a corresponding assessment after it has been applied to the respective media content.

Various analysis modules and AI algorithms examine the content. Based on this, the Media Intelligence tool indicates the likelihood that it has been manipulated, tampered with, or generated. The tool provides support, but the final decision as to whether or not a piece of content can be classified as manipulated is ultimately made by humans.

Image composition:
AFP/MICHAEL KAPPELER/Paramount/Reddit/grenthdascalon; AIT

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
DI (FH) Martin Boyer
Tel. +43(0) 50550 4284
Giefinggasse 4, 1210 Vienna
martin.boyer@ait.ac.at
www.deepfakes.at

AI FOR SAFETY & SECURITY IN CYBER-PHYSICAL SYSTEMS

Artificial Intelligence, together with safety & security requirements, is significantly shaping the systems used in Industry 4.0, highly automated cyber-physical systems, and the Internet of Things (IOT). The Center for Digital Safety & Security has extensive experience in the development and operation of safe and secure systems. For many years specialists at the Center have been working in standardization in order to shape tomorrow's compulsory standards, as well as developing practical solutions and advising companies on the introduction of compliant processes and implementing engineering projects.w

The Center's portfolio includes:

- Training in Artificial Intelligence (AI) for industrial applications, cybersecurity, standard-compliant work
- Verification technologies suitable for AI methods, and which themselves apply AI approaches in order to increase efficiency
- Standard-compliant workflows including tool support, e.g. using AI-based document evaluation
- Tools for automatic, model-based threat analysis of system designs (Security by Design) with an automatically updating threat database (subscription model)
- Real-time monitoring of analogue and digital signals (runtime monitoring)
- Data analysis and machine learning (including explainable AI)
- Secure architectures for legacy systems (secure gateways, etc.)
- Security analyses of network designs, machine code analysis, source code reviews/audits, penetration testing, ISO training
- Tools for automated cybersecurity threat analysis in the automotive field

The special processes, technologies and tools developed at AIT allow the safety & security of systems to be monitored in real-time, during operation, and are currently being deployed globally.

References (excerpt)

Enable-S3 – European Initiative to Enable Validation for Highly Automated Safe and Secure Systems; https://www.enable-s3.eu/ (H2020, ECSEL Joint Undertaking)

ThreatGet– Threat Analysis and Risk Management Tool; https://www.threatget.com/, https://www.threatget.eu

Installations at Tier 1 manufacturers and automotive suppliers

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Stefan Schauer
Tel. +43(0) 664 825 14 55
Giefinggasse 4, 1210 Vienna
stefan.schauer@ait.ac.at

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Ross King
Head of Competence Unit Data Science & Artificial Intelligence
Center for Digital Safety & Security
Tel. +43(0) 50550 4271
Giefinggasse 4, 1210 Vienna, Austria
ross.king@ait.ac.at
www.ait.ac.at/dsai

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Mag. (FH) Michael W. Mürling, MA on AI for Public Service
Marketing and Communications
Center for Digital Safety & Security
Phone +43 50550 4126
Giefinggasse 4, 1210 Vienna, Austria
michael.muerling@ait.ac.at
www.ait.ac.at/dss

Editorial management: Michael W. Mürling, Verena Serini | Place of publication: Vienna, August 2024