Aktuelle Trends in der KI

Analytics, Quality und Human Centered

DI Theodorich Kopetzky
Executive Head Knowledge-Based Vision Systems
theodorich.kopetzky@scch.at

SCCH is an initiative of
JOHANNES KEPLER UNIVERSITY LINZ
Bundesministerium Verkehr, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG
Regio 13
Forschungsland Oberösterreich
SCCH is located in
softwarepark hagenberg

1999 gegründet von JKU Linz

- Mathematik
- Informatik

Focus

- Daten/Algorithmen/ML Optimisierung/Prediction
- Software/Quality/Testing

scch
software competence center
hagenberg

Software Competence Center Hagenberg GmbH

- Unabhängige, anwendungsorientierte Forschungseinrichtung für
  Data Science & Software Science
- Verbindet wissenschaftliche Forschung mit Anwendungen in der Wirtschaft

- COMET-Kompetenzzentrum
  - ~ 70 Mitarbeiter/innen
    (>100 mit Mitarbeiter/innen von Partnern)
  - ~ 7.2 Mio. Euro Umsatz inkl. Förderungen
  - ~ 30 längjährige Firmenpartner

- Enge Zusammenarbeit mit JKU
  - Prof. S. Hochreiter (Deep Learning)
  - Prof. G. Widmer (Computational Perception)
  - Prof. A. Egyed (Software Engineering)

Forschungsschwerpunkte

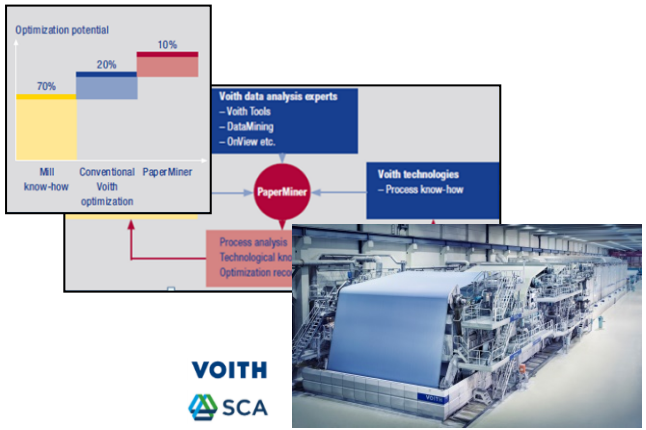
Übersicht

- KI Geschichte des SCCH
- Aktuelle Projekte
- Zukünftige Projekte

20 years ago versus nowadays

PaperMiner

data mining + discovery of unknown dependences + human interpretation



KI als Ingenieurswissenschaft

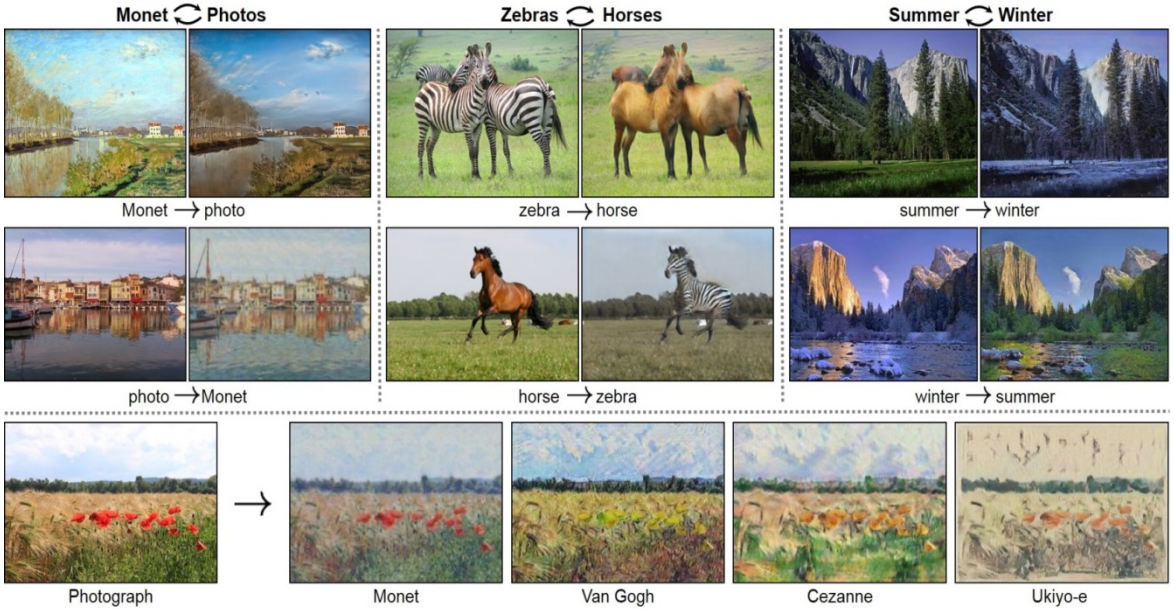
- Nadelöhr Daten
  - derzeit sind AI Methoden sehr datenhungrig
  - Variabilität, Shift in den Daten!

- Methodisch
  - Trustworthiness, XAI
  - Manipulationssicherheit
  - Integrität (z. B. Adversarial Attacks), Betriebssicherheit, Testbarkeit,
    Schutz der Privatsphäre (Personendaten, geschäftskritischen Firmendaten), Wiederholbarkeit

- Psychologisch und rechtlich
  - Mensch-AI Schnittstelle
  - Akzeptanz Problem

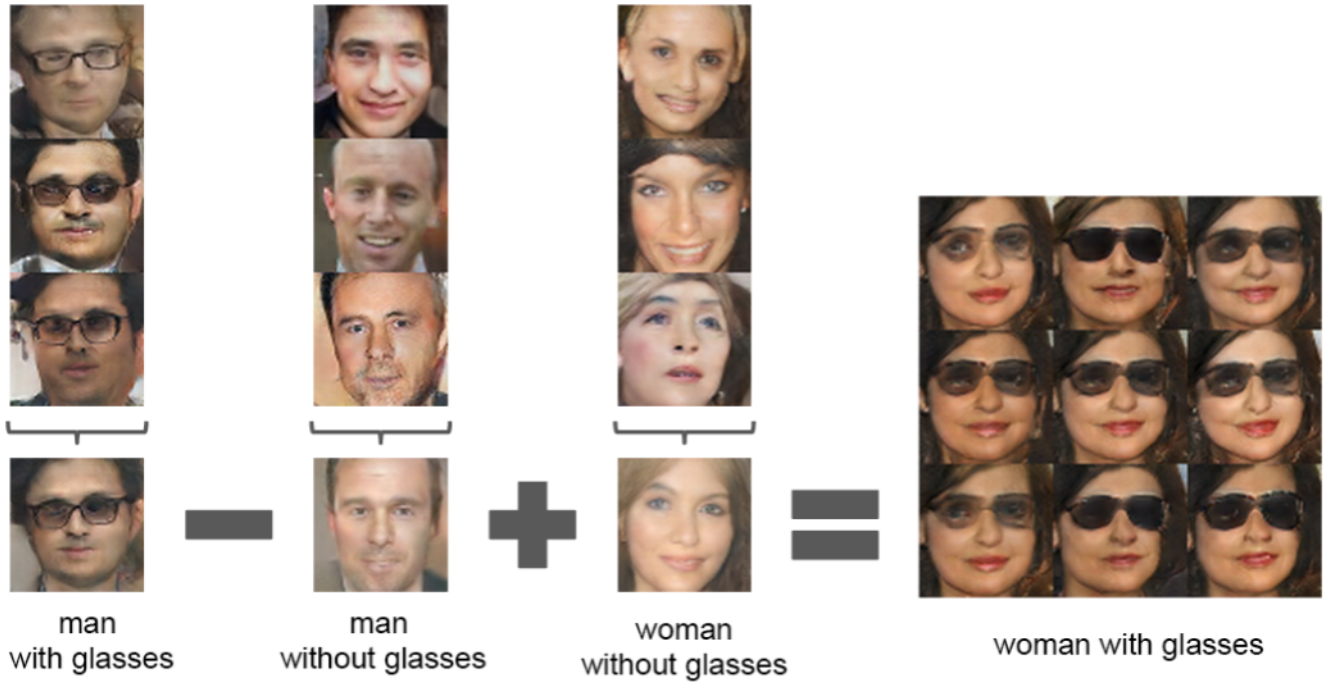
METHODISCH

Potenzial von Deep Learning, GANs



Jun-Yan Z. et al, Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks, arXiv, 2017.

Konzepte lernen mit GANs



StyleGan

https://thispersondoesnotexist.com/

Karras, Tero ; Laine, Samuli ; Aila, Timo: A Style-Based Generator Architecture for Generative Adversarial Networks. In: arXiv:1812.04948 [cs, stat] (2018).

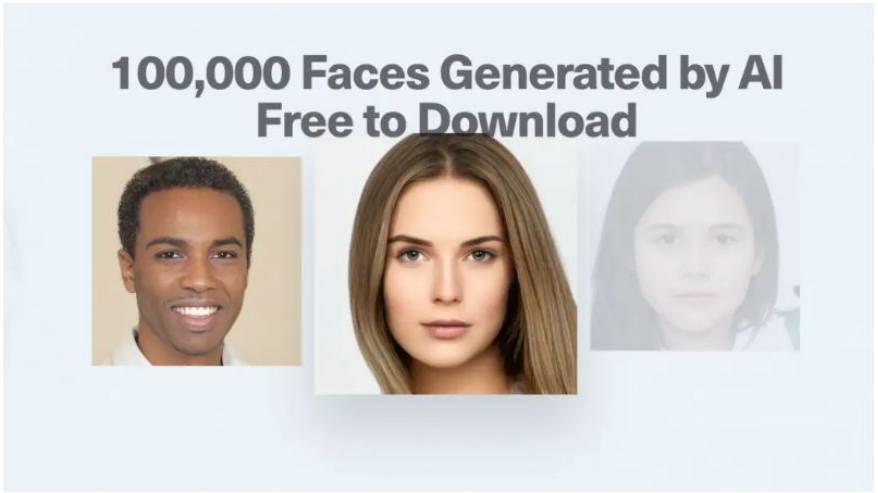
Wo ist der Fehler?

Business Case: Stockfotos

heise online

Stockfoto-Firma veröffentlicht 100.000 KI-Gesichter

24.09.2019 13:48 Uhr
Daniel Berger



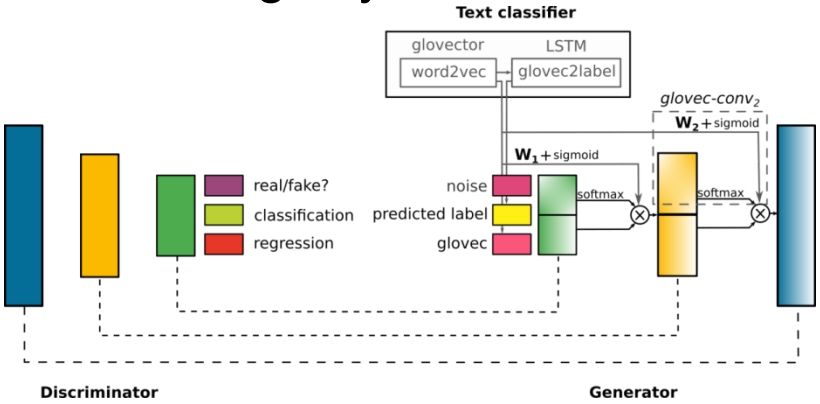
Diese Menschen sind nicht echt: Eine Firma veröffentlicht 100.000 Stockfotos mit Gesichtern, die es gar nicht gibt. Viele der Porträts sind verblüffend gut.

- https://www.heise.de/newsticker/meldung/Stockfoto-Firma-veroeffentlicht-100-000-KI-Gesichter-4537889.html

scch software competence center hagenberg

FashionGen Challenge

Text-to-image synthesis:



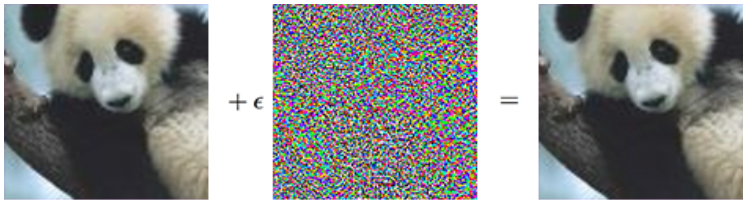
Example:

Long sleeve 'super 120's' wool twi blazer in navy. Notched lapel collar. Three-button closure at front. Welt and flap pockets at body. Padded shoulders. Four-button surgeon's cuffs. Signature tricolor grosgrain pull-tab at back yoke. Double vent at back hem. Pockets at fully lined

- Ontology Generative Adversarial Networks
- Realistic high-resolution images from a text describing the characteristic of the target image.

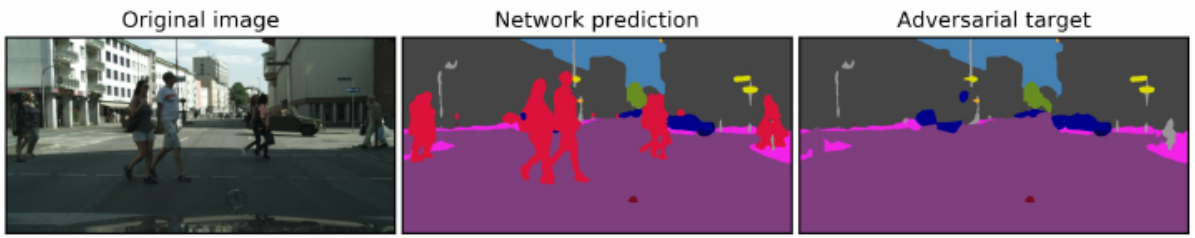
Eghbal-zadeh et al., On Conditioning GANs to Hierarchical Ontologies, DEXA: MLKgraphs2019, submitted.

Integrität und Stabilität



I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," arXiv:1412.6572, 2014.

Varianten



X. Yuan et al, “Adversarial Examples: Attacks and Defenses for Deep Learning,” arXiv:1712.07107v3, July 2018.

Perturbation	Attack Success	A Subset of Sampled Frames $k = 10$
Subtle poster	100%	
Camouflage abstract art	84.8%	

Eykholt et al,
Robust Physical-World Attacks on Deep Learning Visual Classification, CVPR 2018.

Überlisten eines Fingerpint Scanners

real

generiert

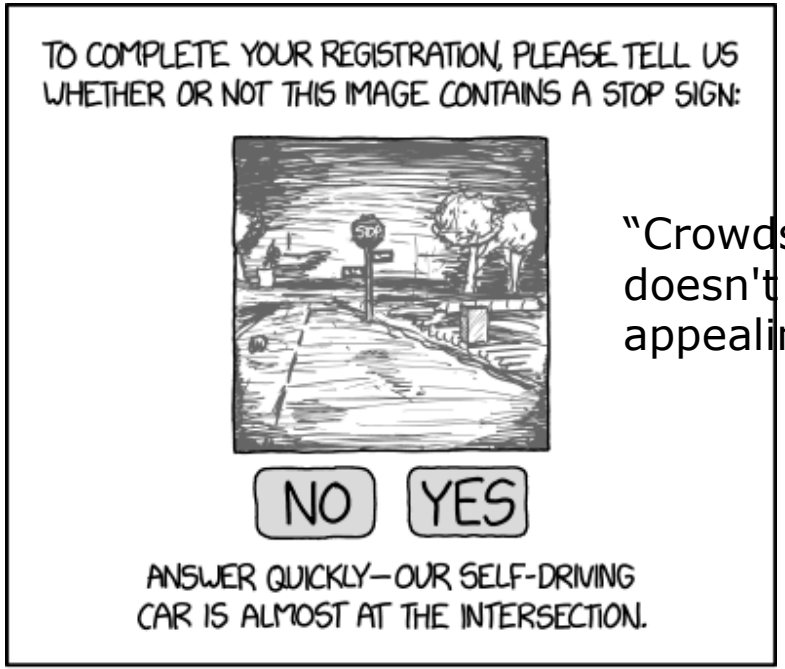
P. Bontrager et al, DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution, arXiv Oct. 2018.

Fake Fingerprint

	Capacitive DeepMasterPrint Matches		
	0.01% FMR	0.1% FMR	1% FMR
VeriFinger Training	6.94%	[illegible]	89.44%
VeriFinger Test	1.11%	22.50%	76.67%

P. Bontrager et al, arXiv Oct. 2018

Auswirkungen



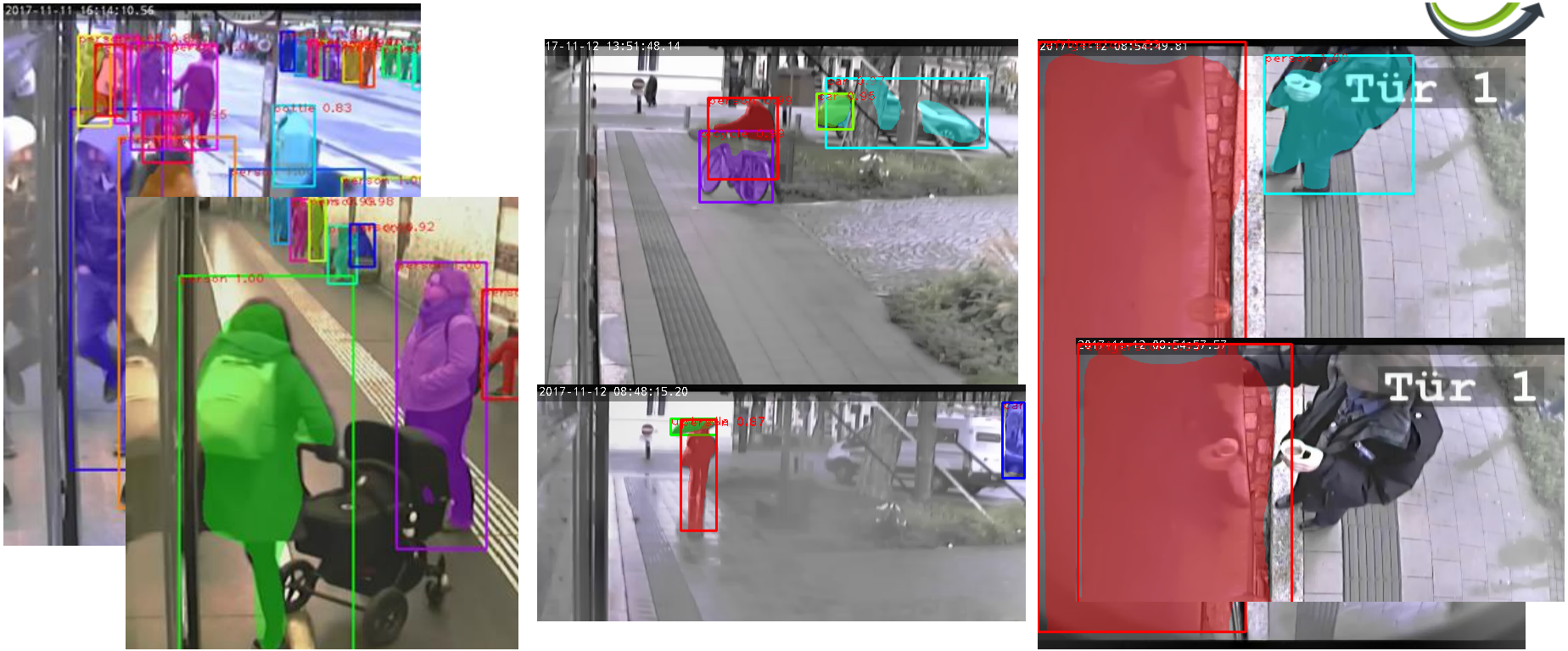
"Crowdsourced steering" doesn't sound quite as appealing as "self driving."

https://xkcd.com/1897/

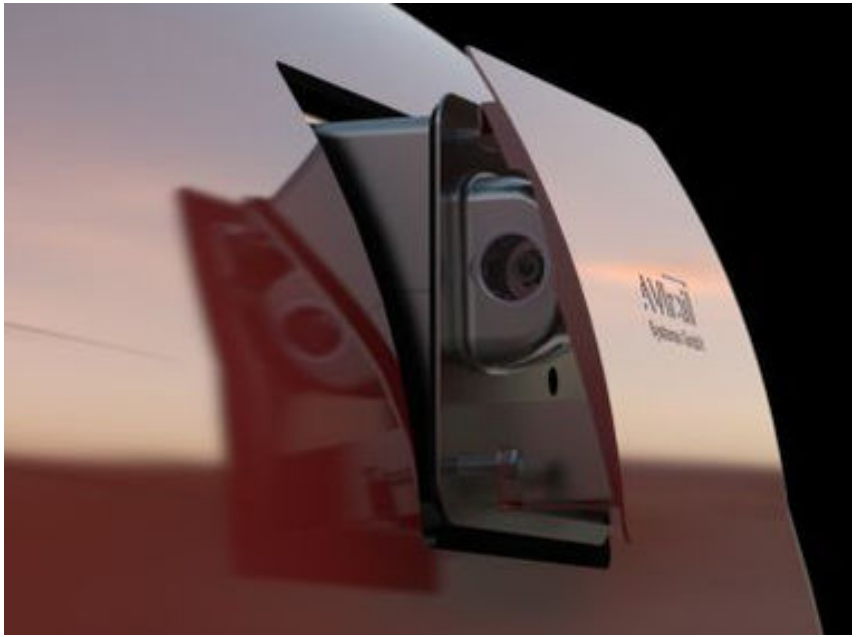
scch software competence center hagenberg

Szenen verstehen

Artificial Intelligence Rearview System

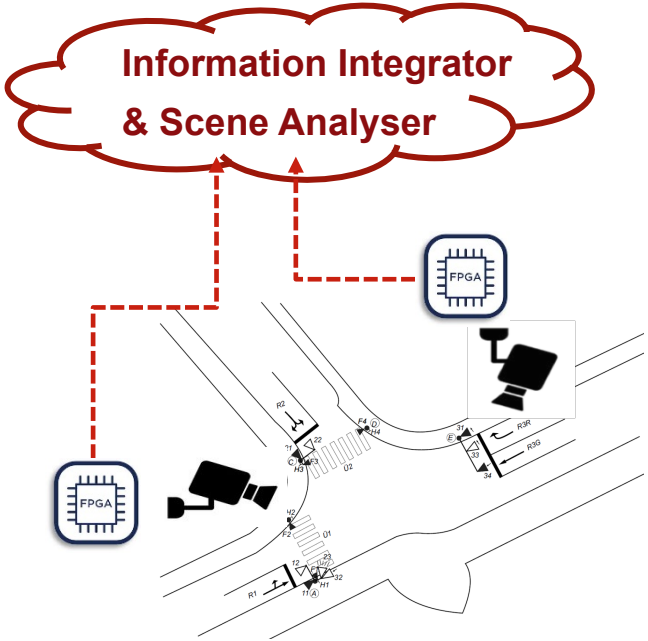


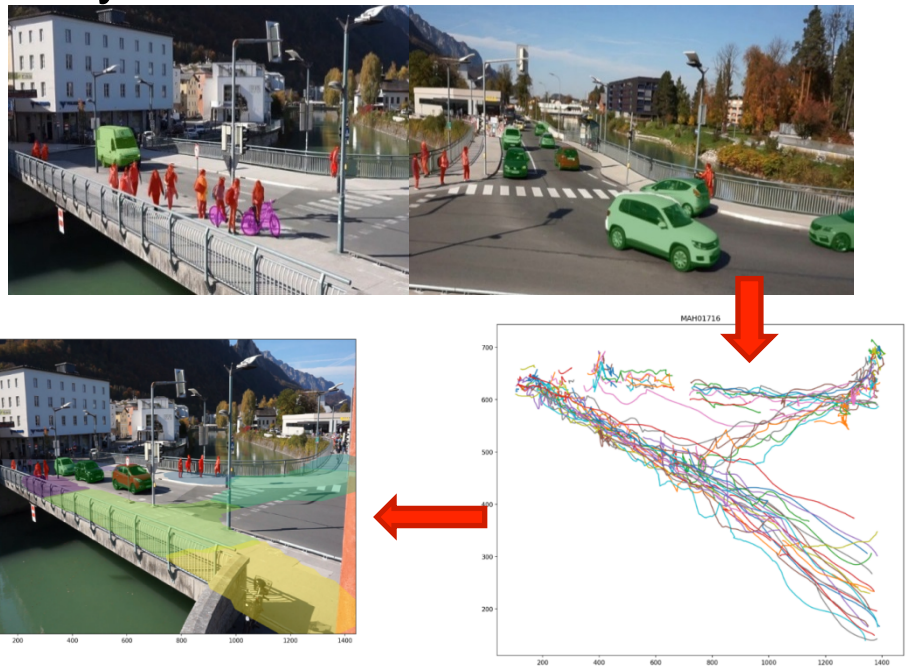
Echter Spiegel



Intelligent Infrastructure

- Traffic Flow Analysis / Traffic Safety





CONNECTING AUSTRIA

scch
software competence center
hagenberg

AI Projektbeispiele am SCCH

- COMET

Smart Factory: Prozessoptimierung durch lernen und optimieren der Produktqualität von Transformatoren.

SCCH SPS-Code-Analyse Software lizensiert durch das CERN (für ~1000 SPS)

SIEMENS

- (inter)national

Qualitätsanalyse für photovoltaische Systeme

Fronius

TRESS PASS

ALOHA

VISIOMICS

IoT4CPS Trustworthy IoT for CPS

Serums

COGNIPLANT

FLEX+

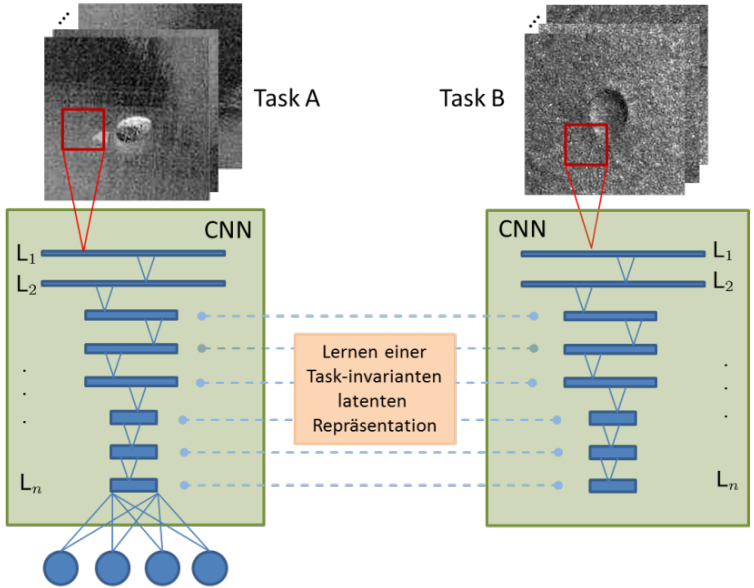
CONNECTING AUSTRIA

Funded by the Horizon 2020 Framework Programme of the European Union

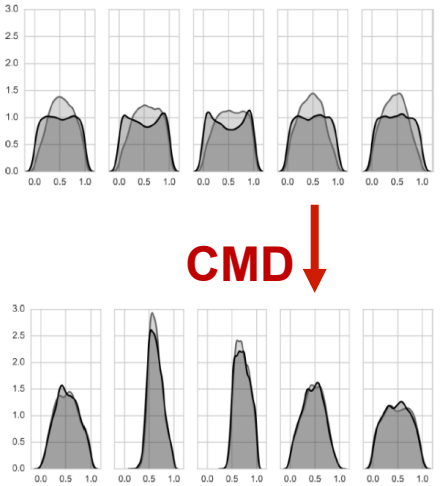
FFG

scch software competence center hagenberg

Deep transfer learning for Quality Inspection



Hidden layer activations:

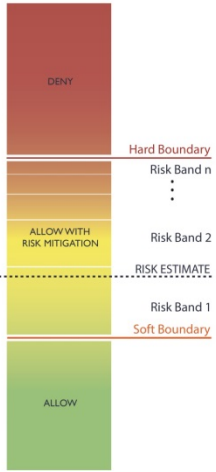


W. Zellinger et al., Central moment discrepancy for domain invariant representation learning, ICLR 2017.

Mehr Sicherheit durch DL

scch
software competence center
hagenberg

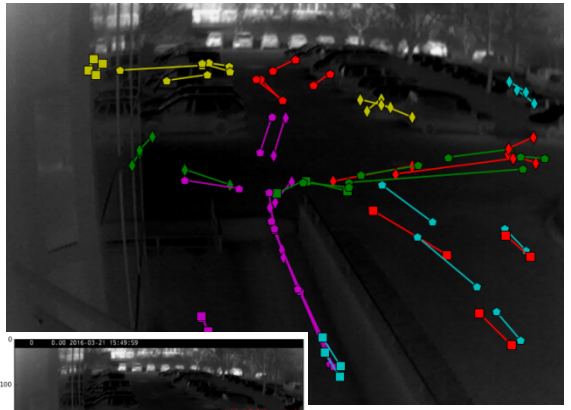
Border Control

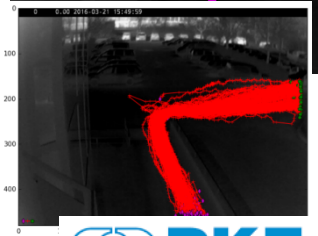


TRESS PASS

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION
HORIZON 2020

Filtern von Störsignalen





PKE

BM.I
BUNDESMINISTERIUM FÜR INNERES

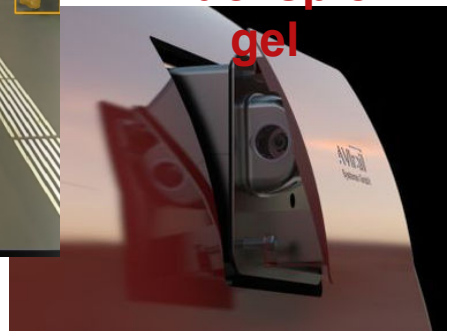
bmlvs.gv.at

KIRAS
Sicherheitsforschung

scch
software competence center
hagenberg

Mehr Sicherheit durch DL

Intelligenter Rückspiegel



AVI SYSTEMS

Intelligente Kreuzung

CONNECTING AUSTRIA

Aber…

- Mit KI Sicherheitschecks überlisten?
- KI Systeme überlisten?
- Tut das KI System das, was es soll?
- Schutz von vertraulichen Daten?

Daten, Variabilität, Robustheit

Projekte und Ausblick

scch
software competence center
hagenberg

ALOHA

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION
HORIZON 2020

SERUMS

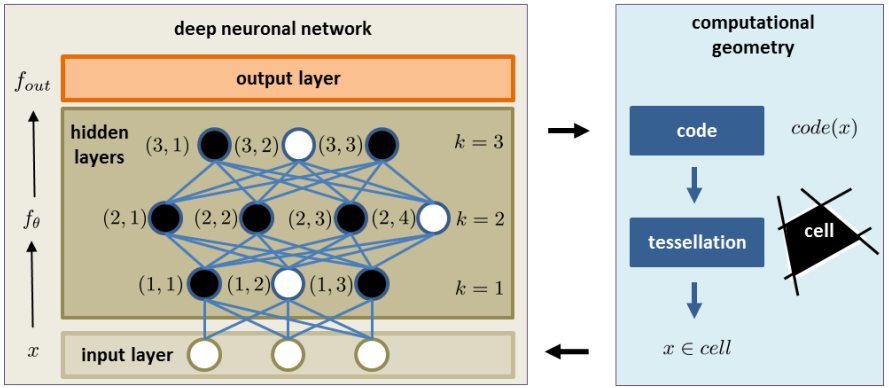
THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION
HORIZON 2020

IoT4CPS
Trustworthy IoT for CPS

Bundesministerium
Verkehr, Innovation
und Technologie

FFG

COMET Modul S3AI

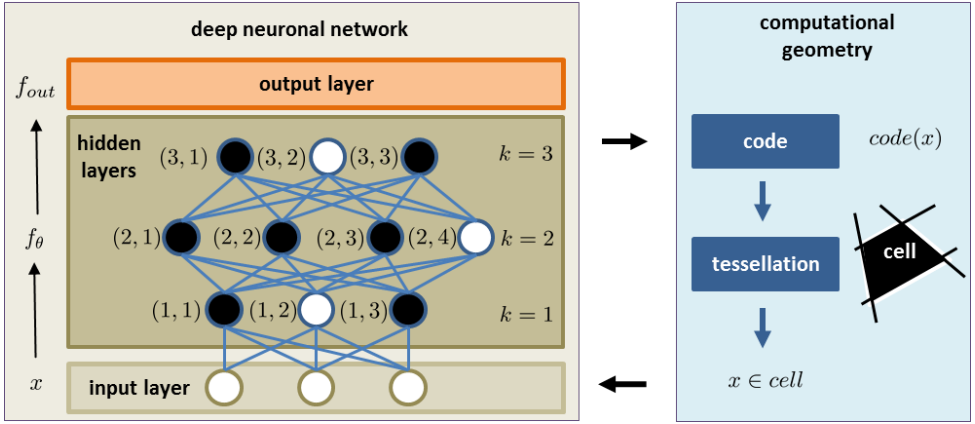


Grundlagen Projekt mit RICAM (Pereversyev), RISC (Schicho), IML (S. Hochreiter), KU Leuven (B.Preneel), Uni Cagliari (B. Biggio)

scch
software competence center
hagenberg

Ausblick 1

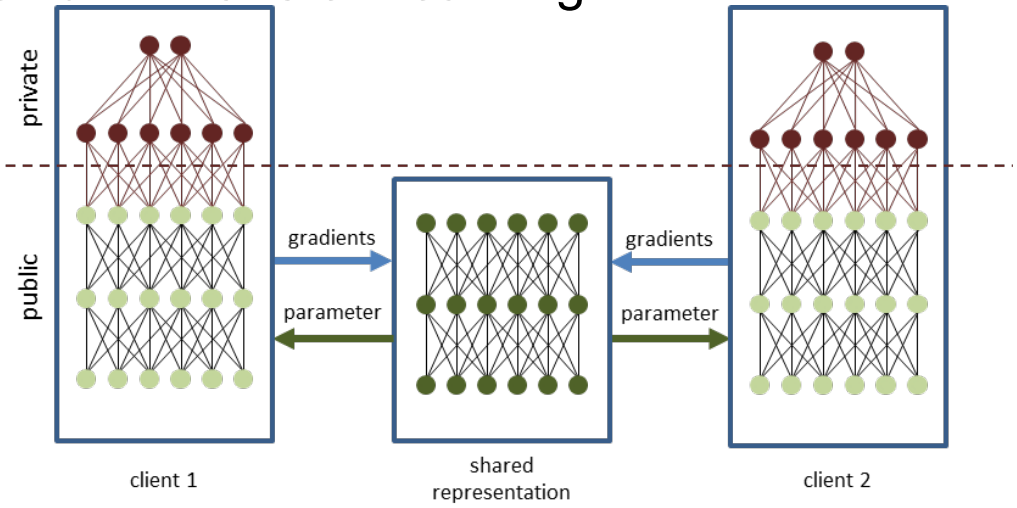
- Projekt: COMET Modul S3AI (Förder Entscheidung April'19)
- Ziel: Trustworthiness / Konfidenzmaß / Verifikation
- Methodik: neuer mathematischer Zugang (computational geometry)



- Grundlagenprojekt mit 7 PhDs mit
- RICAM (Pereversyev),
- RISC (Schicho),
- IML/JKU (S. Hochreiter), KU Leuven (B. Preneel),
- Uni Cagliari (B. Biggio);
- SCCH (Koord., B. Moser)

Ausblick 2

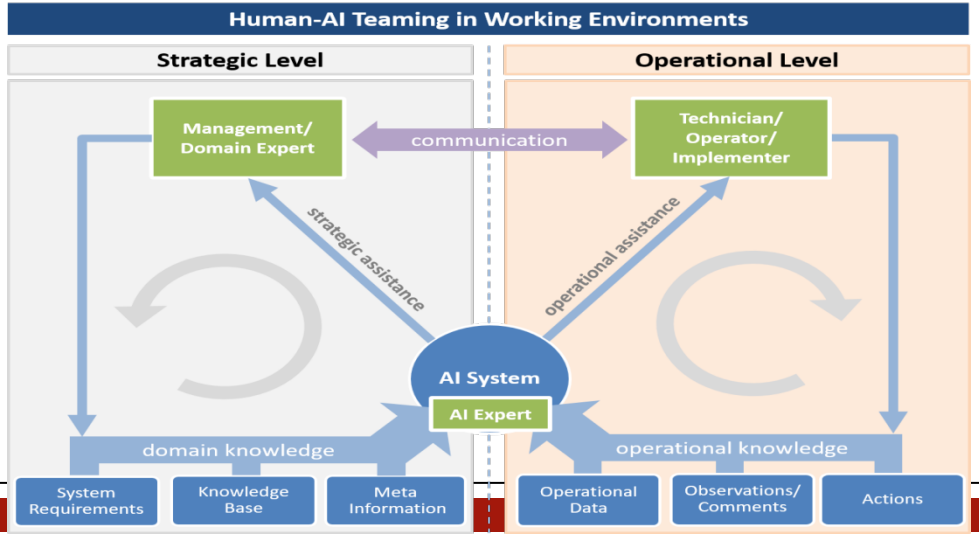
- Projekt: COMET Modul S3AI (April'19) + H2020 SERUMS (1.1.'19)
- Ziel: Trustworthiness / Privacy Preserving Collaborative Learning
- Methodik: neue Architektur + Transfer Learning



- basierend auf
  Deep Transfer Learning mittels
  Central Moment Discrepancy, ICLR 2017
  Information Sciences 2018

Ausblick 3

- Projekt: KI Leitprojekt / FFG (submission März'19)
- Ziel: Human-AI Teaming in der Arbeitswelt
- Methodik: Trustworthiness + Knowledge Graph + Weakly Supervised



mit

- Inst. für Arbeitsforschung IAA/JKU,
- Profactor,
- WU Wien
- apollo.ai,
- SCCH (Koord.)

From the Vault

- *„The Thinking Machine“ (1961) - MIT Centennial Film*.
  - Screen actor David Wayne chats with MIT Professor Jerome Wiesner on developments in computer research and artificial intelligence, as part of the Tomorrow television series produced by CBS for MIT on occasion of MIT’s Centennial in 1961.

Blick von 1961 in die Zukunft

Wenn wir nicht mehr weiterwissen…

Unplugged...