Machine Learning für Datenanonymisierung von Bildern und Videos

AGEO Forum 2024 - GeoKI

Celantur

Boyang Xia | CTO

Datenschutz: Megatrend und Herausfoderungen

Regulierungen und öffentliches Bewusstsein fordern **Datenschutz-orientierte Produkten und Dienstleistungen**.

Massiv wachsende Datenmengen, u.a. photogrammetrische Daten im Mobile Mapping Bereich.

Bestehende Produkte und Dienstleistungen bedenken Datenschutz nicht.

Art. 5 (1) c DSGVO: Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Minimize Data Breach Damages

“[...] ***The principles of data protection should therefore not apply to anonymous information.***” (Recital 26, GDPR)

Minimize notifiable breaches

Since they’re not personal data, breaches of anonymized data might mitigate any notification obligation to the data protection authority. Hence, reducing legal costs (notifications, fines, etc).

Protect your organization

Showing the strongest data privacy measurements (e.g. anonymization) could impact how regulators will take a view at your company in case of a data breach.

Build trust with customers

Attention to data privacy are well-perceived by customers. On contrary, data breaches cause PR backlashes and reputation damages (e.g. Marriott, T-Mobile).

Data Privacy to earn Citizens' Approval

86% of citizens are aware of their privacy rights, and 79% willing to spend time and money to protect data*

Smart Cities drives efficiency and cost-saving, which ultimately might convert into tax-cutting and … **better approval of your government**.

To overcome citizens' over data exploitation, **data transparency and privacy** are great instruments to obtain public approval.

Example: [Wien gibt Raum] (Vienna)

* https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf

Image and Video Anonymization

What can be anonymized?

- Faces
- Persons
- License Plates
- Vehicles
- Others under request

Faces
Round with fading at the edges

License Plates
Bounding box

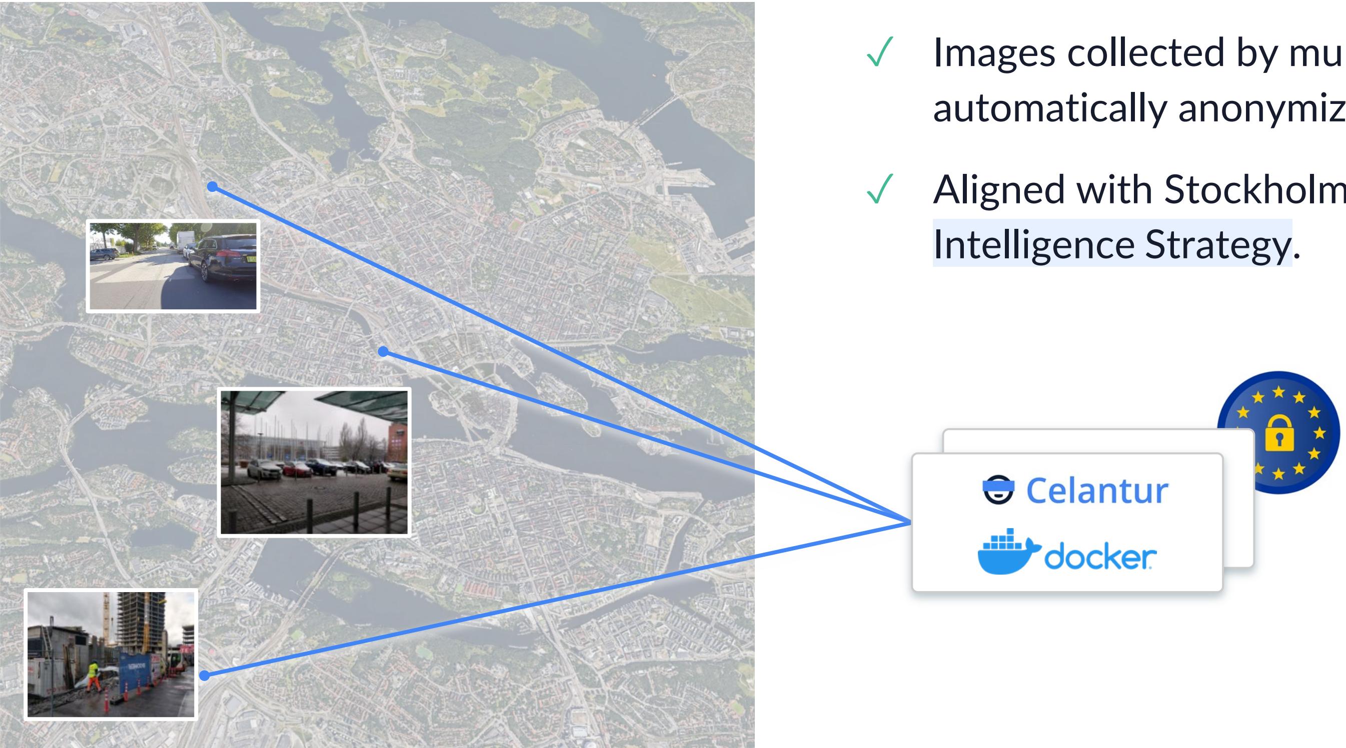
Persons
Segmentation along object outline

Vehicles
Segmentation along object outline

Warum relevant für GI?

Anonymization powered by Celantur. Vehicle far away, persons inside a car.

Celantur powers Stockholm's Centralized Image Blurring Service

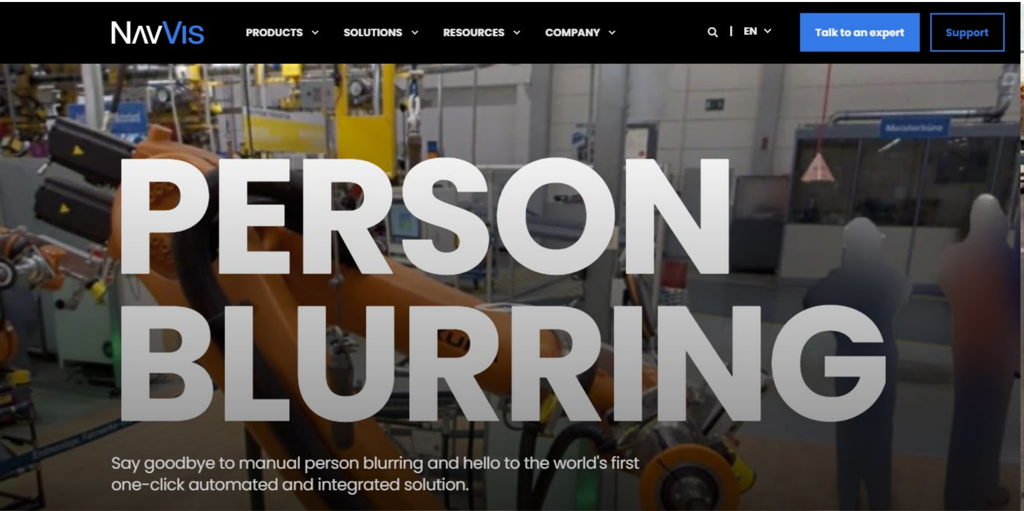


- ✓ Images collected by municipal workers are automatically anonymized.
- ✓ Aligned with Stockholm's Artificial Intelligence Strategy.

Success Story: NavVis

NavVis launched automated image blurring for all NavVis IVION users by integrating Celantur Container into their AWS cloud infrastructure.

- ✓ Notable cost and time savings for larger projects and datasets compared to manual or external workflows.
- ✓ Up to 50% time was saved by using this fully integrated and automated solution.
- ✓ Significant speed improvement in the processing workflows (up to 50-60%).



Success Story: Horus

Horus is streamlining blurring and GDPR compliance for Mobile Mapping applications with Celantur technology

- ✓ Celantur Container has been integrated into Horus' *HORISON automated blurring* software solution.
- ✓ Import and transform imagery in different formats (*.JPEG, *,PGR and *.HRS) to be anonymized.
- ✓ Automatically blur faces, bodies, and license plates on panoramas & planar imagery.

Is 100% anonymization required?

"[…] the outcome of anonymisation as a technique applied to personal data should be, ***in the current state of technology***, […]"

EU (GDPR) Article 29 Working Party, 0829/14/EN WP216
Opinion 05/2014 on Data Anonymisation Techniques
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

❌ **Not even Google achieves 100%:**

Celantur software uses state of the art technology

- ✓ Deep convolutional neural networks (CNN)
- ✓ Instance segmentation (Mask R-CNN with a FPN backbone)
- ✓ Keypoint detection (based on Faster R-CNN)
- ✓ Advanced Computer Vision algorithms
- ✓ Stateless design & no long-time persistence of data (Celantur Container)
- ✓ **Certification for your use-case under request**

TÜV AUSTRIA

scch { } software competence center hagenberg

Benchmarking

Measuring the right machine learning metrics for anonymization.

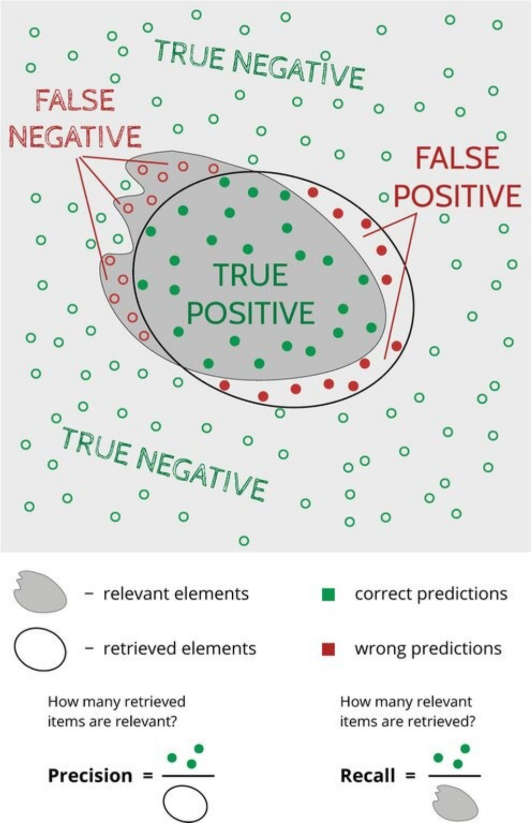
0.95

Recall

of identifiable objects

Explanation: The ratio of correctly predicted positive observations to the total actual positives.

Interpretation: It indicates the **model's ability to capture all positive instances.**



https://en.wikipedia.org/wiki/File:Precision_and_recall.pdf

Wahrheitsmatrix (Konfusionsmatrix)

		Vorhersage / Beobachtung	
		Positiv	**Negativ**
Ground Truth (“Wahrheit”)	**Positiv**	😀 True positive (TP)	😡 False negative (FN)
	Negativ	😡 False positive (FP)	😀 True negative (TN)

Relevanz (Precision) und Sensitivität (Recall)

$\frac{TP}{TP + FP}$ - Relevanz (Precision): Minimiere False Positives. False Negatives (Falsche Auslassungen) irrelevant.

$\frac{TP}{TP + FN}$ - Sensitivität (Recall): Minimiere False Negatives. False Positives (Falsche Erkennungen) irrelevant.

More information: https://www.celantur.com/blog/understanding-specificity-sensitivity/

Beispiel für Sensitivität (Recall): Automatisiertes Fahren

Passanten an einer Kreuzung		Vorhersage / Beobachtung	
		Passant:in erkannt	**Keine Passant:in erkannt**
Ground Truth (“Wahrheit”)	**Passant:in**	🛑 Passant:in korrekt erkannt	💀Passant:in übersehen!
	Keine Passant:in	🛑 Fälschlich Passant:in erkannt	🚗 Keine Passant:in entdeckt

Ziel: Minimiere False Negatives → Maximiere Sensitivität.
Wenn die Konsequenzen von Übersehen schwerwiegender sind als von Falsch-Erkennen.

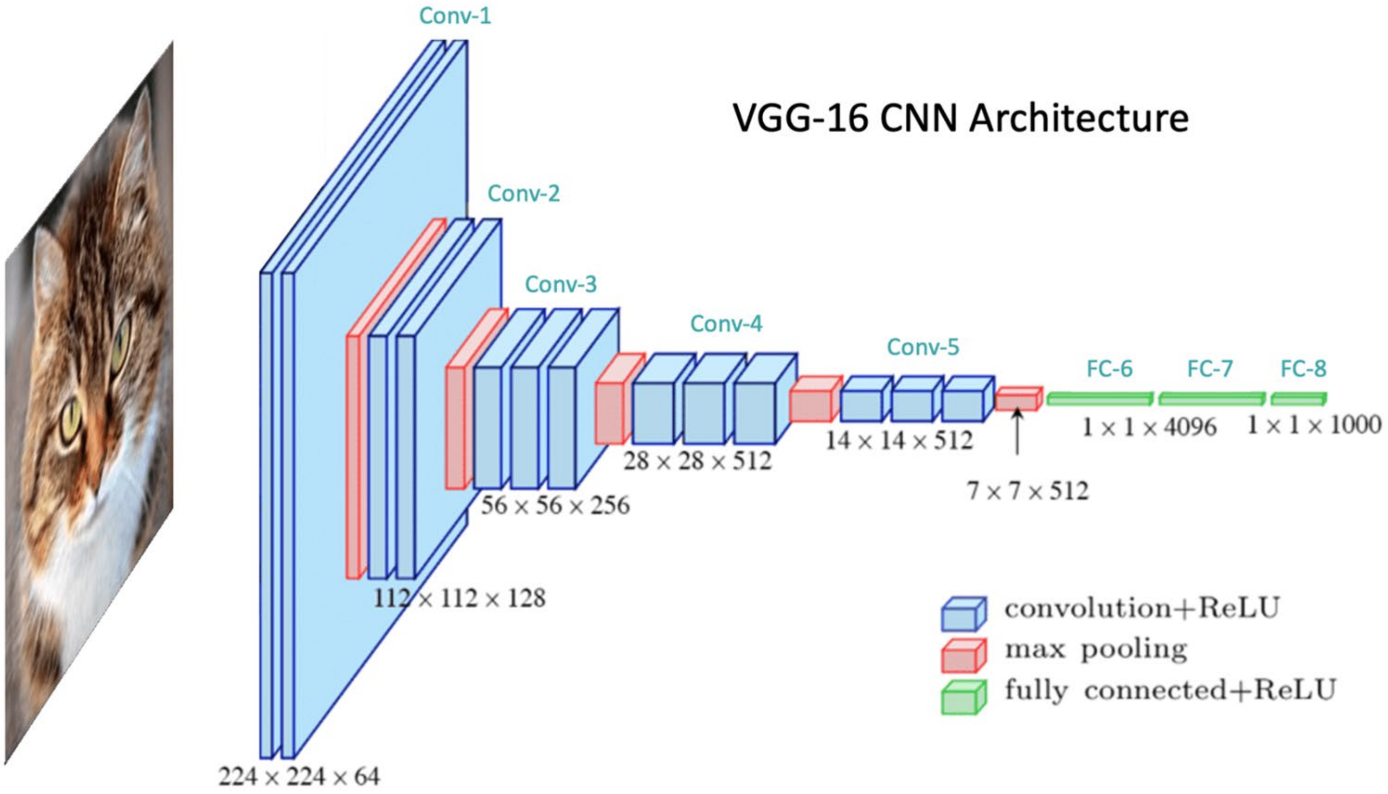
Beispiel für Relevanz (Precision): Strafgerichtsbarkeit

Verurteilungen		Vorhersage / Beobachtung	
		Als schuldig befunden	Als unschuldig befunden
Ground Truth ("Wahrheit")	Schuldig	⚖️ Korrekte Schuldspruch	😈 Fälschlich freigesprochen
	Unschuldig	😭 Fälschlich verurteilt	⚖️ Korrekte Freisprechung

Ziel: Minimiere False Positives → Maximiere Relevanz.
Wenn die Konsequenzen von Falsch-Erkennen schwerwiegender sind als von Übersehen.

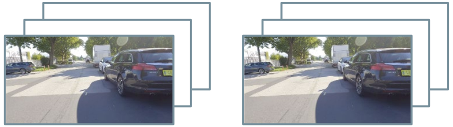
Wie funktioniert es?

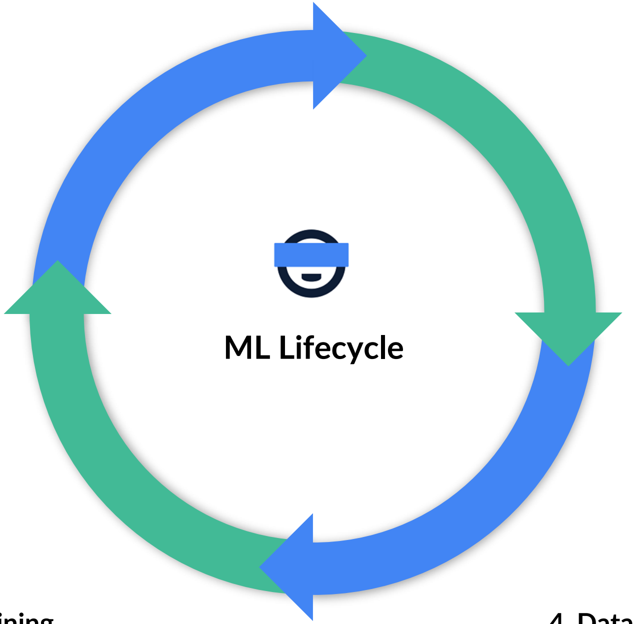
Convolutional Neural Networks



Celantur Model Training

Iterative process to improve ML models.





1. Data Collection

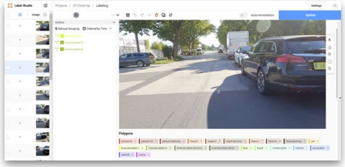
Collected by **ourselves** or attained from **customers**

2. Data Review

Remove **low value** data

3. Data Annotation

Create **segmentation masks** for required objects



4. Data Preparation

Bring data into **right shape**

5. Model Training

Re-train models with **new data**

6. Model Evaluation

Test new model on **reference data**

7. Data Validation

Ensure data quality

Herausforderungen

- Heterogene Daten: verschiedene Auflösungen, FoV, FPS, Dateiformate
- MLOps: Bildannotation und Preprocessing automatisieren.
- Bildverarbeitung: Kompression, Metadaten, nicht nur RGB…
- Skalierung: Wie erreicht man den notwendigen Durchsatz?
- Hardware: Edge Computing

Herausforderung: Durchsatz

Large-scale automotive data collection	
Cars	10
Video h/car	40,000
Total video duration [h]	**400,000**
Total video duration [days]	16,667
Avg. video h file size [GB]	1.3
Total data volume [TB]	**520**
Total data volume [PB]	0.5
Cloud upload bandwidth [MBits/s]	150
Cloud upload time [h]	**27,733,333**.33
Cloud upload parallelization factor	10000
Cloud upload time parallelized [h]	**2,773**.33

Herausforderung: Edge Computing

Celantur