



About Jonghu Jeong (정종후)

- Sr. Machine Learning Engineer
in Research Team @ Deeping Source Inc.
 - A Korea startup that specializes in privacy-safe, AI-based video analytics
- Work Experience @ Deeping Source Inc.
 - Sr. Machine Learning Engineer *Jul 2023 – Current*
 - Machine Learning Engineer *Sep 2019 – Jul 2023*
 - Software Engineer *Dec 2018 – Sep 2019*
 - Intern *Jul 2018 – Dec 2018*
- Education
 - B.S. in CSE @ Seoul National University (Aug 2022)

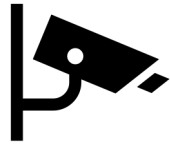
About Jonghu

- Enjoys solving real-world problems with colleagues across various domains
- Consistently focuses on the impact and efficiency of work
- Prefers trying the simplest solution first
- Eager to solve teammates' pain points that can impact team productivity
- Contributes to company culture by leading several clubs,
 - E.g. Hiking, Study, Workout, and MMA!

Jonghu has been working in...

**Computer Vision-Based Video Analytics
&
Privacy Preserving Machine Learning**

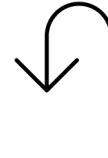
Overview: Computer Vision-Based Video Analytics



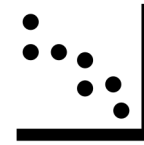
Input Video



Object Detection



Pedestrian Tracking

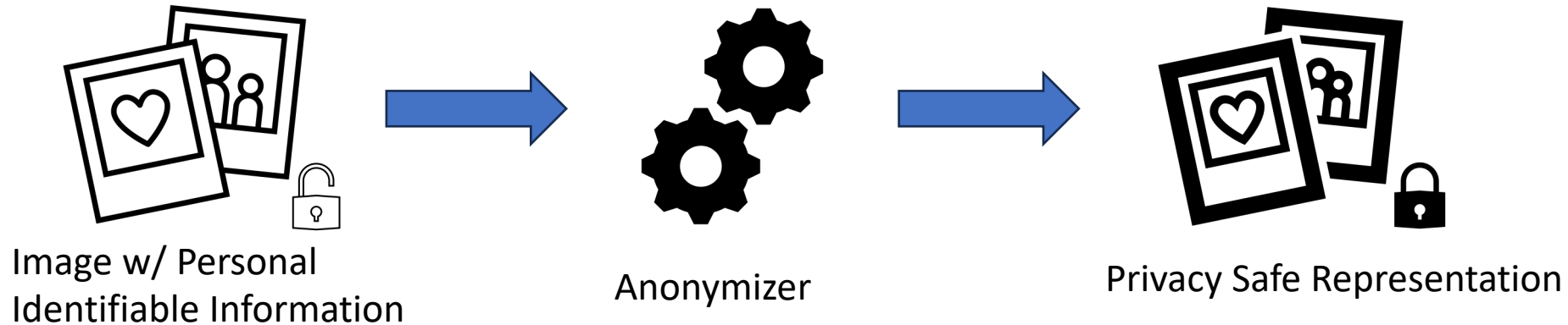


Analysis

[Contributions]

- **New Algorithms**
- **Training and Inference Optimizations**
- **Evaluation System**

Overview: Privacy Preserving Machine Learning



[Contributions]

- **New Anonymization Algorithms**
 - 1 main product, 4 patents, 2 papers
- **Implement Fast and Accurate Anonymizer**
 - From model training to inference optimization

Video Analytics: Object Detection

[Contributions]

- **Data Loader Optimization $\Rightarrow$ 2x faster training!**
 - Reduced inefficient image resize, mem copy, etc for GPU utilization
- **PoC on Synthetic Image Boosted Training $\Rightarrow$ 0.5~2.6%p mAP gain!**
 - Generate synthetic person images (12k) with a diffusion model
 - Use generated images for pedestrian detection training

Video Analytics: Object Detection

[Contributions]

- **Video Object Detector Training $\Rightarrow$ 1%p mAP gain!**
 - An object detector utilizes temporal information and is trained without video object detection datasets
 - US Patented
- **Accuracy Enhancement and Speed Optimizations**
 - Augmentations, pseudo labeling, ...
 - Pre/post processing such as fast image pyramid, numba nms ...

Video Analytics: Pedestrian Tracking

[Contributions]

- **Static Camera Assumption**

- Add heuristics that are not covered with off-the-shelf trackers, i.e. DeepSORT, ByteTrack
- Uncertainty modeling that is aware of unstable input stream
- Implemented python wrapper on NVIDIA DeepStream framework for researchers

- **Evaluation System using ClearML**

- For finding performance boundary of the current product
- Defined new evaluation data and protocols to cover the product's requirement

Video Analytics: Pedestrian Analysis

[Contributions]

- **Reliable Prediction System**

- Model calibration and definition of confidence score
- Explore key conditions and produce reliable predictions
 - e.g. domain gap, consistency of track-wise prediction, image quality, etc

- **2nd place @ UPAR Challenge (WACV 2024 workshop)**

- Predicting 12 categories of person appearance, including age, gender, etc.

- **Synthetic Image Training $\Rightarrow$ 0.5%p accuracy gain**

- A project with an intern
- Generate images of diverse gender and age with a diffusion model and train a model

Video Analytics: Etc

[Contributions]

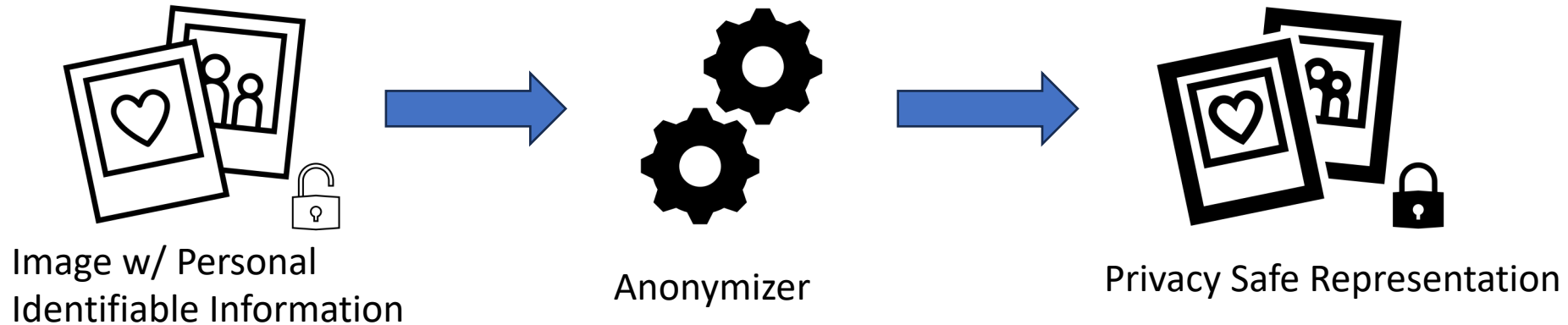
- **Crowd Counting**

- For citizen safety in crowded areas within local government applications

- **And other vision tasks for fast PoCs (shallow experiences)**

- Pose Estimation, Facial Landmark Detection, Depth Estimation ...

Overview: Privacy Preserving Machine Learning



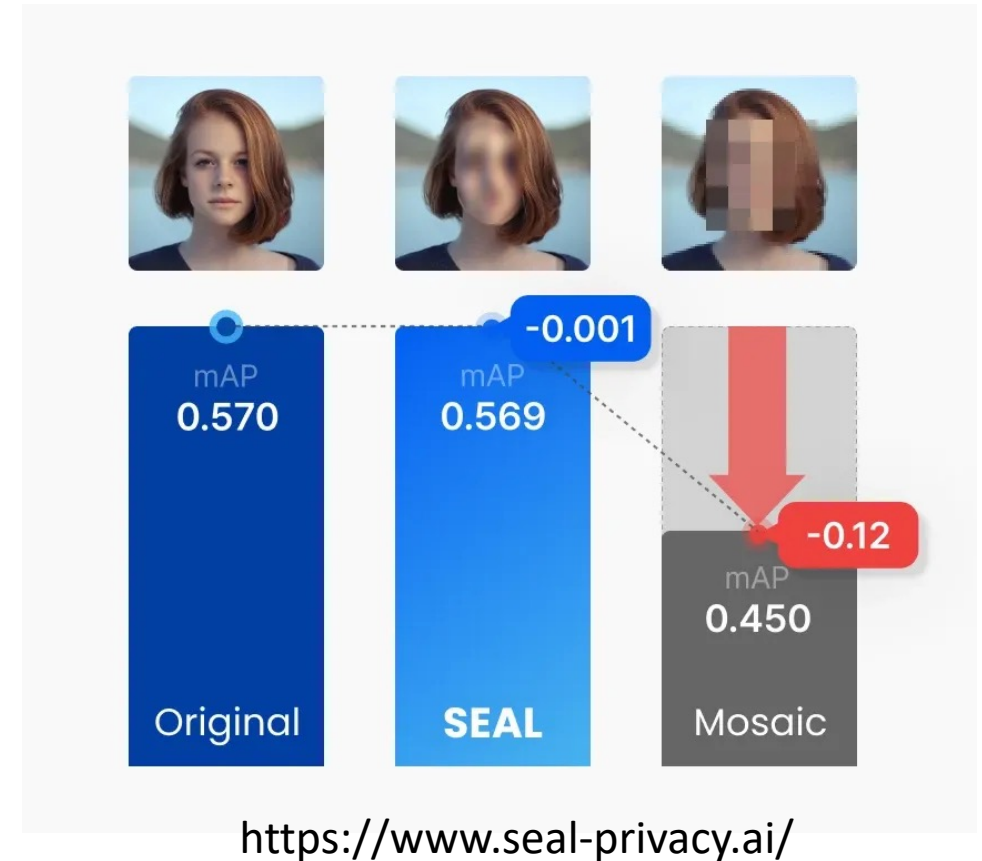
[Contributions]

- **New Anonymization Algorithms**
 - 1 main product, 4 patents, 2 papers
- **Implement Fast and Accurate Anonymizer**
 - From model training to inference optimization

SEAL: Privacy Preserving Visual Data Anonymization

[Key Features]

- Removes Personal Identifiable Information (PII)
 - such as faces, car plates.
- Even after removing PII, the data can still be utilized for AI training/inference.
 - Ex) Training a pedestrian detector with SEALED images results in negligible performance degradation.



SEAL: Privacy Preserving Visual Data Anonymization

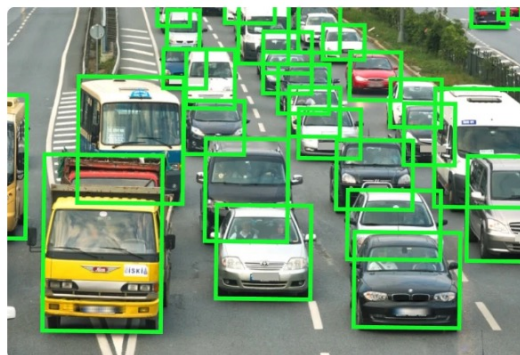
Proven with Mainstream Vision Tasks

<https://www.seal-privacy.ai/>

SEAL is suitable for a wide range of AI vision applications, emphasizing AI utility while ensuring the removal of personal information. SEAL balances rigorous privacy standards with enhanced performance across diverse vision tasks.



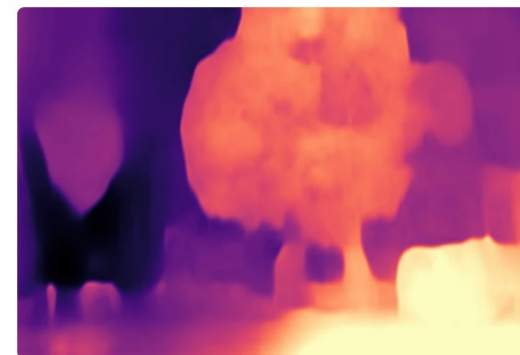
Action Recognition



Car Detection



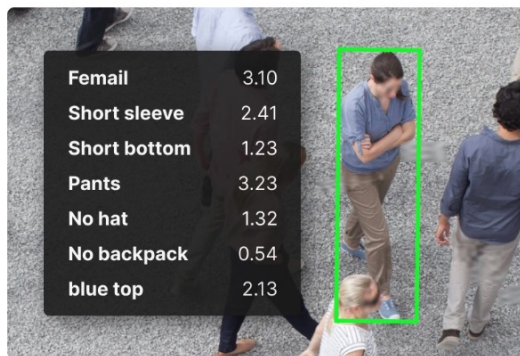
Semantic Segmentation



Depth Estimation



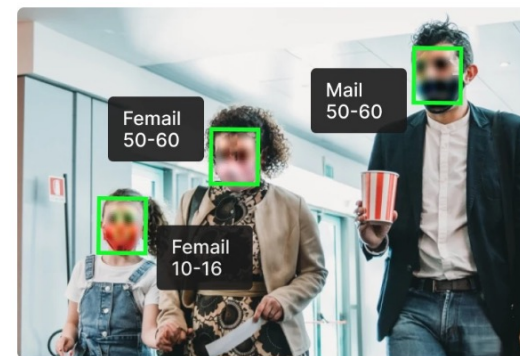
Face Landmark Detection



Person Attribute



Pose Estimation



Gender/Young Classification

SEAL: Privacy Preserving Visual Data Anonymization

PII Detection

- **Various Targets**
 - Face, body, car plates, etc
 - Finegrained shape
- **Recall 100% Targeted**
 - Training strategies
 - Image Pyramid
- **High Speed**
 - Combining multiple models
 - Device specific strategies
 - Pre/Post-processing optimization

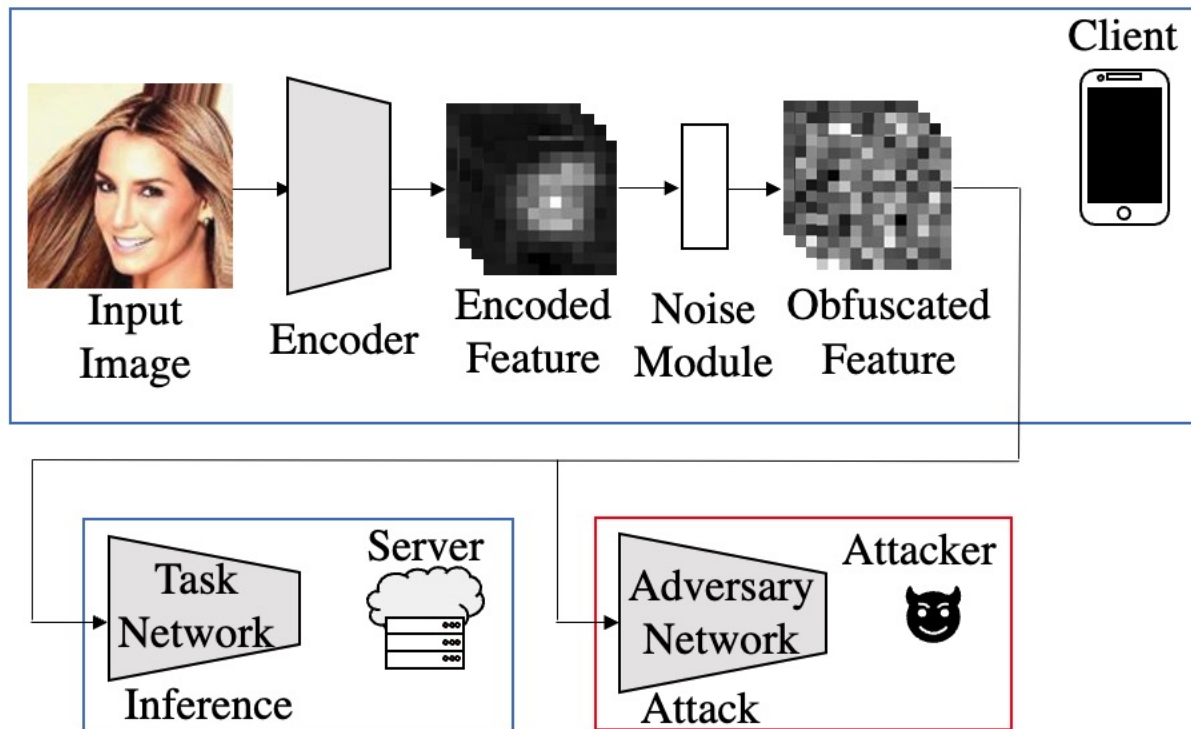
PII Removal

- **Privacy Safe:** should not be recovered
- **Trainability:** processed images should be trainable
- **PII specific strategies**
 - ex) face vs carplate
- **High Speed**
 - Device specific
 - ex) GPU availability
 - Multi threading
- **US Patented**

Trainability

- **PoC on Various Tasks**
 - Depth estimation, pose estimation, ...
- **Comparison** between SEAL vs Simple blur/mosaic
- **Successfully passed verification from customers** in the autonomous driving domain.

Noisy adversarial representation learning for effective and efficient image obfuscation (UAI 2023)



Authors: Jeong, J.*, Cho, M.*, Benz, P., & Kim, T. H

[Motivation]

- **User** doesn't want to reveal **raw data**.
- **Server** wants data for ML service.

⇒ User needs **anonymizer** on their **edge device**!

[Method]

⇒ **Joint training** of **task/adversary networks** with **noisy features**.

Noisy adversarial representation learning for effective and efficient image obfuscation (UAI 2023)

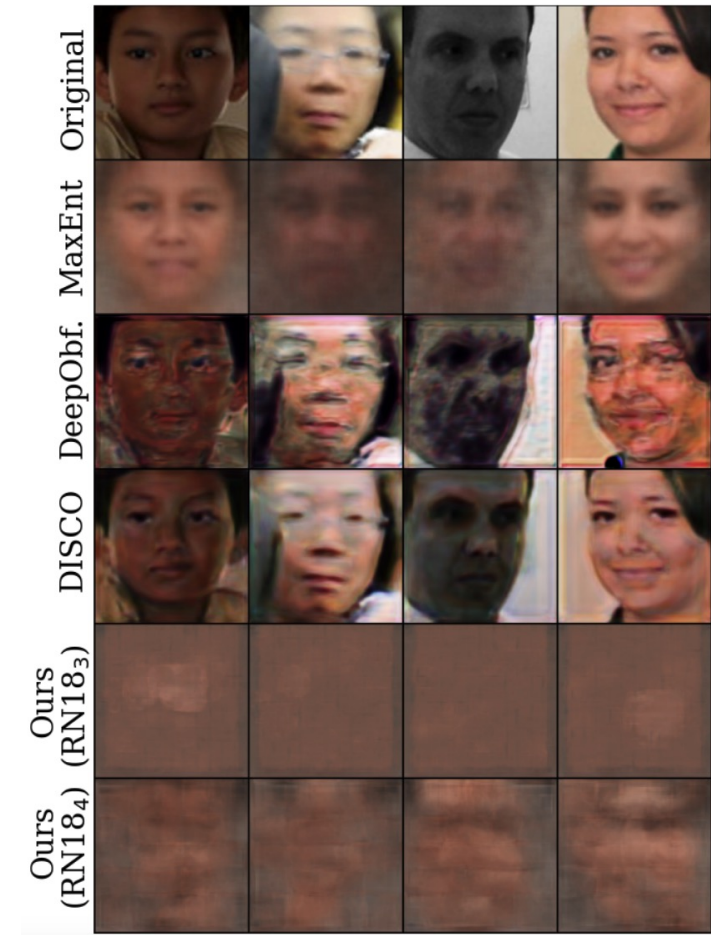
[Evaluation]

1. Performance for target tasks: higher the better.
2. Performance for adversary tasks: lower the better.
3. Robustness to reconstruction attack
4. Less parameters from the client-side

[Results]

- SoTA Privacy-Utility Tradeoff & Reconstruction Attack Defense.
- Less computation and smaller memory footage compared to the existing methods.

[US Patented]



Authors: Jeong, J.*, Cho, M.*, Benz, P., & Kim, T. H

Privacy Safe Representation Learning via Frequency Filtering Encoder (AISafety @ IJCAI-ECAI 2022)

[Motivation]

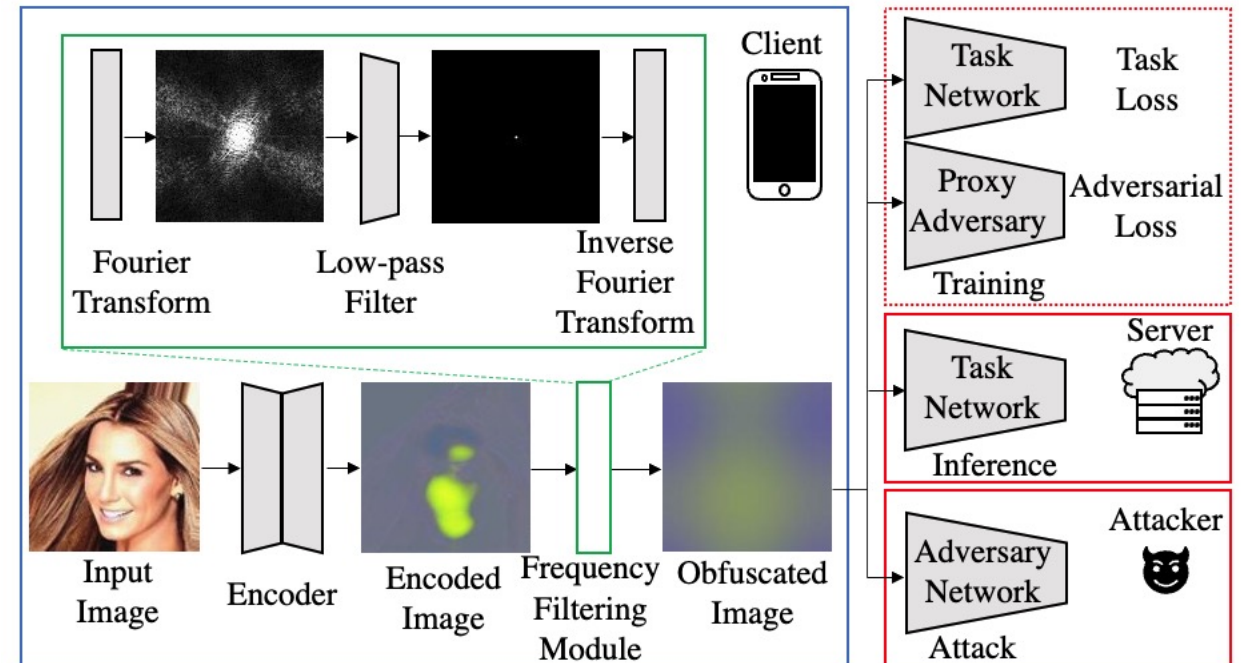
- Same as NoisyARL
- Encoder transforms **from image to image.**

⇒ **Easy Visualization!**

[Method]

⇒ **Joint training of task/adversary networks** with **spatial frequency filtered** features.

[US Patented]



Authors: Jeong, J., Cho, M., Benz, P., Hwang, J., Kim, J., Lee, S., & Kim, T. H

Thank you!