Authorize-on-Demand: Dynamic Authorization with Legality-Aware Intellectual Property Protection for VLMs

Lianyu Wang[1,2,3], Meng Wang[2,3], Huazhu Fu[4], Daoqiang Zhang[1]

[1]The Key Laboratory of Brain-Machine Intelligence Technology, Ministry of Education, China [2]Centre for Innovation and Precision Eye Health, Yong Loo Lin School of Medicine, NUS, Singapore
[3]Department of Ophthalmology, Yong Loo Lin School of Medicine, NUS, Singapore [4]Institute of High Performance Computing, Agency for Science, Technology and Research, Singapore

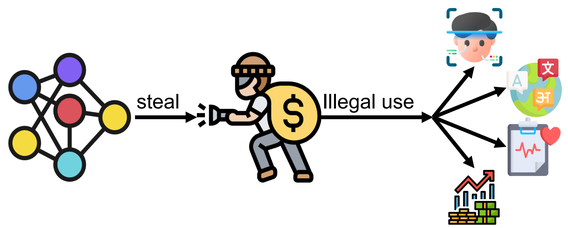
CVPR JUNE 3-7, 2026 DENVER COLORADO

Code: https://github.com/LyWang12/AoD-IP

MOTIVATION

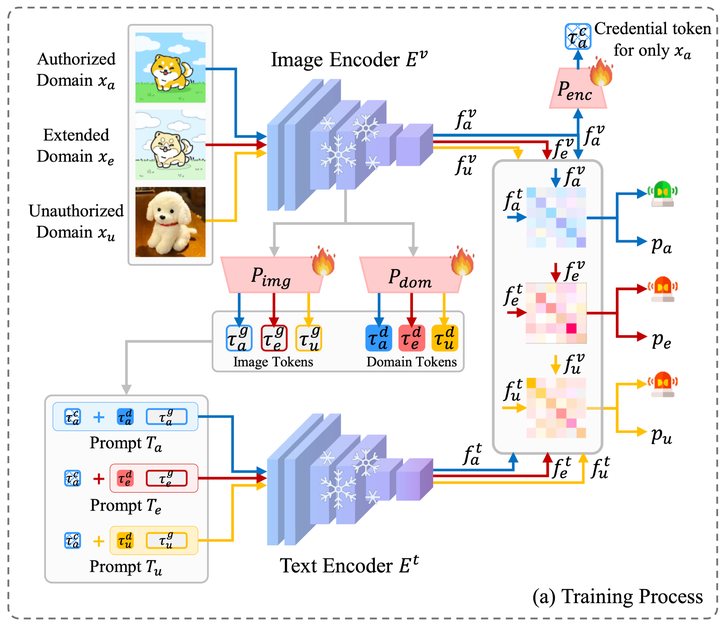
Has your model ever been stolen?

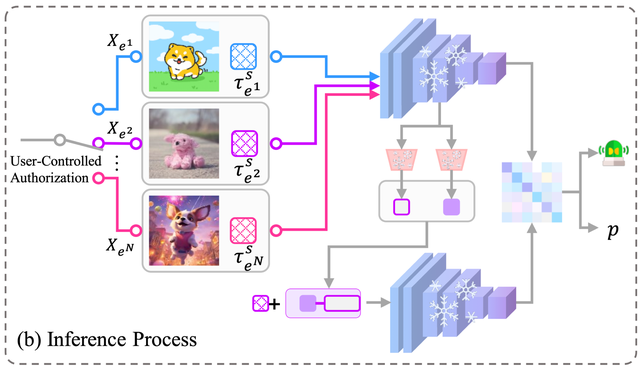
You spent $100K training your VLM. **Are you sure it's not running on your competitor's servers right now?**

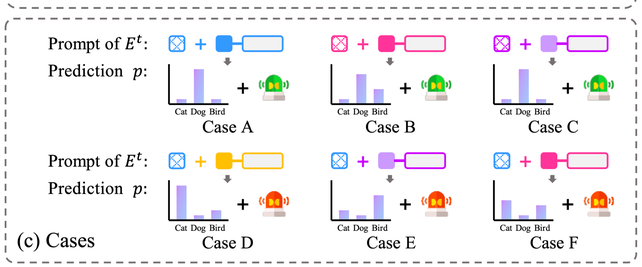


- **Model IP protection** safeguards your AI assets against **illegal deployment**.
- Yet, thieves now exploit your VLMs by **migrating** it to **unauthorized domains**.
- Current defenses block this, but they **fail upon any new domain** and **force a total retraining**.

METHODOLOGY







Architecture:

- **Learnable Projector:** Create image, domain and credential tokens.
- **Credential Token:** Lightweight token bound securely to authorized domain.
- **Extended Domain:** Simulate diverse and unknown domains in real-world scenarios.

Inference:

- ✓ **Case A:** Yields **normal** task predictions and legality-aware outputs.
- ☐ **Cases D–F:** Triggers **error predictions** and **unauthorized flags**.
- ✓ **Cases B–C:** Add **new domains from the provider**.

CONTRIBUTION

1. **Initiating Framework:** The **first authorization** framework for VLMs.
2. **Authorize-on-Demand:** Plug-and-play domain keys with **instant activation**.
3. **Retraining-Free:** Decoupled architecture with **zero** computational nightmare.
4. **Dual-Path Inference:** Simultaneous task prediction and **legality-aware verification**.

EXPERIMENT

Unauthorized Accuracy Drop: **77.54%**

Authorized Accuracy Drop: **↘0.13%**

More evaluations, benchmark comparisons, and ablation studies are detailed in the main paper.

Related Publications

[1] **Lianyu Wang,** et al. Say No to Freeloader: Protecting Intellectual Property of Your Deep Model. ***IEEE TPAMI***, 2024, 46(12):11073-11086.
[2] **Lianyu Wang**, et al. A Compact Un-Transferable Isolation Domain for Model Intellectual Property Protection. ***IEEE/CVF CVPR 2023,*** 2023:20475-20484.
[3] **Lianyu Wang**, et al. Vision-Language Model IP Protection via Prompt-based Learning. ***IEEE/CVF CVPR 2025***, 2025:9497-9506.
[4] **Lianyu Wang,** et al. Authorize-on-Demand: Dynamic Authorization with Legality-Aware Intellectual Property Protection for VLMs. ***IEEE/CVF CVPR 2026***.