Kartik Patwari

kpatwari@ucdavis.edu | kartikpatwari | scholar | kartikp7.github.io | kartikp7

Research Interests

Security & Privacy of Vision Models, Edge AI, MLLMs/VLMs, Multimodal Understanding, GenAI

Education

- **Ph.D. Computer Engineering** — Mar. 2022 – Present
  University of California, Davis — *Davis, CA*
- **M.S. Computer Engineering** — Mar. 2021 – Mar. 2024
  University of California, Davis — *Davis, CA*
- **B.S. Computer Engineering** — Sep. 2016 – Dec. 2020
  University of California, Davis — *Davis, CA*

Select Publications

[Preprint] **K. Patwari***, D. Schneider*, X. Sun, C-N. Chuah, L. Lyu, V. Sharma* (2024). **Rendering-Refined Stable Diffusion for Privacy Compliant Synthetic Data**. Under Submission.

[Preprint] D. Chen, **K. Patwari**, Z. Lai, S. Cheung, C-N. Chuah (2024). **Empowering Source-Free Domain Adaptation with MLLM-driven Curriculum Learning**. Under Submission.

[ICML'24] **K. Patwari***, C-N. Chuah, L. Lyu, V. Sharma* (2024). **PerceptAnon: Exploring the Human Perception of Image Anonymization Beyond Pseudonymization for GDPR**. ICML.

[TMLR'23] A. Chhabra, **K. Patwari**, C. Kuntala, Sristi, D. Sharma, P. Mohapatra (2023). **Towards Fair Video Summarization**. TMLR.

[EuroS&P'22] **K. Patwari**, S. M. Hafiz, H. Wang, H. Homayoun, Z. Shafiq, and C-N. Chuah (2022). **DNN Model Architecture Fingerprinting Attack on CPU-GPU Edge Devices**. Euro S&P.

Work Experience

- **Research Intern at Sony AI [🌐]** — Jun. 2023 – Sep. 2023
  Team: Privacy-Preserving Machine Learning (PPML) — *Tokyo, Japan*
  - Developed and trained lightweight task-specific object detectors to detect PIIs to anonymize.
  - Adapted MobileNet-based architectures for on-camera detector inference.
  - Developed anonymization tool (mask, blur, inpaint, synthesize) for full body & face images.
- **Research Engineer Intern at Sony [🌐]** — Jul. 2022 – Sep. 2022
  Team: Sony Semiconductor Solutions (SSS) – Imaging & Sensing — *Tokyo, Japan*
  - Investigated Deep Learning (DL) based 3D reconstruction from images - SfM, MVS, & Mesh generation.
  - Tested and evaluated learning & non-learning based pipelines on custom datasets.
  - Modified and suggested suitable SOTA DL methods to integrate into existing pipeline.

Ongoing Research

- **Watermarking Pre-trained Vision and Language Models** — *Oct. 2024 – Present*
  - Embedding watermark signatures into pre-trained models for IP verification.
- **Pruning & Compressing Low Light Image Enhancement Models** — *Jul. 2024 – Present*
  - Designing loss functions for gradient-based pruning of LLIE CNN, transformer, & diffusion models.

Projects

- **D-SLAM: Monocular V-SLAM with Depth Estimation** — *Dec. 2019 – Mar. 2020*
  Python, Pytorch, C++, LibTorch [🐙]
  - Designed and implemented a RGB-D SLAM system that performs monocular depth estimation and SLAM.
  - Benchmarked results on KITTI odometry dataset, deployed on NVIDIA Jetson TX2 at 3.3 FPS.
  - Project won Outstanding Senior Design Project Award in UC Davis ECE Department.

Technical Skills

- **Relevant Courses:** Machine Learning, Vision and Language Research, ML Hardware, Image Processing
- **Programming & Tools:** Python, C/C++, CUDA, Docker, Git, Jupyter, Conda, Latex
- **Programming/Frameworks:** PyTorch, PyTorch3D, HuggingFace, OpenCilk, OpenCV, OpenMP, Scikit-Learn
- **ML:** Multimodal LLMs, Pruning, Adversarial Attacks, Diffusion, Domain Adaptation, Knowledge Distillation