Kartik Patwari

kpatwari@ucdavis.edu | linkedin | homepage | scholar

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 (GPA: 3.79/4.0)*

M.S. Computer Engineering Mar. 2021 - Mar. 2024
University of California, Davis *Davis, CA (GPA: 3.79/4.0)*

B.S. Computer Engineering Major, Computer Science Minor Sept. 2016 - Dec. 2020
University of California, Davis *Davis, CA (GPA: 3.01/4.0)*

Select Publications

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

- D. Chen, **K. Patwari**, Z. Lai, S. Cheung, C-N. Chuah, "Empowering Source-Free Domain Adaptation with MLLM-driven Curriculum Learning," **Preprint 2024**.

- **K. Patwari**, C-N. Chuah, L. Lyu, V. Sharma, "PerceptAnon: Exploring the Human Perception of Image Anonymization Beyond Pseudonymization for GDPR," to appear in **ICML 2024**.

- A. Chhabra, **K. Patwari**, C. Kuntala, Sristi, D. Sharma, P. Mohapatra, "Towards Fair Video Summarization," **TMLR 2023**.

- B. Vora*, **K. Patwari***, S. M. Hafiz, Z. Shafiq, and C-N. Chuah, "Establishing a Benchmark for Adversarial Robustness of Compressed Deep Learning Models After Pruning," **ICML W. AdvML Frontiers 2023**.

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

Work Experience

ML Research Intern at SonyAI June 2023 – Sept. 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 July 2022 – Sept. 2022
Team: Sony Semiconductor Solutions (SSS) – Imaging & Sensing *Tokyo, Japan*

- Focused on 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.

Technical Skills & Relevant Courses

Courses: Machine Learning, Unsupervised Learning, Image Processing, Performance Engineering, Embedded Systems
Languages: Python, C/C++, CUDA
Frameworks: PyTorch, TensorFlow, PyTorch3D OpenCilk, OpenCV, OpenMP
Developer Tools: Docker, Git, VS Code, Linux, Google Cloud Platform

Ongoing Research

Watermarking Pre-trained Vision and Language Models Sept. 2024 – Present

- Embedding watermark signatures into pre-trained models for IP verification.

Pruning & Compressing Low Light Enhancement Models Jul. 2024 – Present

- Designing loss functions for gradient-based pruning of LLIE transformer/diffusion models.

Projects

Neural Network Quantization and Pruning on Edge devices Sept. 2022 – Jun. 2023

- Deployed various ResNet-based models on NVIDIA Jetson GPU-enabled edge devices
- Benchmarked accuracy and runtime of models before and after compression.
- Assessed security vulnerability analysis on pruned and quantized models running on edge devices.

D-SLAM: Monocular V-SLAM with Depth Estimation | Github Dec. 2019 – Mar. 2020

- Designed and implemented a RGB-D SLAM system that performs monocular depth estimation and SLAM
- Benchmarked accuracy and runtime results on KITTI odometry dataset.
- Deployed system to run on NVIDIA Jetson TX2 at 3.3 FPS
- Project won Outstanding Senior Design Project Award in UC Davis ECE Department

Teaching/Mentoring

Lead Teaching Assistant Fall '21, '22, '23; Winter '22, '23, '24

EEC 193/174AY: Applied ML Senior Design *University of California, Davis*

- Developed assignments for image classification, object detection & tracking, segmentation & inpainting.
- Gave lectures on security & privacy in ML, model compression & optimization
- Mentoring & leading teams in projects related to computer vision, scene understanding, autonomous driving.

Professional Services

Reviewer

- AISTATS 2025
- ACM Computing Surveys
- IEEE IoT Journal

Awards

ECE Best Teaching Assistant Award May 2024

University of California, Davis

Smita Bakshi Digital Learning and Teaching Award May 2024

University of California, Davis

Advanced to Candidacy (AC) Fellowship Apr. 2024

University of California, Davis

EuroS&P Conference Student Grant May 2022

EuroS&P 2022, Genoa

ECE Outstanding Senior Design Project Award June 2020

University of California, Davis