# 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

(*equal contribution)

**[Preprint '25]** **K. Patwari***, D. Chen*, Z. Lai, X. Zhu, S. Cheung, C-N. Chuah. **Empowering Source-Free Domain Adaptation with MLLM-driven Curriculum Learning**. Under Submission at ICCV 2025.

**[Preprint '24]** **K. Patwari***, D. Schneider*, X. Sun, C-N. Chuah, L. Lyu, V. Sharma*. **Rendering-Refined Stable Diffusion for Privacy Compliant Synthetic Data**. Under Submission at ICCV 2025.

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

**[EuroS&P '22]** **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**. Euro S&P 2022.

## Work Experience

- **Applied Scientist Intern at Amazon [🌐]** — Apr. 2025 – Aug. 2025
  *Team: Amazon Ring Devices* — *Sunnyvale, CA*
  - Investigating VLM-based conditional image retrieval and image understanding.
  - Using Multi-modal LLMs and foundation knowledge distillation.
- **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/Projects

- **Aligning VFM for Medical Pathology Images** — *Mar. 2025 - Present*
  *UC Davis*
  - Adapted vision foundation models for pathology-related image classification and text-based image retrieval.
  - Trained adapter layers and optimal transport loss for aligning text and visual features in the probabilistic embedding space.
- **Video Diffusion model for Human Anonymization** — *Mar. 2025 - Present*
  *UC Davis, SonyAI (Collaboration)*
  - Proposed new video-to-video diffusion model that preserves human structure by fine-grain conditioning.
- **Dementia and Depression Detection using Text and Speech** — *Feb. 2025 - Present*
  *UC Davis*
  - Developing LLM-based framework for joint speech and language based dementia detection.
- **Pruning Low-Light Image Enhancement (LLIE) Models** — *Nov. 2024 - Present*
  *UC Davis*
  - Benchmarking SOTA LLIE models under SOTA pruning strategies.
  - Evaluationg utility (PSNR) vs perforamnce (FLOPS) trade-offs.
  - Proposed novel task-specific loss functions for gradient-based pruning.

## 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

## Other Projects

- **D-SLAM: Monocular V-SLAM with Depth Estimation** *Dec. 2019 – Mar. 2020*
  *Python, Pytorch, C++, LibTorch* [GitHub]
  - 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.

## Teaching / Mentoring

- **Lead Teaching Assistant** *Fall '22, '23, '24; Winter '23, '24, '25*
  *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 Service

- **AISec | 2025** | Reviewer
- **VISION | 2024, 2025** | Reviewer
- **AISTATS | 2025** | Reviewer
- **ACM Computing Surveys | 2024** | Reviewer
- **IEEE IoT Journal | 2024** | Reviewer

## Certifications

- **NVIDIA** Fundamentals of Accelerated Data Science *March 2022*

## Awards

- **Outstanding Graduate Student Teaching Award** *June 2025*
  *Graduate Studies, UC Davis*
- **ECE Best Teaching Assistant Award** *May 2024*
  *Electrical and Computer Engineering (ECE), UC Davis*
- **Smita Bakshi Digital Learning and Teaching Award** *May 2024*
  *Electrical and Computer Engineering (ECE), UC Davis*
- **Advanced to Candidacy (AC) Fellowship** *April 2024*
  *Electrical and Computer Engineering (ECE), UC Davis*
- **EuroS&P Conference Student Grant** *May 2022*
  *IEEE EuroS&P 2022, Genoa*
- **ECE Outstanding Senior Design Project Award** *June 2020*
  *Electrical and Computer Engineering (ECE), UC Davis*