

Kartik Patwari

[✉ kpatwari@ucdavis.edu](mailto:kpatwari@ucdavis.edu) | [in kartikpatwari](https://www.linkedin.com/in/kartikpatwari/) | [g scholar](https://scholar.google.com/citations?user=KartikP7&hl=en) | kartikp7.github.io | [G kartikp7](https://github.com/kartikp7)

RESEARCH INTERESTS

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

EDUCATION

- | | |
|--|-----------------------|
| • Ph.D. Computer Engineering
<i>University of California, Davis</i> | Mar. 2022 – Mar. 2026 |
| • M.S. Computer Engineering
<i>University of California, Davis</i> | Mar. 2021 – Mar. 2024 |
| • B.S. Computer Engineering (Major), Computer Science (Minor)
<i>University of California, Davis</i> | Sep. 2016 – Dec. 2020 |

SELECT PUBLICATIONS

(*EQUAL CONTRIBUTION) | GOOGLE SCHOLAR FOR ALL.

- [Preprint] [K. Patwari*](#), D. Schneider*, X. Sun, C-N. Chuah, L. Lyu, V. Sharma*. [Rendering-Refined Stable Diffusion for Privacy Compliant Synthetic Data](#). Under Submission.
- [WACV '26] [K. Patwari*](#), D. Chen*, Z. Lai, X. Zhu, S. Cheung, C-N. Chuah. [Empowering Source-Free Domain Adaptation via MLLM-Guided Reliability-Based Curriculum Learning](#), to appear in IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), March 2026.
- [ICML '24] [K. Patwari*](#), C-N. Chuah, L. Lyu, V. Sharma*. [PerceptAnon: Exploring the Human Perception of Image Anonymization Beyond Pseudonymization for GDPR](#). International Conference on Machine Learning (ICML), July 2024.
- [ICML W '23] [K. Patwari*](#), B. Vora*, S.M. Hafiz, Z. Shafiq, C-N. Chuah. [Establishing a Benchmark for Adversarial Robustness of Compressed Deep Learning Models After Pruning](#). ICML Workshop New Frontiers in Adversarial Machine Learning (AdvML Frontiers), August 2023.
- [EuroS&P '22] [K. Patwari](#), S. M. Hafiz, H. Wang, H. Homayoun, Z. Shafiq, C-N. Chuah. [DNN Model Architecture Fingerprinting Attack on CPU-GPU Edge Devices](#). IEEE European Symposium on Security and Privacy (EuroS&P), June 2022.
- [AAAI-SS '25] L.C. Oliviera, [K. Patwari](#), X. Zhu, S. Cheung, B. Dugger, C-N. Chuah. [Co-HSF: Resource-Efficient One-Shot Semi-Supervised Adaptation of Histopathology Foundation Models](#). AAAI Spring Symposium Series (SSS-25), March 2025.
- [TMLR '23] A. Chhabra, [K. Patwari](#), C. Kuntala, Sristi, D. Sharma, P. Mohapatra (2023). [Towards Fair Video Summarization](#). Transactions on Machine Learning Research, December 2023
- [DATE '22] H. Wang, S. M. Hafiz, [K. Patwari](#), Z. Shafiq, C-N. Chuah, H. Homayoun. [Stealthy Inference Attack on DNN via Cache-based Side-Channel Attacks](#). IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE), May 2022.

WORK EXPERIENCE

- **AI Machine Learning Engineer Intern at Cisco Systems** Sep. 2025 – Dec. 2025
Team: *MLM Security* San Jose, CA
◦ Investigating vision-based prompt injection attacks and defenses on MLLMs.
◦ Developing novel DPO scheme for VLMs for image safety understanding.
- **Applied Scientist Intern at Amazon** Apr. 2025 – Aug. 2025
Team: *Amazon Ring Devices* Sunnyvale, CA
◦ Used Multi-modal LLMs and foundation knowledge distillation to improve recall on retrieval datasets.
◦ Developed novel multimodal framework from CLIP and loss for conditional image retrieval.
◦ Achieved new SOTA results on Person Image Retrieval task.
◦ Paper under submission at CVPR 2026.
- **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.
◦ Developed anonymization tool (mask, blur, inpaint, synthesize) for full body & face images.
◦ Paper accepted at ICML 2024.
- **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.

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

ONGOING RESEARCH

- **Multimodal DPO for Aligning Medical Vision Language Models**

Oct. 2025 - Present

UC Davis

- Improve modality alignment and disentangle direct bias while preserving the informative joint dependency between relevant regions and contextual cues.

OTHER 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.

TEACHING / MENTORING

- **Lead Teaching Assistant**

Fall '22, '23, '24; Winter '23, '24, '25

University of California, Davis

EEC 193/174AY: Applied ML Senior Design

- 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

- AAAI [🌐] | 2026 | Reviewer

- AISTATS [🌐] | 2026, 2025 | Reviewer

- Vision-based InduStrial InspectiON (VISION), ICCVW [🌐] | 2025, 2024 | 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