SPVis '24

Security and Privacy of Machine Learning-Based Vision Processing in Autonomous Systems

27 - 30 October 2024 | Abu Dhabi, UAE

CALL FOR PAPERS

PAPER SUBMISSION

IEEE

SPVis workshop aims to bring together experts, researchers, and practitioners in image/vision processing and machine learning security/privacy to discuss the latest advancements, challenges, and solutions in the critical domain of adversarial machine learning, backdoors, DNN obfuscation, attacks on visual forensics, deepfake detectors for images/videos, etc. Through a combination of keynote speeches, invited talks, panel discussions, and peer-reviewed paper sessions, the workshop promises a comprehensive overview of the current state and future directions of machine learning security and privacy in vision processing.

Topics of interest include:

- Adversarial Attacks on Neural Networks for Visual Data
- Physical-world Adversarial Attacks
- Defenses against Adversarial Attacks
- Certified Defenses
- Deep Learning Privacy
- Adversarial Vulnerabilities in Generative Models and Multi-Modal LLMs / LVMs
- Adversarial Vulnerabilities in Vision Transformers
- Adversarial Attacks on Forensic Classifiers and Deepfake Detectors
- Backdoor Attacks and Defenses
- Robustness Evaluation Metrics and Benchmarks
- Homomorphic Encryption for Collaborative Model Training
- Cost-efficient input-level defenses against adversarial and backdoor attacks

Original technical submissions are invited.

SUBMISSION GUIDELINES

The **SPVis 2024** paper submission and review process is being conducted according to ICIP guidelines.

IMPORTANT: The page count restrictions have changed. Papers may now contain up to **6 pages of technical content** and an optional **7th page with references/bibliography**.

- Authors who wish to participate in the conference will create documents consisting of a complete description of their ideas and applicable research results in compliance with the ICIP submission format.
- Submit the paper and copyright form electronically. This paper submission must be submitted in final, publishable form before the submission deadline listed below.
- Paper submissions will be reviewed by experts and the progress and results of the review process will be posted on SPVis website, and authors will also be notified of the review results by email.

For further details regarding format, please refer to the ICIP Paper Kit: https://cmsworkshops.com/ICIP2024/papers/paper_kit.php

ORGANIZING MEMBERS

- **Muhammad Shafique** (Director eBRAIN Lab, New York University (NYU), Abu Dhabi)
- **Bassem Ouni** (Principle Researcher, TII)
- **Michail Maniatakos** (Director MOMA Lab, NYU Abu Dhabi)
- **Ozgur Sinanoglu** (Director Cyber Security Center, NYU Abu Dhabi)
- **Christina Pöpper** (Director CSP-Lab, NYU Abu Dhabi)
- **Nasir Memon** (Dean CS and Engineering, NYU Shanghai)

ICIP abu dhabi 2024 | CENTER FOR CYBER SECURITY | BRAIN | TII Technology Innovation Institute | MOMA LAB | Design-for-Excellence Lab | CSP-lab Cyber Security and Privacy Lab

IMPORTANT DATES

Paper Submission Deadline
May 13, 2024

Paper Acceptance Notification
June 6, 2024

Final Paper Submission Deadline
June 19, 2024

Author Registration Deadline
July 11, 2024

Conference / Workshop Dates
October 27 – 30, 2024