SPVis '24

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

27 - 30 October 2024 | Abu Dhabi, UAE

CALL FOR POSTERS

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

SUBMISSION GUIDELINES

- Authors are invited to submit a 1-2 page proposal that describes the main contributions of the poster to the **ICIP SPVis Workshop**.
- Proposals should contain a brief abstract, demonstrate the motivation for the work, and summarize contributions being presented.
- Preliminary results may also be included. The submitted proposals will be evaluated primarily on their potential to stimulate interesting discussions, facilitate the exchange of ideas, and promote collaborations.
- Authors of accepted poster proposals will receive instructions for preparing the posters in an **e-poster session** format.
- Proposals are not blinded, and must contain the authors' names, affiliations, and contact information.
- All poster titles must begin with the keyword "POSTER:". Submissions should be sent to the Poster Chair via the email listed below.
- All submissions must designate a single corresponding author. At least one presenter per accepted poster must register for the ICIP SPVis Workshop.
- *The poster will not be included in the ICIP proceedings, and authors reserve the right to submit the work elsewhere.*

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)

POSTER CHAIR

- **Alberto Marchisio** (Research Team Leader, eBRAIN Lab, NYU Abu Dhabi)
  Submit to email: alberto.marchisio@nyu.edu

IMPORTANT DATES

Poster Submission Deadline
June 27, 2024 11:59 AoE

Poster Acceptance Notification
July 02, 2024 11:59 AoE

Author Registration Deadline
July 11, 2024 11:59 AoE

Conference / Workshop Dates
October 27 – 30, 2024

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