Mohammadreza **Teymoorianfard**

Manning College of Information and Computer Sciences, University of Massachusetts, Amherst, MA, USA
+1 413-313-9653 | mteymoorianf@umass.edu | mrteymoorian.github.io | mrteymoorian | teymoorian

Education

University of Massachusetts Amherst — *Massachusetts, USA*
PhD in Computer Science — *Sep 2023 - present*
- GPA: 3.87/4

University of Massachusetts Amherst — *Massachusetts, USA*
MSc in Computer Science — *Sep 2023 - May 2025*
- GPA: 3.87/4

University of Tehran — *Tehran, Iran*
BSc in Electrical Engineering — *Sep 2018 - Jun 2023*
- GPA: 19.06/20 (4/4)
- Ranked **3rd** among 120 Electrical Engineering students

University of Tehran — *Tehran, Iran*
Minor in Computer Engineering — *Sep 2019 - Jun 2023*
- GPA: 17.05/20

Research Interests

- Trustworthy Machine Learning
- Watermarking for Video Generation Systems
- Privacy and Security in Generative AI Models
- Privacy and Security of AI Agents

Publications

Jeong, H., **Teymoorianfard, M.**, Kumar, A., Houmansadr, A. and Badasarian, E., 2025. *Network-Level Prompt and Trait Leakage in Local Research Agents*. arXiv preprint arXiv:2508.20282.

Teymoorianfard, M., Ma, S. and Houmansadr, A., 2025. *VIDSTAMP: A Temporally-Aware Watermark for Ownership and Integrity in Video Diffusion Models*. arXiv preprint arXiv:2505.01406.

Amini, S., **Teymoorianfard, M.**, Ma, S. and Houmansadr, A., 2024. *MeanSparse: Post-Training Robustness Enhancement Through Mean-Centered Feature Sparsification*. arXiv preprint arXiv:2406.05927.

Research Experience

Umass Amherst - The Secure, Private Internet (SPIN) Research Group — *Amherst, MA*
Advisor: Amir Houmansadr — *Sep. 2023 - Present*
- **Privacy Analysis of Local Web/Research Agents** — Exposed vulnerabilities in locally deployed agents enabling prompt and trait recovery from observed IP activity, and proposed a coherent synthetic-query defense.
- **Watermarking and Attribution for Video Generation Models** — Created watermarking and model attribution techniques for video generation systems, enhancing security and traceability of generative models.
- **Robustness in Neural Networks** — Increased neural network robustness by reducing feature variation, achieving state-of-the-art AutoAttack accuracy on CIFAR-10, CIFAR-100, and ImageNet.

University of Tehran - Smart Networks Lab — *Tehran, Iran*
Advisor: Hamed Kebriaei — *Jun. 2022 - Jun. 2023*
- Implemented a Model Predictive Control (MPC) for autonomous taxi navigation.

University of Tehran *Tehran, Iran*

Advisor: Reshad Hosseini *Jun. 2021 - Sep. 2021*

- Developed a text detection system for card images, enhancing accuracy in document recognition.

Skills

Programming Languages	Python, C/C++, MATLAB, Verilog
Python Libraries & Frameworks	PyTorch, TensorFlow, Transformers, OpenCV, scikit-learn, NumPy, Pandas, Matplotlib, RL-Glue, PuLP, MIP

Honors & Awards

2023 **Recipient of an industry-sponsored award for outstanding bachelor's thesis work**

2020 **Awarded the University of Tehran Sponsors Foundation Honorable Award for Academic Excellence**

2020 **Recipient of the Faculty of Engineering (FOE) Award for achieving 2nd rank in the 2019-2020 academic year**

2018 **Ranked in the top 0.4% of over 150,000 students in the Iranian National University Entrance Exam**

2011 **Admitted to National Organization for Exceptional Talents (NODET) for middle and high school**

Teaching Experience

Fall '24 & Spring '25	**CICS 160: Object-Oriented Programming,** TA	*Umass Amherst*
Summer '24	**COMPSCI 589: Machine Learning,** TA	*Umass Amherst*
Spring '24	**COMPSCI 119: Intro to Programming,** TA	*Umass Amherst*
Fall '22	**Intelligent Systems,** TA	*University of Tehran*
Spring '22	**Mechatronics,** TA	*University of Tehran*
Spring '22	**Signal and Systems** TA	*University of Tehran*
Fall '21	**Engineering Probability and Statistics,** TA	*University of Tehran*
Spring '21	**Electronics1,** Head TA	*University of Tehran*

Relevant Courses

University of Massachusetts Amherst

- COMPSCI603: Robotics
- COMPSCI611: Advanced Algorithms
- COMPSCI685: Adv Natural Language Processing
- COMPSCI682: Neural Networks, Modern Intro
- COMPSCI660: Advanced Information Assurance

Coursera

- Motion Planning for Self-Driving Cars
- Introduction to Self-Driving Cars

University of Tehran

- Deep Learning
- Reinforcement Learning
- Machine Learning
- Artificial Intelligence
- Mechatronics
- Linear Algebra
- Engineering Probability and Statistics
- Modern Control Systems

Language

◇ English: Advanced Proficiency

◇ Persian: Native