

ANKITA RAJ

rajankita.github.io | +91 9971973864 | ankita.raj@cse.iitd.ac.in

SUMMARY

I am a doctoral researcher at IIT Delhi (thesis submitted) specializing in the robustness of computer vision systems. My research addresses security and privacy vulnerabilities in learning-based systems, including adversarial, backdoor, and model stealing attacks in safety-critical domains such as medical imaging and surveillance. My broader research interests encompass computer vision for satellite imagery, continual learning, and machine unlearning. I have extensive hands-on experience developing end-to-end vision pipelines using both conventional and foundation models to solve real-world problems.

EDUCATION

Indian Institute of Technology Delhi, New Delhi, India *Dec 2018 - Present*
Ph.D. in Computer Science and Engineering | CGPA: 8.46/10
Advised by Prof. Chetan Arora

Indraprastha Institute of Information Technology Delhi, India *Jul 2014 - Jun 2016*
M.Tech in Electronics and Communication Engineering | CGPA: 9.25/10
Advised by Prof. Pravesh Biyani

North Eastern Regional Institute of Science and Technology, India *Jul 2010 - May 2014*
B.Tech in Electronics and Communication Engineering | CGPA: 4.96/5

EXPERIENCE

Indian Institute of Technology Delhi *Jan 2019 - Dec 2022*
Teaching Assistant *New Delhi, India*

- Supported faculty and mentored students across advanced technical courses, including Computer Vision, Machine Learning, Digital Image Processing, and Data Structures and Algorithms.

Tata Consultancy Services *Aug 2016 - Dec 2018*
Researcher, Robotics Lab *Noida, India*

- Developed computer vision solutions for warehouse robotics applications, including object detection using RGBD data and incremental learning, with a focus on real-world deployment.
- Secured [fourth position](#) globally at the Amazon Robotics Challenge, 2017 in Nagoya, Japan, as part of the IITK-TCS team.

Indraprastha Institute of Information Technology Delhi *Aug 2014 - May 2016*
Teaching Assistant *New Delhi, India*

- Supported faculty and mentored students across courses: Probability and Statistics, Engineering Optimization, Signals and Systems, Maths I (Linear Algebra), Maths II (Differential Equations).

Indian Institute of Technology Guwahati *Jun 2013 - Jul 2013*
Research Intern *Guwahati, India*

- Developed a specialized algorithm for gender identification through speech under Dr. S.R.M. Prasanna.

ONGOING WORKS

Computer Vision for Geospatial Applications

Team VedaEarth, NCIIPC AI Grand Challenge

- Developing computer vision solutions for visual search, retrieval, and change detection using high-resolution satellite imagery.
- Selected among top-six teams nationally to advance to Stage 2 of the [challenge](#).

SELECTED PUBLICATIONS

Backdoor Attacks on Open Vocabulary Object Detectors via Multi-Modal Prompt Tuning [\[link\]](#)

Ankita Raj, Chetan Arora.

AAAI, 2026.

Mimicking Human Visual Development for Learning Robust Image Representations [\[link\]](#)

Ankita Raj, Kaashika Prajaapat, Tapan Kumar Gandhi, Chetan Arora.

ICVGIP, 2025.

Rethinking Detection Heads: Enhancing YOLO for Drone Image Object Detection [\[link\]](#)

Rutvik Patel, Anureet Chhabra, **Ankita Raj**, Chetan Arora.

ICVGIP, 2025.

Examining the Threat Landscape: Foundation Models and Model Theft [\[link\]](#)

Ankita Raj, Deepankar Varma, Chetan Arora.

BMVC, 2024.

Assessing Risk of Stealing Proprietary Models for Medical Imaging Tasks [\[link\]](#)

Ankita Raj, Harsh Swaika, Deepankar Varma, Chetan Arora.

MICCAI, 2024.

Identifying Physically Realizable Triggers for Backdoored Face Recognition Networks [\[link\]](#)

Ankita Raj, Ambar Pal, Chetan Arora.

IEEE ICIP, 2021.

Weighted- A^* Based Energy Efficient Resource Allocation in G.Fast [\[link\]](#)

Ankita Raj, Pravesh Biyani.

IEEE Transactions on Communications, 2019.

HiFi: A Hierarchical Framework for Incremental Learning using Deep Feature Representation [\[link\]](#)

Ankita Raj, Anima Majumder, Swagat Kumar.

IEEE RO-MAN, 2019.

A^* algorithm based power minimization for discontinuous operations in G.fast [\[link\]](#)

Ankita Raj, Pravesh Biyani, Sandip Aine.

IEEE ICC, 2017.

AWARDS AND ACHIEVEMENTS

Top-six team in NCIIPC AI Grand Challenge as part of Team VedaEarth

2025

Best M.Tech Thesis in Communication and Signal Processing, IIT Delhi

2016

Gold Medal for securing first position, Degree Module, NERIST

2014

TECHNICAL STRENGTHS

Programming

Python

Deep Learning & Vision

PyTorch, TensorFlow, Keras, OpenCV

Data Analysis & ML

Scikit-Learn, Pandas, NumPy, MATLAB