Subrat Kishore Dutta

+49 1575 3348940 | subrat.dutta@cispa.de | github.com/subratkishoredutta | linkedin.com/in/subrat-kishore-dutta-70a9a316b/ | Subrat Kishore Dutta

Education

University of Hamburg *Germany*

Doctorate in Philosophy *May 2025 - Present*

- Main research interest: Adversarial Machine Learning, Fairness, Subpopulation
- Tutoring: Algorithmic Foundations of Adversarial Robustness

UNIVERSITÄT DES SAARLANDES *Saarbrücken, 66123, Germany*

M.Sc. in Informatik *April 2022 - Feb 2025*

- Courses: Machine Learning, Image Processing and Computer Vision, High-Level Computer Vision, Neural Network Theory and Implementation, Robustness in Machine Learning
- Grade: 1.3 / 1.0

ASSAM ENGINEERING COLLEGE, ASTU *Guwahati, Assam, India*

B.E. in Computer Science and Eng *Aug 2017 - Aug 2021*

- First Class (Honors) Agg. percentage: 83.67% (Rank: 1)

Work Experience

CISPA Helmholtz Center for Information Security *Saarbrucken, Germany*

PhD Researcher *May 2025 – Present*

- My research focuses on the intersection of adversarial machine learning and representational fairness of minority subpopulation in generative models and how the former can aid the later.
- Supervisors: Dr. Xiao Zhang and Anne Lauscher

CISPA Helmholtz Center for Information Security *Saarbrucken, Germany*

Research Assistant *Jan 2024 – Present*

- Conducting Visually Imperceptible Targeted Adversarial Patch Attacks through Perceptibility-Aware Optimization, under Dr. Xiao Zhang.
- Developed perceptibility-Aware Optimization for patch localization.
- proposed a novel patch update rule for colour constancy.

Max Plank Institute for Informatics *Saarbrucken, Germany*

Research Assistant *Mar 2023 – Nov 2023*

- D2:Computer Vision and Machine Learning
- Studying the performance improvements with generated samples using latent diffusion models in a few-shot learning setup under the guidance of Prof. Dr. Bernt Sciele and Dr. Anna Kukleva.

Projects

Stealthy Targeted Adversarial Patch Attacks through Perceptibility-Aware Optimization. *Saarbrücken, Germany*

UNIVERSITÄT DES SAARLANDES *Jan 2024 - Present*

- The study explores the possibilities of conducting targeted patch attacks while achieving high level of perturbation imperceptibility.
- We proposed a novel two stage perceptibility-aware optimization methods which locates optimal location for patch placement as well as optimizes the perturbation considering human perception.
- The method surpasses the state-of-the-art targeted adversarial patch attacks in terms of imperceptibility convincingly while achieving equivalent or better attack success rates.
- The method is also able to by-pass existing state-of-the-art defense methods designed specifically for adversarial patch attacks.
- **Technical Skills:** Pytorch

Leveraging Realistic Templates generated from text-to-image model for Enhanced Universal Adversarial Attacks on Detectors. *Saarbrücken, Germany*

UNIVERSITÄT DES SAARLANDES *Dec 2023 - Present*

- The study investigates the concept of context homogeneity within adversarial patches and examines their impact on advanced object detectors in both white-box and black-box scenarios.
- We introduced a novel physical adversarial attack using a joint fine-tuning approach, adapting a text-to-image model to produce contextually homogeneous adversarial templates that effectively compromise advanced object detectors.
- We have evaluated our method on SOTA detector like YOLOv10, YOLOv8, and DETR with resnet50 backbone on a black box setting and have achieved attack success rate which surpasses the existing literature by achieving around 6% improvement in average precision and around a 5% increase in the fooling rate.
- **Technical Skills:** Pytorch

AEC Undergraduate Thesis: Assamese Text Generation using Deep Learning Architectures *Assam, India*

Assam Engineering College *Sep 2020 – Aug 2021*

- Created a standardized dataset containing 1.4 million sentences in Assamese for deep learning-based research.
- Studied the performance of multiple RNN-based architectures for text generation in the Assamese language.
- **Technical Skills:** TensorFlow 2.0, Keras, FastAPI

Publications

S. K. Dutta, X. Zhang. IAP: Invisible Adversarial Patch Attack through Perceptibility-Aware Localization and Perturbation Optimzation. In **Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)**, 2025. (**Accepted**)

Dutta, Subrat K. et al. "Study On Enhanced Deep Learning Approaches For Value-Added Identification And Segmentation Of Striation Marks In Bullets For Precise Firearm Classification". Applied Soft Computing, vol 112, 2021, p. 107789. Elsevier BV, doi:10.1016/j.asoc.2021.107789.

Chen, Z., **Dutta, S. K.**, Zhao, Z., Lin, C., Shen, C., & Zhang, X. (2024). Can Targeted Clean-Label Poisoning Attacks Generalize?. arXiv preprint arXiv:2412.03908.

Position of Responsibility

Google Developer Student Clubs *Assam, India*

Assam Engineering College *2020-2021*

- Lead for Assam Engineering College (2020-2021). Created a community of more than 450 students and organized multiple technical sessions and hosted the largest collaborative devfest in North-East India under the banner of DSC-EXPLORE.

Google Cloud Facilitator *Assam, India*

Assam Engineering College *2020-2021*

- Facilitated the 30 Days of Google Cloud program in Assam Engineering College.

Achievements

2021	**Merit Overseas Research Scholarship Award 2021,** Government of Assam	*India*
2020	**Merit Awards Fund for 3rd, 4th and 8th semesters,** Assam Engineering College	*India*
2020	**Among Top 5 Teams,** Smart India Hackathon(SIH)	*India*

Languages

English	Professional proficiency
Hindi	Native proficiency
Assamese	Native proficiency