Amit Singha

Indianapolis–46202, USA
E-mail: singha3@purdue.edu
Contact: (+1)3175405578

Profile Links: Google Scholar, ResearchGate, LinkedIn, GitHub

Academic Credentials

- **Doctor of Philosophy (PhD) in Electrical and Computer Engineering (ECE)**, Elmore Family School of Electrical and Computer Engineering, Purdue University (Indianapolis Campus), Aug 2024 – Present
- **Doctor of Philosophy (PhD) in Electrical and Computer Engineering (ECE)**, Indiana University–Purdue University Indianapolis (IUPUI), CGPA: 3.78/4.00 (30 credits completed/60 credits), Aug 2022 – Aug 2024
- **Master of Science (M.Sc.) in Computer Science**, Jahangirnagar University (JU), CGPA: 3.71/4.00 (39 credits), April 2021 – June 2022
- **Bachelor of Science (B.Sc.) in Information and Communication Engineering (ICE)**, Bangladesh University of Professionals (BUP), CGPA: 3.10/4.00 (155 credits), January 2016 – January 2020

Research Experience

- **Graduate Research Assistant (Aug 2022 – Present)**, School of Engineering Technology, Purdue University
  Engaged in cutting-edge research on mmWave-based wireless systems, advancing adversarial machine learning techniques to enhance AI robustness, security, and privacy, and to develop resilient, privacy-preserving wireless solutions.
  Research Supervisor: Dr. Tao Li, Assistant Professor, Department of Computer and Information Technology, Purdue University.
  ****Lab:**** Purdue Indy Security Lab.
  ****Affiliation:**** Recognized as a graduate student researcher at the Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, demonstrating involvement in advanced research on information security and assurance. CERIAS Profile
- **Undergraduate Research Work (January 2019 – January 2020)**, Bangladesh University of Professionals (BUP)
  Developed advanced text steganography techniques utilizing Bengali Unicode and whitespace characters to securely embed sensitive information within plain text, enhancing data security and privacy. Thesis: "A Text Steganography Method Using Bengali Unicode and Punctuation Marks." Research Supervisor: K. M. Akkas Ali, Professor, IIT, Jahangirnagar University.

Teaching Experience

- **Graduate Teaching Assistant (Aug 2024 – Present)**, School of Engineering, Purdue University (Indianapolis Campus)
  Courses: **ENGR 29700 - MATLAB - Computer Tools For Engineering**,
  Responsible for managing 110 students across 2 sections, grading assignments, preparing lecture materials and homework, conducting office hours three times per week, and assisting students in solving engineering problems using MATLAB.

Research Interests

Information Security & Privacy, Wireless & Mobile Security, AI Robustness & Adversarial Machine Learning, mmWave Radar Sensing, Cryptography & Steganography, AR/VR Security, Signal Processing, Deep Learning

Research Publications

1. Ziqian Bi, **Amit Singha**, Hongfei Xue, Tao Li, Yimin Chen, Yanchao Zhang. "Physical Backdoor Attacks against mmWave-based Human Activity Recognition." **Under review** at IEEE International Conference on Computer Communications (INFOCOM 2025). This work presents the first systematic approach to physical backdoor attacks on mmWave-based human activity recognition (HAR) systems, leveraging passive metal reflectors to manipulate signal patterns and induce targeted misclassifications in wireless HAR.
2. **Amit Singha**, Ziqian Bi, Tao Li, Yimin Chen, Yanchao Zhang. "Securing Contrastive mmWave-based Human Activity Recognition against Adversarial Label Flipping." In Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Seoul, Korea, 2024. 23 papers accepted out of 109 submitted, acceptance rate 21%. https://dl.acm.org/doi/abs/10.1145/3643833.3656123.
3. Paul Jiang, Ellie Fassman, **Amit Singha**, Yimin Chen, and Tao Li. 2023. "Evaluating the Impact of Noisy Point Clouds on Wireless Gesture Recognition Systems." In Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), Association for Computing Machinery, New York, NY, USA, 480–485. https://doi.org/10.1145/3565287.3617626
4. J. Xu, Z. Bi, **A. Singha**, T. Li, Y. Chen, Y. Zhang, "mmLock: User Leaving Detection Against Data Theft via High-Quality mmWave Radar Imaging." 2023 32nd International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, pp. 1-10. DOI: https://doi.org/10.1109/ICCCN58024.2023.10230151.
5. **A. Singha**, N. Mumenin, N. I. Akhter, M. U. Ahmed, "Implementation of Lightweight Cryptographic Schemes to Secure Wireless Sensor Networks Data in Agriculture." 2021 International Conference on Trends in Electronics and Health Informatics (TEHI, INDIA). https://link.springer.com/chapter/10.1007/978-981-16-8826-3_53
6. M. Shazzad-Ur-Rahman, M. M. Hosen Ornob, **A. Singha**, M. S. Kaiser, N. I. Akhter, "An Effective Text Steganographic Scheme Based on Multilingual Approach for Secure Data Communication." 2021 Joint 10th International Conference on Informatics, Electronics & Vision (ICIEV, JAPAN) and 2021 5th International Conference on Imaging, Vision & Pattern Recognition (ICIVPR, JAPAN), pp. 1-8. DOI: https://doi.org/10.1109/ICIEVicIVPR52578.2021.9564231
7. **A. Singha**, N. Mumenin, N. I. Akhter, M. U. Ahmed, "A New Stegano-Cryptographic Approach for Enhancing Text Data Communication Security." 2021 International Conference on Electronics, Communications and Information Technology (ICECIT), pp. 1-4. DOI: https://doi.org/10.1109/ICECIT54077.2021.9641144
8. Shazzad-Ur-Rahman M., **Singha A.**, Ibne Akhtar N., Fahim Ashhab M., Ali K.M.A., "An Efficient Bengali Text Steganography Method Using Bengali Letters and Whitespace Characters." Proceedings of International Conference on Trends in Computational and Cognitive Engineering. DOI: https://doi.org/10.1007/978-981-33-4673-4_38

Ongoing Research Works

Funding for all projects: Supported by the National Science Foundation (NSF) and the Army Research Laboratory (ARL).

- **Universal Physical Adversarial Attacks on mmWave-Based Human Activity Recognition Systems in Black-Box Settings**
Status: (In Progress) – Investigating black-box universal physical adversarial attacks on mmWave-based HAR systems by optimizing aluminum reflectors placed on the human body to induce targeted and untargeted misclassifications, exposing critical security vulnerabilities in real-world HAR applications.
- **Privacy-Preserving Defense Against Attribute Inference Attacks in mmWave-Based Human Activity Recognition Using Autoencoder and Diffusion Models**
Status: (In Progress) – Developing autoencoder and diffusion-based methods to balance data

utility and privacy by sanitizing mmWave-based HAR data, protecting sensitive attributes (e.g., gender, age, body shape) while preserving activity recognition performance.

Standardized Test Scores

- IELTS (November 2021) Overall: 7.5 (Reading- 8, Listening- 8, Speaking- 6.5, Writing- 6.5)
- GRE (December 2021) Overall: 310 (Quant: 160, Verbal: 150, AWA: 3.5)

Selected Projects

1. **Deep Dream with VGG16 and DenseNet121** (Mar 2023 - Mar 2023)
   Applied the Deep Dream algorithm with VGG16 and DenseNet121 models to enhance and visualize features in an image of a monkey. Implemented creative adaptations by guiding the algorithm with images of bananas and cherries for unique, surreal visual effects.
2. **Audio-Effects-Generator** (Aug 2022 - Dec 2022)
   Developed audio effects using input audio processed through a FRDM-K64 board. Achieved effects like ECHO, REVERB, SLAPBACK, PANNING, and CHORUS. Utilized tools like the Wolfson Pi Audio Card, Keil MDK-ARM, and MATLAB Simulink. Aimed to extend the project for wireless and IoT applications.
3. **Self Supervised Contrastive Learning in PyTorch with Point Clouds from Shapenet Dataset** (Oct 2022 - Nov 2022)
   Created a self-supervised learning model for 3D shape representation using ShapeNet dataset's point clouds. Employed PyTorch, PyTorch Geometric, and DynamicEdgeConv, with InfoNCE/NT-Xent loss for contrastive learning. Achieved effective representation and separation of entities in the embedding space.
4. **End-to-End Deep Learning for Potato Blight Disease Classification** (Dec 2021 – Apr 2022)
   Developed a web/mobile application to diagnose potato blight disease using deep learning techniques and convolutional neural networks.
5. **RyDE** (January 2019 – June 2019)
   Developed a ride-sharing app with live GPS location, integrated rider and user apps. Utilized the Firebase database for the coding environment and employed Java and Android Studio for development.
6. **Smart Wheelchair for Disabled People** (Jan 2018 – May 2018)
   Conceptualized a cost-effective smart wheelchair controllable through hand gestures, aimed at increasing mobility for disabled individuals.

Technical Skills

- Languages: C, Python, C++, JAVA, Solidity
- Radar Technology: mmWave radar operation, mmWave Studio for data collection, Cascade radar systems
- Simulation & Analysis Tools: MATLAB, SAS, Excel, SPSS
- Data Processing & Visualization Tools: Matplotlib, Tableau
- Python Library and Operating Systems: PyTorch, TensorFlow, Scikit-learn, Windows, Linux
- Documentation & Presentation Application: Microsoft Office, LaTeX

Professional Activities

- Presented research in person at the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2024, Seoul, South Korea
- Presented research poster titled "Securing Contrastive mmWave-based Human Activity Recognition against Adversarial Label Flipping" at the CERIAS Symposium 2024, Purdue University. CERIAS Poster Link
- Presented research in person at the 32nd International Conference on Computer Communications and Networks (ICCCN), 2023, Hawaii, USA

- Presented research virtually at multiple conferences, including TEHI 2021, ICIEV 2021, ICIVPR 2021, ICECIT 2021, and TCCE 2020.
- Reviewer for the 2nd International Conference on Mechanics, Electronics, Automation, and Automatic Control (MEAAC), 2024
- Reviewer for the 11th International Conference on Informatics, Electronics & Vision (ICIEV), 2023

Affiliations

- Member, Eta Kappa Nu (HKN), the International Honor Society for Electrical and Computer Engineering (September 2024 – Present)
- Professional Member, Association for Computing Machinery (ACM) (April 2024 – Present)
- Member, IEEE (February 2017 – Present)
- Member, Bangladesh Student Association, Indiana University-Purdue University Indianapolis (IUPUI) (August 2022 – Present)
- Member, International Club, Indiana University-Purdue University Indianapolis (IUPUI) (August 2022 – Present)
- Organizing Secretary, BUP Robotics Club, BUP Infotech Club (February 2018 – December 2019)

Extra-curricular Activities, Awards, and Achievements

- Awarded the National Science Foundation (NSF) Student Travel Grant, receiving $2,000 to present research at the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2024, Seoul, South Korea.
- Invited to join Eta Kappa Nu (HKN), the International Honor Society for Electrical and Computer Engineering, in recognition of exceptional academic performance and commitment to excellence in the field of Electrical and Computer Engineering.
- Volunteer, IT Fest and MATLAB contest, organized by the Department of ICT, BUP (2019).
- Promoted to Organizing Secretary of the BUP INFOTECH Club for excellent coordinating and organizing skills (2019).
- Instructed Mathematics & Physics to over 100 students for the Higher Secondary Certificate Examination (2017-2020).
- Recipient of the National Education Board Scholarship in the Higher Secondary Certificate Examination (2014).
- Member, Badhon (Blood Donation Organization).

Personal Development

- Deep Learning Specialization (November 2021 – June 2022), Course Instructor: Andrew Ng (Co-founder, Coursera; Adjunct Professor, Stanford University), Coursera
- Machine Learning (June 2021 – September 2021), Course Instructor: Andrew Ng (Co-founder, Coursera; Adjunct Professor, Stanford University), Coursera
- Complete Machine Learning and Data Science Zero to Mastery (November 2020 – May 2021), Course Instructor: Ross Mahan (MS, New York University), Udemy
- Information Security A-Z™: Complete Cyber Security Bootcamp (March 2020 - October 2020), Course Instructor: SecuritasX™ IT Training, Udemy
- Python for Everybody Specialization (November 2019 – June 2020), Course Instructor: Charles Russell Severance (Professor, University of Michigan), Udemy