GLOBAL INITIATIVE OF ACADEMIC NETWORKS

A
Course
on

Security and Threats of Generative AI in Biometric

December 18-23, 2025

Organized in Physical Mode

PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur, India

Course Overview

Biometric systems aim to provide secure and convenient access control by leveraging individuals' distinct biological or behavioral traits. Emergent generative tools, such as DALL-E, Deep-AI, Adobe Firefly, and analogous platforms, can generate visual outputs based on provided prompts. These tools are accessible to a broad user base, which raises concerns related to the potential generation of deceptive images. If attackers can produce synthetic images that convincingly resemble the biometric data of an authorized individual, they can potentially bypass biometric security protocols and gain unauthorized access. The unique nature of biometric data amplifies the consequences of a security breach. Unlike passwords that can be reset, compromised biometrics are irreplaceable.

Striking a balance between the innovation brought by generative AI and the imperative to secure sensitive biometric information is crucial for ensuring the responsible and effective deployment of biometric technologies in our interconnected and digitized society. To address these challenges, ongoing research focuses on developing robust and secure generative models, implementing adversarial training techniques, and enhancing the interpretability of AI systems in biometric applications.

This course aims to provide participants with a comprehensive understanding of the security challenges and potential threats associated with biometric systems due to generative AI. Participants will gain insights into the principles of biometric systems, the role of generative AI, and the potential security vulnerabilities that may arise. Practical strategies and countermeasures to mitigate these threats will also be explored. The course includes lectures, case studies, and hands-on exercises to ensure a comprehensive understanding of the security and threats associated with generative AI in biometric systems.

Course Instructor

Dr. Kiran Raja is an Associate Professor in the Department of Computer Science at the Norwegian University of Science and Technology (NTNU), Norway. His research focuses on statistical pattern recognition, image processing, and machine learning, particularly in biometrics, security, and privacy protection. He has contributed to EU projects like SOTAMD and iMARS, focusing on generation and detection of attacks on biometrics systems. His works have exploited the advancements in Generative Adversarial Networks to create morphing attacks to improve resilience of biometric systems. He also contributed to synthetic identity creation for the euLISA project. Dr. Raja also works as a consultant for various national agencies within Norway. His works have been recognized and bagged positions at major conferences like CVPR, BIOSIG, BTAS, IAPR/IEEE-IWBF, IEEE-ISBA, ACM-SIN etc. He is a senior IEEE member, Section Chair of IEEE Norway, and chairs the Academic SIG at the European Association of Biometrics (EAB). He is also an NTNU Pedagogic Academy member and was awarded excellent teaching practitioner in 2023.

Course Overview

This course will cover the following topics:

Introduction to Biometric Systems: Biometric Modalities, Biometric System Architecture, Applications, Challenges and Limitations of Biometric Systems, Multi-Modal Biometric.

Biometric System Evaluation: Feature Extraction and Representation, Template Matching and Verification, Performance Metrics in Biometric Systems.

Implementation of a face/fingerprint-based Biometric Authentication System.

Generative AI in Biometric: Discriminative vs Generative Models, Types of Generative AI, Emerging Applications of Generative AI in Biometrics.

A Case Study on Fingerprints with Demonstration: Use of generative AI in synthetic fingerprint generation and their applications in privacy preservation, Building a deep generative model for fingerprints.

Attack Landscape on Biometric Recognition: Identity Thefts, Presentation Attacks and Impersonation Risks, and Adversarial Attacks with case studies on fingerprints and face.

Countermeasures against Attacks: Privacy-Preserving Generative AI Techniques, Security Considerations and Countermeasures against Spoofing and Adversarial Attacks, Continuous Monitoring and Update Mechanisms.

Deepfake (Face) Generation and Detection as a Case Study.

Biometric Systems - Breaches and Best Practices:

Examples of Biometric Security Breaches in the Real World and Lessons Learned, Best Practices in Deploying Secure Biometric Systems.

Ethical Implications and Fairness of Generative AI in Biometrics: Ethical Implications of Biometric Data Generation, Bias and Fairness in AI-Generated Biometric Data, Regulatory Compliance and Standards, Emerging trends and research directions.

For more information, please contact

Prof. Pritee Khanna
9425324241

Prof. Aparajita Ojha
9425800334

bm.gian@iiitdmj.ac.in

Who can Attend

- Students pursuing BTech/MTech/MS/MSc/Ph.D. degrees.
- Faculty, researchers, educators, postdocs, and professionals from academia, technical institutions, and industry.
- Engineers and researchers from industry and R&D laboratories, national laboratories, government agencies, and other sectors.

Course Coordinators

Prof. Pritee Khanna is a Computer Science and Engineering professor at PDPM IIITDM Jabalpur, India, with over 24 years of experience in academia, research, and administration. Her research focuses on image processing and computer vision. She earned Ph.D. in Computer Science from Kurukshetra University and has research experience at Tokyo Institute of Technology through JSPS Fellowship. She serves as an Associate Editor for Engineering Applications of Artificial Intelligence, Neural Networks and Computers & Electrical Engineering journals. With over 130 publications, she has supervised eleven PhD students. She has completed many government and industry-sponsored projects.

Prof. Aparajita Ojha is a Professor of Computer Science and Engineering at PDPM IIITDM Jabalpur, India. Her research interests include applications of AI in various domains like medical image processing, precision agriculture, smoke detection etc. With over 41 years of experience, she has also served as Director of IIITDM Jabalpur from 2009-2015. She has over 95 publications and has supervised eleven doctoral graduates. Prof. Ojha has led several government, industry, and international projects, including MeiTy's Electronics and ICT Academy and the Asi@Connect project on empowering girls in IT. A Senior IEEE Member and recipient of many academic awards, she is also affiliated with ACM and several scientific societies.

Course Objectives

- To make the participants familiar with biometric systems.
- To ensure a comprehensive understanding of the security and threats associated with generative AI in biometric systems.
- To make participants familiar with theoretical foundations, practical implementations, and real-world use cases of generative AI in biometric systems by taking case studies on fingerprint and face modalities.
- To familiarize the participants with a comprehensive understanding of innovative applications and advancements brought about by generative AI in the field of biometrics.

How to Register

- The participation fee (including GST@18%):
  - Industry/Research Organizations: INR 5,900 (INR 5,000 +GST)
  - Faculty: INR 2,950 (INR 2,500+GST)
  - Students: INR 1,180 (INR 1,000 + GST)
  - Participants from abroad: US $125
- The above fee includes all instructional materials, assignments, tutorials, laboratory equipment usage, and internet facility.
- No TA/DA will be provided to the participants. Participants have to pay for accommodation and food as per actuals. Limited accommodation may be available in the Institute Visitor Hostel/ Student Hostel on request.
- Last Date of Registration: Monday, December 1, 2025
- Targeted participants 35 only, first come first serve basis.
- The fee can be paid to the account number mentioned under bank details. After successful payment of the fee, the participants must register for the GIAN course by filling out the registration form: https://forms.gle/SVGbf8ZoTjoS922Q7

Account Name	:	Project Account PDPM IIITDM JABALPUR
Account No.	:	50210022387
Bank MICR Code	:	482019014
Bank IFS Code	:	IDIB000M694
Bank Name	:	Indian Bank
Branch Name	:	Mehgawan, IIITDM, Campus Branch Jabalpur