IITB-Monash Research Academy

Indian Institute of Technology Bombay | MONASH University

An Indian-Australian research partnership

Project Title:	**Optimizing Deep Adversarial Learning**	
Project Number	**IMURA0842**	
Monash Main Supervisor (Name, Email Id, Phone)	**Pierre Le Bodic** Pierre.LeBodic@monash.edu	*Full name, Email*
Monash Co-supervisor(s) (Name, Email Id, Phone)		
Monash Head of Dept/Centre (Name,Email)	Geoff Webb	*Full name, email*
Monash Department:	**Data Science & AI**	
Monash ADGR (Name,Email)	Bernd Meyer	*Full name, email*
IITB Main Supervisor (Name, Email Id, Phone)	**P. Balamurugan** balamurugan.palaniappan@iitb.ac.in	*Full name, Email*
IITB Co-supervisor(s) (Name, Email Id, Phone)		*Full name, Email*
IITB Head of Dept (Name, Email, Phone)	**Narayan Rangaraj** narayan.rangaraj@iitb.ac.in	*Full name, email*
IITB Department:	**IEOR**	

Research Clusters:

Highlight which of the Academy's CLUSTERS this project will address?
*(Please nominate JUST **one.** For more information, see www.iitbmonash.org)*

1	*Material Science/Engineering (including Nano, Metallurgy)*
2	*Energy, Green Chem, Chemistry, Catalysis, Reaction Eng*
3	*Math, CFD, Modelling, Manufacturing*
4	***CSE, IT, Optimisation, Data, Sensors, Systems, Signal Processing, Control***
5	*Earth Sciences and Civil Engineering (Geo, Water, Climate)*
6	*Bio, Stem Cells, Bio Chem, Pharma, Food*
7	*Semi-Conductors, Optics, Photonics, Networks, Telecomm, Power Eng*
8	*HSS, Design, Management*

Research Themes:

Highlight which of the Academy's Theme(s) this project will address?
(Feel free to nominate more than one. For more information, see www.iitbmonash.org)

1	***Advanced computational engineering, simulation and manufacture***
2	*Infrastructure Engineering*
3	*Clean Energy*
4	*Water*
5	*Nanotechnology*
6	*Biotechnology and Stem Cell Research*
7	*Humanities and social sciences*
8	Design

The research problem

Deep Neural Networks have shown remarkable improvement in several machine learning tasks and applications, prominent of which are computer vision applications, and challenging problems related to video, text and multi-media analytics. However, training a deep neural network is not without its problems. An important issue is to understand the effect of an adversary who can derail the training process which degrades the generalization performance of the deep neural network.
In this project, we will aim to optimize the learning strategies of a deep neural network so that the network becomes robust to the adversary. The project will broadly encompass development of new optimization and learning theoretic tools which aid in the training procedures of deep neural networks. The developed tools will also be applied to several real-world problems.

Project aims

1. To understand and analyze the state of the art in adversarial deep learning methods.
2. Develop novel optimization models to address adversaries in deep learning scenarios for image, video and other multi-media data, with an emphasis on scalability and generality of the tools.
3. Extending the optimization methods to deep variants of RNNs.
4. Develop rigorous learning theoretic tools for proposed optimization tools.

Expected outcomes

1. The project will result in the development of novel optimization algorithms to be used in adversarial deep learning settings.
2. The project will also lead to development of novel learning theoretic tools to understand the nature of proposed tools.
3. Codes for the newly developed tools will be made available for further research purposes.

How will the project address the Goals of the above Themes?

The development of sophisticated optimization and learning theoretic tools will naturally help in advancements in computational methods and engineering. Since the tools developed will be general-purpose, they would be able to handle imaging, video and multimedia-based applications in other themes like biotechnology and nanotechnology.

Capabilities and Degrees Required

1. Exposure to Machine Learning and Deep Learning
2. Exposure to mathematical optimization is preferable
2. Proficiency in programming and coding.
3. Knowledge in Python programming language is preferable.

Potential Collaborators

Please visit the IITB website www.iitb.ac.in OR Monash Website www.monash.edu to highlight some potential collaborators that would be best suited for the area of research you are intending to float.

Select up to **(4)** keywords from the Academy's approved keyword list **(available at http://www.iitbmonash.org/becoming-a-research-supervisor/)** relating to this project to make it easier for the students to apply.

Data Science, optimization, algorithms