Akshayvarun Subramanya

CONTACT 1000 Hilltop Circle ITE E-mail: akshayv1@umbc.edu INFORMATION Baltimore, MD 21250 Webpage: aksvarun.github.io

EDUCATION University of Maryland, Baltimore County (UMBC)

2017- (Expected)2022

Ph.D in Computer Science

PES Institute of Technology(PESIT), Bangalore India

2012-2016

Bachelor of Engineering

Publications

Akshayvarun Subramanya, Vipin Pillai, Hamed Pirsiavash,

Fooling Network Interpretation in Image classification, International Conference on Computer Vision (ICCV) 2019, arXiv:1812.02843.

Akshayvarun Subramanya, Vipin Pillai, Hamed Pirsiavash,

Towards Hiding Adversarial Examples from Network Interpretation, NeurIPS 2018 workshop on Security in Machine Learning (link).

Aniruddha Saha, Akshayvarun Subramanya, Hamed Pirsiavash, Hidden Trigger Backdoor Attacks, AAAI 2020, (link).

Aniruddha Saha, Akshayvarun Subramanya, Koninika Patil, Hamed Pirsiavash,

Role of Spatial Context in Adversarial Robustness for Object Detection, CVPR 2020 Workshop on Adversarial Machine Learning in Computer Vision, (link).

Akshayvarun Subramanya, Konda Reddy Mopuri, R. Venkatesh Babu,

BatchOut: Batch-level feature augmentation to improve robustness to adversarial examples, Indian conference on Computer Vision, Graphics and Image Processing 2018. (link)

Suraj Srinivas, Akshayvarun Subramanya, R. Venkatesh Babu,

Training Sparse Neural Networks, Embedded Vision Workshop, CVPR 2017. (link).

Akshayvarun Subramanya, Suraj Srinivas, R. Venkatesh Babu,

Confidence Estimation in Deep Neural Networks via density modelling, (link).

RESEARCH EXPERIENCE Deep Learning Intern, Applied AI, Dolby Laboratories. June, 2019 - September 2019

- Proposed a method to reduce the artifacts due to quantization in decoded audio signals, using a new class of generative models called Normalizing Flows.
- Results shown on Wall Street Journal Speech dataset and working towards extending to other music domains.

Research Assistant, Dept. of CDS, Indian Institute of Science. Jul, 2016 - May, 2017

- Proposed a novel algorithm to improve robustness of deep neural networks towards adversarial examples. The method, **BatchOut** was shown to improve robustness towards adversarial examples created using Fast Gradient Sign Method and DeepFool for networks trained on MNIST and CIFAR-10 datasets.
- Proposed a novel confidence measure in deep neural networks to overcome the drawbacks of softmax function. This made use of activations of penultimate layer in a deep neural network

to measure the confidence of a test point w.r.t data distribution.

- Conducted research in deep neural networks to obtain a sparse neural network model by removing redundant parameters. A novel learning mechanism was established to learn neural networks which are implicitly sparse.
- Developed a generative deep neural network which can output desired sketches from the Eitz sketch database. A Graphical User Interface was created which used word2vec to allow user inputs in textual format.

Student Intern, Dept. of ECE, Carnegie Mellon University.

Jun 2015-Aug 2015

• Investigated the effect of using different sampling algorithms for selecting initial centroids in k-means clustering. Results were shown on synthetic data from UCI data repository and Yale face database.

Workshops

Student Participant, Winter school workshop by Carnegie Mellon University Dec 2014

- Created a database of audio samples containing the shots from tennis. MFCC feature extraction was performed and a simple naive bayes classifier was used to detect the time slot of tennis shot.
- Extracted Histogram of Optical Flow(HOF) features from video frames and simple actions such as Serve, Hit were detected.

AWARDS

Best project award for **Automatic commentary generation for tennis** awarded by Dr. Rita Singh and Dr. Bhiksha Raj during CMU Winter School.

Relevant Coursework Digital Signal Processing Statistical Signal Processing Principles of Artificial Intelligence Computer Vision Applied Machine Learning Linear Algebra Introduction to Machine Learning Design and Analysis of Algorithms Probability and Random Process Coursera Machine Learning Advanced Operating Systems Foundations of Optimization

Computer Skills

Programming - Python, Java

Deep learning libraries - PyTorch, Keras, TensorFlow, Caffe

TEACHING EXPERIENCE

• Graduate level Machine Learning, Computer Vision.

Aug, 2018 -

• Undergraduate level Introduction to Algorithms, Artificial Intelligence and Machine Learning.