**Abstract**

The project focuses on building a speech recognition application using robust neural networks and aims on realising a comprehensive comparison between different types of fully connected models: unconstrained, L2-norm constrained and trained using adversarial examples.

and the Google dataset, speech commands,

Constanta Lipschitz

Tensorflow, keras, numpy, adversarial robustness toolbox

Audio -> MFCC -> NN -> result

Atacuri white-box, black-box

The project focuses on a new approach for building a robust Automatic Speech Recognition system. The aim of the project is a comprehensive comparison between different types of Fully Connected Neural Networks, by controlling the Lipschitz constant of the models. The classifiers are trained based on Google’s speech commands dataset and will be used to only classify digits. The robustness of the constrained model will be demonstrated in multiple scenarios, using both white-box and black-box attacks. The implementation will be done in Python using the Tensorflow framework and Keras API for building the models, Numpy and Librosa for data manipulation and the adversarial robustness toolbox for adversarial attacks.

That can fool