CLEVERHANS

BENCHMARKING TOOLS FOR ADVERSARIAL EXAMPLES

41

CLEVERHANS: LIBRARY FOR VARIOUS ATTACK

- Cleverhans is an adversarial example library for constructing attacks, building defences, and benchmarking both.
- Contains most of the existing attacks
- Written in TensorFlow and compatible with models in tensorflow or keras.
- Under Active Development
- https://github.com/tensorflow/cleverhans
- https://groups.google.com/forum/#!forum/cleverhans-dev

BENCHMARKING TOOLS FOR ADVERSARIAL EXAMPLES

CLEVERHANS