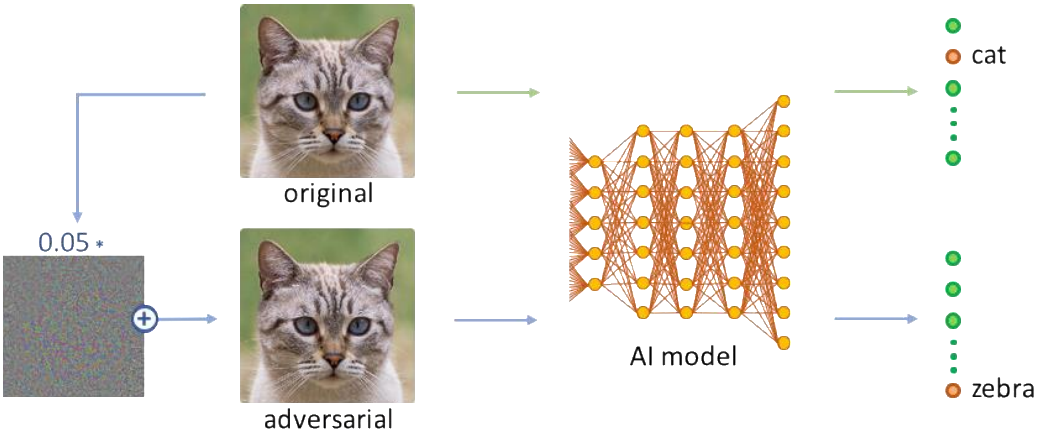
IJCAI-19
Alibaba Adversarial AI Challenge
Secure the AI sysyems against adversarial attacks
SIGN UP >>
IJCAI 2019 MACAO
阿里安全
TIANCHI天池
IJCAI-19

IJCAI-19 Alibaba Adversarial AI Challenge

Motivation, impact, and expected outcomes

Recent years have seen dramatic increase in applications of deep learning techniques to solve real world problem, range from social network to online ecommerce etc. However, the intelligence system powered by deep learning itself is vulnerable and lucrative target to attackers. In 2014, Christian Szegedy et al. firstly found that the highly accurate modern deep learning models are susceptible to adversarial samples that are derived from the original images by adding small perturbations. To address the security problem of AI system, many methods for model attack and defense have been proposed. However, the problem is far from being solved.

The IJCAI-2019 Alibaba Adversarial AI Challenge (AAAC2019) aims at providing a venue for AI practitioners to explore the security of the AI models. Our competition this year focus on image classification tasks, and includes model attacks and model defenses. The participants can play as an attacker to fool our models, or can play as a defender to provide robust model against the adversarial samples.



Three tasks are proposed in this competition including non-targeted attack, targeted attack, and model defense. Specifically,

- **non-targeted attack**: aims at generating adversarial samples to make the AI models output a wrong decision.
- **targeted attack**: aims at generating adversarial samples to make the AI models output a specific wrong decision.
- **model defense**: aims at generating AI models to output correct decisions to adversarial samples.

Problems Abstract

Different from previous competitions, it is the first time that utilizes the images from online e-commerce as the underlining dataset. Totally, 110,000 product images, which come from 110 categories, will be released. The participants can use these data to train more robust defense models or generate adversarial samples with higher quality.

Infrastructures

Tianchi platform (http://tianchi.aliyun.com/):

We plan to use the data competition platform Tianchi developed by aliCloud (part of the Group). Since 2014, More than 100 competitions have been successfully hosted on Tianchi, which gathered 250,000 players from 93 countries and regions. This platform is well developed, tested and can be tailored to this contest as needed. Since 2015, Tianchi has cooperated with IJCAI conference for many times. Four impressive IJCAI competitions have successfully lauched on Tianchi.

2018：https://tianchi.aliyun.com/competition/introduction.htm?&raceId=231647

2017：https://tianchi.aliyun.com/competition/introduction.htm?&raceId=231591

2016：https://tianchi.aliyun.com/competition/introduction.htm?&raceId=231532

2015：https://tianchi.aliyun.com/datalab/dataSet.html?&dataId=42

Tentative Competition Schedule

February 15 - May 31, 2018

Website URL

The competition webpage has been released at https://tianchi.aliyun.com/markets/tianchi/ijcai2019

Organizers

Dr. Yuan He is a Staff Engineer in the Security Department of Alibaba, and working on artificial intelligence based content moderation system. His research interests include computer vision, pattern recognition and machine learning. Before joining Alibaba, He was a research manager at Fujitsu working on document analysis system. He received his B.S. and Ph.D. degrees from Tsinghua University.

Mrs. Yiting Wang is the leader of Tianchi platform. She specializes in organizing and promoting data mining contest.

Dr. Hui Xue is Director of Algorithm and Data Science in Alibaba Group，and have 8+ years industrial experience in computer vision, NLP and fraud risk management. Dr. Xue currently lead a team of 50+ engineers and scientists to build AI abilities for Alibaba Security Department.

Bibliographic references

Tianchi Competition Platform: https://tianchi.aliyun.com/

Alibaba group: http://www.alibabagroup.com/