Proceedings

2021 International Workshop on Safety and Security of Deep Learning

Virtual

19 Aug 2021

2021 International Workshop on Safety and Security of Deep Learning (SSDL 2021)

Yuanfang Guo[1], Bo Li[2], Xianglong Liu[1], Jiantao Zhou[3]
1. Beihang University
2. University of Illinois Urbana-Champaign
3. University of Macau

Deep learning, which is the current representative technology in artificial intelligence, has demonstrated tremendous success in various tasks, such as computer vision, natural language processing, data mining, etc. Unfortunately, deep learning models have also encountered critical safety and security threats in recent years. Due to its implicit vulnerability, deep learning models can be easily affected by the adversarial perturbations and perform abnormally, which may yield serious consequences in certain applications such as autonomous driving, etc. Meanwhile, deep learning models may also be utilized by the malicious attackers to generate forged multimedia content, such as fake images/videos, to deceive people, which may induce trust issues among different people and organizations.

In this workshop, we aim to bring more attentions from the researchers in the fields of adversarial attack & defense, forensics, robust deep learning, explainable deep learning, etc., to discuss the recent progresses and future directions for tackling the various safety and security issues of deep learning models.

This workshop has received 12 high-quality submissions. Each paper was peer-reviewed by at least two experienced reviewers, in a double-blind reviewing manner. The workshop chairs decided to accept 10 papers, resulting in an acceptance rate of 83%. Note that the authors of 1 accepted paper have decided to only present in the workshop while withdraw from the workshop proceeding. Therefore, the proceeding of this workshop has included 9 papers. Based on the review comments and discussions among the workshop chairs, the paper, whose title is “Lip Forgery Video Detection via Multi-phoneme Selection”, was selected as the best paper of this workshop.

This workshop was virtually held in conjunction with IJCAI 2021, on Aug. 19, 2021. The workshop chairs invited Dr. Dacheng Tao (JD Explore Academy), Dr. Xiangui Kang (Sun Yat-sen University), Dr. Siwei Lyu (University at Buffalo, the State University of New York), and Dr. Jun Zhu (Tsinghua University) to give invited talks during the workshop. For each accepted paper, one of the authors gave an oral presentation to introduce their contributions, followed by a short Q&A session to let the audiences further understand the papers.

We, the workshop chairs, would like to express their sincere appreciations to all

the authors, reviewers, invited speakers, and audiences who participated the workshop, for their valuable contributions and participations.

We would also like to express their sincere appreciations to Miss Yating Su, Mr. Lingfeng Tan and Miss Xiaohan Zhao for their valuable efforts in supporting this workshop, including website construction, call-for-paper production, proceeding preparation, etc.

At last, we would like to express their sincere appreciations to the IJCAI 2021 organization for providing an excellent framework for this workshop.