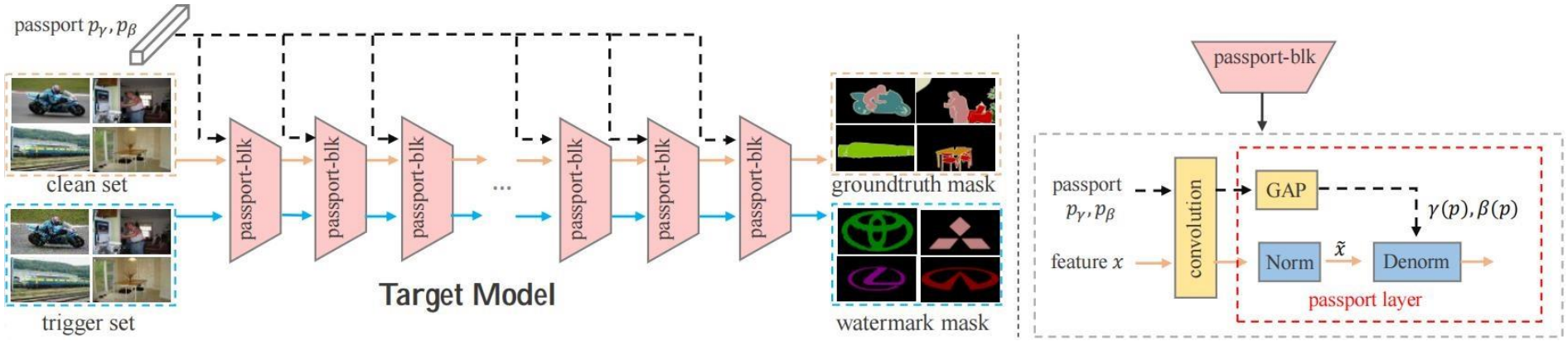
# Intellectual Property Protection for Deep Semantic Segmentation Models

**Hongjia RUAN, Huihui SONG, Bo LIU, Yong CHENG, Qingshan LIU**

Frontiers of Computer Science, DOI: 10.1007/s11704-021-1186-y

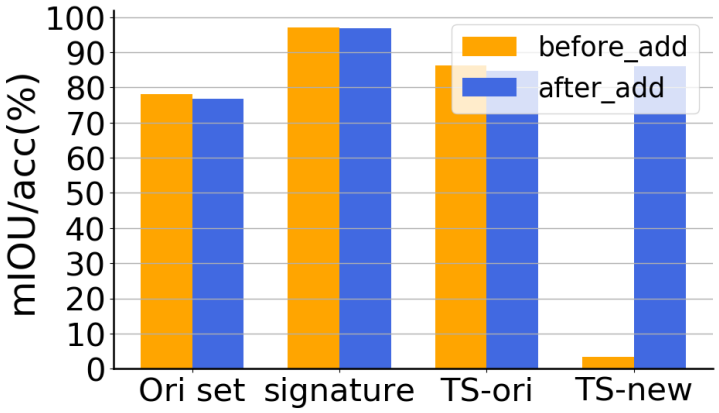
# Problems & Ideas

- Problems of deep model IP protection:
  - Deep model IP protection is still under-researched and most existing methods focus on the image classification models.
- Ideas: We propose a hybrid IP protection framework that combines the trigger set based and passport based watermarking mechanism.

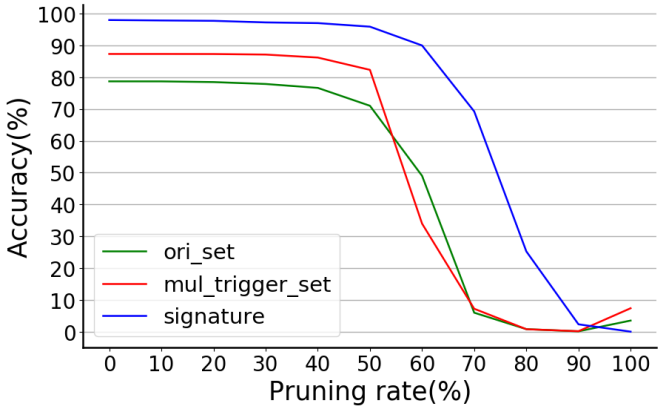


# Main Contributions

- Contributions:
  - We are the first to study the IP protection problem for deep segmentation networks;
  - We propose a hybrid IP protection framework that combines the trigger set based and passport based watermarking mechanism, which can enable black-box verification and resist ambiguity attack, respectively;
  - Extensive experiments have been conducted and demonstrate both the effectiveness and robustness of the proposed framework.




The performance of our framework(hybrid watermark) towards the fine-tuning attack that tries to embed a new trigger set.




The performance of trigger set based and passport signature based verification by applying different model pruning rates.