SPEECH ANNOUNCEMENT

WEDNESDAY, JULY 13 | 14:00 – 16:00

BUILDING 7 (R.70507)
YUAN ZE UNIVERSITY - TAIWAN

EYES TELL ALL : REVEALING GAN-GENERATED FACES

Generative Adversarial Network (GAN) based techniques can generate and synthesize realistic faces that cause profound social concerns and security problems. Existing methods for detecting GAN-generated faces can perform well on limited public datasets. However, images from existing datasets do not represent real-world scenarios well enough in terms of view variations and data distributions, where real faces largely outnumber synthetic ones. The state-of-the-art methods do not generalize well in real-world problems and lack the interpretability of detection results. Performance of existing GAN-face detection models degrades accordingly when facing data imbalance issues.

In the first part of my talk, I will present a method that can expose GAN-generated faces by checking the pupil shape artifacts. We demonstrate that such artifacts exist widely in high-quality GAN generated faces. Our automatic method can segment the pupils from the eyes and analyze their shapes to distinguish GAN-generated faces from real ones.

In the second part of my talk, I will present a robust, attentive, end-to-end framework that spots GAN-generated faces by analyzing eye inconsistencies. Our model automatically learns to identify inconsistent eye components by localizing and comparing artifacts between eyes. After the iris regions are extracted by Mask-RCNN, we design a Residual Attention Network (RAN) to examine the consistency between the corneal specular highlights of the two eyes. Our method can effectively learn from imbalanced data using a joint loss function combining the traditional cross-entropy loss with a relaxation of the ROC-AUC loss via Wilcoxon-Mann-Whitney (WMW) statistics. Qualitative and quantitative evaluations of our methods on the Flickr-Faces-HQ dataset and a StyleGAN2 generated face dataset demonstrate the effectiveness and simplicity of our method.

Prof. Ming-Ching Chang

GUEST SPEAKER

Prof. Ming-Ching Chang is the Co-Director of the Computer Vision and Machine Learning (CVML) Lab at the University at Albany-SUNY. He has rich experience in leveraging expertise from multiple domains to accomplish multi-discipline programs and projects, including: AI video analytics in smart city in collaboration with NVIDIA and scientific machine learning applied to physics and chemistry in collaboration with the Oak Ridge National Laboratory (ORNL) on neutron scattering.

Prof. Chang is the recipient of :

- The IEEE Advanced Video and Signal-based Surveillance (AVSS) 2011 Best Paper Award - Runner-Up,
- The IEEE Workshop on the Applications of Computer Vision (WACV) 2012 Best Student Paper Award,
- The GE Belief - Stay Lean and Go Fast Management Award in 2015, and
- The IEEE Smart World NVIDIA AI City Challenge 2017 Honorary Mention Award.

Prof. Chang frequently serves the program chair, area chair, and referee of leading journals and conferences.

- The AI City Challenge, a multi-year IEEE Computer Vision and Pattern Recognition (CVPR) Workshop 2017-2022,
- Program chair of the IEEE Advanced Video and Signal-based Surveillance (AVSS) 2019.,
- TPC chair lead of the IEEE Multimedia Information Processing and Retrieval (MIPR) 2022 conferences,
- The Area Chair of IEEE ICIP (2017, 2019-2022) and an outstanding area chair of ICME (2021),
- He chairs the steering committee of the IEEE AVSS Conference since 2022.

He has authored more than 100 peer-reviewed journal and conference publications, 7 US patents and 15 disclosures. He is a senior member of IEEE and member of ACM.

SPEECH ANNOUNCEMENT

THURSDAY, JULY 14 | 14:00 – 16:00

BUILDING 7 (R.70507)
YUAN ZE UNIVERSITY - TAIWAN

TOWARDS MORE SECURE, ROBUST, AND TRUSTWORTHY COLLABORATIVE AND FEDERATED LEARNING

The advancement of deep learning has taken us to a new era of ``data-centric" AI, where the quality, privacy and security of the valuable data might have a bigger impact over the availability of AI models or machine learning solutions that can be directly applied. Many distributed, collaborative, or federative learning solutions are under active development; and the key design ideas are about how data and model privacy are protected in the decoupling of data vs. model during the decentralized model training.

In the first part of my talk, I will present a robust collaborative learning framework that uses data digests to represent absent clients. Specifically, we handle the problem of client unreliability or absence during the online decentralized model training. We address this issue by introducing the notion of data digests of the training samples from the clients. The expansion of digests called synonyms can represent the original samples on the server, which bypass the data privacy issues, and at the same time maintain overall model accuracy, even after the clients become unavailable. We compare our CLSyn implementations against three centralized Federated Learning algorithms, namely FedAvg, FedProx, and FedNova as baselines. Results on CIFAR-10, CIFAR-100, and EMNIST show that CLSyn consistently outperforms these baselines by significant margins in various client absence scenarios.

In the second part of my talk, I will present a Federated Learning (FL) framework that mitigates the strong assumption of trust by incorporating cryptographic tools. We examine various scenarios with different trust demands in FL, and then design the corresponding practical protocols with lightweight cryptographic tools. We propose three solutions for secure and trustworthy aggregation with increasing sophistication: (1) a single verifiable moderator, (2) a single secure and verifiable moderator, and (3) multiple secure and verifiable moderators, which can handle adversarial behaviors with different levels. We evaluate the performances of all our proposed protocols on the test accuracy and the training time, showing that our protocols maintain the accuracy with time overhead from 30% to 156% depending on the secure and trustworthy levels. The protocols can be deployed in practical FL settings with appropriate optimizations.

Prof. Ming-Ching Chang

GUEST SPEAKER

Prof. Ming-Ching Chang is the Co-Director of the Computer Vision and Machine Learning (CVML) Lab at the University at Albany-SUNY. He has rich experience in leveraging expertise from multiple domains to accomplish multi-discipline programs and projects, including: AI video analytics in smart city in collaboration with NVIDIA and scientific machine learning applied to physics and chemistry in collaboration with the Oak Ridge National Laboratory (ORNL) on neutron scattering.

Prof. Chang is the recipient of :

- The IEEE Advanced Video and Signal-based Surveillance (AVSS) 2011 Best Paper Award - Runner-Up,
- The IEEE Workshop on the Applications of Computer Vision (WACV) 2012 Best Student Paper Award,
- The GE Belief - Stay Lean and Go Fast Management Award in 2015, and
- The IEEE Smart World NVIDIA AI City Challenge 2017 Honorary Mention Award.

Prof. Chang frequently serves the program chair, area chair, and referee of leading journals and conferences:

- The AI City Challenge, a multi-year IEEE Computer Vision and Pattern Recognition (CVPR) Workshop 2017-2022,
- Program chair of the IEEE Advanced Video and Signal-based Surveillance (AVSS) 2019.,
- TPC chair lead of the IEEE Multimedia Information Processing and Retrieval (MIPR) 2022 conferences,
- The Area Chair of IEEE ICIP (2017, 2019-2022) and an outstanding area chair of ICME (2021),
- He chairs the steering committee of the IEEE AVSS Conference since 2022.

He has authored more than 100 peer-reviewed journal and conference publications, 7 US patents and 15 disclosures. He is a senior member of IEEE and member of ACM.