Bo-Wei Tseng

About Me

My name is Bo-Wei Tseng (Scott). I received my master degree from the Graduate Institute of Communication Engineering, National Taiwan University. My primary research area is Privacy Preserving Machine Learning, and I have other AI related course experience, including natural language process (NLP) and computer vision (CV). It is worth mentioning I enjoy doing the literature survey while reproducing the empirical results with respect to each area of machine/deep learning, and several projects completed by me are specified in my resume. I believe that I can encompass this job in your enterprise with my strong background in artificial intelligence. About my personality, I am always optimistic and aggressive to face every challenge around my life.

Master Thesis

My master thesis aims to solve the privacy issue raised by the machine learning model, it is well known that attaining high performance of the ML model is dependent on the amount of collected data, but part of the data may be sensitive, e.g. the disease record of the patient, conversation acoustic signal between the couple, and user's face image used by the recognition system. Thus, how to protect user's privacy in the machine learning model is the first priority. More specifically, I develop the local compression neural network (NN) learned by the GAN formulation to defend the reconstruction attack occurring in the real world applications, while the data compressed by the NN must retain enough utility information to do supervised learning task. Most importantly, this manuscript co-working with my advisor Prof. Pei-Yuan Wu is published to the Journal *IEEE Transactions on Information Forensics and Security*. [Link: https://ieeexplore.ieee.org/document/8963921]

Self Assessment

With the cultivation of my advisor Prof. Wu, I become the person who has strong independent thinking and scientific research ability. Prof. Wu also promotes me as the principal of machine learning and estimation theory lab because of my responsibility and planning ability, and gives me a lot of opportunities to attend the conference/seminar held by AI center and CSSP of Academia Sinica. Furthermore, I have strong leadership and interactive skill since I joined and served as the vice captain on the school volleyball for high school and college life, meanwhile, I was awarded Dean's List Honor for four semesters in Da-Yeh university. This can be seen that I am very self-disciplined so that it is not difficult for me to balance between extracurricular activities and academics. Finally, I always keep a sentence in my mind *"The more efforts you devote in, the more wonderful process and brilliant results you can attain"*.

Work Expectation

I look forward to contributing to the company with my expertise in the field of machine learning (ML), and collaborating well with all colleagues. As a fresh graduate, learning how to apply ML technique to industry is the first priority. Furthermore, a copy of my resume is enclosed for your reference. I would appreciate an opportunity to discuss my qualifications of this job, and I am available to be contacted by phone call or e-mail. Thank you for your time and consideration.

Hsinchu Country, Taiwan
(+886)930-983-816 • *live8169@gmail.com*

BO-WEI TSENG

Machine Learning/AI Researcher

@ live8169@gmail.com 0930-983-816 Hsinchu, Taiwan
in https://www.linkedin.com/in/bo-wei-tseng github.com/r06942098
Born on 6th December, 1994

PUBLICATIONS

- **B. W. Tseng** and P. Y. Wu, *"Compressive Privacy Generative Adversarial Network"*, IEEE Transactions on Information Forensics and Security, Jan, 2020.
  Available: https://ieeexplore.ieee.org/document/8963921

EXPERIENCE

Teaching Assistant

National Taiwan University

Sep 2018 – Jan 2019 Taipei, Taiwan

- Course "Practicum of Attacking and Defense of Network Security" instructed by Prof James T. Yu.
- Learn the knowledge of network security, defense and attack.
- Experience with SEED project and network setting in Ubuntu.
- Guide the students to complete each lab/exam successfully.

ACHIEVEMENTS

- Participate in the MOST project "Privacy Preserving Machine Learning", which co-works with my advisor Prof. Pei-Yuan Wu.
- Placed on 3rd prize in the final project competition of the Course "Deep Learning for Computer Vision".
- Placed on 3rd prize in the basketball competition hold by GICE.

SKILLS

Python, Tensorflow, Keras, Unix
Keras, C++, Java, Git, SQL
Language: TOEIC 840

COURSE

Machine Learning/ Deep Learning

- Kernel Method in Machine Learning, Machine Learning, Deep Learning and Having it Deep and Structured, Deep Learning for Computer Vision.

Theoretical/ Mathematical

- Linear algebra, Probability/Statistic, Communication system.
- Information Theory, Random Process, Digital signal processing.

EDUCATION

Master's Degree

Graduate Institute of Communication Engineering, National Taiwan University

Sep 2017 – Jun 2019 Taipei, Taiwan

Bachelors's Degree

Electrical Engineering, Da-Yeh University

Sep 2013 – Jun 2017 Changhua, Taiwan

EXTRACURRICULAR ACTIVITIES

- Serve as the vice captain of Da-Yeh school volleyball team.
- Serve as the principal of the Machine Learning and Estimation Theory Lab (Jan, 2018 - Jun, 2019).
- Serve as a speaker of the AI poster organized by NTU AI center in Dec, 2018.
- Serve as a speaker of CSSP seminar organized by IIS (Institute of Information science) in Apr, 2019.

PROJECTS

Listen and Translate

- Develop the model which inputs the acoustic signal and then answer the multiple choice questions.
- Extract the MFCC spectrum and build the QA-LSTM with Attention Model.

Image Caption

- Develop the model to generating textual description of an image.
- Extract sequential features from pre-trained VGG-16 model and build the Bi-LSTM seq2seq attention model.

Chat-Bot

- Develop the model to simulate the conversion with human users.
- Reproduce word embedding technique (BoW, gensim, jieba, fasttext word vectors) and build Bi-LSTM seq2seq attention model.

Few Shot Learning

- Few shot learning is the promising approach to learn good feature when little data is available.
- Implement the Matching Network, Relation Network, Siamese Network and Graphical Neural Network on CIFAR-100 dataset.

Image Generation

- Develop the model to synthesize the images or transfer the style of original images.
- Implement the DCGAN, WGAN, Conditional-GAN, AC-GAN, Info-GAN and UNIT.

Reinforcement Learning

- Implement Policy Gradient, Double DQN, A2C.

Privacy Preserving Machine Learning

- Developed a local compression network to prevent the sensitive data from getting exposed to the cloud whilst enjoying the MLaaS.

曾柏偉

(+886)930-983-816 live8169@gmail.com Hsinchu, Taiwan

關於我

我是曾柏偉，為臺灣大學電信工程研究所碩士班應屆畢業生，並服完兵役，希望能盡快進入職場先熟悉工作內容，並設立自己未來的工作目標。在碩士班，我主要的研究領域是隱私維護機器學習，但是我也有其他機器學習及深度學習的課程實作經驗：深層化結構、電腦視覺以及自然語言處理，在修課當中我會盡可能地要求自己把上課所說明的技術做文獻回顧，以了解不同技術的想法來源，讓我可以更靈活的運用這些觀念，並且讓自己在不同領域上都能建立基本的知識庫。雖然實作模型的能力固然重要，但是機器學習背後的理論才是根深此領域的重要因素，而我有修習一些相關理論課程：核方法機器學習、消息理論、隨機程序、旁聽機器學習數學原理還有一些數位訊號處理的課程，從以上這些課程經驗，我可以在機器學習的實作與理論間交錯思考，也有基本能力探索深度學習神秘的黑盒子。

碩士論文　Compressive Privacy Generative Adversarial Network

這個研究主題旨在解決大量機敏性資料應用於訓練機器學習模型所導致的隱私洩露問題。在實際應用中，為了得到高準確率或是低誤差的模型，機器學習服務(MLaaS)提供者需要搜集大量的使用者資料，而這些資料可能會包含病人的病史、情侶之間對談的語音訊號或是使用者臉部照片，為了讓避免這些機敏性的資料直接上傳至雲端後被攻擊者直接取得，我們使用了目前火紅的生成式對抗網路(GANs)模擬實際應用中攻防的情境，並學習出一個提供使用者本地隱私維護的壓縮網路，此架構可以應用於語音訊號、圖像以及文字對話內容。許多問題需要將研究傳統的技術(密碼學、差分隱私、壓縮隱私)並應用至機器學習的模型內，藉此我培養了獨立思考並且解決問題的能力。最後，此為科技部(MOST)計畫，且我和指導教授吳沛遠博士已經將此篇文章投稿至期刊 IEEE Transactions on Information Forensics and Security。[Link: https://ieeexplore.ieee.org/=document/8963921]

人格特質

- 抗壓及團隊經營:

  我在大二時設立一個目標就是考進台大電信所，開始準備訊號與系統、通信原理、線性代數及機率與統計等科目，並且利用閒暇時間閱讀英文讀物，加強自身外語能力。從那時我便成為一個自我約束力較高的人，並在大學時期拿到四次書卷獎。我在大學時是以排球項目績優入學(十六萬元獎學金)，因此我在有長時間的球隊(團隊生活)經驗，球隊其實就是一個小型社會，在當上副隊長之後，我必須要學習在三十多人的隊伍中規劃大家能夠訓練的時間、承受訓練量的大小、處理球員對於教練產生的負面情緒，及外出比賽的交通住宿規劃等等，我從中學習了良好的溝通協調模式、培養了訓練上遇到低潮時的抗壓性，還有在分配學科及術科時間的能力。
- 負責且積極態度:

  在研究所中，我的指導教授吳沛遠，看重我對於事情規劃以及負責任的態度，指派我擔任機器學習與估計理論實驗室室長，讓我安排學弟妹的週會時間、規劃實驗室研究設備以及輔助研究/專題生們解決研究/報告上遇到的困難。積極求知是我的另一個特質，我很感謝教授給我很多機會參與中研院的演講及台大人工智慧中心的海報展等會議，讓我從會議中能找到不同領域上的文獻可以閱讀。

工作期望

我希望我能夠在職場上發揮研究所兩年培養的解決問題的能力，並將所習得的人工智慧背景知識應用於業界。我能和同事相處融恰並且合作、短時間內熟悉環境並且分擔公司的業務、為公司貢獻，且細心完成主管交待事項。最後，我的履歷表也附加在這份檔案內，希望貴公司能給我一個面試機會。

曾柏偉

機器學習研究員，研究方向：機器學習/深度學習、壓縮隱私、核方法、最佳化

(+886)930-983-816 live8169@gamil.com 1994/12/6

教育背景

臺灣大學電信工程研究所 2017年9月 – 2019年6月

- 指導教授: 吳沛遠博士
- 碩士論文: Compressive Privacy Generative Adversarial Network
- 投稿期刊: IEEE Transactions on Information Forensics and Security
- 論文連結: https://ieeexplore.ieee.org/=document/8963921
- 修習課程:
  - 實作課程: 機器學習、機器學習及其深層與結構化、深度學習於電腦視覺
  - 理論課程: 核方法機器學習、消息理論、隨機程序、數位訊號處理

大葉大學電機工程學系 2013年9月 – 2017年6月

- 修習課程: 線性代數、機率與統計、訊號與系統、通信系統原理

經歷及課外活動

教學助理 (Teaching Assistant) 2018年9月 – 2019年1月

課程: 網路攻防實習 授課教授: Prof. James T. Yu 臺灣大學

工作內容:

- 指派作業並協助修課學生完成，期中、期末考問題回覆
- 學習網路資安知識、Ubuntu 16.04上的網路安全配置、SEED專題實作

課外活動 2013年9月 – 2019年6月

- 擔任高中、大學排球校隊副隊長
- 擔任一次AI中心海報展、中研院CSSP會議講者
- 擔任機器學習與估計理論實驗室室長

專案

隱私維護機器學習 (PPML) 科技部(MOST)計畫 與Prof. Wu及DARPA團隊合作 2018年1月 – 2019年5月

壓縮隱私生成對抗網路 (CPGAN)、 Kernel Discriminant Component Analysis (KDCA)

自然語言處理 (NLP) ML/MLDS課堂專題 2018年3月 – 2018年6月

聊天機器人 (Chat-bot), 機器看圖說故事 (Image Caption), 語音訊號對話翻譯 (Listen and Translate)

電腦視覺 (CV) DLCV課堂專題 2018年3月 – 2018年6月

圖像合成 (Synthesis)、 影像切割 (Segmentation)、 小樣本機器學習 (Few-shot Learning)

強化學習 (RL) MLDS課堂專題 2018年3月 – 2018年6月

策略梯度 (Policy Gradient)、 DQN/DDQN、 A2C

IT 技能及語言能力

- 研究方面: 具有快速文獻回顧、自我解決問題及找題目的能力
- 程式編譯: Python > C++ >Java, Git, SQL Tensorflow, Keras
- 作業系統: Linux, Windows, MacOS
- 外語能力: TOEIC 840分

獲獎經歷

3^{rd} prize, DLCV期末專題競賽(Sponsored by Microsoft) 2018年6月

3^{rd} prize, 電信工程研究所三對三籃球賽 2019年4月