Bo-Wei **TSENG**

Machine Learning Researcher/Engineer

linkedin.com/in/bo-wei-tseng github.com/bwtseng
+886 930-983-816 @ bwtseng1994@gmail.com
Hsinchu, Taiwan
Born on 6th Dec, 1994.

Bo-Wei Tseng was born in Hsinchu, Taiwan, in 1994. He received the M.S. degree from the Graduate Institute of Communication Engineering, National Taiwan University, Taipei, Taiwan, in 2019. He and Prof. Pei-Yuan Wu published a manuscript in IEEE Transactions on Information Forensics and Security in Jan 2020. Currently, he joins Andes Technology, Hsinchu, Taiwan, as a RD ML software engineer. His research interest lies in artificial intelligence, privacy preserving machine learning and model compression.

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
  Privacy Preserving Machine Learning | Data Compression | GAN | Kernel Method | Convex Optimization

Competences

Programming Language	**Python**, C/C++, JavaScript
Deep Learning Frameworks	**Pytorch**, Tensorflow/TensorflowLite Micro, Keras, Darknet, Caffe
Machine Learning Knowledge	Privacy Preserving Machine Learning, Model Compression Generative Adversarial Net, Few-shot Learning, Reinforcement Learning
Related Courses Experience	Including **Machine Learning**, **Communication System** and **Mathematics** › Machine Learning, Machine Learning and Having its structure, Deep Learning and Computer Vision › Random Process, Digital Signal Processing, Information Theory › Linear Algebra, Probability and Statistic, Kernel Method, Convex Optimization
Operating System	Mac OS X, Windows 10, Linux, Ubuntu
Other Skills	Git, SQL, LaTeX

Experience

Present – Mar. 2020 — RD Software Engineer, Andes Tech Inc., Hsinchu, Taiwan

- Develop automatic deep neural network optimization/compression algorithms.
- Develop model conversion tool for different deep learning frameworks.
- Reproduce the performance of image classification/object detection models, and implement the image processing algorithms.
- Port deep learning model to Andes processor by slightly revising the open source C++ NN SDK.
- Be familiar with RISC-V architecture.

Andes | Pruning | Quantization | Model Conversion | Classification | Object detection | Python | Pytorch | TFLM | RISC-V

Mar. 2020 – Jan. 2020 — Research Scientist, Mediatek Research Lab Inc., Taipei, Taiwan

- Collaborate with MRUK. It's worth mentioning all of the team members in MRUK/MRTW have Ph.D degree (except me) with the research interests lying in machine learning.
- Collaborate with the Mediatek colleagues on physical design (PD) code-conversion projects.
- Apply natural language processing to Mediatek's TV applications.

NLU | NLP | Seq2seq | Amazon Alexa Platform

Jan. 2019 – Sep. 2018 — Teaching Assistant, National Taiwan University, 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

Cyber security | SEED | Leadership

References

Pei-Yuan Wu
Assistant Professor, NTU
@ peiyuanwu@ntu.edu.tw
+886 905-236-121

Sam Meng
Deputy Director, CICS
@ sam.meng@coretronic.com

Nick Wang
Senior SW Engineer, ViewSonic
@ seark1219@gmail.com
+886 975-252-871

Education

Jun. 2019 – Sep. 2017 | **National Taiwan University, Taiepi, Taiwan**
Master of Science of Graduate Institute of Communication Engineering
- Supervised by Prof. Pei-Yuan Wu
- Thesis : **Compressive Privacy Generative Adversarial Network**
  - My master thesis aims to solve the privacy issue raised by the machine learning model. Toward this end, we 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 retains enough utility information to be applied on supervised learning task.

Sep. 2017 – Jul. 2013 | **Da-Yeh University, Changhua, Taiwan**
Bachelor of Science of Electrical Engineering
- Strong communication system background
- Admission based on sports recommendation
- 160 thousand scholarship for high score of the General Scholastic Ability Test.

Languages

- Chinese
- English (TOEIC 840)

Characteristics

- Passionate and optimistic
- Self-motivation and strong research ability
- Innovative

Projects

Model Compression — Mar. 2020 - now
github.com/bwtseng/Model-Compression
Structure Pruning, Model Quantization, Neural Architecture Search, Lottery Ticket Hypothesis
Object detection | Classification

Privacy Preserving Machine Learning — Jan. 2018 - May. 2019
github.com/bwtseng/Compressive-Privacy-Generative-Adversarial-Network
Compressive Privacy, Kernel Method, Differential Privacy, Homomorphic Encryption, Convex Optimization
Privacy Preserving Machine Learning | CPGAN

Few-Shot Learning on Cifar100 dataset — Apr. 2018 - Jun. 2018
github.com/bwtseng/DLCV2018SPRING/blob/master/Final
Implement Siamese Network, Relation Network and **Matching Network**.
3rd prize in the final project competition (sponsored by Microsoft) | Attention | Meta Learning | Few-shot Learning

Image Caption and Chat Bot — Mar. 2018 - Apr. 2018
github.com/bwtseng/MLDS2018SPRING/tree/master/hw2
Implement Seq2seq, attention mechanism, word embedding, MFCC feature processing, Jeiba
Natural Language Processing

Image Generation — Mar. 2018 - Apr. 2018
github.com/bwtseng/DLCV2018SPRING/tree/master/hw4
Implement DCGAN, WGAN, ACGAN, Info GAN and UNIT
GAN-based architecture/algorithm

Reinforcement Learning — Mar. 2018 - Apr. 2018
github.com/bwtseng/MLDS2018SPRING/tree/master/hw4
Implement Policy gradient, Actor-critic, PPO, DDQN, DDPG
Basic RL algorithms

Achievements

2017-2019	Serve as the principal of the Machine Learning and Estimation Theory Lab
2019	Serve as a presenter of the AI poster organized by NTU AI center
2019	Serve as a presenter of CSSP seminar organized by Institute of Information science
2019	3rd place in the basketball competition hold by GICE, NTU
2018	3rd place in the final project competition of the Course ”Deep Learning for Computer Vision”
2015-2017	Da-Yeh school volleyball team

曾柏偉 Scott, 機器學習演算法工程師

https ://bwtseng.github.io/ github.com/bwtseng linkedin.com/in/bo-wei-tseng
(+886)930-983-816 bwtseng1994@gmail.com live8169@gmail.com 新竹市 1994/12/6

我是曾柏偉，畢業於台灣大學電信工程研究所，主要的研究領域是機器學習及資料隱私，包含了差分隱私、同態加密及電腦視覺。碩士期間，我和指導教授吳沛遠博士發表了一篇期刊論文，旨在解決大量機敏性資料應用於機器學習模型訓練時所導致的隱私洩露問題，因此我們採用了最火紅的對抗式學習的優化函式及壓縮網路，以去除資料機敏性的部分，並同時保留足夠的特性使資料能夠應用於監督式學習。目前，我正於晶心科技服務，職稱為機器學習軟體研發工程師，開發輕量化深度學習模型演算法(Model Compression)，主要研究方向為剪枝(Pruning) 及量化(Quantization)，最後再 porting 優化模型至晶心科技處理器運行，其應用包含物件偵測及分類(Computer vision based)。

學術論文

- **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
  隱私維護機器學習 | 資料壓縮 | 生成對抗網路 | 核方法 | 線性最佳化分析

相關技能

編程語言： **Python**, C/C++, JavaScript, Java
深度學習框架： **Pytorch**, Tensorflow/Tensorflow Micro, Keras, Darknet, Caffe
AI 相關經驗： 隱私維護機器學習 , 模型壓縮 , 生成對抗網路 , 小樣本學習 , 強化學習
課程經驗： 主要分為以下三部分
- 人工智慧 -> 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
- 訊號處理 -> 數位訊號處理 , 隨機程序 , 深度學習於電腦視覺
- 理論基礎 -> 線性代數 , 機率與統計 , 核方法 , 最佳化理論

作業系統： MacOs, Windows 10, Linux, Ubuntu
其他技能： Git, SQL, LaTeX

工作經歷

現在 / 2020 年 3 月 | **機器學習軟體研發工程師 , 晶心科技 , 新竹 , 臺灣**
- 開發全自動化的深度學習模型壓縮軟體工具，實現了剪枝及量化演算法
- 轉換不同深度學習框架間的模型，且不損失精度
- 實現物件偵測/分類的模型以及影像前處理演算法
- Porintg 深度學習模型在晶心科技處理器運行，修改開源的 C++ 演算法
- 接觸 RISC-V 架構及指令集

ANDES | 剪枝 | 量化 | 模型框架轉換 | 物件偵測 | 影像辨識 | Python | Pytorch | TensorflowLite Micro | RISC-V

2020 年 3 月 / 2020 年 1 月 | **深度學習研究科學家 , 聯發科技前瞻實驗室 , 台北 , 臺灣**
- 團隊主要由坎伯恩九位博士(MRUK) 及台灣兩位博士(MRTW) 組成
- 與聯發科技合作程式轉換專案(Physical Design)
- 自然語言處理於聯發科電視產品的應用

自然語言處理 | 自然語言理解 | Seq2seq | Amazon Alexa Platform

2019 年 1 月 / 2018 年 9 月 | **教學助理 , 臺灣大學 , 台北 , 臺灣**
- 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

網路攻防實習 | SEED

推薦人

吳沛遠
助理教授 , 台灣大學
peiyuanwu@ntu.edu.tw
+886 905-236-121

孟令三
副總監 , 中光電智能雲服務
sam.meng@coretronic.com

王能謙
資深軟體工程師 , ViewSonic
seark1219@gmail.com
+886 975-252-871

教育背景

2019 年 6 月
2017 年 9 月

電信工程研究所 , 台灣大學 , 台北 , 臺灣

- 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
- 論文摘要 : 機器學習服務(MLaaS) 近年來為我們日常生活帶來了很多便利，事實上這些部署在雲上的機器學習服務造成了嚴重隱私洩露的問題。此篇論文提出了壓縮隱私生成式對抗網路(CPGAN)，這是一個數據驅動化的模型並且運用了正火紅的對抗式學習概念。我們的目標是，在上傳資料至雲端前先經過設計好的非線性壓縮類神經網路(privatizer)，產生的壓縮信號可保留原機敏性數據的可用性且移除侵犯隱私的相關訊息，在此框架下可以提供二階段的隱私保護：原始資料只會保留在本地端、此壓縮信號可以防禦重建攻擊。要評量此壓縮網路的好壞，可以由壓縮隱私生成式對抗網路的分類器來衡量數據可用性，並另外學習一個重建網路(adversary reconstructor) 來衡量隱私保護的程度。我們實驗不同種類的資料集並和過去文獻方法比較，由此證實壓縮隱私生成式對抗網路可以在數據可用性及隱私維護間達到較好的平衡(trade-off)。

2017 年 6 月
2013 年 9 月

電機工程學系 , 大葉大學 , 彰化 , 臺灣

- 體育推薦入學，排球校隊
- 學測成績優良獎學金十六萬元
- 通信系統背景

專案經驗

模型壓縮 (Model Compression) 2020 年 3 月 - 現在

github.com/bwtseng/Model-Compression

結構剪枝 , 模型量化 , 神經網路架構搜索 , 彩票假說

圖像辨識 | 物件偵測

隱私維護機器學習 2018 年 1 月 - 2019 年 5 月

github.com/bwtseng/Compressive-Privacy-Generative-Adversarial-Network

壓縮隱私生成對抗網路 , 核方法分析 , 差分隱私 , 同態加密

資料隱私 | CPGAN

小樣本機器學習在 Cifar100 資料集 2018 年 3 月 - 2018 年 6 月

github.com/bwtseng/DLCV2018SPRING/blob/master/Final

實作 Siamese Network, Relation Network and **Matching Network**.

期末競賽第三名(Sponsored by Microsoft) | Meta Learning | Few-shot Learning | Attention

圖像描述及聊天機器人 2018 年 2 月 - 2018 年 6 月

github.com/bwtseng/MLDS2018SPRING/tree/master/hw2

Implement Seq2seq, attention mechanism, word embedding, MFCC feature processing, Jeiba

Natural Language Processing

圖像生成及風格變換 2018 年 2 月 - 2018 年 6 月

github.com/bwtseng/DLCV2018SPRING/tree/master/hw4

Implement DCGAN, WGAN, ACGAN, Info GAN and UNIT

GAN-based architecture/algorithm

語言

- 中文
- 英文 (多益分數 : 840)

個人特質

- 團隊溝通 , 樂觀積極 , 研究能力
- 自我約束強 , 自我解決問題 , 快速文獻回顧

個人成就

2018-2019 機器學習與估計理論實驗室市長 , DLCV 期末專題競賽(Sponsored by Microsoft) 第三名
2019 中研院 ICCP 會議講者 , 科技部 AI 跨域觀摩交流會講者(台大), 電信所三對三籃球賽第三名
2013-2016 大葉大學排球隊