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 software engineer. His research interest lies in artificial intelligence, privacy preserving machine learning and efficient AI.

Publications

2020 **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

Competences

Programming Language	**Python**, C/C++, JavaScript
Deep Learning Frameworks	**Pytorch**, Tensorflow, Keras, Darknet, TVM
Operating System	Mac OS X, Windows 10, Linux, Ubuntu
Related Courses	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
Machine Learning Knowledge	Privacy Preserving Machine Learning, Generative Adversarial Net, Few-shot Learning, Tiny-ML
Other Skills	Git, SQL, LaTeX

Experience

Now / Mar. 2020 — RD Software Engineer, Andes Tech Inc., Hsinchu, Taiwan
- Optimize deep neural network using with pruning and quantization mechanisms.
- Develop deep learning inference acceleration engine.
- Be familiar with RISC-V architecture.

ANDES | Tiny-ML | Pruning | Quantization | Deep Learning Accelerator | TVM | RISC-V

Mar. 2020 / Jan. 2020 — Research Scientist, Mediatek Research Lab Inc., Taipei, Taiwan
- MRTW is collaborated with MRUK. It's worth mentioning all of the team members in MRUK/MRTW have Ph.D degree (except me) with the research interesting lying in machine learning.
- Collaborate with the Mediatek colleagues on code-conversion, which is related to the pysical design.
- Natural language processing projects on TV applications.

NLU | NLP | Seq2seq | Alexa Platform | Tensorflow-Lite

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 | Leadership

Education

Jun. 2019 / Sep. 2017 — National Taiwan University, Taiepi, Taiwan
Master of Science of Graduate Institute of Communication Engineering (GICE)
- 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 | **Da-Yeh University, Changhua, Taiwan**
Jul. 2013 | Bachelor of Science of Electrical Engineering (EE)
- Sport recommendation enrollment with 160 thousand scholarship for high score (60/75) of the GSAT.

Languages

- Chinese
- English (TOEIC 840)

Forces

- Passion and Optimistic
- Self-motivation
- Innovation

Projets

Model Compression
Mar. 2020 - now

github.com/bwtseng/Model-Compression

Revised version of Intel Distiller. We incorporated more state-of-the-art pruning mechanisms into this framework, including ADMM, channel pruning (FMR), network slimming and compression ratio selection algorithms

Python | C++ | Pytorch | Pruning | Object detection | Classification

Privacy Preserving Machine Learning
Jan. 2018 - May. 2019

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

Code release for our manuscript Compressive Privacy Generative Adversarial Network.

Python | Tensorflow | Reconstruction adversarial Net | Differential Privacy | Kernel Method

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**.

Python | Tensorflow | Attention Network | Meta Learning | Few-shot Learning

Image Caption and Chat Bot
Mar. 2018 - Apr. 2018

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

Develop two models, one is to generate textual description of an image and the other is to simulate the conversation with human users.

Python | Tensorflow | Seq2seq | Attention | Word Embedding | Feature extraction | Jieba

Image Generation
Mar. 2018 - Apr. 2018

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

Develop the model to synthesize the images or transfer the style of original images

Python | Tensorflow | DCGAN | ACGAM | Info GAN | UNIT

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 IIS (Institute of Information science)
2019	Placed on 3rd prize in the basketball competition hold by GICE
2018	Placed on 3rd prize in the final project competition of the Course ”Deep Learning for Computer Vision”
2015-2017	Serve as the vice captain of Da-Yeh school volleyball team

References

Pei-Yuan Wu
Assistant Professor, National Taiwan University
@ peiyuanwu@ntu.edu.tw
+886 905-23-121

Bo-Kai Tseng
RD Process Engineer, Lam Research
@ bokai@gmail.com
+886 935-160-816

曾柏偉

機器學習工程師/研究員

(+886)930-983-816 bwtseng1994@gamil.com 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，職稱為人工智慧軟體研發工程師，開發優化深度學習模型演算法(Model Compression)及深度學習加速引擎(DLA)，並將其應用至Andes嵌入式系統，其應用包括物件偵測及分類。

文獻發表

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

專業技能

- 編程語言: Python, C/C++, JavaScript
- 深度學習框架: Pytorch, Tensorflow, Keras, Darknet, TVM
- 作業系統: MacOS, Windows 10, Linux, Ubuntu
- 課程經驗:
  * AI: 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, 消息理論
  * 理論基礎: 線性代數, 機率與統計, 核方法, 最佳化
- AI領域知識: Privacy Preserving Machine Learning, Generative Adversarial Net, Few-shot Learning, Tiny-ML
- 其他技能: Git, SQL, LaTeX

工作經驗

人工智慧演算法工程師 2020年3月 – 現在

軟體研發處 晶心科技

工作內容:

- 優化類神經網路，包含剪枝及量化技巧
- 開發深度學習推論加速引擎
- 接觸不同深度學習框架(Tensorflow-Lite, ONNX)
- 熟悉RISC-V架構

人工智慧研究員 2020年1月 – 2020年3月

聯發科技前瞻實驗室(MRTW) 聯發科技

工作內容:

- 前瞻實驗室是聯發科的研究單位，單位成員組成來自九位坎伯恩的博士(MRUK)，及台灣兩位博士(MRTW)
- 和聯發科技合作程式碼轉換專案 (Pysical Design)
- 自然語言處裡於電視上的應用

教學助理 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

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
- 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)。

大葉大學電機工程學系 2013年9月 – 2017年6月

- 體育推薦入學，學測成績優良獎學金十六萬元 (60/75)

專案

模型壓縮 (Tiny-ML) Repository 2020年3月 – 現在

模型量化(Quantization)及剪枝(Pruning), AI推論引擎(TVM), RISC-V, 物件偵測

隱私維護機器學習 (PPML) Repository 2018年1月 – 2019年5月

壓縮隱私生成對抗網路 (CPGAN), 核方法分析(KDCA), 差分隱私, 同態加密

小樣本機器學習 Repository 2018年3月 – 2018年6月

Siamese Network, Matching Network, Relation Network, Meta Learning

圖像描述及聊天機器人 Repository 2018年3月 – 2018年6月

Seq2seq, Attention, Word Embedding, 語音訊號處理, 中文斷詞

圖像生成及風格變換 Repository 2018年3月 – 2018年6月

GAN-based, DCGAN, ACGAN, Info GAN, UNIT

語言能力

- 英文: TOEIC 840
- 中文: 母語

個人特質

- 團隊溝通, 樂觀
- 自發性, 快速文獻回顧, 自我解決問題

個人成就

- 機器學習與估計理論實驗室市長 2018年1月 – 2019年6月
- 中研院ICCP會議講者 2019年4月
- 科技部AI跨域觀摩交流會講者(台大) 2019年4月
- 3^{rd} prize, 電信工程研究所三對三籃球賽 2019年4月
- 3^{rd} prize, DLCV期末專題競賽(Sponsored by Microsoft) 2018年6月
- 大葉大學排球隊副隊長 2015年7月 – 2017年1月