CHIN-YUAN YEH

marrch30@gmail.com ⋄ Google Scholar

EDUCATION

Doctor of Philosophy, National Taiwan University (Major in Data Science)	2020 - Present
Master of Science, National Taiwan University (Major in Data Science)	2018 - 2020
Bachelor of Science, National Taiwan University (Major in Physics)	2013 - 2017

PUBLICATIONS

- "Does Audio Deepfake Detection Rely on Artifacts?" T.-H. Shih, **C.-Y. Yeh**, & M.-S. Chen, *ICASSP (2024)*.
- "FedGCR: Achieving Performance and Fairness for Federated Learning with Distinct Client Types via Group Customization and Reweighting," S.-L. Cheng, **C.-Y. Yeh**, T.-A. Chen, E. Pastor & M.-S. Chen, *AAAI (2024)*.
- "Planning Data Poisoning Attacks on Heterogeneous Recommender Systems in a Multiplayer Setting," **Chin-Yuan Yeh**, H.-W. Chen, D.-N. Yang, W.-C. Lee, P. S. Yu, & M.-S. Chen, *ICDE (2023)*.
- "Attack as the Best Defense: Nullifying Image-to-image Translation GANs via Limit-aware Adversarial Attack," **Chin-Yuan Yeh**, H.-W. Chen, H.-H. Shuai, D.-N. Yang, & M.-S. Chen, *ICCV (2021)*.
- "Disrupting Image-Translation-Based DeepFake Algorithms with Adversarial Attacks," **Chin-Yuan Yeh**, H.-W. Chen, S.-L. Tsai, & S.-D. Wang, *WACVW (2020)*.

SKILLS

Technical Skills	Python, Pytorch, Bash scripts in Unix Systems; Academic Writing

RESEARCH SUMMARY

Equilibrium-Based Pricing and Purchasing Recommendation for NFT Projects with Breeding. (Paper under submission.)

Research Assistant, National Taiwan University May 2023 - April 2024

- First to solve dual Pricing and Purchasing Recommendation problems based on equilibrium market analysis.
- Developed Breeding-aware NFT Equilibrium Recommendation (BANTER) to simultaneously address diverse buyer preferences and budgets, NFT trait rarity encoded by the traist system, and NFT breeding mechanisms.
- Analyzed three breeding mechanisms (Homogeneous, Child-project, and Heterogeneous Breeding) and introduced acceleration techniques, including optimal parental pair selection (OPPS) and heterogeneous parental set selection (HPSS) for faster convergence to equilibrium.
- Tested on five real-world NFT datasets, achieving higher revenue for the seller and greater average utility for buyers with low run-time across all scenarios.

Does Audio Deepfake Detection Rely on Artifacts? (Presented at ICASSP 2024.)

Research Assistant, National Taiwan University July - September 2023

- Introduced BEAR protocol for balanced artifact/noise conditions in audio deepfake detection tests.
- Created "White-BEAR" and "Gray-BEAR" evaluation protocols which add deepfake-specific artifacts to genuine samples by constructing "self-deepfakes," and Gaussian noise to both genuine and forged samples, respectively.
- Significant detection challenges in models were observed under these conditions, highlighting the dependence on artifacts for current audio deepfake detection technologies.

FedGCR: Achieving Performance and Fairness for Federated Learning with Distinct Client Types via Group Customization and Reweighting (Presented at AAAI 2024)

Research Assistant, National Taiwan University May - July 2023

- Initiated research on Federated Learning tailored to distinct client types, encompassing groups with homogenous characteristics within each group.
- Implemented Vision Transformers using learnable prompts to enhance performance across diverse domains.
- Developed a novel anonymized clustering technique to identify client groups and employed a reweighting algorithm to ensure fairness among them.

Planning Data Poisoning Attacks on Heterogeneous Recommender Systems in a Multiplayer Setting. (Presented at ICDE 2023.)

Research Assistant, National Taiwan University September 2021 - October 2022

- First to address multi-attacker scenario on data poisoning against Recommender Systems (RecSys).
- Developed Multilevel Stackelberg Optimization over Progressive Differentiable Surrogate (MSOPDS), a data poisoning technique against heterogeneous RecSys that assists the first attacker against subsequent attackers.
- Leveraged Stackelberg game analysis between the first attacker (as leader) and subsequent attackers' (as followers) to obtain the optimal data poisoning strategy for the first attacker based on Stackelberg equilibrium.
- Developed a surrogate GNN-based RecSys model that separately incorporates poison edges and ratings into the graph convolution process and the training loss, respectively, for gradient derivation.

Attack as the Best Defense: Nullifying Image-to-image Translation GANs via Limit-aware Adversarial Attack. (Presented at ICCV 2021.)

Graduate Research Assistant, Academia Sinica *May 2020 - March 2021*

- Developed Limit-Aware Self-Guiding Gradient Sliding Attack (LaSGSA), the first query-based black-box norm-bounded adversarial attack against Img2Img GANs.
- Enhanced attack efficiency using norm-bound acceleration techniques including: Limit-aware RGF, which restricts random query sampling within the ϵ-limit, and the gradient sliding mechanism that allows perturbations to extend its step along the limit boundary.
- Developed the *self-guiding prior*, a constant-time operation for gradient approximation, based on the diagonality of the Jacobian matrix of Img2Img GANs due to the semantic consistency of Img2Img translations.
- Demonstrated superior attack success rates with fewer queries compared to existing methods.

Disrupting Image-Translation-Based DeepFake Algorithms with Adversarial Attacks. (Presented at WACV 2020 DeepPAB Workshop)

Research Assistant, National Taiwan University August 2019 - January 2020

- Pioneered adversarial attacks against image translation GANs such as CycleGAN, pix2pix, and pix2pixHD, addressing deepfake technologies.
- Developed two distinct attack strategies: *Nullifying Attack* to minimizes deepfake modification on target images, and *Distorting Attack* to maximized distortion on deepfake outputs.
- Defined quantitative evaluation scores and conducted sensitivity tests over different loss function designs, case studies of robustness over repeated inference, and ensembled attack against multiple deepfake models.

PROFESSIONAL EXPERIENCE

AI Engineer Taiwan AI Academy October 2021 - August 2022

- Developed and delivered educational presentations on advanced AI topics, including graph embedding algorithms, graph neural networks and adversarial robustness.
- Conducted lectures on the fundamentals of operating cloud-based machine learning systems, enhancing attendees' practical skills in online AI resources and tools.
- Assisted in organizing artificial intelligence summer camps for high school and college students as a team leader.