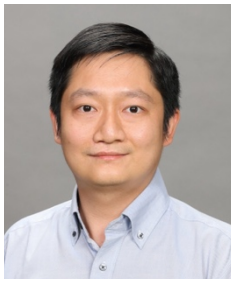
Huy H. Nguyen (Nguyễn Hồng Huy)



***Address**: National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda City, Tokyo, Japan*
***Cell**: +81 70 4478 4325* ***Homepage**: https://honghuy127.github.io*
***Email**: nhhuy@nii.ac.jp honghuy127@gmail.com*
***Nationality**: Vietnamese*

RESEARCH INTERESTS

Machine Learning and Deep Learning, Computer Vision, NLP, Security and Privacy.

EDUCATION

2016 – 2022 **The Graduate University for Advanced Studies, SOKENDAI, Japan**
School of Multidisciplinary Sciences, Department of Informatics
Doctor of Philosophy

2009 – 2013 **VNUHCM - University of Science, Vietnam**
Faculty of Information Technology
Bachelor of Science – Honors Program

RESEARCH EXPERIENCES

2022 – Current **National Institute of Informatics (NII), Japan**
Specially Appointed Assistant Professor (Since Nov. 2022)
Project Postdoctoral Researcher (Apr. – Oct. 2022)
Research projects: JST-ANR VoicePersonae, JST CREST FakeMedia.
Topics: Security for AI and AI for security.

2016 – 2022 **The Graduate University for Advanced Studies, SOKENDAI, Japan**
Ph.D. Student - *Echizen Lab and the Global Research Center for Synthetic Media, NII, Japan*
Advisors: *Prof. Junichi Yamagishi and Prof. Isao Echizen*
Research projects: JSPS Kakenhi (S) Media Clones, JST-ANR VoicePersonae, JST CREST FakeMedia.

Oct. 2019 – Feb. 2020 **Idiap Research Institute, Switzerland (Internship)**
Biometrics Security and Privacy (BSP) group – Advisor: Dr. Sébastien Marcel
Research project: Deep master faces (IJCB 2020 & IEEE T-BIOM 2022)

Feb. – Aug. 2015 **National Institute of Informatics, Japan (Internship)**
Echizen Laboratory – Advisor: Prof. Isao Echizen
Topic: Image spoofing attack detection (IWDW 2015).

2013 **Bachelor Thesis** – *Advisor: Prof. Thuc D. Nguyen*
Applied sequence alignment in virus detection and classification.
Topic: Apply biological sequence alignment to detect and classify computer virus.
Result: Excellent

Jul. – Oct. 2012 **Pohang University of Science and Technology, South Korea (Internship)**
Member of High Performing Computing Laboratory – Advised by Prof. Jong Kim
Topic: Coding guidelines for secure, reliable, and fault-tolerant Java applications.

TEACHING & INDUSTRIAL EXPERIENCES

July 1 – Nov 18, 2020 **Amazon.com, Inc ("Virtual" Summer internship)**
Amazon Selection and Catalog Systems (ASCS) team
Project: Session analyzer - A toolset to assist AutoML session debugging

Updated: Apr.11, 2024

Sep. 13 – Jun. 16 **Department of Knowledge Engineering, Faculty of Information Technology, VNUHCM - University of Science, Vietnam**
Teaching Assistant – Data Structures and Algorithms, Networks Security Techniques, Computer Architecture and Assembly Language, Computer Vision.

Jul. 13 – Feb. 15 **Universal Technology Services Corporation, Vietnam**
OPSWAT Metascan Splunk app, VoxyPAD, R&D

AWARDS

Research papers & poster:

- **BTAS/IJCB 5-Year Highest Impact Award**: H. H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos," *International Conference on Biometrics: Theory, Applications and Systems (BTAS) 2019* (2023).
- **Excellent paper award: 3** journal papers by the Institute of Electronics, Information and Communication Engineers (IEICE), Japan (2022).
- **Ph.D Forum Best Poster Award:** H. H. Nguyen, J. Yamagishi, and I. Echizen, "Real or Fake Images: Attacking and Reinforcing the Machine Learning Systems," *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 2018.
- **Best Paper Award**: T. N.-D. Tieu, H. H. Nguyen, H. Nguyen-Son, J. Yamagishi, and I. Echizen, "An approach for gait anonymization using deep learning," *IEEE Workshop on Information Forensics and Security (WIFS*), 2017.

Academic activities:

- **Telecom Interdisciplinary Research Award** by the Telecommunication Advancement Foundation, Japan (2023).
- **Best Student Award** awarded by the National Institute of Informatics, Japan (2022).

Competitions:

- **Consolation prize** in Student with Information Security 2012 Contest in South Region, organized by Vietnam Information Security Associate (VNISA) (http://vnisa.org.vn/).
- **Consolation prize** in Snatching the H@t, a security contest organized by IDG at the 4th CSO ASEAN AWARDS 2012, Vietnam (http://cso.org.vn/contest/).

SCIENTIFIC CONTRIBUTIONS

Reviewer:

- Conferences: NeurIPS, ICLR, ICML, CVPR, ECCV, WACV, ICME, ACL RR, APSIPA ASC.
- Journal: IEEE (Access, TIP, TIFS), IEEE/CAA JAS, ACM TOMM, Elsevier (PRLETTERS, EAAI), EURASIP JIVP, IEICE.

Session chair:

- APSIPA ASC 2023 Special Session: Multimedia Security and Privacy in the Age of Deep Learning
- APSIPA ASC 2020 Special Session: Deep Generative Models for Media Clones and Its Detection.

SELECTED PUBLICATIONS

Full version: https://scholar.google.com/citations?user=8q1km_cAAAAJ&hl=en

Journal Papers

1. H. Felouat, **H. H. Nguyen**, T.-N. Le, J. Yamagishi, and I. Echizen, "eKYC-DF: A Large-Scale Deepfake Dataset for Developing and Evaluating eKYC Systems," IEEE Access (2024).

2. K.-D. Nguyen, **H. H. Nguyen**, T.-N. Le, J. Yamagishi, and I. Echizen, "Analysis of Fine-Grained Counting Methods for Masked Face Counting: A Comparative Study," IEEE Access (2024).
3. C. C. Chang, **H. H. Nguyen**, J. Yamagishi, and I. Echizen. "Cyber Vaccine for Deepfake Immunity," IEEE Access (2023).
4. **H. H. Nguyen**, S. Marcel, J. Yamagishi, and I. Echizen, "Master Face Attacks on Face Recognition Systems," IEEE Transactions on Biometrics, Behavior, and Identity Science (2022).
5. **H. H. Nguyen**, M. Kuribayashi, J. Yamagishi, and I. Echizen, "Effects of Image Processing Operations on Adversarial Noise and Their Use in Detecting and Correcting Adversarial Images," IEICE Transactions on Information and Systems (2022). [Best paper award]
6. N. Babaguchi, I. Echizen, J. Yamagishi, N. Nitta, Y. Nakashima, K. Nakamura, K. Kono, F. Fang, S. Myojin, Z. Kuang, **H. H. Nguyen**, N. T. Tieu, "Preventing Fake Information Generation Against Media Clone Attacks," IEICE Transactions on Information and Systems (2021). [Best paper award]
7. I. Echizen, N. Babaguchi, J. Yamagishi, N. Nitta, Y. Nakashima, K. Nakamura, K. Kono, F. Fang, S. Myojin, Z. Kuang, **H. H. Nguyen**, N. T. Tieu, "Generation and detection of Media Clones," IEICE Transactions on Information and Systems (2021). [Best paper award]

Conference Papers

1. F. B. Baldassini, **H. H. Nguyen**, C. C. Chang, and I. Echizen, "Cross-Attention Watermarking of Large Language Models," International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2024.
2. F. Shalabi, H. Felouat, **H. H. Nguyen**, and I. Echizen, "Leveraging Chat-Based Large Vision-Language Models for Multimodal Out-of-Context Detection," International Conference on Advanced Information Networking and Applications (AINA), 2024.
3. Z. Dou, Y. Guo, **H. H. Nguyen**, C. C. Chang, and I. Echizen, "Enhancing Robustness of LLM-Synthetic Text Detectors for Academic Writing: A Comprehensive Analysis," International Conference on Advanced Information Networking and Applications (AINA), 2024.
4. F. Shalabi*, **H. H. Nguyen***, H. Felouat, C. C. Chang, and I. Echizen, "Image-Text Out-Of-Context Detection Using Synthetic Multimodal Misinformation," Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2023.
5. M. Niu, Z. Li, Y. Zhan, **H. H. Nguyen**, I. Echizen, and Y. Zheng, "Physics-Based Adversarial Attack on Near-Infrared Human Detector for Nighttime Surveillance Camera Systems," ACM Multimedia (MM) 2023.
6. **H. H. Nguyen**, J. Yamagishi, and I. Echizen, "How Close are Other Computer Vision Tasks to Deepfake Detection?" International Joint Conference on Biometrics (IJCB) 2023, 229-238.
7. **H. H. Nguyen**, T. N. Le, J. Yamagishi, and I. Echizen, "Analysis of Master Vein Attacks on Finger Vein Recognition Systems," Winter Conference on Applications of Computer Vision (WACV) 2023.
8. F. Waseda, S. Nishikawa, T. N. Le, **H. H. Nguyen**, and I. Echizen, "Closer Look at the Transferability of Adversarial Examples: How They Fool Different Models Differently," Winter Conference on Applications of Computer Vision (WACV) 2023.
9. T. N. Le*, T. Gu*, **H. H. Nguyen***, and I. Echizen, "Rethinking Adversarial Examples for Location Privacy Protection," International Workshop on Information Forensics and Security (WIFS) 2022.
10. M. Treu*, T. N. Le*, **H. H. Nguyen***, J. Yamagishi, and I. Echizen, "Fashion-Guided Adversarial Attack on Person Segmentation," Conference on Computer Vision and Pattern Recognition Workshop (CVPR-W) 2021.
11. T. N. Le, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, "OpenForensics: Large-Scale Challenging Dataset for Multi-Face Forgery Detection and Segmentation In-The-Wild," International Conference on Computer Vision (ICCV) 2021. [35 citations]
12. S. Gupta, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, "Viable Threat on News Reading: Generating Biased News Using Natural Language Models", NLP+CSS workshop at Empirical Methods in Natural Language Processing (EMNLP) 2020.
13. R. Huang, F. Fang, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, "Security of Facial Forensics Models Against Adversarial Attacks," International Conference on Image Processing (ICIP) 2020.

Updated: Apr.11, 2024

14. D. I. Adelani, H. Mai, F. Fang, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, “Generating Sentiment-Preserving Fake Online Reviews Using Neural Language Models and Their Human- and Machine-based Detection,” International Conference on Advanced Information Networking and Applications (AINA) 2020. [129 citations]
15. **H. H. Nguyen**, J. Yamagishi, I. Echizen, and S. Marcel, “Generating Master Faces for Use in Performing Wolf Attacks on Face Recognition Systems,” International Joint Conference on Biometrics (IJCB) 2020. [27 citations]
16. **H. H. Nguyen**, F. Fang, J. Yamagishi, and I. Echizen, “Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos,” International Conference on Biometrics: Theory, Applications and Systems (BTAS) 2019. [BTAS/IJCB 5-Year Highest Impact Award , 455 citations]
17. **H. H. Nguyen**, J. Yamagishi, and I. Echizen, “Capsule-Forensics: Using Capsule Networks to Detect Forged Images and Videos,” International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 2019. [580 citations]
18. **H. H. Nguyen**, T. N.-D. Tieu, H.-Q. Nguyen-Son, V. Nozick, J. Yamagishi, and I. Echizen, “Modular Convolutional Neural Network for Discriminating between Computer-Generated Images and Photographic Images,” International Conference on Availability, Reliability and Security (ARES) 2018. [64 citations]
19. **H. H. Nguyen**, T. N.-D. Tieu, H.-Q. Nguyen-Son, J. Yamagishi, and I. Echizen, “Transformation on Computer-Generated Facial Image to Avoid Detection by Spoofing Detector,” International Conference on Multimedia and Expo (ICME) 2018.
20. T. N.-D. Tieu, **H. H. Nguyen**, H. Nguyen-Son, J. Yamagishi, and I. Echizen, “An Approach for Gait Anonymization using Deep Learning,” International Workshop on Information Forensics and Security (WIFS) 2017 [Best Paper Award].

Book Chapter

1. **H. H. Nguyen**, J. Yamagishi, and I. Echizen, “Capsule-Forensics Networks for Deepfake Detection,” Handbook of Digital Face Manipulation and Detection – From DeepFakes to Morphing Attacks (2022).
2. R. Tolosana, C. Rathgeb, R. Vera-Rodriguez, C. Busch, L, Verdoliva, S. Lyu, **H. H. Nguyen**, J. Yamagishi, I. Echizen, P. Rot et al. “Future Trends in Digital Face Manipulation and Detection.” Handbook of Digital Face Manipulation and Detection – From DeepFakes to Morphing Attacks (2022).
3. T. N. Le, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, “Robust Deepfake on Unrestricted Media: Generation and Detection,” Frontiers in Fake Media Generation and Detection (2022).
4. 越前功, 馬場口登, 笹原和俊, Trung-Nghia Le, **Huy H. Nguyen**, 山岸順一, Canasai Kruengkrai, 中島悠太, 李良知, 王博文, 宮崎邦洋, 小林正啓, “インフォデミック時代の AI とサイバーセキュリティ”, 映像情報メディア学会誌（2022）[Telecom Interdisciplinary Research Award].

Updated: Apr.11, 2024