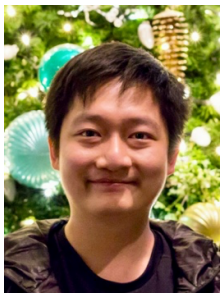
Huy H. Nguyen (Nguyễn Hồng Huy)

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



RESEARCH INTEREST

Image and Video Processing, Machine Learning and Deep Learning, Security and Privacy.

EDUCATION

2016 – Current **The Graduate University for Advanced Studies, SOKENDAI, Japan**
School of Multidisciplinary Sciences
Department of Informatics (Associated with the National Institute of Informatics, Japan)
5-Year Doctoral Program

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

RESEARCH EXPERIENCE

2016 – Current **The Graduate University for Advanced Studies, SOKENDAI, Japan**
Associated with the **National Institute of Informatics, Japan**
Member of Echizen Laboratory and the Global Research Center for Synthetic Media, National Institute of Informatics, Japan
Advised by Prof. Junichi Yamagishi and Prof. Isao Echizen
Research projects: Communication System for Defending against Attacks of Media Clones, JST-ANR VoicePersonae Project, CREST FakeMedia Project.

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

Oct. 10, 2019 – Feb 07, 2020 **Idiap Research Institute, Switzerland (Internship)**
Member of the Biometrics Security and Privacy (BSP) group – Advised by Dr. Sébastien Marcel
Research project: Deep Master Face (A publication in IJCB 2020 proceeding)

Feb. – Aug. 2015 **National Institute of Informatics, Japan (Internship)**
Member of Echizen Laboratory– Advised by Prof. Isao Echizen
Topic: Detecting spoofing attacks on images (A publication in IWDW 2015 proceeding).

2013 **Bachelor Thesis** – *Advised by Prof. Thuc D. Nguyen*
Applied sequence alignment in virus detection and classification.
Topic: Studying about computer virus, biological sequence alignment and applying this method 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: Gathering coding guidelines, requirements, international standards, and testing methods to build secure, reliable and fault-tolerant Java applications, especially in financial aspect.

WORK EXPERIENCE

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

- **National Institute of Informatics Best Student Award** (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," *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*.
- **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," *2017 IEEE Workshop on Information Forensics and Security (WIFS*).
- **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 (http://cso.org.vn/contest/).

SCIENTIFIC CONTRIBUTIONS

- Reviewer: APSIPA, ICME, WACV; IEEE Access, IEEE TIFS, IEEE/CAA JAS.
- Sub-reviewer: IWDW, APSIPA, IFIP SEC.
- APSIPA 2020 Special Session Chair: Deep Generative Models for Media Clones and Its Detection.

PUBLICATIONS

1. **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)*.
2. **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)*.
3. 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)*.
4. 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)*.
5. 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*.
6. 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 (CVPRW) 2021.*
7. D.K. Nguyen, T. N. Le, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, "Effectiveness of Detection-based and Regression-based Approaches for Estimating Mask-Wearing Ratio," *Workshop on Face and Gesture Analysis for COVID-19 2021*.
8. Y. Yamasaki, M. Kuribayashi, N. Funabiki, **H. H. Nguyen**, I. Echizen, "Feature Extraction Based on Denoising AutoEncoder for Classification of Adversarial Examples," *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2021*.

9. 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)*.
10. 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," *IEICE Transactions on Information and Systems (2021)*.
11. T.L. Do, M.K. Tran, **H. H. Nguyen**, M.T. Tran, "Potential Threat of Face Swapping to eKYC with Face Registration and Augmented Solution with DeepFake Detection," *International Conference on Future Data and Security Engineering (FDSE) 2021*.
12. R. Huang, F. Fang, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, "A Method for Identifying Origin of Digital Images Using a Convolution Neural Network," *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2020*.
13. A. Higashi, M. Kuribayashi, N. Funabiki, **H. H. Nguyen**, and I. Echizen, "Detection of Adversarial Examples Based on Sensitivities to Noise Removal Filter," *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2020*.
14. 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*.
15. 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*.
16. 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*.
17. **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*.
18. **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*.
19. N.-D. Tieu, **H. H. Nguyen**, F. Fang, J. Yamagishi, and I. Echizen, "An RGB Gait Anonymization Model for Low Quality Silhouette," *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2019*.
20. N.-D. Tieu, **H. H. Nguyen**, H.-Q. Nguyen-Son, J. Yamagishi, and I. Echizen, "Spatio-temporal generative adversarial network for gait anonymization," *Journal of Information Security and Applications (2019).*
21. **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*.
22. H.-Q. Nguyen-Son, **H. H. Nguyen**, N.-D. Tieu, J. Yamagishi, and I. Echizen, "Identifying Computer-Translated Paragraphs using Coherence Features," *Pacific Asia Conference on Language, Information and Computation (PACLIC) 2018*.
23. **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*.
24. **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 **[Top 15% papers]**.

25. T. N.-D. Tieu, **H. H. Nguyen**, H. Nguyen-Son, J. Yamagishi, and I. Echizen, "An Approach for Gait Anonymization using Deep Learning," Proc. of the *9th IEEE International Workshop on Information Forensics and Security (WIFS) 2017* **[Best Paper Award]**.

26. H.-Q. Nguyen-Son, N.-D. Tieu, **H. H. Nguyen**, J. Yamagishi, and I. Echizen, "Identifying computer-generated text using statistical analysis," Proc. of the *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2017*.

27. **H. H. Nguyen**, H. Nguyen-Son, and I. Echizen, "Discriminating between computer-generated facial images and natural ones using smoothness property and local entropy," *International Workshop on Digital Watermarking (IWDW) 2015*.

28. H. Nguyen, **H. H. Nguyen**, T. Hoang, D. Choi, and T. D. Nguyen, "A Generalized Authentication Scheme for Mobile Phones Using Gait Signals", *International Conference on E-Business and Telecommunications 2015*.