Selective Fuzzy Ensemble Learner for Cognitive Detection of Bio-identifiable Modality Spoofing in MCPS

Nishat Mowla*, Inshil Doh**, KiJoon Chae*

Department of Computer Science and Engineering, Ewha Womans University, Seoul, Korea
Department of Cyber Security, Ewha Womans University, Seoul, Korea
nishat.i.mowla@gmail.com, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

Abstract— **Biometric features are widely used for user authentication and equally important to national and global technology systems. Various forms of biometric features, such as face, iris, fingerprint, are commonly used while more recently palm, vein and gait are also getting attention. Simultaneously various spoofing approaches have also been developed over time, which are capable of failing traditional biometric detection systems. Image synthesis with play-doh, gelatin, ecoflex etc. are some of the ways used in spoofing bio-identifiable property. Success of traditional detection systems are related to custom tailored solutions where feature engineering for each attack type must be developed. This is not a feasible process when we consider countless attack possibilities. Also, a slight change in the attack can cause the whole system to be redesigned and therefore becomes a limiting constraint. The recent success of machine learning inspires this paper to explore weak and strong learners with ensemble learning approaches using AdaBoost. Therefore, the paper proposes a selective ensemble fuzzy learner approach using Ada Boost, feature selection and combination of weak and strong learners to enhance the detection of bio-identifiable modality spoofing. Our proposal is verified on real dataset, LiveDet 2015, with a focus on fingerprint modality spoofing detection that can be used for authentication in Medical Cyber Physical Systems (MCPS).**

Keyword— **MCPS, Biometric spoofing, Spoofing Detection, Ensemble Learning, Feature selection.**

Nishat Mowla received the B.S degree in Computer Science from Asian University for Women, Chittagong, Bangladesh in 2013, an M.S. degree in Computer Science and Engineering from Ewha Womans University, Seoul, Korea in 2016. She is currently a PhD student at Ewha Womans University, Seoul, Korea. Her research interests include next generation network security, IoT network security and network traffic analysis.

Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995-1998, she worked in Samsung SDS of Korea to develop a marketing system. She was a research professor of Ewha Womans University in 2009~2010 and of Sungkyunkwan University in 2011. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. Her research interests include wireless network, sensor network security, and M2M network security.

Prof. Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990. He is currently a professor in Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include sensor network, smart grid, CDN, SDN and IoT, network protocol design and performance evaluation.