Department of Management and Information Sciences

Department of Management and Information Sciences	Key words	Multimedia Processing, Artificial Intelligence, Trusted Communication, Machine Learning

Ph.D. Eng. / Professor

Noboru Babaguchi

Education

Noboru Babaguchi received the B.E., M.E. and Ph.D. degrees in communication engineering from Osaka University, in 1979, 1981 and 1984, respectively.

Professional Background

He was Research Associate of Ehime University, Research Associate and Assistant Professor of Department of Engineering, Osaka University, Associate Professor of ISIR, Professor and Dean of Graduate School of Engineering, Osaka University. He is now Professor Emeritus of Osaka University.

Consultations, Lectures, and Collaborative Research Themes

Intelligent media technologies: AI based multimedia generation and recognition, Visual privacy protection, General topics on multimedia processing

e-mail address

babaguchi@fukui-ut.ac.jp

Main research themes and their characteristics

「Communication System for Defending against Attacks of Media Clones」

Distribution of non-authentic (fake) media has become a potential threat in our daily life. Its typical example is a fraud by voice impersonation of family members or friends. It is therefore of great importance to protect the receivers of such non-authentic but skillfully fabricated replicas of authentic media, called media clones, by means of media processing technologies towards safe and reliable society. The purpose of this research project is to realize a trusted communication system that can defend against attacks of media clones. As an example of our research results, Fig.1 shows a framework of generating a clone of facial image sequences with synchronized voices. This work was supported in part by JSPS KAKENHI Grant-in-Aid for Scientific Research (S).

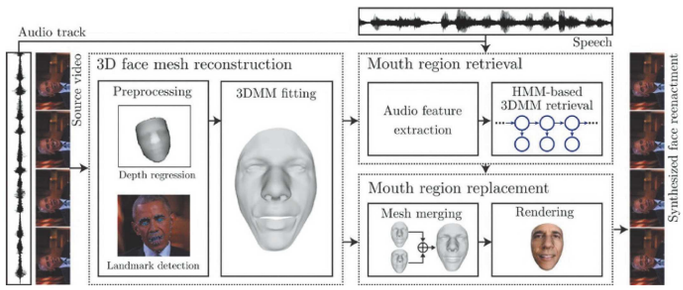

Fig.1 Framework of generating a clone of facial image sequences with synchronized voices

「Social Information Technologies to Counter Infodemics」

The purpose of this research project is to deal appropriately with the potential threats posed by FM generated by AI and, at the same time, to establish social information technologies that support diverse means of communication and decision-making. This technology should be able to detect and prevent advanced attacks based on FM of various modalities such as fake video, fake voice data, and fake documentation generated by AI as well as detect various types of highly reliable media. Incorporating these technologies into a cyber society will promote human decision-making and consensus building and lead to the establishment of social information infrastructure technologies that enhance cyberspace security.

Fig.2 is a conceptual sketch of this project. Recently, the MEXT has decided a strategic objective of "Trusted AI" and the JST/CREST research area named "Core technologies for trusted quality AI systems" has launched. This theme is being conducted as a part of the area and a collaborative project with National Institute of Informatics and Tokyo Institute of Technology.

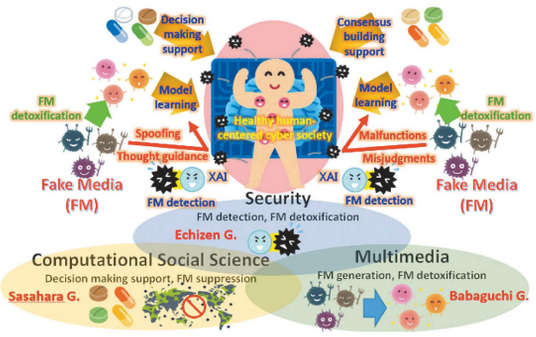

Fig.2 Conceptual sketch of this project

Major academic publications

M. Khosravy, K. Nakamura, Y. Hirose, N. Nitta, and N. Babaguchi: "Model Inversion Attack by Integration of Deep Generative Models Privacy-Sensitive Face Generation from a Face Recognition System", IEEE Transactions on Information Forensics and Security, Vol. 17, pp. 357-372, Jan 2022.

N. Babaguchi, et al.: "Preventing Fake Information Generation Against Media Clone Attacks", IEICE Transactions on Information and Systems, vol. E104-D, no.1, pp. 2-11, January 2021.

N. Babaguchi and S. Yamada, "Fundamentals of Artificial Intelligence (2nd Edition)" , Ohm-sha, 2015 (in Japanese).