【Grant-in-Aid for Scientific Research (S)】

Integrated Disciplines (Informatics)

Title of Project : Communication System for Defending against Attacks of Media Clones

Noboru Babaguchi
(Osaka University, Graduate School of Engineering, Professor)

Research Project Number : 16H06302 Researcher Number : 30156541
Research Area : Human informatics, Perceptual information processing
Keyword : Visual Media Processing, Speech Information Processing, Privacy Protection

【Purpose and Background of the Research】

Distribution of non-authentic 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 communication system that can defend against attacks of media clones.

【Research Methods】

Figure 1 shows a framework of this research. A sender Alice sends her authentic media such as video or audio to a receiver Bob through physical and cyber channels. At this time, a malicious sender Eve stealthily acquires privacy, biological, and environmental information of Alice, to make fake information. Based on the fake information, she generates Alice's media clones and sends them to Bob to deceive him.

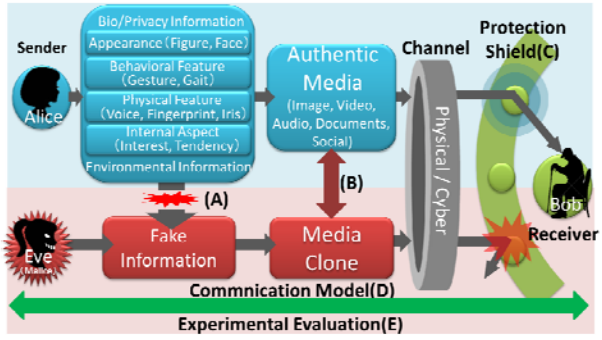

Figure 1 Framework of this research.

To realize a communication system for defending the receivers attacked by the media clones, we pursue the following five topics. (A) Development of methods for protecting the privacy, biological, and environmental information to prevent fake information generation. (B) Verification of the capability of generating various types of media clones such as audio, visual, text, and social media derived from the fake information. (C) Realization of a protection shield for media clones' attacks by recognizing them. We focus on analysis of liveness resulting from biological living features. (D) Modeling of the proposed communication system. (E) Experimental evaluation for a total system and its components. We build benchmark databases of both authentic media and media clones, and open them to the public.

【Expected Research Achievements and Scientific Significance】

This research will realize a safe, reliable, and easy-to-use means of communication even for the aged and infirm. The technologies for generating and recognizing media clones can lead to production of media beyond time, space, and culture, to novel innovations in diverse areas such as media art and medical welfare engineering, and to a paradigm shift in recognizing subtle difference and qualitative change that support the authenticity in media expression. The research is further expected to contribute to the data and open science by systematic collection of diverse media data, as well as to creation of a new academic field that lies in the boundary of media processing, security, and communication.

【Publications Relevant to the Project】

・Y. Nakashima, T. Ikeno, and N. Babaguchi: "Evaluating Protection Capability for Visual Privacy Information," IEEE Security & Privacy, Vol. 14, No. 1, pp. 55-61, 2016.
・N. Babaguchi and Y. Nakashima: "Protection and Utilization of Privacy Information via Sensing," Invited Paper, IEICE Transactions on Information and Systems, Vol. E98-D, No. 1, pp. 2-9, 2015.

【Term of Project】 FY2016-2020
【Budget Allocation】 120,700 Thousand Yen
【Homepage Address and Other Contact Information】
http://www2c.comm.eng.osaka-u.ac.jp/proj/mc/index.html