Cyber-Physical Integrated Analysis Technology for Criminal Investigation Support

TANI Masahiro

Abstract

Cyberspace is the new frontier and like any frontier it is plagued by lawlessness. Criminals of all types from teenage pranksters to organized crime and even terrorists roam the virtual spaces of the online world wreaking havoc on individuals, businesses and governments alike. The problem is one that cannot be ignored and requires immediate attention from law enforcement entities around the world. What makes cybercrime especially intractable is that it can be extraordinarily difficult to identify the individuals and groups perpetrating these crimes — particularly since they can be located anywhere in the world and may be launching attacks using servers that are located in yet another jurisdiction. Developing simple countermeasures is no easy task, taking proactive measures is even more difficult. In this paper, we take a look at one of NEC's current projects aimed at dealing with this problem, which involves building a system that can perform integrated analysis by extracting information useful for criminal investigations from the massive amount of data in cyberspace and applying biometrics including face recognition and object recognition technologies, as well as various analysis technologies.

Keywords

public safety, security, cyberspace, cyber-physical integrated analysis, biometrics, soft biometrics

1. Introduction

The Internet is here to stay. It is as embedded in our lives as electricity. As of April 2017 roughly the half of the world's population was online[1]. With the exploding popularity of social networking services (SNSs), the amount of data shared everyday by people all over the world is growing at a rapid rate. The information shared takes various forms including text, images, video, and audio (music and voice) and people conducting more and more aspects of their lives online. In Japan, for example, the rate of Internet shopping is increasing across all age groups[2].

The very same convenience and easy access to data makes cyberspace tempting to criminals, both as a space for planning and preparation of crimes in the real world and as a place to conduct actual cyber-enabled crimes. Cyberspace is nebulous and borderless, providing criminals with a cloak of invisibility while handcuffing law enforcement which remains bound by real world restrictions on its ability to cope with criminal activities that know no boundaries. Terrorists, for example, make extensive use of the Internet, disseminating propaganda via video sharing websites, recruiting new members and conducting espionage via social media, and procuring funds and weapons at anonymous sites. In addition to terrorism, criminal activities conducted in cyberspace include the buying and selling of illegal drugs and Internet auction frauds. In Singapore, for example, online crimes such as Internet shopping fraud increased dramatically in 2015, showing a 46.5% increase over the previous year, and prompting concern among the public and authorities alike[3] [4].

Unfortunately, what happens in cyberspace doesn't stay in cyberspace. Cybercrime bleeds over into the real world, having a very real impact on real people in their daily lives. It is no longer enough for law enforcement to help maintain a safe and secure society in physical space, that is, in the real world. Now, the authorities must extend that protection to cyberspace as well.

In section 2 below, we give an overview of NEC's research into cyber-physical integrated technology for criminal investigation support. In section 3, we discuss NEC's critical analysis technology which supports that research. Future issues are outlined in section 4, and this paper is summarized in the conclusion at the end of the document.

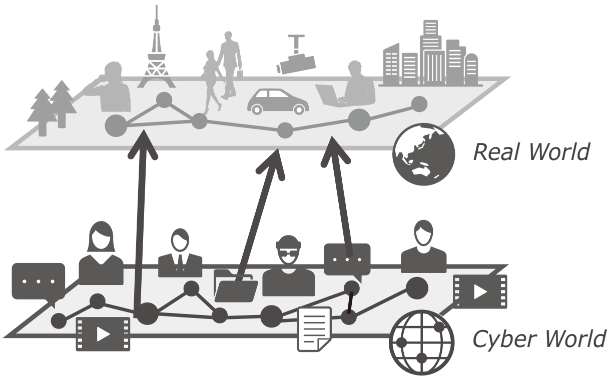


Fig. 1 Correlating cyber-enabled crimes with real world information.

2. Cyber-Physical Integrated Analysis Technology for Supporting Investigations

NEC is conducting research and development into cyber-physical integrated analysis technology with the goal of providing crucial support for criminal investigations. This technology integrates a variety of tools to analyze information extracted from cyberspace that may be applicable to a criminal investigation. By sifting through a massive amount of data in cyberspace and applying various analysis technologies to the images and text contained in that data, this system is designed to facilitate proactive detection of suspicious activity and post-crime identification of perpetrators. Cyber-enabled crimes continue to grow more sophisticated and complex, as is evident for example in the use of tools to anonymize communication paths. We are focusing in particular on linking these crimes with incidents in the real world (**Fig. 1**). Since there is an immense amount of publicly available information in various forms such as text, images, video, and audio (music and voice), we believe that a critical area of research is find a way to extract information that can be used to correlate cyber-enabled crimes with phenomena in the real world by using a wide variety of technologies to analyze the public data.

More specifically, our goal is to be able to pull out information that can help identify and locate suspects or missing persons. For example, even if a photo of the individual in question exists, it is not always easy to determine where the picture was taken. However, if the country or region where the clothes worn by the individual can be identified, then it may be possible to narrow down the location where the image was capture. If buildings and structures in the background can be identified, then the location can be further narrowed down. This research is intended to support investigations conducted by law enforcement agencies by developing a tool that uses various analysis technologies to extract relevant information from publicly available information on the Internet, including images in cyberspace.

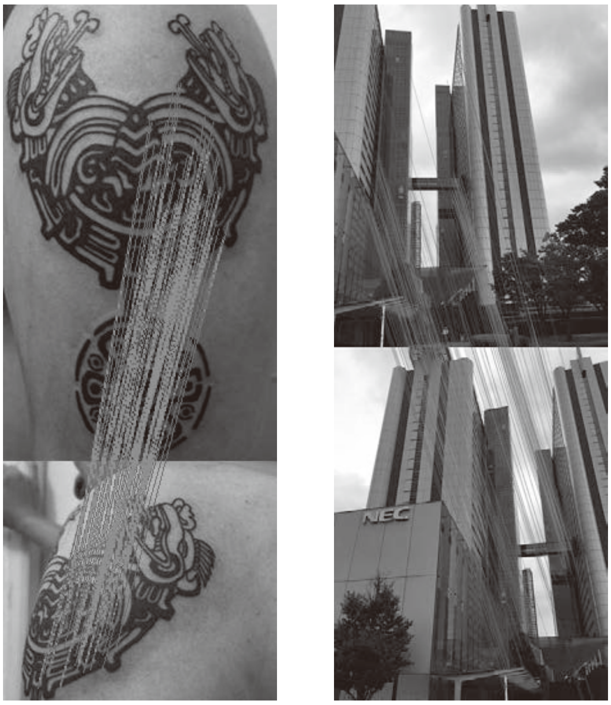
3. Key Component Technologies

3.1 Biometrics

When a person of interest such as a suspect or missing person is directly searched from public information in cyberspace such as images and movies, biometric authentication technology will prove very helpful in identifying that person. NEC has devoted itself for many years to conducting R&D into biometrics such as fingerprint recognition and face recognition. NEC’s face recognition technology, for example, achieved the highest performance evaluation four times in the benchmark tests conducted by the U.S. National Institute of Standards and Technology (NIST). NEC’s products using this technology have been introduced into more than a hundred systems in over forty countries all around the world[5]. For instance, claims of responsibility in the form of a video posted on the Internet provide investigators with all kinds of precious information including the speaker’s voice which can be processed by speaker recognition technology to help identify the individual. NEC is also engaged in speaker recognition R&D, in addition to face recognition. Large-scale database searches using voices have already been put into practical use by government agencies[6].

3.2 Soft Biometrics

When biometric features such as the face of a person of interest cannot be obtained, soft biometrics can be used to narrow down who that person might be and where they might be located. Soft biometrics refers to information that is insufficient on its own to definitively identify an individual even though the information describes certain characteristics of that individual — for example, hair color, skin color, and the presence and design of tattoos, as well as the clothes and accessories worn. Locations related to the person in question can also be considered as soft biometric features in a broader sense since the sphere of activity in everyday life — such as frequently visited places — can potentially have a certain individuality, albeit relatively small. NEC owns object recognition technology that combines high speed with high precision[7], and this technology has been applied to soft biometrics. **Fig. 2** shows examples of soft biometric test results. Fig. 2 (a) shows an example of



(a) Tattoo comparison (b) Building comparison

Fig. 2 Examples of results of soft biometric tests.

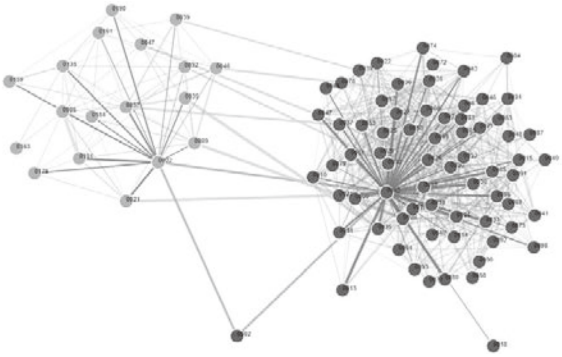


Fig. 3 Correlational analysis of accounts.

tattoo comparison, in which similar characteristics in the upper and lower pictures are connected by straight lines. Fig. 2 (b) is an example of the result of scenery comparison — buildings in this case. It would generally be difficult to specify the location from the upper picture alone unless the scenery looks familiar. However, if the upper picture can be linked to the lower picture, it would be possible to know that the upper picture was taken in the vicinity of the NEC buildings.

We are also investigating ways of correlating accounts on the Internet by applying soft biometrics (**Fig. 3**). When a person of interest has multiple accounts, information such as images and text in those accounts can be aggregated to perform detailed analysis of the person's attributes and associations, as long as we can be fairly certain those accounts belong to the same person. This can be assessed based on various factors including writing style, details mentioned in posts, and so on.

In cooperation with international law enforcement agencies, NEC is studying the application feasibility of soft biometrics.

4. Issues to Be Addressed

We have so far discussed our commitment from a technological viewpoint. When law enforcement agencies actually use these technologies, they need to comply with the laws of the countries concerned. It is essential that any data pertaining to users that is irrelevant to crimes must be protected even if that information is open to the public. NEC will strive to achieve an appropriate balance between security and privacy in cooperation with law enforcement agencies around the world. In this way, we can build a world that protects both an individual's security and their privacy.

5. Conclusion

In this paper, we have introduced NEC's R&D efforts to develop analytical systems based on various proprietary technologies including face recognition and object recognition that take advantage of the massive amount of data — such as images — available in cyberspace to support criminal investigations. We believe that one of the keys to combatting cyber-enabled crimes is to be able to correlate anonymous and global cyber-enabled crimes with phenomena in the real world. Solving this issue will make it possible to develop powerful solutions that will help tame the lawless frontiers of cyberspace and bring real security to both the real and virtual worlds.

Reference

1) We Are Social: The state of the Internet in Q2, 2017, 2017.4
2) The Ministry of Internal Affairs and Communications: Whitepaper of Information and Communications in Japan 2016
http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2016/2016-index.html
3) Singapore Police Force: Annual Crime Brief 2015, 2016.2
4) Singapore Police Force: Annual Crime Brief 2016, 2017.2
5) NEC Press Release: NEC's Video Face Recognition Technology Ranks First in NIST Testing, 2017.3
http://www.nec.com/en/press/201703/global_20170316_01.html
6) KOSHINAKA Takafumi, et al.: Speech/Acoustic Analysis Technology - Its Application in Support of Public Solutions, NEC Technical Journal, Vol. 9, No. 1, pp.82-85, 2014.11
7) K. Iwamoto, et al.: BRIGHT: A Scalable and Compact Binary Descriptor for Low-Latency and High Accuracy Object Identification, IEEE ICIP, 2013.9
http://ieeexplore.ieee.org/document/6738600/

Authors' Profiles

TANI Masahiro

Principal Researcher
Data Science Research Laboratories

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

\Orchestrating a brighter world NEC
NEC Technical Journal
Cybersecurity
- Building Futureproof Security to Support Business Safety and Reliability -
Vol.12 No.2

Vol.12 No.2
January 2018

Special Issue TOP