Points of View

Abuse Prevention of Street Camera Network by Browsing-History Disclosure

Yusaku Fujii
Division of Mechanical Science and Technology, Faculty of Science and Technology, Gunma University, Japan.
Corresponding Author.
fujii@e-jikei.com

Noriaki Yoshiura
Department of Information and Computer Science, Graduate School of Science and Engineering, Saitama University, Japan
yoshiura@fmx.ics.saitama-u.ac.jp

Naoya Ohta
Division of Electronics and Informatics, Faculty of Science and Technology, Gunma University, Japan
ohta@cs.gunma-u.ac.jp

Akihiro Takita
Division of Mechanical Science and Technology, Faculty of Science and Technology, Gunma University, Japan
takita@gunma-u.ac.jp

Hiroshi Ueda
Academic Center for Computing and Media Studies, Kyoto University, Japan.
uep@media.kyoto-u.ac.jp

Koichi Maru
Department of Electronics and Information Engineering, Faculty of Engineering, Kagawa University, Japan.
maru@eng.kagawa-u.ac.jp

A street camera network, in which many street cameras are installed at a high density, similar to street lights throughout a nation, will have a stronger positive effect in suspect tracking and crime deterrence in the near future. On the other hand, it will also have a stronger negative effect related to the violation of privacy of ordinary citizens. In order to make such a stronger surveillance camera system, which forcibly captures the images of passersby for the public interest, be accepted as an essential social infra-

Fujii, Y., Yoshiura, N., Ohta, N., Takita, A., Ueda, H., Maru, K. (2016). Abuse Prevention of Street Camera Network by Browsing-History Disclosure. *The Journal of Community Informatics*, 12 (1), 152–156.

Date submitted: 2015-09-16. Date accepted: 2016-02-14.

structure by a society, it is necessary for this camera system to make ordinary citizens be convinced that it is used only for the public interest. To realize this, a new concept, in which the abuse of a street camera network is deterred by browsing-history disclosure, is proposed.

Introduction

In developed countries in the near future, street camera networks and/or street lights with network camera functionality will be installed at a high density, similar to street lights, in busy and quiet areas. They will be connected using the Internet, and high-speed access to the recorded images will take place. These events will happen owing to the reduction in price of electrical devices and Internet connections. Then, manual or automatic tracking [1] of any suspect will take place with a high efficiency.

As for the type of camera, an LED street light camera will be advantageous because the costs associated with the installation of the camera and street lights are similarly high As for the storage of the captured images, it is reasonable to assume that images are to be recorded on the camera itself and transferred as the need arises, because most cameras will be installed in quiet areas, of which there many more than busy areas.

At present, many surveillance cameras have been installed at a high density in urban areas in developed countries, such as London [2]. In the near future, a street camera network, as a powerful social infrastructure throughout the nation, will appear by means of the additional installation of cameras at a higher density, the connection to a high-speed network, and the introduction of an automatic tracking system. This infrastructure will have a strong positive effect in the tracking of suspects, kidnapped children, and aged wanderers and also a strong negative effect related to the violation of privacy of ordinary citizens.

With this powerful infrastructure, it might be possible that a kidnapped child is rescued [3,4]. First, a child exiting a house is observed by the cameras in front of his/her house. Then, he/she is tracked by switching the cameras according to his/her motion. Next, his/her present location is known. Finally, police cars are sent to that location to rescue him/her. This can be easily carried out with this powerful infrastructure.

With this powerful infrastructure, people can be assured that all criminals are arrested. Then, people who do not want to be arrested will be deterred from committing a crime. Although this belief cannot deter a person who does not care about being arrested from committing a crime, he/she cannot commit another crime again because he/she will be arrested after the first crime.

It will be a serious problem if the operators of this powerful system can use the system for private reasons such as stalking and tracking a specific person. In order to make this powerful infrastructure be accepted by society, it is necessary for this system to make the ordinary citizens be convinced that the abuse is perfectly prevented and their privacy is perfectly protected.

Proposed concept

To realize this, a new concept [5], in which the abuse of a street camera network is deterred by browsing-history disclosure, is proposed. Figure 1 shows an example of the system based on the proposed concept.

The system shown in Figure 1 works as follows:

(1) The city government operates many cameras, which are installed at a high density, similar to street lights, throughout the city.

(2) The manager of the city government publicizes the method of operation of the camera system, i.e., the "control condition," and inputs it into the "recording server" operated by a reliable third party.

(3) The operator of the city government starts operation by order with "reason code."

(4) The operator sends a "request code," which consists of the inputs of the "browser ID," "reason code," "camera ID," and "time period," to the "recording server" using the "browsing device."

(5) The "recording server" issues a "permission code" to the "browsing device" on the basis of the "control condition" and records all processes as the "browsing history."

(6) The operator can browse the image files within the permitted range defined by the "permission code."

(7) The recording server discloses the entire "browsing history" to everyone throughout the Internet.

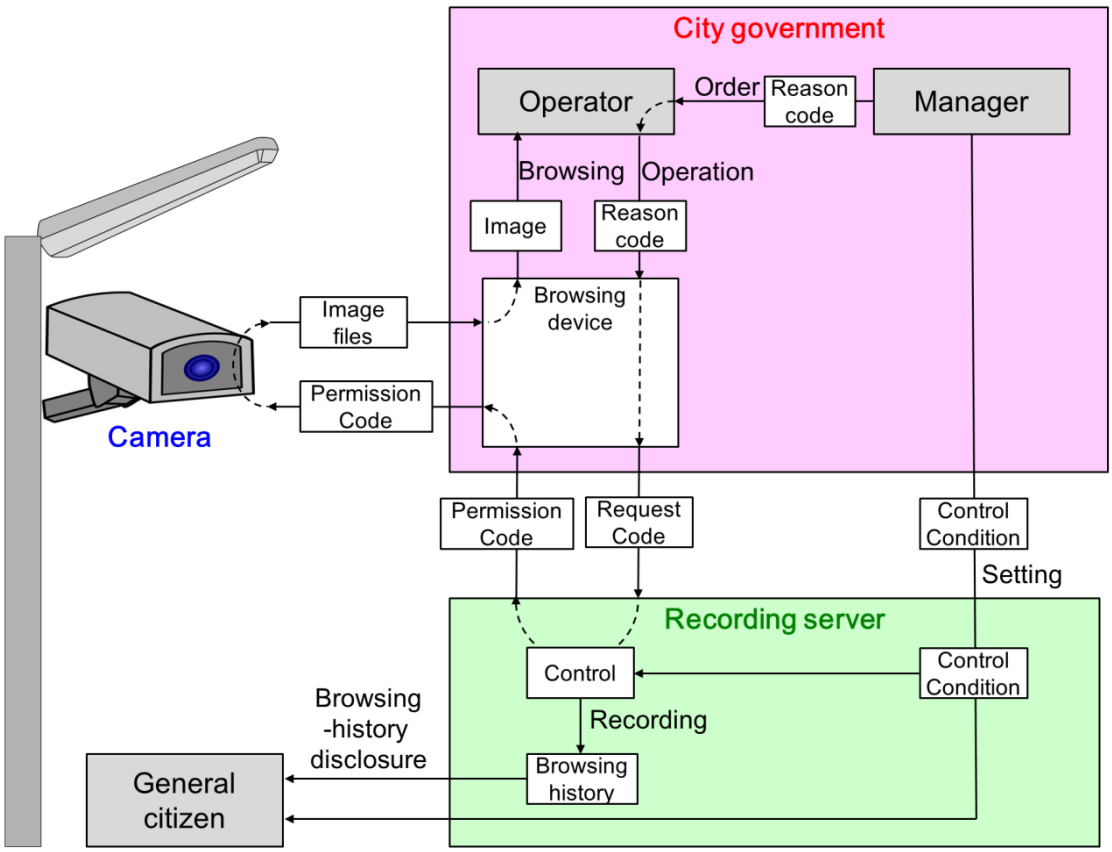

Figure 1. Example of a system based on the concept of abuse prevention of a street camera network by browsing-history disclosure

In the above system, all browsing acts are visualized and verifiable. Abuse of the system is strongly deterred. An ordinary citizen is free from the mental stress by believing that it is very difficult to abuse the system, and their privacy is protected at a sufficient level.

Discussion

With this concept, people can believe that abuse should be surely revealed. Then, people who do not want to be revealed will be deterred from abuse. Although this belief might not deter a person who does not care about being revealed from abuse, he/she cannot commit another abuse again because he/she will be resigned owing to the first one.

To complement this concept, another concept of "self-identification using wireless camera communication" is proposed [6]. In the second concept, each camera should identify itself to the persons around it using wireless communication. For example, each camera sends URL of the website, in which the operator in charge, the operating method, the above mentioned "browsing history" are shown, to nearby smartphones using short-distance wireless communication such as Bluetooth.

We wish to make possible a society in which no criminal can escape and kidnapped children can be rescued and the privacy of noncriminal citizens is perfectly protected.

Acknowledgements

This study was supported by the research aid fund of the Research Foundation for Safe Society and the Grant-in-Aid for Scientific Research (B) 15H02887 (KAKENHI 15H02887).

References

[1] Mazzon, R. & Cavallaro, A. (2013). Multi-camera tracking using a Multi-Goal Social Force Model, *Neurocomputing*, Vol.100: 41-50.

[2] *Surveillance road map, A shared approach to the regulation of surveillance in the United Kingdom*, Surveillance Camera Commissioner, 2015. https://www.gov.uk/government/publications/surveillance-road-map

[3] Y. Fujii, N. Ohta, H. Ueda, Y. Sugita and K. Maru (2008). *New concept regarding management of security cameras*, 4 (3).

[4] Y. Fujii, K. Maru, K. Kobayashi, N. Yoshiura, N. Ohta, H. Ueda and P. Yupapin. (2010). e-JIKEI Network using e-JIKEI Cameras: Community security using considerable number of cheap stand-alone cameras. *Safety Science*, 48 (7), 921-925.

[5] Japanese Patent Application No.2015-167298.

[6] Japanese Patent No.5757048.