Protection and Utilization of Privacy Information via Sensing

Noboru BABAGUCHI†‡, Fellow and Yuta NAKASHIMA††, Member

SUMMARY  Our society has been getting more privacy-sensitive. Diverse information is given by users to information and communications technology (ICT) systems such as IC cards benefiting them. The information is stored as so-called big data, and there is concern over privacy violation. Visual information, such as images and videos, is also considered privacy-sensitive. The growing deployment of surveillance cameras and social network services has caused privacy problems of information given from various sensors. To protect privacy of subjects presented in visual information, their face or figure is processed by means of pixelization or blurring. As image analysis technologies have made considerable progress, many attempts to automatically process flexible privacy protection have been made since 2000, and utilization of privacy information under some restrictions has been taken into account in recent years. This paper addresses the recent progress of privacy protection for visual information, showing our research projects: PriSurv, Digital Diorama (DD), and Mobile Privacy Protection (MPP). Furthermore, we discuss Harmonized Information Field (HIF) for appropriate utilization of protected privacy information in a specific area.

key words: privacy information, sensing, visual abstraction, privacy protection, information disclosure and utilization

1. Introduction

In recent years, our society has been getting more privacy-sensitive or privacy-aware. We are facing various information and communications technology (ICT) systems, e.g., an IC card system, in our daily life, and receiving a lot of benefit and convenience from them. At this moment, we are unconsciously giving diverse information such as personal data and movement history to them. The information is stored as so-called big data, which leads to concern over privacy violation. Visual information such as images and videos is also considered privacy-sensitive. As systems and services using visual information have been developed, privacy issues of subjects in the visual information have attracted considerable attention [1]–[4]. In Japan, the lawsuit about infringement on the privacy right by Google Street View triggered public attention. Video surveillance is also an essential ICT system to maintain safety at surveillance areas; however, it can be viewed as a critical source of privacy disclosure.

In fact, visual information distributed via TV broadcasts and the Internet contains privacy-sensitive information (PSI) [5], [6], e.g., subjects’ faces, which may cause privacy violation in its acquisition, distribution, and share. Therefore, some protection procedures for the PSI are strongly required. In Google Street View, regions of subjects’ faces are blurred to prevent their identification. In surveillance video, whichever the camera is static or mobile, various protection methods are proposed. In TV broadcasts, not only subjects’ region but also the background region is sometimes blurred so that the viewer cannot guess where the video was taken.

Formerly, this kind of protection procedures was manually carried out, which was very time-consuming. Nowadays, automated procedures are tried using image analysis technologies. After detecting PSI regions in an image, an image processing operator, such as pixelization and blurring, is performed onto all the regions so that they cannot be seen. This can be viewed as exhaustive privacy protection. For Google Street View images, all the regions of human faces and car license plates are blurred. This automated method [7] has drawn attention as a practical example of visual privacy protection. A similar method is also provided on YouTube [8]. In social network services (SNSs), such as Twitter, Facebook and Flickr, the number of users who upload images is surprisingly increasing. A system is proposed that alerts users to potential privacy violation due to uploaded images based on image content analysis [9]. In this way, the technologies of visual privacy protection and those of image analysis are mutually correlated.

In this paper, we address the recent progress of privacy protection for visual information, showing our research projects: PriSurv, Digital Diorama (DD), and Mobile Privacy Protection (MPP). They aim at flexible privacy protection in contrast to exhaustive privacy protection. Furthermore, we discuss the importance of utilizing privacy-protected information appropriately in some special situations.

The rest of the paper is organized as follows. Section 2 overviews the related work. Section 3 discusses the PSI in detail. Section 4 presents our research projects about visual privacy protection. Section 5 presents our new attempt to build an information field to realize both protection and utilization of privacy information. Section 6 concludes the paper.

Manuscript received March 13, 2014.
†The author is with the Graduate School of Engineering, Osaka University, Suita-shi, 565–0871 Japan.
‡The author is with the Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma-shi, 630–0192 Japan.
††This work is supported in part by a Grant-in-Aid for scientific research from the Japan Society for the Promotion of Science.

a) E-mail: babaguchi@comm.eng.osaka-u.ac.jp
DOI: 10.1587/transinf.2014MU10001

Copyright © 2015 The Institute of Electronics, Information and Communication Engineers
2. Related Work

In the last decade, research efforts have been dedicated to privacy protection for visual information. For removing PSI such as faces, entire bodies, or other specific objects [10], wide variety of image processing techniques, e.g., blurring, pixelization, blocking out, and edge detection, are applied to them, and some of which capability of privacy protection was evaluated [11]–[16]. Some research attempts were made for preserving some specific visual content such as facial details [17] and body motion [18]. An eigen-space filtering-based technique [19] determines visual content to be preserved based on a preliminarily calculated set of image bases. With these techniques, PSI is permanently lost so that the visual information is viewed without infringing on others’ privacy. In other words, they are irrecoverable abstraction of the image/video content.

Recoverable abstraction is another interesting research direction, which allows authorized entities to view the original visual content recovered from an abstracted one. This type of techniques also involves the problem of privacy protected images/video delivery to designated entities. Recoverable abstraction is beneficial for video surveillance systems that require further investigation once an abnormal event happens. Dufaux and Ebrahimi [20] proposed to encrypt some PSI regions in a compressed domain. This technique was adapted for compressed video streams [21]–[24] and uncompressed ones [25], [26]. Instead of using encryption techniques, information hiding is also employed to embed PSI into the abstracted images/video [27]–[29].

With the development of these abstraction techniques, various applications with image/video privacy protection have been developed. Privacy protection for video surveillance is one of such applications that has been widely studied [30]. The basic approach is locating PSI regions in surveillance video, e.g., using background subtraction, and applying such visual abstracting techniques as blurring, blocking out, and pixelization as in [31], [32]. Some systems provide removed PSI through a different data channel for later investigation. Since the main purpose of video surveillance is security, recoverable abstraction techniques have been employed, which are based on encryption and data hiding to allow authorized entities to access PSI as mentioned above, for example, [33]–[38]. An important idea of privacy is that people have the right to control information on them, leading to video surveillance systems that allow people who are captured in surveillance video to choose whether their appearance is disclosed [39]–[41], which often use RFID or other techniques for identification of people in video. A new attempt for video surveillance potentially provides various additional values by selectively disclosing PSI to public [42].

Compared with video surveillance systems that can assume fixed cameras, mobile camera-based applications confront the difficulty in locating PSI regions in images/video because of the inapplicability of background subtraction, and an object detection technique such as face or pedestrian detection is used instead. For mobile surveillance, which captures suspicious people using mobile cameras, some privacy-aware systems are summarized in [43], e.g., [44], [45], and a more recent work focused on automatically discriminating people of interests based on the videographer’s intention [46]. Besides mobile video surveillance, privacy protection has been designed for various applications. Google Street View is a well-known example of such applications, and some researchers focus on removing pedestrian regions from the images with less visual artifacts [47] or on improving the recall of PSI detection (i.e., face or pedestrian detection) [7]. Some systems are proposed for other applications such as life-log [48], video conferencing [49], and consumer generated videos [50], [51].

Some techniques do not rely on visual abstraction to protect privacy in images/video. For example, systems for knowledge discovery from unpublished videos have been proposed for medical purposes [52], [53]. PicAlert [9] automatically finds images from an image collection that potentially contain privacy sensitive contents and notify the user to prevent their disclosure to public. Privacy Visor [54] is another interesting approach to privacy protection, which physically masks face regions by goggles with a tailored patterns to hinder face detection.

Privacy protection is generally considered as a subdiscipline of information security and often adopts techniques of information hiding, encryption, secret sharing, and access control for abstraction and identification (e.g. [20], [29], [37], [55]).

3. Privacy Sensitive Information

Privacy sensitive information (PSI) can be defined as information that may invade somebody’s privacy in case it is extracted from the entire information acquired from sensors located in the real world [5]. We classify the PSI into 1) information accessible to personal ID, 2) information related to personal ID, and 3) information on one’s private area.

The information accessible to personal ID is the information with which a corresponding individual is distinguishable from others. This kind of PSI includes person’s appearance, such as faces, full figures, clothes, gait, gestures, or expressions in images, as well as utterance in audio signals. Behavioral information, such as locations and trajectories, is also included. As a special case, text on nameplates or car license plates is included as well.

The information related to personal ID is not essentially privacy-sensitive in itself, but turns into PSI once it is associated with personal ID. This kind of PSI includes one’s belongings and possessions. For example, an animal is usually not concerned with privacy; however, if it is possessed by someone as his/her pet and is known to be his/her possession, it turns into PSI.

The information on one’s private area is the third kind of PSI. The private area implies where most people feel private. For example, the inside of one’s house, a clothes-
drying place, and displays of PCs or smartphones are in this case.

Let us think about a scene in an image as indicated in Fig. 1(a). Which region in the image is privacy-sensitive? Figure 1(b) shows the regions corresponding to three kinds of PSI, i.e., 1), 2), and 3) as stated above. If we take advantage of exhaustive privacy protection, most parts of the image cannot be seen, and the image becomes meaningless as shown in Fig. 1(c). Therefore, a framework that flexibly deals with the PSI depending on the subject and the viewer will be needed.

4. Privacy Protection for Visual Information

In the following, we proceed to describe our research projects about visual privacy protection.

4.1 PriSurv

PriSurv (Privacy Protected Video Surveillance System) project was an attempt to construct a pilot system of video surveillance with protection of subjects’ privacy. The purpose of PriSurv is to make video surveillance a social system offering both safety and security. Our prototype of PriSurv [41] works in spatially local community such as a school zone while preserving community members’ privacy. PriSurv is capable of generating a surveillance video that dynamically changes the appearance of subjects in order to protect his/her privacy. In contrast to the existing systems by exhaustive privacy protection, PriSurv is characterized by selective privacy protection [56].

To control disclosure of the subject’s visual PSI, PriSurv provides multiple image processing operators named visual abstraction. The subject’s appearance can be changed via visual abstraction operators. PriSurv offers 12 operators: transparency, dot, bar, box, silhouette, border, edge, mosaic, blur, monotone, see-through, and as-is.

One of the main characteristics of PriSurv is that the content of generated video is changeable based on the relationship between the viewer and the subject. Figure 2 shows privacy control in PriSurv. From the original image $I$, visual abstraction operator $a$ for the subject $s$ and the viewer $v$ produces an privacy protected image $I'_{a,v}$ that is different for each viewer. PriSurv works in a community where there are preliminarily registered members and non-members. Each member can describe in PriSurv’s privacy policy how his/her appearance should be presented to various viewers: family, neighbors, strangers, etc. The relationship between the visual abstraction and the human sense of privacy was investigated from a psychological viewpoint [57], which was reflected on design of PriSurv’s privacy policy. It should be noted that PriSurv is embodiment of self-information control, which is modern interpretation of the privacy right.

4.2 Digital Diorama

In Sensing-Web project, we addressed how appearance of each person should be represented in surveillance video that captures a scene of a public space when the video is open to public through the Internet. Our main focus was to protect privacy of subjects in a strict way. In this project, we built a real-world content named Digital Diorama (DD) [58] that displays real-time information acquired from various sensors. In DD, movement of people in the 3D environment can
be observed from an arbitrary viewpoint. Location of each person is estimated from the video stream from surveillance cameras, and is presented in a texture mapped 3D model of the target scene.

Because DD deals with a public space, privacy of the people should be strictly protected. We think that the appearance of all the subjects in surveillance video should not be presented to viewers. In DD, a subject is represented as a human-shaped stick figure. Furthermore, DD displays specific subjects in a different color: If a viewer is a member of a certain group registered to DD and is authenticated, he/she can find other members easily by showing them in a color different from other people. This function is very useful for locating family or friends. DD realizes identification of the subjects, authentication of the viewer, and registration of group members using RFID tags. Figure 3 shows privacy control in DD. The human-shaped stick figure in pink belongs to the same group as the viewer, and the other people are colored blue.

DD’s privacy control [42] is similar to PriSurv’s one, because it is based on the relationship between the viewer and subject. DD was demonstrated at a shopping mall ‘Shin-Pu-Kan’ in Kyoto for actual visitors. The questionnaire survey indicated that DD’s privacy protection was favorable to most visitors.

4.3 Mobile Privacy Protection

Our mobile privacy protection (MPP) project aims at automatically generating privacy protected videos captured by videographers using mobile cameras. One of the essential differences between surveillance videos and ones captured by videographers is that the videographers have their capture intentions, e.g., to record a child’s growth. A video captured by a videographer contains important persons, without whom the video becomes meaningless and thus the videographer captures them intentionally (intentionally captured persons; ICPs), as well as objects that are not important for the intentions (non-ICPs). For this, we developed a method for automatically detecting ICPs and their abstraction [46], [51], [59]–[61]. Figure 4 shows an overview of privacy protection for mobile cameras.

One of the fundamental techniques in MPP is ICP detection [59], [61], which automatically locates ICPs in video. After locating all people using face/pedestrian detection [62], [63], assuming that videographers’ intention is reflected in how they move their mobile camera, ICP detection extracts visual features such as each detected persons’ position, size, and similarity between the person’s motion and the camera motion. Using these features, a machine learning technique-based ICP model, e.g., a support vector machine and a Markov random field (MRF)-based model, classifies each detected person into ICP or non-ICP.

Our MPP then obscures non-ICPs identified by ICP detection. Considering that most videos captured with mobile
cameras are watched by others, possibly through video sharing services, MPP must provide various types of abstraction so that its users can choose appropriate one for their video contents. In [60], we implemented blurring, blocking out, and removal by seam carving [64]. We also developed a background estimation technique for mobile cameras and adopted it for abstraction as shown in Fig. 5 [50], which can be a preprocessing for various abstraction operators used in PriSurv [41]. In addition, we proposed a mobile system that automatically obscures non-ICPs in real-time as in Fig. 6.

5. Protection and Utilization of Privacy Information

Based on the research results on sensing and privacy, we have deepen our ideas, and launched Harmonized Information Field (HIFI) project [65]. Table 1 summarizes the comparison of our projects in terms of sensors, subjects, and sensing targets.

HIFI is an information infrastructure that underlies a field, which is a certain area in the real world, and provides its inside people with timely recommendations based on privacy information intentionally released by the people. In our project, the field is a bounded space for specific purposes, for example, shopping malls, stations, and theme parks. We regard, as privacy information in a broad sense, various information that links to a person’s ID: face, figure, expression, motion, location, trajectory, preference, interest, and so on. A user, who is a visitor to HIFI, will intentionally release his/her privacy information and gain profit in exchange.

Let us describe HIFI’s goal in the following scenario. Everybody knows that he/she can get useful information and premium services by giving, to a some extent, his/her privacy information to trusted organizations and shops. An expert salesclerk in a shop will recommend some goods that suit the preference or interest of his/her familiar guest. This comfortable recommendation can be derived from privacy information released by the guest. In other words, it is very difficult for the guest to obtain premium services without giving his/her privacy information. Note that the disclosure of privacy information and the obtained profit in exchange for the disclosure will be balanced in HIFI.

Figure 7 shows a conceptual sketch of HIFI. A visitor who comes into the field submits his/her privacy infor-
information to HIFI. The privacy information acquired from active or passive sensors is securely stored and structuralized in the spatio-temporal database (STDB). Mining the STDB produces useful information that will be fed back to the visitor as recommendation of useful or premium information and services tailored for him/her. HIFI’s privacy information processing consists of four steps: 1) collection and disclosure, 2) protection, 3) storing and structuring, and 4) utilization.

We are now pursuing the following research issues:
- Fusing environmental and social sensing
- Acquiring spatial and temporal attributes of users to be stored in the STDB
- Data cleansing for privacy protection
- Recommendation by utilizing privacy information
- Information entry at HIFI’s entrance and exit gates
- Evaluation of the balance between the disclosure and profit

Among them, we here describe the information entry system (IES) placed in entrance/exit gates of HIFI. At the gate, the visitor will be able to enter his/her privacy information and to determine its disclosure level. Then HIFI will obtain his/her consent on privacy management in HIFI. Namely, the visitor can decide, according to his/her own intention, whether his/her privacy information is stored or discarded at the entrance and exit. Thus, IES plays an important role in HIFI.

As illustrated in Fig. 8, IES exists at the boundary of HIFI and the external world (EW), and has two sides: the HIFI- and EW-sides. IES consists of a camera, Kinect sensors, and a touch-screen monitor for interactively collecting visitors’ privacy information, e.g., their face, clothing, age, gender, and so on, with a less load on its visitors. In IES, a visitor first passes through the EW-side gate and moves to the front of the monitor. Next he/she chooses the ID type during his/her stay at HIFI, interacting with the monitor. Then he/she comes into HIFI through the HIFI-side gate.

The ID type is divided into three classes: autonym, pseudonym, and anonym, which mean that the visitor is identifiable in both HIFI and EW, identifiable in HIFI but not in EW, and not identifiable in both HIFI and EW, respectively. With the ID type, the visitor can determine the level of his/her privacy information disclosure by himself/herself. The autonym ID will make all privacy information in EW disclosed in HIFI. The pseudonym ID will make abstracted or partial privacy information disclosed. The anonym ID will make no information disclosed.

While the visitor passes through IES, Kinect sensors continually detect his/her body region on depth images using background subtraction. His/Her clothing information is represented as a color histogram based on the extracted body region. The camera installed on the top of the monitor extracts his/her frontal face region by a face detection technique during the behavior in front of the monitor when he/she chooses his/her ID type. The face information is represented as facial images. The facial images are used for visitor identification and age/gender estimation for autonym ID, and are immediately discarded for pseudonym and anonym IDs. IES tries to collect privacy information with interaction in order to facilitate the visitor’s manipulations.

6. Conclusion

The trend of privacy information processing has been changing from exhaustive protection and selective protection to appropriate disclosure and utilization. In HIFI, we focus on ‘profit’ as the opposed concept of ‘disclosure’ of privacy information, and try to harmonize them. It is impossible for everybody to disclose his/her privacy information at any time, at any place. We therefore consider ‘disclosure’ at the bounded space called the field. HIFI’s usefulness depends on how much benefit the visitor can obtain in it. It should be noted that ‘protection’, ‘disclosure’ and ‘profit’ are related to human factors, subjectivity, and situation/context-awareness. Human-centered perspective is indispensable for system development. In addition, we point out that not only technological approaches but also psychological, social, and legal approaches are of great importance in privacy information processing.

References

[4] Special Issue on Intelligent Video Surveillance for Public Security &


[47] A. Flores and S. Belongie, “Removing pedestrians from google


