December 12, 2012

Privacy Protection Techniques Using Differences in Human and Device Sensitivity
-- Protecting Photographed Subjects against Invasion of Privacy Caused by Unintentional Capture in Camera Images --

The National Institute of Informatics (NII, Director General, Masao Sakauchi) associate professor, Isao Echizen is the first in the world to develop new technology for protecting photographed subjects from the invasion of privacy caused by photographs taken in secret and unintentional capture in camera images jointly with Prof. Seiichi Gohshi of Kogakuin University. Due of the popularization of portable terminals with built-in cameras and developments in SNS and image search technologies, information such as when and where photographed subjects were is easily disclosed via photos taken and disclosed without their permission, which has resulted in a greater need to protect the privacy of these subjects. This new technological development can disable facial recognition of photographed subjects only when photos are taken. It achieves this by the photographed person wearing a privacy visor that incorporates a near-infrared light source that affects only the camera and not people's vision. Besides being able to protect photographed subjects from the invasion of privacy resulting from the facial recognition functionality of SNSs, which has become a problem in recent years, this new technology is expected to enjoy extensive application in preventing the invasion of privacy of photographed subjects due to widespread use of augmented reality applications.

Outline

Due to developments in the ubiquitous information society, computers, sensors and their networks are located in all places, and useful services can now be received at all times and in all spaces of our lives. On the other hand, however, there is now the actual problem that privacy information is easily disclosed as a result of the popularization of portable terminals with built-in cameras or GPS and other sensors. In particular, invasion of the privacy of photographed subjects is becoming a social problem due to photographs taken of those concerned and photos unintentionally captured in camera images by portable terminals with built-in cameras being disclosed by the photographer on SNS together with photographic information. As a result of developments in facial recognition technology in Google images, Facebook, etc. and the popularization of portable terminals that append photos with photographic information (geotags), such as photo location and time, as metadata when the photo is taken, information such as when and where photographed subjects were is revealed from the disclosed photo of the person concerned via photos taken and disclosed without their permission. Essential measures for preventing the invasion of privacy caused by photographs taken in secret and unintentional capture in camera images is now required.

The possibility of photographs taken in secret and unintentional capture in camera images resulting in the invasion of privacy has already been pointed out in Europe and other regions. It has been reported that, according to experiments conducted at Carnegie Mellon University (CMU), for close on a third of tested subjects who had agreed to being photographed for the experiment, their names could be identified by comparison with information of photos, etc. on disclosed SNSs, and, further, that there were also cases where the interests of the tested subjects and some social security numbers also were found out. Furthermore, due to concerns about the invasion of privacy from SNS facial recognition functions, the European Union (EU) has requested the invalidation of facial recognition in Facebook intended for European users.

Against this backdrop, NII associate professor Echizen has become the first in the world to develop new technology for protecting photographed subjects from the invasion of privacy caused by photographs taken in secret and unintentional capture in camera images jointly with Prof. Seiichi Goshi of Kogakuin University. This technology focuses in the differences on human senses and the spectral sensitivity characteristics of imaging devices on cameras, and facial recognition of photographed subjects can be made to fail only when photos are being taken without the addition of any new functions to existing cameras. This is achieved by the photographed subject wearing a wearable device – a privacy visor – equipped with a near-infrared light source that appends noise to photographed images without affecting human visibility.

Conventional Measures to Prevent Unintentional Capture in Camera Images

Techniques for protecting people's privacy by physically shielding their faces or techniques for causing detection of people's faces to fail by coloring their face or altering their hairstyle have been proposed as measures so far for preventing unintentional capture in camera images. As a technique for physically hiding people's faces, a flexible shell-shaped base called a "Wearable Privacy Shell" was used to physically protect its user's privacy. This protects the user's privacy and at once physically protects unintentional capture in camera images. As a method for causing detection of people's faces to fail, facial recognition was made to fail to prevent the identification of people by coloring people's faces with a special pattern or changing hairstyle to a special shape. Yet, with each of these conventional measures from here on, there is still the problem that man-to-man communications in physical space will be obstructed since hiding or coloring of most part of the face is required.

Privacy Protection Techniques Using Differences in Human and Device Sensitivity

This technique uses the differences in human senses and the spectral sensitivity characteristics of imaging devices on cameras. As shown in Fig.1, the visible range of humans according to the International Commission on Illumination which recommends standard specifications relating to light is 380 to 780 nm. On the other hand, image sensors, such as CCD or CMOS, used in digital cameras have a sensitivity over a wide area of roughly 200 to 1100 nm including outside the visible light range to maintain sensitivity. The technique we propose is prevents recognition of people's faces by adding noise to imaged facial images by irradiating near-infrared rays, that react with only the imaging device on the camera from people's faces and not affecting people's vision and causing misjudgment of facial detection, which is preprocessing for facial recognition.

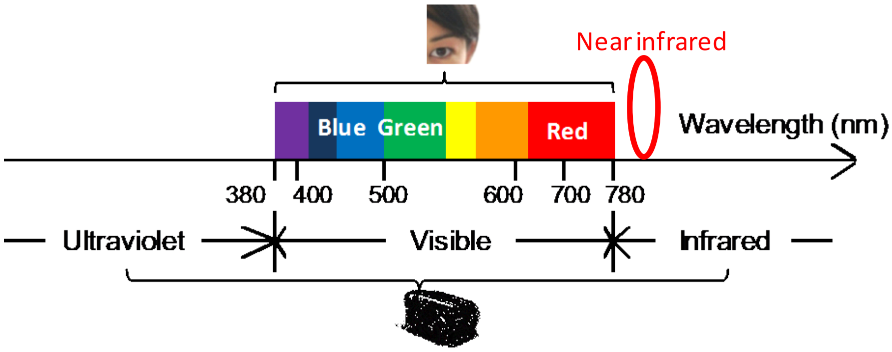

Fig.1 Difference in Sensitivity between Humans and Digital Cameras

Near-infrared ray irradiation from the face can be achieved by incorporating a near-infrared light source into spectacles or goggles regularly worn by people as a noise light source. This was the reasoning behind our development of a wearable device – a privacy visor – equipped with a near-infrared LED in commercially available goggles (Fig.2).

When the near-infrared LED in the privacy visor is not lit, people's faces can be seen in regular goggles as shown in Fig.3(a), and so facial detection is not affected (Fig.4(a)) and man-to-man communications in the physical world is never obstructed. On the other hand, when the near-infrared LED in the privacy visor is lit, near-infrared rays are recorded as noise in the camera's imaging device, as shown in Fig.3(b). Because this noise appended to the facial image causes a considerable change in the amount of features that is referenced at facial detection, facial detection is misjudged and recognition of people's faces is prevented (Fig.4(b)).

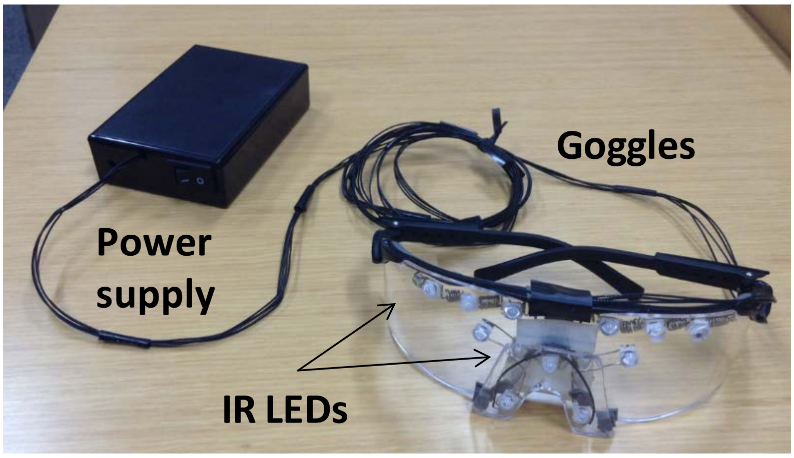

Fig.2 External Appearance of Privacy Visor

(a) Near infrared LED not lit

(b) Near infrared LED lit

Fig.3 Privacy Visor Attachment (Examples)

(a) Near infrared LED not lit (detection successful)

(b) Near infrared LED lit (detection failed)

Fig.4 Execution of Facial Detection (Examples) (Area in Green Frame Indicates Successful Detection)

For more information about this technology, contact:

National Institute of Informatics, Digital Content and Media Sciences Research Division

Associate Professor, Isao Echizen

TEL: +81-3-4212-2516　Mobile: +81-90-2306-4623

E-mail: iechizen@nii.ac.jp

For more information about press statements, contact:

2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430

National Institute of Informatics, Publicity Team (in-charge: Bannai)

TEL: +81-3-4212-2164　E-mail: bannai@nii.ac.jp