Privacy Visor: Method for Preventing Face Image Detection by Using Differences in Human and Device Sensitivity

Takayuki Yamada[1], Seiichi Gohshi[2], and Isao Echizen[1]

[1] National Institute of Informatics, Japan
[2] Kogakuin University, Japan
s5152331@yahoo.co.jp, gohshi@cc.kogakuin.ac.jp,
iechizen@nii.ac.jp

Abstract. A method is proposed for preventing unauthorized face image revelation through unintentional capture of facial images. Methods such as covering the face and painting particular patterns on the face effectively prevent detection of facial images but hinder face-to-face communication. The proposed method overcomes this problem through the use of a device worn on the face that transmits near-infrared signals that are picked up by camera image sensors, which makes faces in captured images undetectable. The device is similar in appearance to a pair of eyeglasses, and the signals cannot be seen by the human eye, so face-to-face communication is not hindered. Testing of a prototype "privacy visor" showed that captured facial images are sufficiently corrupted to prevent unauthorized face image revelation by face detection.

Keywords: Privacy, Unauthorized face image revelation, Face detection, Haar-like feature, Near-infrared LED.

1 Introduction

Due to the popularization of portable devices with built-in cameras and advances in social networking services and image search technologies, information such as when and where a photographed person was at the time the photograph was taken is revealed by the posting of photos online without the person's permission [1,2]. This has resulted in a greater need to protect the privacy of photographed individuals. A particularly serious problem is unauthorized face image revelation through the posting of images of people captured unintentionally and shared over the Internet. If, for example, your face or figure is unintentionally captured in an image taken by someone, and then that image is shared by posting it on a social networking site, information about where you were and when can be revealed through the face recognition process of an image retrieval service (e.g., Google Images) that can access the geographic location and shooting date and time information contained in the image's geotag, without your permission [3]. An experiment conducted at Carnegie Mellon University showed that the names of almost one-third of the people who participated could be determined by comparing the information in photographs taken of them with the information in

B. De Decker et al. (Eds.): CMS 2013, LNCS 8099, pp. 152–161, 2013.

photographs posted on a social networking site. Furthermore, other information about some of the participants, including their interests and even their social security number, was found [4].

In this paper, we describe a method we have developed for preventing unauthorized face image revelation through facial recognition from images captured with a digital camera that does not hinder face-to-face communication. It is based on a method for preventing video recording in movie theaters using near-infrared (IR) signals [5]. No new functions need to be added to existing cameras or networking services because IR signals are used to add noise to the facial portions of captured images. We have developed a prototype wearable device (a "privacy visor") that implements this method. The device is worn on the face like a pair of eyeglasses, so the user does not have a feeling of strangeness. Near-IR light emitting diodes (LEDs) on the device are located near the eyes and nose. Prototype testing demonstrated that our method effectively prevents unauthorized face image revelation through image capture.

The next section describes previous methods for preventing unauthorized face image revelation. Section 3 describes various methods developed for detecting faces. Our proposed method for making faces in captured images undetectable is presented in Section 4, and our prototype wearable device implementing this method is described in Section 5. In Section 6, we describe our evaluation of the prototype implementation, present the results, and discuss them. We close in Section 7 with a summary of the key points.

2 Previous Methods

Methods proposed for preventing unauthorized face image revelation include hiding one's face with an unfolded shell [6] and painting particular patterns on one's face [7]. The first method physically protects the user's privacy by using material in the shape of a shell (a "Wearable Privacy Shell") that can be folded and unfolded. When folded, it functions as a fashion accessory; when unfolded, it functions as a face shield, preventing unintentional capture of the wearer's facial image. The second method prevents identification of the person by using particular coloring of the hair and special paint patterns on the face that cause facial recognition methods to fail. However, such methods interfere with face-to-face communication because they hide a large portion of the face and/or distract the attention of the person to whom the wearer is communicating.

The method we have developed for preventing unauthorized face image revelation through the unintentional capture of facial images does not hinder face-to-face communication. It is implemented in a wearable device (a privacy visor) that makes face detection impossible by irradiating near-IR signals, which do not affect human vision. They affect only the imaging devices used in cameras.

3 Face Detection

Face detection is the key to facial image processing [8] as it is the first step in facial recognition. The method most commonly used for face detection is the one reported

by Viola and Jones in 2004 [9]. The "Viola-Jones method" is based on a multi-scale detection algorithm that uses cascade composition of the Haar-like features, image integration, and a cascade architecture with strong classifiers. It achieves highly accurate and high-speed detection.

3.1 Haar-Like Features

Haar-like features are rectangular image features used for object recognition. Figure 1 shows the basic patterns of Haar-like features. The black areas represent dark features (negative areas), and the white ones represent bright features (positive areas). As shown in Figure 2, Haar-like features are superposed on a detection area, and their values are calculated by subtracting the average of the pixel values in the black areas $s(r_2)$ from that of those in the white areas $s(r_1)$ for each detection area. That is, the value of the Haar-like features $h(r_1,r_2)$ is given by

$$h(r_1, r_2) = s(r_1) - s(r_2)\,. \tag{1}$$

Changing the position and size of the basic patterns of the Haar-like features in a detection area makes various Haar-like features applicable to the detection area.

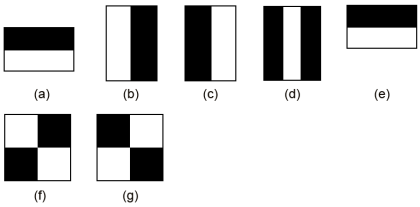


Fig. 1. Basic patterns of Haar-like features

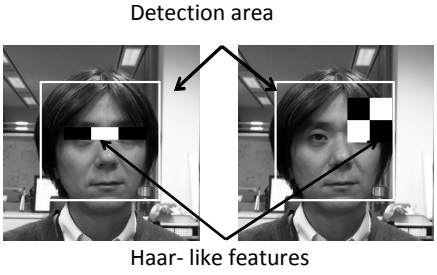


Fig. 2. Example of Haar-like features in detection area

3.2 Cascade Architecture

A weak classifier is composed of several different Haar-like features. It calculates the value of a given feature, and the value is compared with a threshold value. A strong classifier comprises various weak classifiers. Strong classifiers are arranged in a cascade architecture in order of complexity, as shown in Figure 3. The composition of

the weak classifiers and the connection order of the strong classifiers are determined in advance by supervised learning using positive (facial) and negative (non-facial) images. Haar-like features effective for face detection are chosen by supervised learning. As shown in Figure 3, a strong classifier determines "1: True" or "0: False" for each detection area. In the case of "False," the process is terminated and then restarted for the next detection area. In the case of "True" for the Nth strong classifier, the detection area is identified as a face candidate.

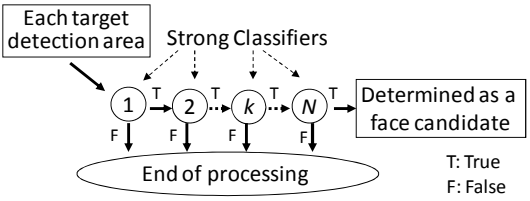


Fig. 3. Cascade architecture

4 Proposed Method

The proposed method for preventing unauthorized face image revelation through unintentional capture of facial images does not interfere with face-to-face communication in physical space. The near-IR signals used to add noise to the facial portion of a captured image cannot be seen by the human eye and hence do not hinder face-to-face communication. Moreover, no new functions need to be added to existing cameras and/or networking services.

4.1 Principle

Our proposed method is based on the difference between human sensory perception and recording device characteristics. It uses near-IR signals to corrupt images captured by a charge-coupled device (CCD) or CMOS device. According to the International Commission on Illumination (CIE), the wavelength of visible light ranges from 380 to 780 nm [10]. In contrast, the wavelengths that can be picked up by such image sensor devices as the CCDs and CMOS devices used in digital cameras and camcorders range from 200 to 1100 nm. This ability to pick up wavelengths outside the visible range gives digital camcorders the high level of luminous sensitivity needed for shooting in the dark [11].

Our proposed method adds a noise signal corresponding to the near-IR signals between 800 and 1000 nm, which people cannot see but to which sensor devices react. This noise signal is generated by LEDs located near the eyes and nose so that it prevents face detection, the first step in the face recognition process. In particular, the noise signal distorts the Haar-like features [9] around the eyes and nose, which are used in the face detection process. This means that new functions do not need to be added to cameras, social networking services, or image retrieval services. Our purpose is to establish a method that prevents identification of a person without causing

physical discomfort to the user. We do this by irradiating near-IR signals from near a person's eyes and nose that react with only the imaging device in a camera, thereby adding noise to captured facial images. These signals do not affect the person's vision but do cause facial detection misjudgment. The near-IR irradiation from near the eyes and nose can be prototyped by implementing a near-IR light source in a pair of glasses or goggles, which is something that is commonly worn, as a noise source. The means we propose for achieving our purpose is a wearable device (a privacy visor) in the shape of goggles that incorporates near-IR LEDs. The transmitted near-IR signals act as a noise source, which makes the face in captured images undetectable.

4.2 Arrangement of Near-IR LEDs

The near-IR LEDs must be effectively arranged to prevent the strong and weak classifiers from classifying the input image as an object. To interfere with the weak classifiers, it is necessary to change the difference in luminance between the positive and negative areas of each feature. We analyzed the Haar-like features effective in face detection by using supervised learning and determined into which portion of the face a noise light source should be arranged.

To determine the composition of the Haar-like features to be trained by supervised learning, we used an Open CV [12] example cascade that had been trained in advance by using 5000 facial and 3000 non-facial images [13]. By setting the pixel value of the positive area r_1 to +1 and setting the pixel value of the negative area r_2 to −1, we identified the partial regions that have a large absolute value and determined the part where the effect of face detection using the change in the luminosity value is large. The superposition of the Haar-like features as determined by using the first strong classifier (k=1) and by using the 10-th strong classifier (k=10) is shown in Figure 4. A positive area representing bright features is concentrated on the circumference of the nose, and a negative area representing dark features is concentrated on the circumference of the eyes and nose. To make face detection fail, we have to make the negative area bright or make the positive area dark so that features are obscured. Near-IR LEDs can make a dark area bright. We therefore focus on the negative area.

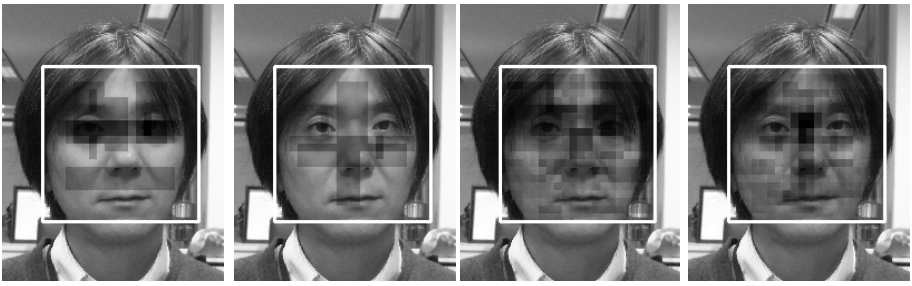


Fig. 4. Superposition of Haar-like features in detection area

By considering the combination of the negative area with the area where a device with a goggle form could be worn, we determined that the near-IR LEDs should be arranged around the eyes and along the periphery of the nose bridge.

5 Prototype

5.1 Description

An overview of the prototype privacy visor is shown in Figure 5, and the specifications are listed in Table 1. The prototype is a pair of commercial goggles to which near-IR LEDs have been attached. The LEDs have a peak wavelength of 870 nm and are positioned so as to maximize the distortion of the Haar-like features.

Table 1. Specifications of prototype privacy visor

Near-IR LEDs	Type: Chip-type with lens; Number: 11; Peak wavelength: 870 nm; Radiation intensity: 600 mW/sr; Radiation angle: ±15°; Rated current: 1 A; Rated power consumption: 2.1 W
Goggles	Materials: Plastic frame; Polycarbonate lenses
Power	Lithium-ion battery (3.7 V×3) 2000 mA/h

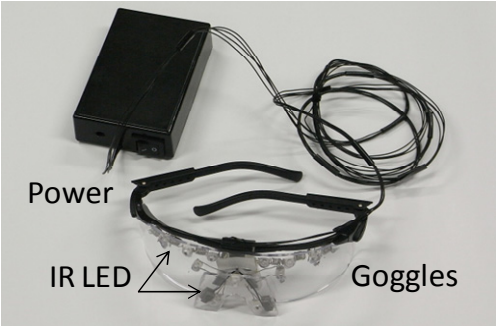


Fig. 5. Overview of prototype privacy visor

5.2 Configuration

Near-IR LEDs
We used chip-type-with-lens near-infrared LEDs based on the sensitivity of human eye and imaging sensor device characteristics by considering the basic types of LEDs (bullet, reflective, and chip with lens), the peak wavelength, the spectral width, etc.

Goggles

We used goggles with a plastic frame and polycarbonate lenses because goggles facilitate the "attachment" and "detachment" of near-IR LEDs to the human body. To effectively interfere with face recognition and maximize the noise effect in captured images, the noise light source must be carefully placed on the face. Because face detection uses the Haar-like features of several areas on the face, face detection cannot be prevented by simply wearing sunglasses. Therefore, to distort the large Haar-like features around the eyes and along the bridge of the nose, we attached 11 near-IR LEDs to commercial goggles on the basis of the analysis results described in Section 4.2. They were positioned around the eyes (3 above each eye; 1 on the inside of each eye) and around the nose (1 on each side of the nose; 1 on the glabella). Because unintentional image capture can also occur from a slant as well as from the front, image capture from a slant must also be prevented. Therefore, the six LEDs above the eyes were arranged in the normal direction of the curved surface of the lenses.

An example of the privacy visor in use is shown in Figure 6. When the noise light source is turned on (right-side images in Figure 6 (i) and (ii)), the near-IR signals are picked up by the image sensor device of a camera as noise. Detection of the face is thus impossible because this added noise greatly changes the Haar-like feature. When the noise light source is turned off, the goggles revert to a form common in the physical world (left-side images in Figure 6 (i) and (ii)), and thus do not interfere with face-to-face communication in physical space.

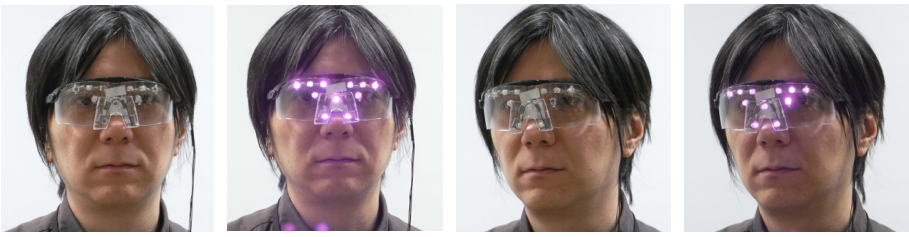


Fig. 6. Example of privacy visor in use

6 Evaluation

We evaluated our prototype privacy visor with the assistance of ten participants (age: 20–40) using a commercial digital camera (1/2.3-inch CCD; ~10 million effective pixels). The room illumination had a light intensity of 67.5 lux. The camera was set to "Camera focus: spot AF," "Photometry: multi-aperture," "Iris: f/3.3 (automatic setup)," "Exposure time: 1/10 s (automatic setup)." We took images of each participant under three conditions: (a) not wearing the privacy visor, (b) wearing it

without IR emission, and (c) wearing it with IR emission. They were taken from three directions (0°, 10° off centerline, and 20° off centerline) and at distances of 1–20 m.

6.1 Method

The images were evaluated using an Open CV face detection API and the same example [7] used to consider the arrangement of the near-IR LEDs. The images had a resolution of 3264 × 2448 pixels, and the cascade was used to set the detection area to various sizes (from 20 × 20 pixels to the maximum number of pixels so that it fit into the image, magnified by a scale factor of 1.1) and to various positions (a loop stride of program is at least two pixels, determined by the scale) from corner to corner.

A detection area classified as an object by all strong classifiers was considered to be a face candidate. After all face candidates were detected, a single candidate was focused on, and the number of neighbor candidates M, that had a size different from and were included in the focused on candidate was counted. If M was two or more, it was determined that there was a face in the detection area, and the face was detected. If M was less than two, especially if the scales of the included candidate were not continuous, it was determined that there was not a face in the detection area, and a face was not detected.

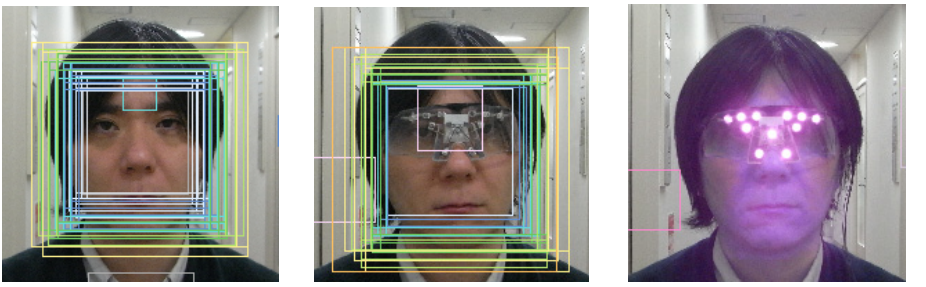
6.2 Results

The face detection results for the images taken from the closest distance (1 m) are shown in Figure 7. Each rectangle indicates a candidate classified as an object by all the classifiers in the cascade. The different colors represent different scales. The number of people detected is plotted in Figure 8. The number of people detected increased in the order of (c), (b), and (a). The plots show that a person not wearing the privacy visor or wearing it without noise could be detected for certain directions and distances while a person wearing the privacy visor with noise could not be detected for any direction or distance. This means that the near-IR signals had a greater noise effect than the visor itself. Details of the evaluation results for each angle are given below.

Images Taken from Front
As shown in Figure 7 (i), for conditions (a) and (b), a face was detected because other candidates were included in the outer candidate for more than two continuous scales. For (c), a face was not detected because there was no candidate on the actual face. As shown in Figure 8 (i), for conditions (a) and (b), all the faces were detected when the distance was less than 16 m. When it was 16 m or more, the number of faces detected decreased moderately. For (c), no face was detected at any distance.

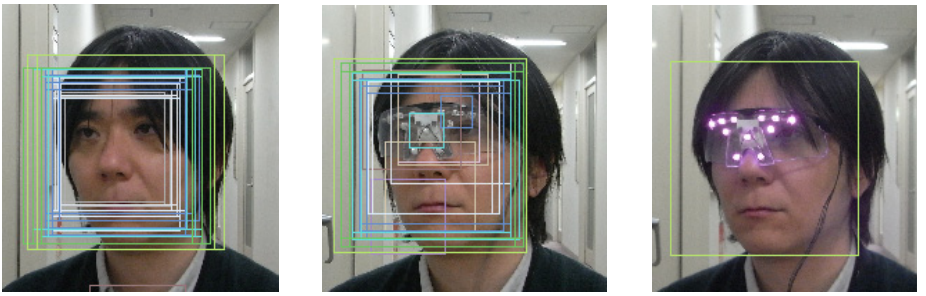
Images Taken from 20° off Centerline
As shown in Figure 7 (ii), for conditions (a) and (b), a face was detected because other candidates were included in the outer candidate for more than two continuous scales. For (c), a face was not detected because there was no other candidate in the

outer candidate. As shown in Figure 8 (ii), for conditions (a) and (b), all the faces were detected when the distance was less than 11 m. When it was 11 m or more, the number of faces detected decreased rapidly. For (c), no face was detected at any distance, the same as for (i). In this evaluation, the maximum slant was up to 20° off the centerline. If it is 20° or more, face detection becomes difficult.



(a) Not wearing visor (b) Wearing visor without noise (c) Wearing visor with noise

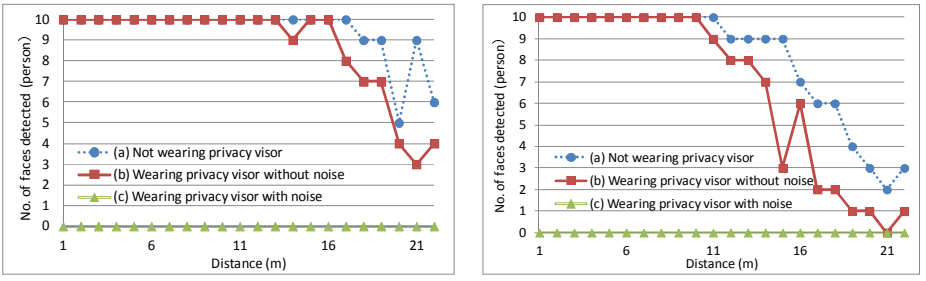
(i) Taken from front (0°)



(a) Not wearing visor (b) Wearing visor without noise (c) Wearing visor with noise

(ii) Taken from 20° off centerline

Fig. 7. Face detection results for pictures taken from 1 m



(i) Taken from front (0°). (ii) Taken from 20° off centerline.

Fig. 8. Number of faces detected

7 Conclusion

The method we proposed in this paper prevents unauthorized face image revelation through unintentional capture of facial images. It adds invisible noise signals to images captured with an image sensor, thereby preventing the revelation of sensitive information via the face recognition process of image retrieval services. Specifically, our method prevents the recognition of people's faces by adding noise to imaged facial images by irradiating from near a person's eyes and nose near-IR signals that react with only the imaging device on a camera and do not affect the user's vision. These noise signals cause facial detection to fail, and facial detection is required for facial recognition. Testing of a prototype privacy visor implementing this method demonstrated that it can effectively prevent unauthorized face image revelation by interfering with the facial images, thus validating the feasibility of our proposed method.

We are now working on a method that uses absorption/reflective material and the reflection properties of light so that a power supply is not needed.

References

1. Cutillo, L., Molva, R.: Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Communications Magazine 47(12), 94–101 (2009)
2. Debatin, B., Lovejoy, J., Horn, A.: Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication 15(1), 83–108 (2009)
3. Blackman, J.: Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image Over the Internet. 49 Santa Clara Law Review 313, 341–392 (2009)
4. Face Recognition Study FAQ, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/
5. Yamada, T., Gohshi, S., Echizen, I.: Preventing re-recording based on difference between sensory perceptions of humans and devices. In: Proc. of the 17th International Conference on Image Processing, ICIP 2010, pp. 993–996 (2010)
6. GAIA, VEASYBLE, http://www.veasyble.com/index.html
7. Harvey, A.: CV Dazzle, http://ahprojects.com/projects/cv-dazzle
8. Feris, R.S., de Campos, T.E., Cesar Jr., R.M.: Detection and Tracking of Facial Features in Video Sequences. In: Cairó, O., Cantú, F.J. (eds.) MICAI 2000. LNCS, vol. 1793, pp. 127–135. Springer, Heidelberg (2000)
9. Viola, P., Jones, M.: Robust Real-Time Face Detection. International Journal of Computer Vision (IJCV) 57(2), 134–157 (2004)
10. Schanda, J. (ed.): Colorimetry: Understanding the CIE System. Wiley-Interscience (2007)
11. Holst, G., Lomheim, T.: CMOS/CCD Sensors and Camera Systems. SPIE-International Society for Optical Engine (2007)
12. Bradski, G., Kaehler, A.: Learning Open CV Computer Vision with the Open CV Library. O'Reilly Media (2008)
13. Lienhart, R., Kuranov, A., Pisarevsky, V.: Empirical Analysis of Detection Cascades of Boosted Classifiers for Rapid Object Detection. In: Michaelis, B., Krell, G. (eds.) DAGM 2003. LNCS, vol. 2781, pp. 297–304. Springer, Heidelberg (2003)