Press release: 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 -

National Institute of Informatics
Isao ECHIZEN
iechizen@nii.ac.jp

Outline

1. Background
2. Proposed method
   ～Add disturbance that prevents unintentional capture of facial images～
3. Prototype privacy visor
4. Evaluation experiment
5. Summary
6. Demonstration

Background

Spread of cell phones with digital camera and advances in SNSs and image search technology have created invasion of privacy problems.

Increasing public self-disclosure through social network systems:

Image search engines, such as Google Images, can reveal when and where a photograph of a person was taken.

Invasion of privacy by unintentional capture of facial images has become a social problem.

Face recognition and invasion of privacy

- **Experiment using Facebook at Carnegie Mellon University（2011）**

- 1 in 3 participants could be identified on basis of comparison with photograph on Facebook.
- Their personal interests and some identifying information could be determined.

- **Use of facial-recognition technology in Europe（2012）**

Facebook deactivated facial recognition function for European users in response to request from EU authorities anxious about privacy.

- **Google Project Glass（2012）**
- **Apple iGlass（2012）**

-Augmented reality application comprising camera and head mounted display
- Name and affiliation can be detected in real
  -> Identify person captured

iGlass
Reality reinvented

Face recognition leads to invasion of privacy.

Previous methods

- Change coloring of face and hairstyle to prevent detection of human face.

- Physically hide the face with a Wearable Privacy Shell .

Wearable Privacy Shells:
http://www.toxel.com/tech/2011/08/20/wearable-privacy-shells/

How to camouflage yourself from facial recognition technology:
http://venturebeat.com/2010/07/02/facial-recognition-camouflage/

Hinder face-to-face communication

Outline

1. Background
2. Proposed method
   ～Add disturbance that prevents unintentional capture of facial images～
3. Prototype privacy visor
4. Evaluation experiment
5. Summary
6. Demonstration

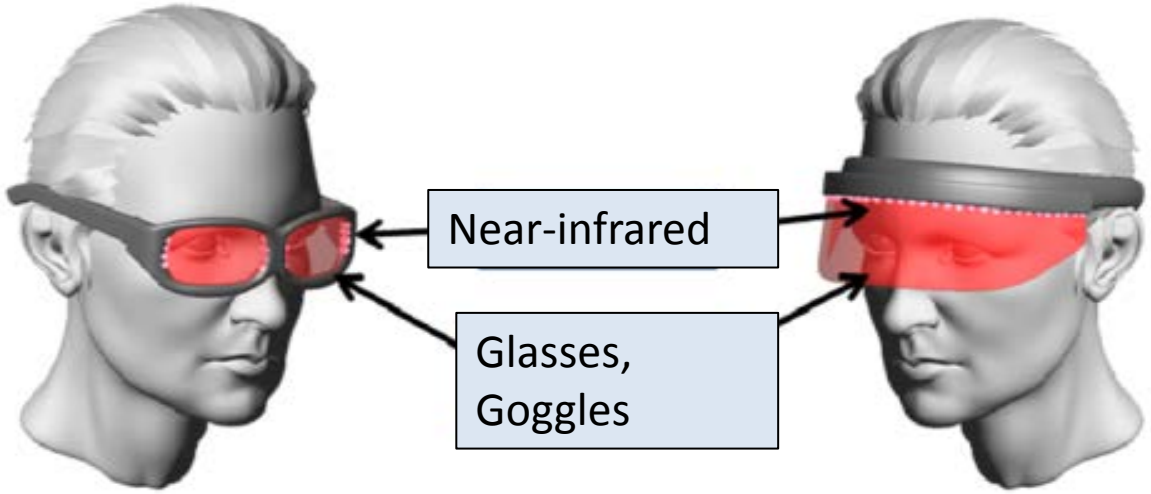
Purpose and means

Purpose

Establish a method that prevents identification of a person without causing physical discomfort.

Means

Equip person with a unit transmitting near-infrared rays as a noise light source, which makes the face in captured images undetectable.



How should noise light source be arranged?

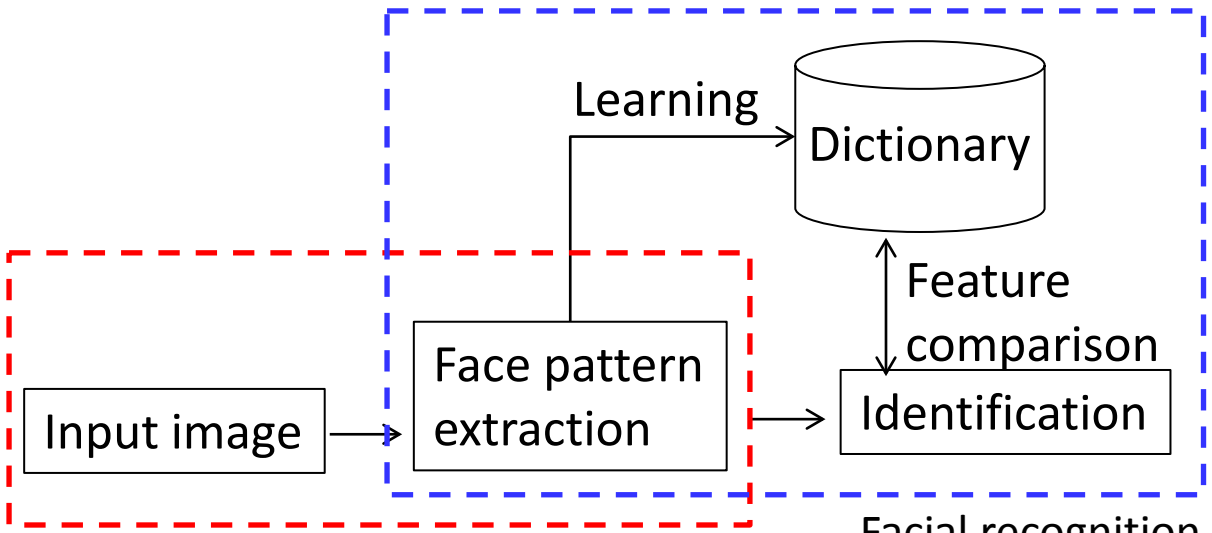
Face detection and face recognition

Face detection

Detection of faces in input image

Face recognition

Recognition of face of specific person from among detected faces



Face recognition

- Variety of methods
- Use of personal characteristics

Facial recognition follows face detection.

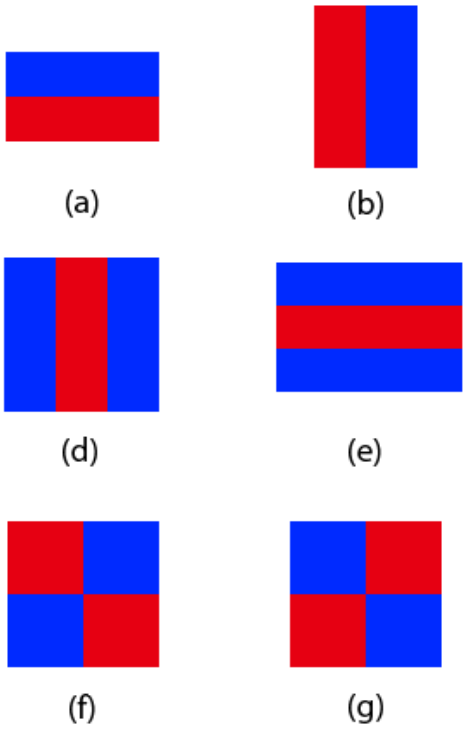
Face detection

Typical technique is Viola-Jones method.

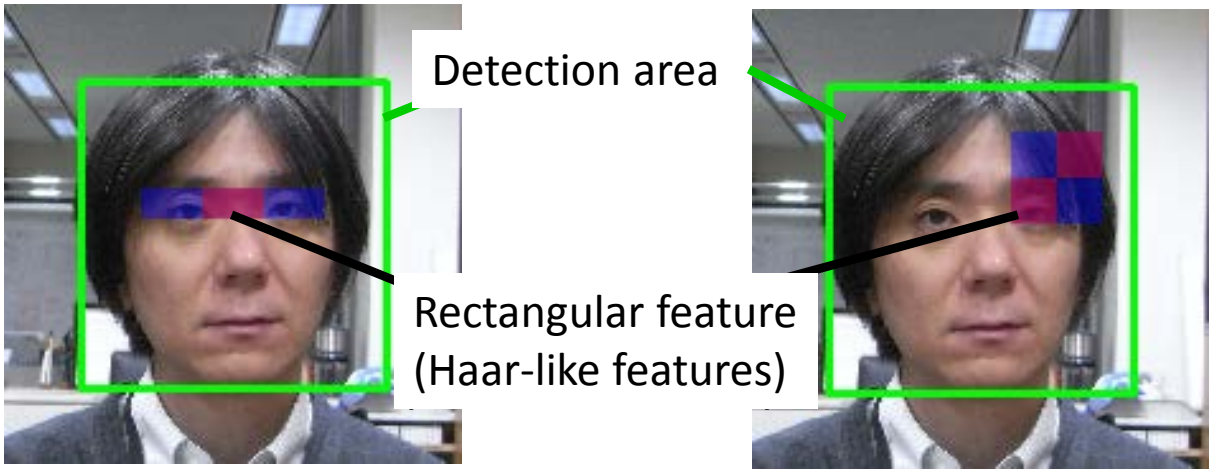
Focusing on Viola-Jones method results in detection failure.

Viola-Jones method

- Feature extraction using Haar-like features
- Multi-scale detection algorithm
- Constructs strong classifier with many weak classifiers (boosting)
- Achieves high-accuracy and high-speed detection



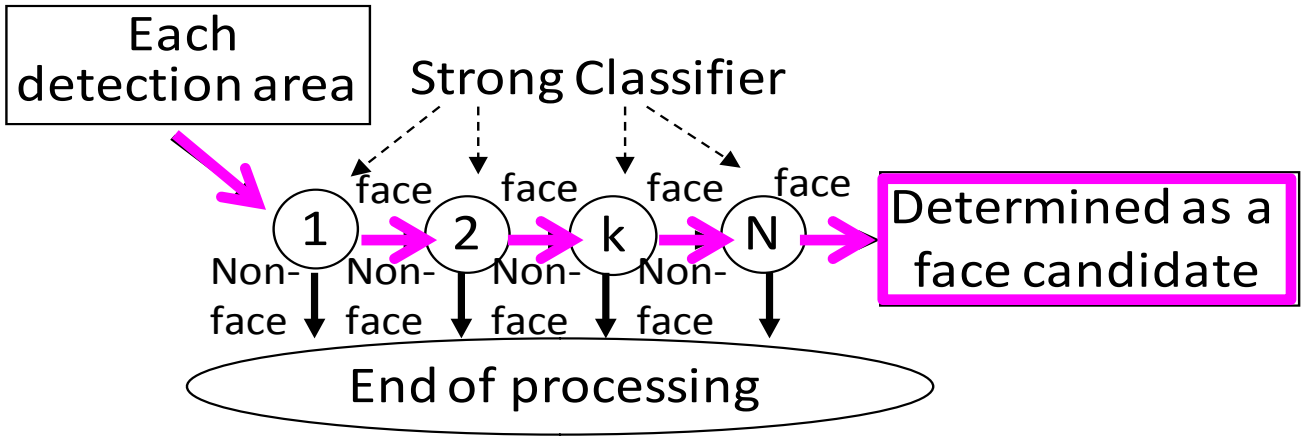
Examples of Haar-like features



Example of superposition of detection domain and rectangular feature

Principle of Viola-Jones method

- A weak classifier compares sum of luminance in Haar-like feature with a threshold value to distinguish the feature.
- A series of strong classifiers consisting of two of more weak classifiers composes multiple stages arranged in order.
- By supervised learning, rectangular features effective for face detection are chosen.
- Composition of weak classifiers and connection order of strong classifiers are determined in advance.



Face determination

- For each detection region, determine "face, non-face”; in the case of "non-face”, the process ends.
- **In the case of "face" on the *N* th strong classifiers,**

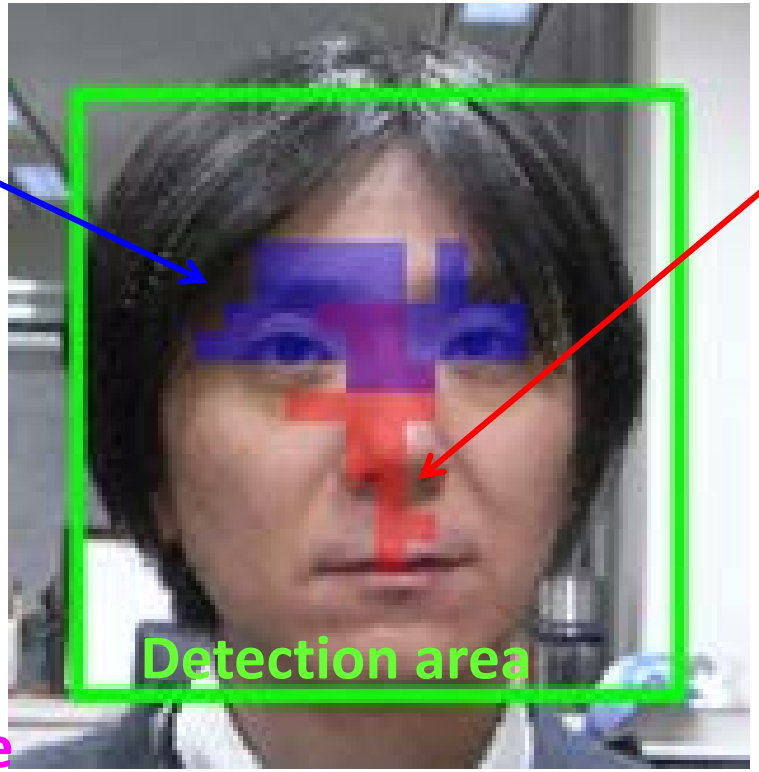
Processing in the area concerned ends.

Arrangement of noise light source

Analysis of effective arrangement for preventing feature extraction of Haar-like features.

Blue area: dark features → make bright so that features are obscured

Red area: bright features → made dark so that features are obscured



- **Specification of arrangement**
  - -Use Haar-like features of boosted classifiers.
  - -Calculate sum over detection area.
    - **+1: value in red area**
    - **–1: value in blue area**

- **Analysis result**
  - **- Red area:** Nose
  - **- Blue area:** Around eyes and around nose.

Best arrangement of light source noise

➡ **Around eyes and around nose.**

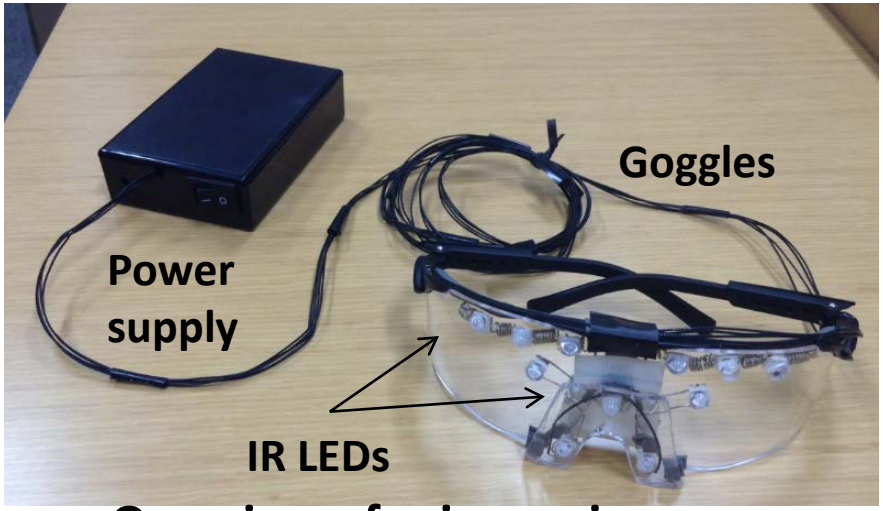
Outline

1. Background
2. Proposed method
   ～Add disturbance that prevents unintentional capture of facial images～
3. Prototype privacy visor
4. Evaluation experiment
5. Summary
6. Demonstration

Privacy visor

Eleven near-infrared LEDs were implemented in commercial goggles on basis of arrangement of noise light source.

- **Around eyes: 8 LEDs**
  - 6 placed on both sides of eyelids
  - 2 placed on both sides of pupils
- **Around nose: 3 LEDs**
  - 2 placed on both sides of nose
  - 1 placed between eyebrows.



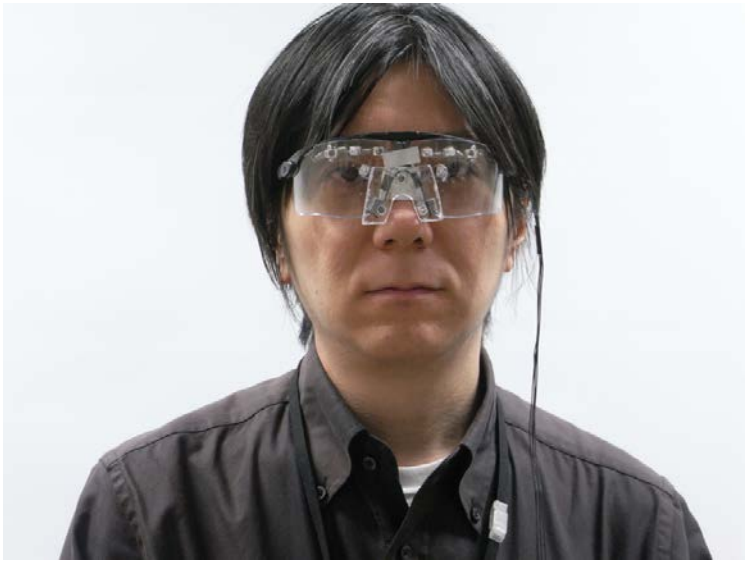
Overview of privacy visor

Specifications of a privacy visor

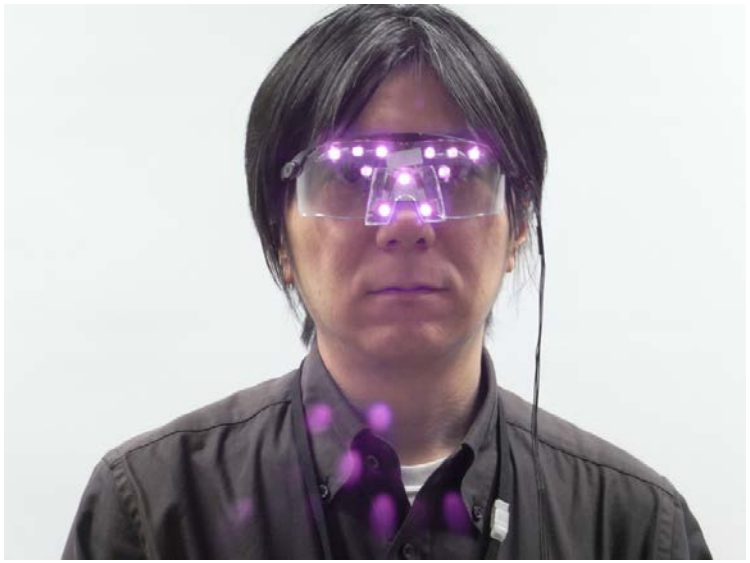
IR LEDs	Number：11, Peak wavelength：870 nm, Radiation intensity：600 mW/sr, Radiation angle：±15°, Rated current：1 A, Rated power consumption: 2.1 W
Goggles	Material frame: Plastic Lens: Polycarbonate,
Power supply	Li-Ion battery chargers (3.7V x 3) 2000mA/h

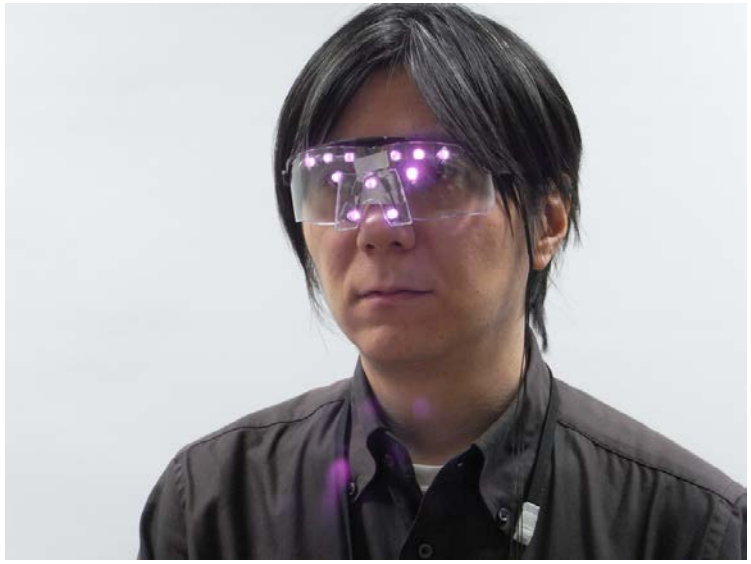
Prevents face detection with almost no facial discomfort.

Effect of wearing privacy visor



Without noise





With noise

Outline

1. Background
2. Proposed method
   ～Add disturbance that prevents unintentional capture of facial images～
3. Prototype privacy visor
4. Evaluation experiment
5. Summary
6. Demonstration

Evaluation experiment

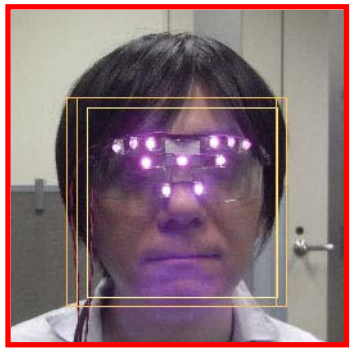
▪ Method

- Evaluators: 10
- Distance: 1 – 22 m
- Angle: 0°, 10°, 20°
- Using OpenCV face detector (strong classifier N=20)
- Distribution of number of people detection

	Capture conditions
(i)	Non-mounted privacy visor
(ii)	Mounted privacy visor without noise
(iii)	Mounted privacy visor with noise

▪ Detect face using Open CV algorithm

- Detection areas that pass all strong classifiers are candidate face.
- Detection area M (size variable) is determined as shown below.



M≥2: Face detected **M<2: Face not detected**

M ≥ 2: Determined that there is a face → Face is detected.

M < 2: Determined that there is no face → Face is not detected.

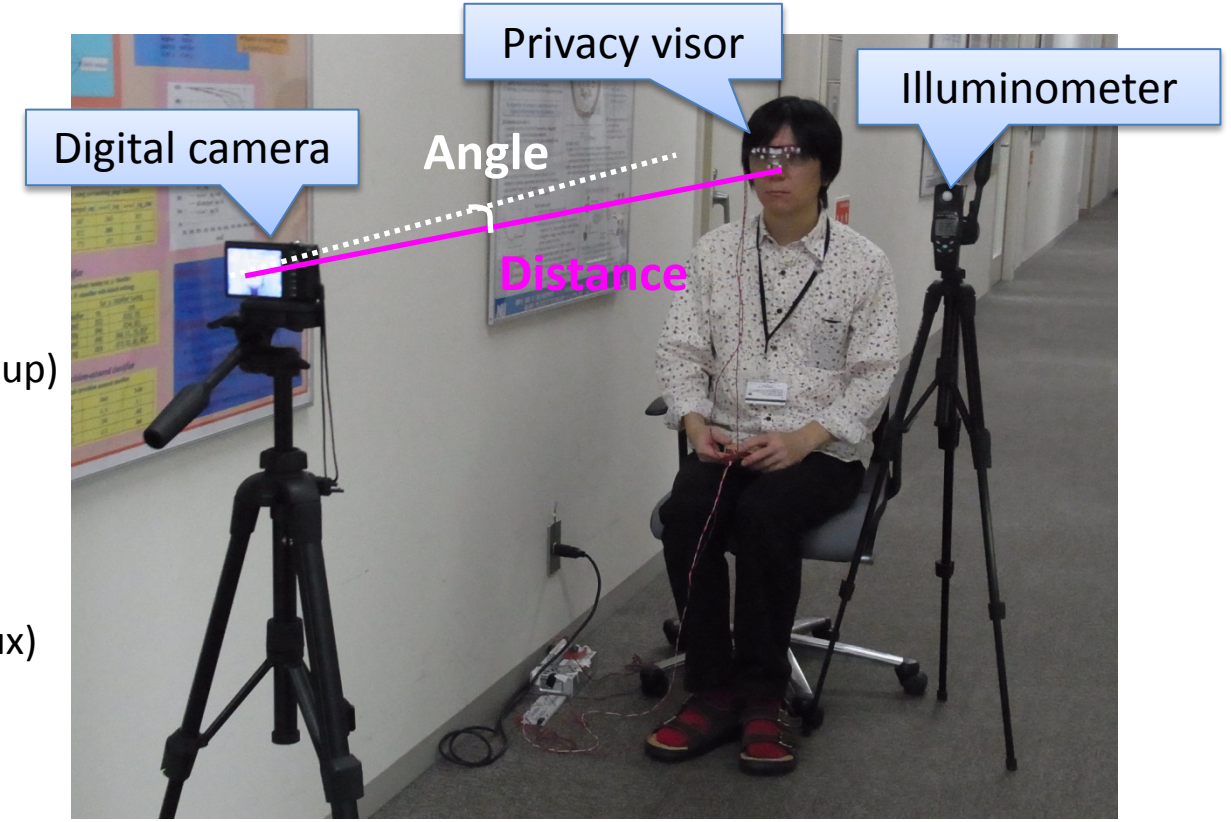
Evaluation environment

Digital camera

Manufacturer/Model: Ricoh R10
Number of pixels: 3264 x 2448 (8M)
Focus: Spot AF
Photometry: multi-aperture
Iris: f/3.3 (automatic setup)
Exposure time: 1/10 s (automatic setup)

Capture environment

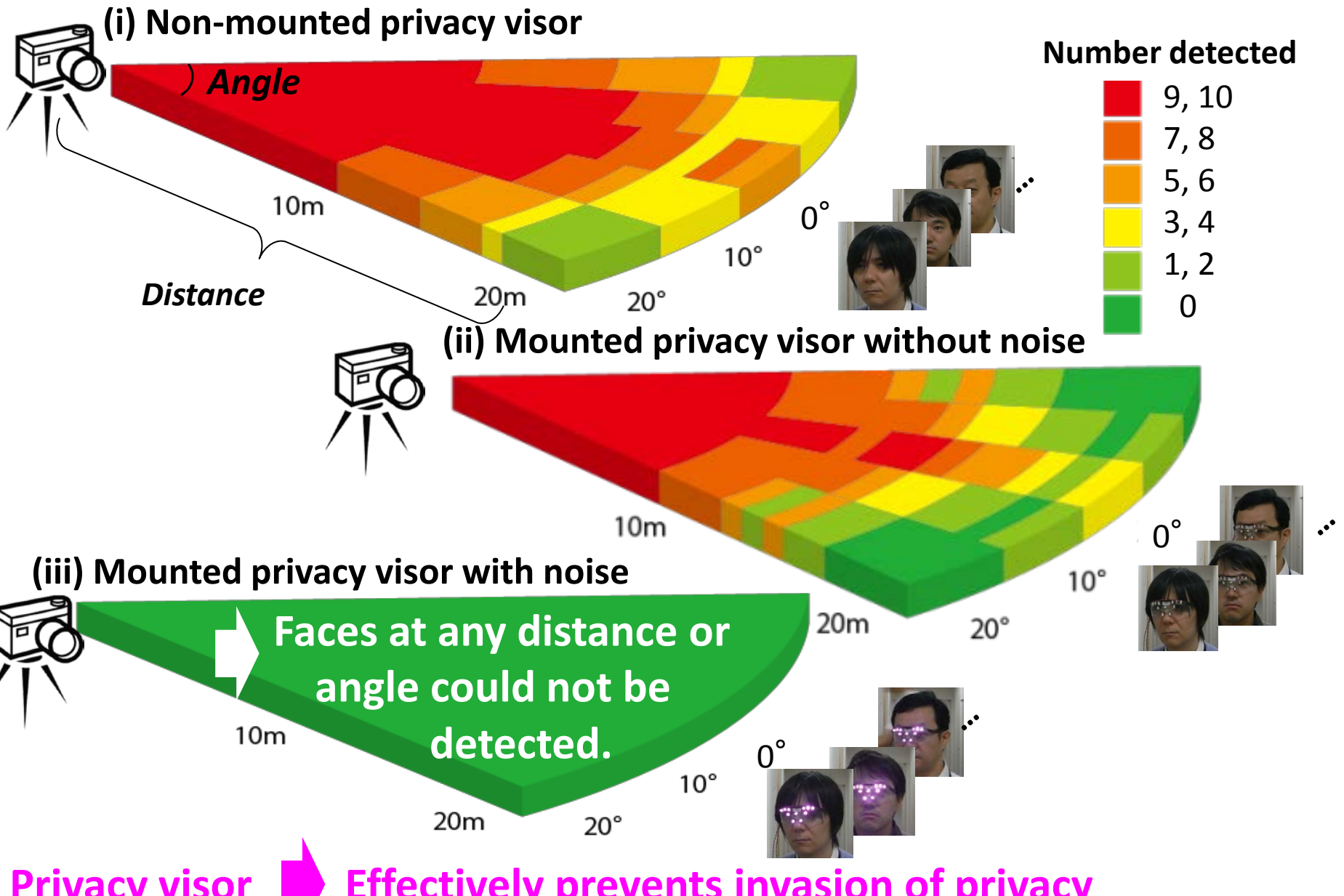
Distance: 1–22 m (1-m accuracy)
Angle: 0°/10°/20°
Lighting: Fluorescent light (67.5 Lux)



Images of ten evaluators captured at different angles and distances.

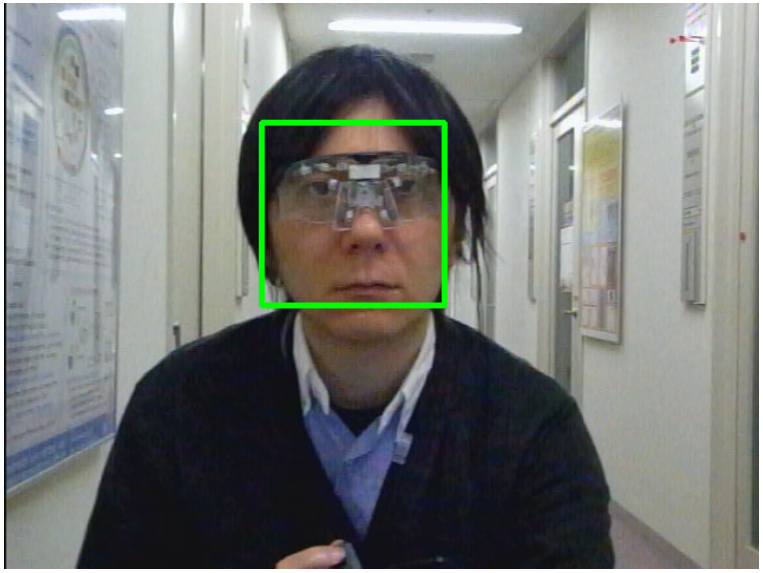
Image capture at 19 m

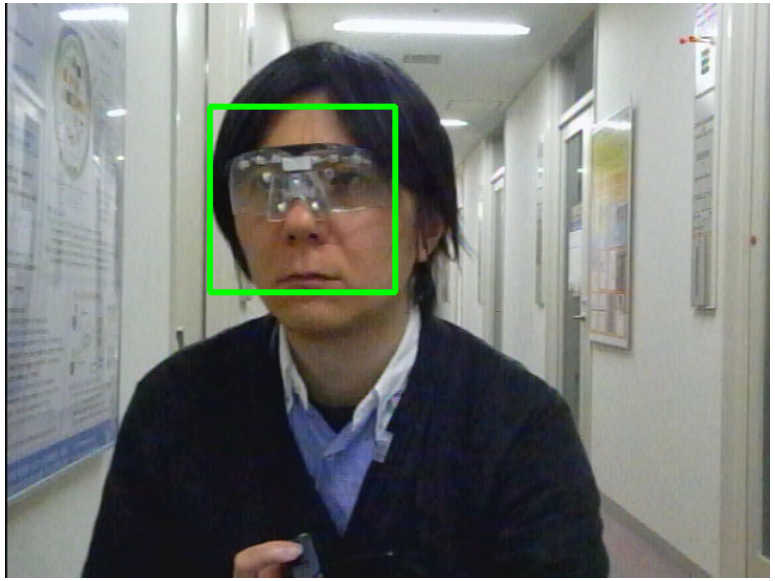
Evaluation result (Number of people detected)



Privacy visor ➡ **Effectively prevents invasion of privacy**

Detection results

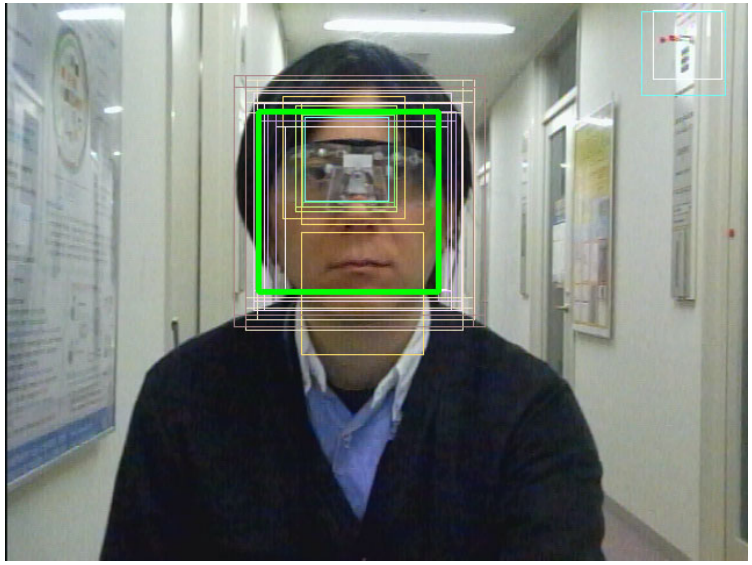


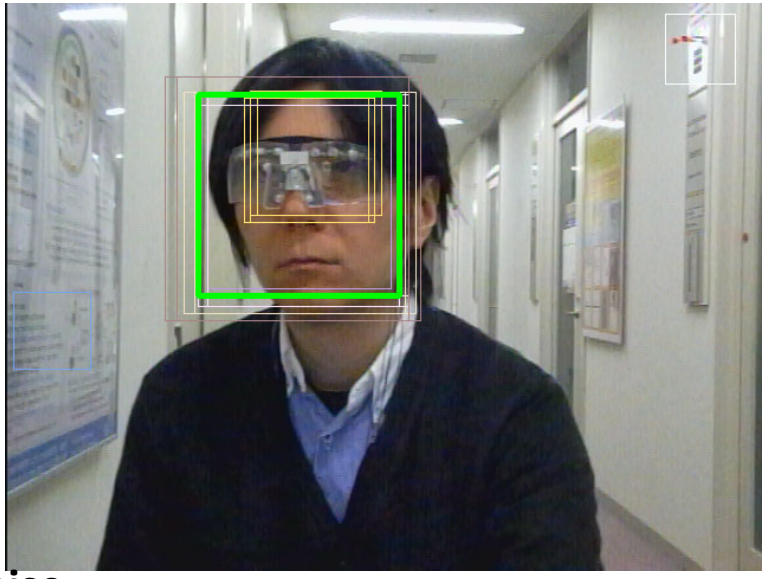


Without noise

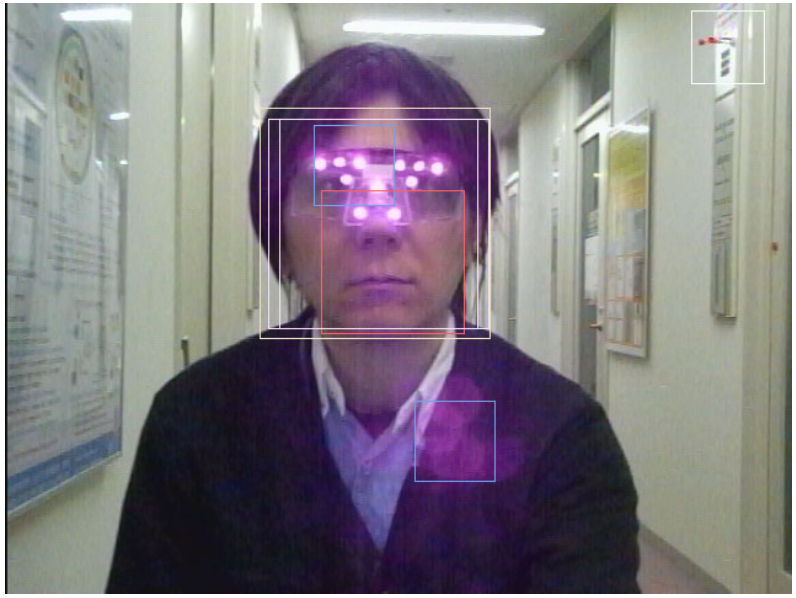
With noise

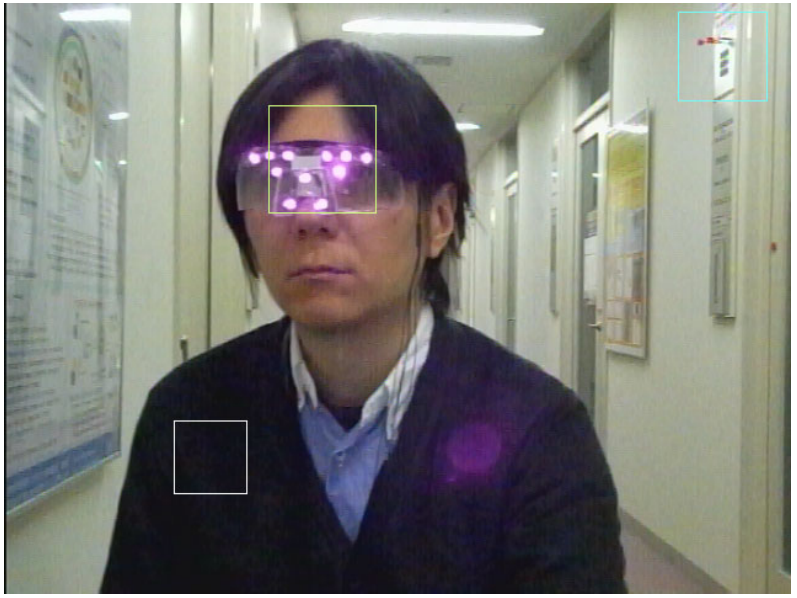
Detection results (detailed mode)





Without noise





With noise

Outline

1. Background
2. Proposed method
   ～Add disturbance that prevents unintentional capture of facial images～
3. Prototype privacy visor
4. Evaluation experiment
5. Summary
6. Demonstration

Summary

- **Spread of cell phones with digital camera, advances in SNSs and image search technology** → Invasion of privacy
- **Previous methods**

  Change coloring of face and hairstyle; wear “privacy shell”

  → The problem which hinder face-to-face communication in physical space

- **Requirements**

  Prevent face detection without causing facial discomfort.

- **Analyzed typical face detection method (Viola-Jones method)**

  Best arrangement of light source noise → Around eyes and around nose.

- **Prototype (privacy visor)**

  On basis of noise light source arrangement, 11 near-infrared LEDs were implemented in commercial goggles.

- **Evaluation experiment**

  Attached privacy visor (with noise): Face not detected (1–22m, ±20°)

  Privacy visor effectively prevents invasion of privacy.

Reference:

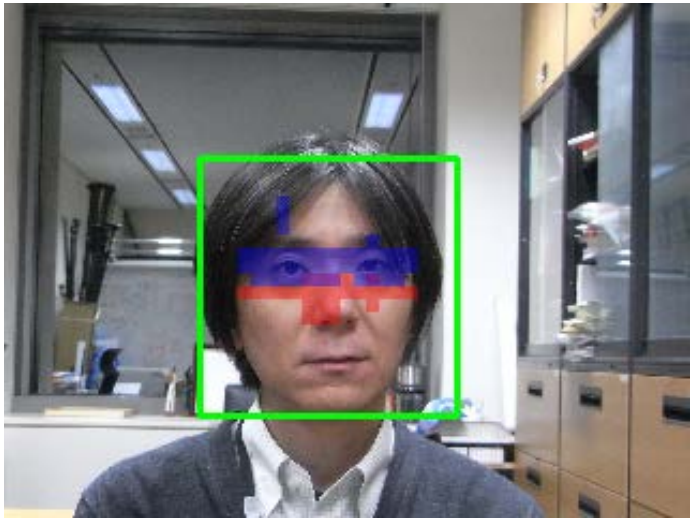
Privacy visor without power supply

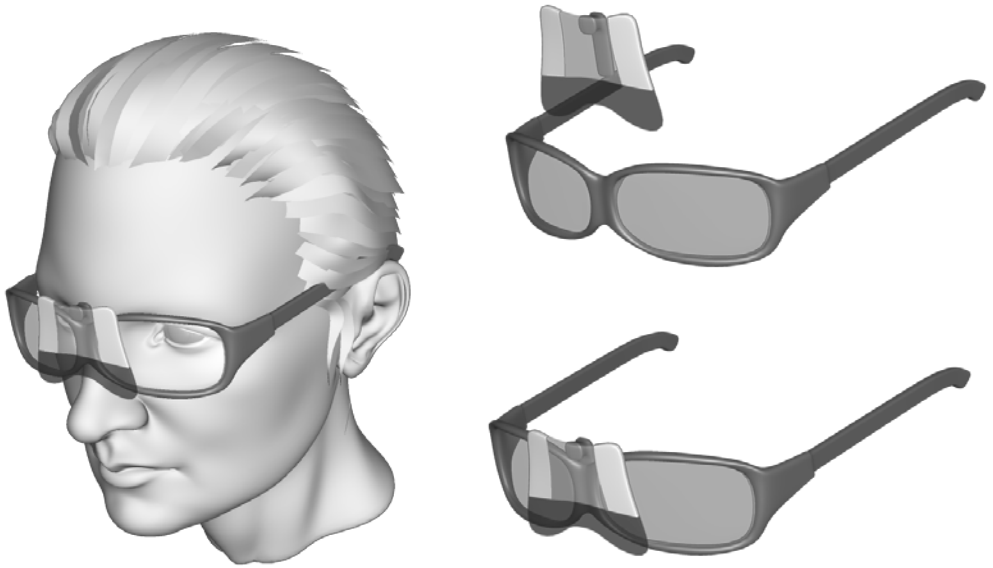
Low luminance area

High-intensity component consisting of materials that reflect specific wavelength or full wavelength of incident radiation in fixed direction (example: optical filter)

High luminance area

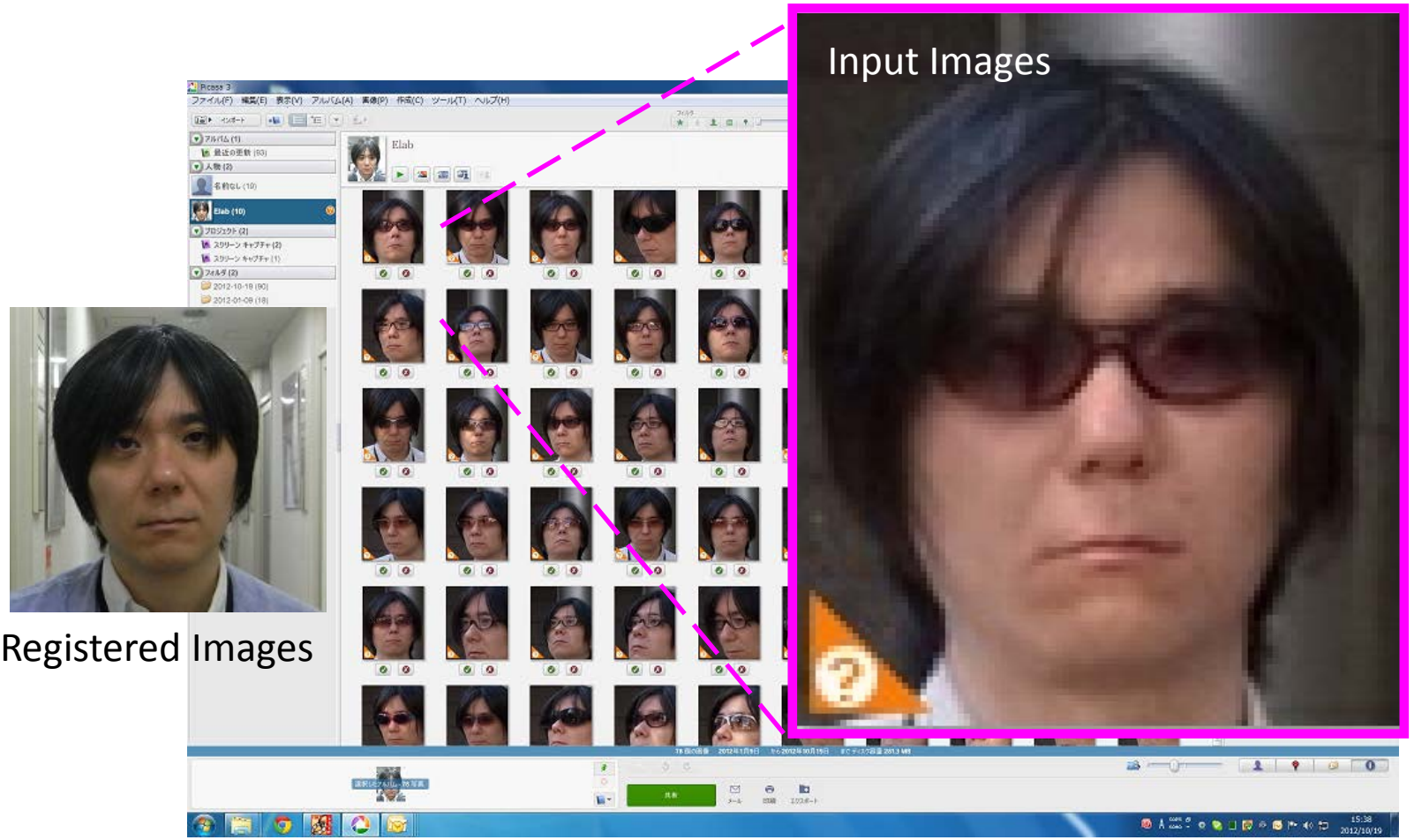
- Low-intensity component consisting of materials that absorb specific wavelength or full wavelength of incident radiation (example: optical filter)
- Component that makes domain concerned low-intensity to the visual confirmation from more than a fixed angle and beyond a fixed distance (example: privacy filter)





Reference:

Effect of using sunglasses



Input images with person wearing five different kinds of sunglasses were all recognized using Google Picasa image management software.

Face detection cannot be prevented with sunglasses.

Outline

1. Background
2. Proposed method
   ～Add disturbance that prevents unintentional capture of facial images～
3. Prototype privacy visor
4. Evaluation experiment
5. Summary
6. Demonstration