プライバシーバイザー：人間とデバイスの感度の違いを利用したプライバシー保護技術

越前 功
国立情報学研究所 コンテンツ科学研究系

研究背景

カメラ付き携帯端末の普及，SNSや画像検索技術の進展
- **カメラの写り込みによるプライバシー侵害**
- **Google Imagesなどの画像検索技術により，撮影者がいつ・どこにいたか暴露**

・写真撮影に合意した匿名の**被験者のうち1/3がFacebook上の写真と比較**することで人物を同定（CMUによるFacebookの実験，2011）
・Facebook，欧州で顔認識機能を無効に−規制当局の監査を受け(CNET Japan，2012.9.22)

顔認識技術がプライバシー侵害につながる危険性

従来対策

- **顔面への着色や髪形の変更により人物の顔検出を失敗させる手法**
  顔面への特殊パターンの着色や髪形を特殊な形状にする
  → 顔認識の前処理である顔検出を失敗させ，人物の同定を防止

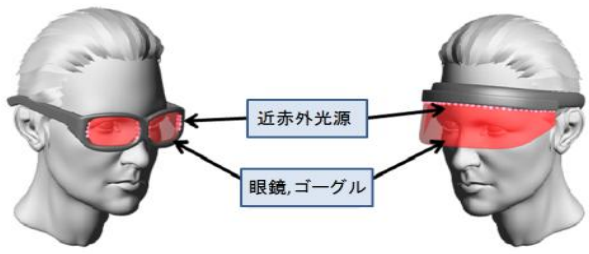
- **顔面を物理的に隠し人物のプライバシーを保護する手法**
  Wearable Privacy Shellと呼ばれる伸縮可能なShell状素材で覆う
  → ユーザのプライバシーを物理的に保護

物理空間における人対人のコミュニケーションに支障をきたす

目的と手段

目的：
人対人のコミュニケーションに支障をきたすことなく，カメラの写りこみによるプライバシー侵害を被撮影者側から防止する方法の確立

手段：
ウェアラブルデバイス（プライバシーバイザー）の顔面への装着により，人の視覚に影響を与えず，カメラの撮像デバイスのみに反応するノイズ（近赤外線）を顔面から照射し，顔検出を失敗させる

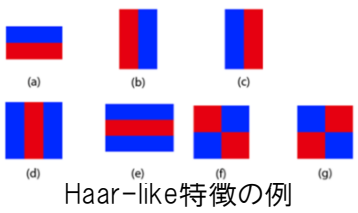


ノイズ光源をどのように配置すれば未検出となるか？

ノイズ光源の配置

代表的な顔検出法(Viola-Jones法)を解析
- Haar-like 特徴による特徴抽出
- 教師あり学習による判別器構成
- マルチスケール検出アルゴリズム

学習後の判別器構成(Haar-like特徴)を解析
→ 顔面上の違和感少なく，特徴抽出を失敗させる箇所にノイズ光源を配置

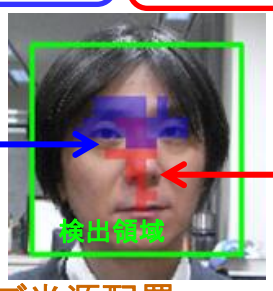


Haar-like特徴の例

配置の特定
・ 学習後の Haar-like 特徴の重合せ
赤い矩形内の数値：+1
青い矩形内の数値：−1
として，検出領域上に足し合わせ

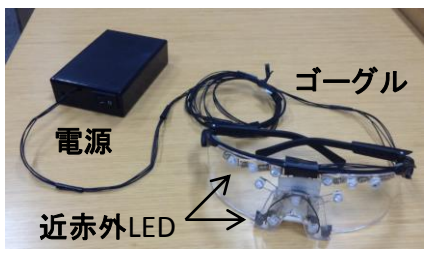
解析結果
・赤領域：鼻の周囲
・青領域：目の周辺および鼻筋

青い部分：暗い箇所 → 明るくすることで，特徴を破壊
赤い部分：明るい箇所 → 暗くすることで，特徴を破壊



青領域（目の周辺および鼻筋周辺）にノイズ光源配置

プライバシーバイザー



プライバシーバイザーの概観

プライバシーバイザーの仕様

近赤外LED	個数：11個，ピーク波長：870 nm，放射強度：600mW/sr，放射角：±15° 定格電流：1A，定格消費電力：2.1W
ゴーグル	フレーム材料：プラスティック， レンズ：ポリカーボネート，
電源	リチウムイオン電池(3.7V×3)， 2000 mA/h

市販ゴーグルに11個の近赤外LEDを取付け
顔検出を不能にするノイズ光源の配置に基く

目の周辺 8個（瞼両側：6個，瞳両側：2個）
最内側2個：0°，その内側2個：20°，外側2個：30°

鼻筋周辺 3個（鼻両側：2個，眉間：1個）

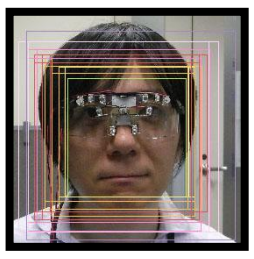

プライバシーバイザーの装着イメージ

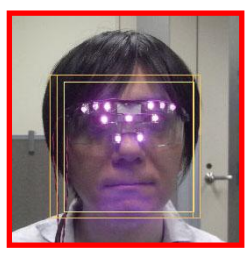
顔面上の違和感少なく，撮影時の顔検出を失敗させる

評価実験

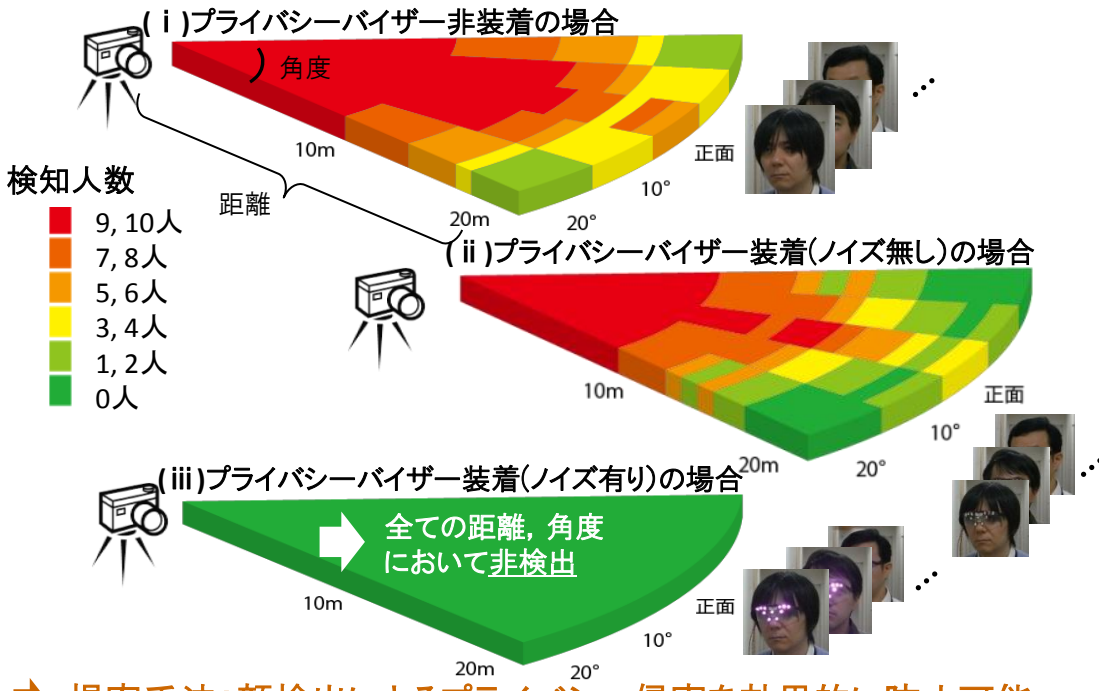
評価方法：
・評価者：10人
・撮影距離：1 – 22 m
・撮影角度：0°，10°，20°
・10人の評価者の検出人数の分布図より評価

被写体の条件	
(i)	プライバシーバイザー非装着
(ii)	プライバシーバイザー装着(ノイズ無し)
(iii)	プライバシーバイザー装着(ノイズ有り)


M≧2：検出


M<2：非検出

OpenCVによる顔検出：
・ 全ての強判別器を通過した検出領域は“顔候補”となる
・“顔候補”が含まれると判定された領域内に，その他の“顔候補”が含まれると判定された（近接するサイズの）検出領域の数M（個）が
M≧2 →当該領域に顔があると判定し検出
M<2 →当該領域に顔がないと判定し非検出



提案手法：顔検出によるプライバシー侵害を効果的に防止可能

NII 国立情報学研究所 National Institute of Infomation
連絡先：〒101-8430 東京都千代田区一ツ橋2-1-2
国立情報学研究所 コンテンツ科学研究系 越前研究室
TEL：03-4212-2516 FAX：03-3556-1916
Email：iechizen@nii.ac.jp

Privacy Visor: wearable device for preventing privacy invasion through face recognition from camera images

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

Background

Spread of cell phones with digital camera and Advances in SNS and image search technology had created invasion of privacy problems

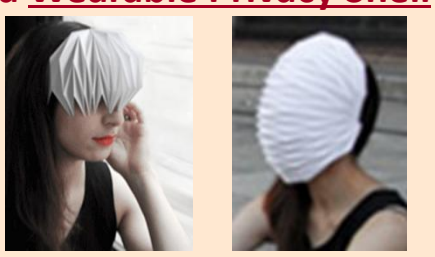
Increasing public self-disclosures through online social networks:

- Faces of Facebook: Privacy in the Age of Augmented Reality (BlackHat USA, Aug. 4, 2011)
- Germany: Facebook must destroy facial recognition database (Artstechnica.com, Aug. 16, 2012)

➡ **Invasion of privacy by unintentional capture of images of one's face**

Previous methods

- **Change coloring of face and hairstyle to prevent detection of human face**
- **Physically hide face by wearing, for example, a Wearable Privacy Shell**



(www.toxel.com/tech/2011/08/20/wearable-privacy-shells/)

(venturebeat.com/2010/07/02/facial-recognition-camouflage/)

➡ **Hinder face-to-face communication**

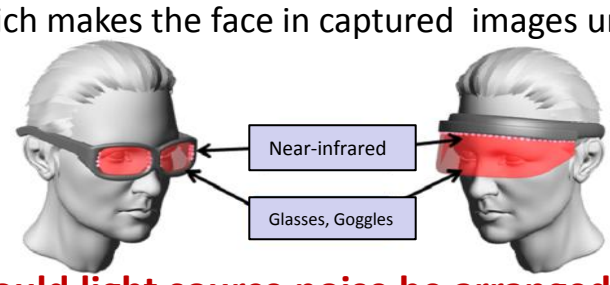
Purpose and means

Purpose:

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

Means:

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



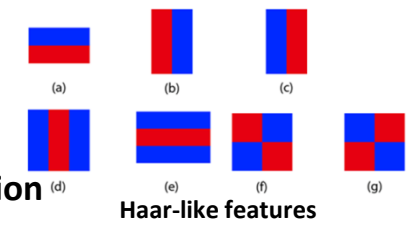
➡ **How should light source noise be arranged?**

Arrangement of light source noise

Use of Viola-Jones Face Detector

-Feature extraction with Haar-like features
-Classification using boosting
-Multi-scale detection algorithm

Analyze effect of arrangement on extraction of Haar-like features of boosted classifiers



Haar-like features

Specification of arrangement

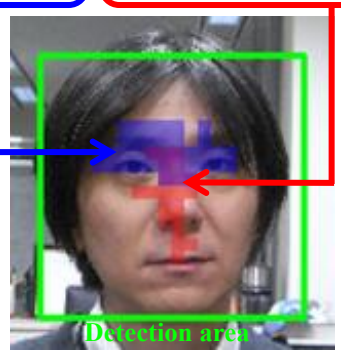
-Use of Haar-like features of boosted classifiers
-Calculate sum over the detection area
+1: value in red rectangle
-1: value in blue rectangle

Blue area: dark features → made bright, so features are obscured

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

Analysis result

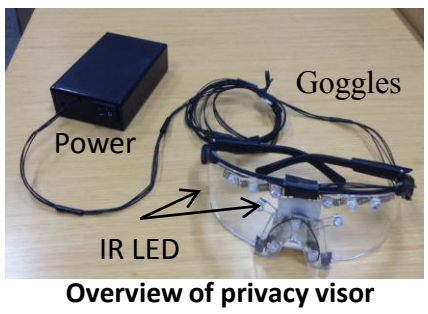
- **Red area:** Nose
- **Blue area:** Around eyes and around nose



Arrangement of light source noise:

➡ **Around the eyes and around the nose**

Privacy visor



Overview of privacy visor

Specifications of privacy visor

IR LEDs	**Number: 11; Peak wavelength: 870 nm, Radiation intensity: 600mW/sr; Radiation angle: 15°, Rated current 1A; Rated power consumption: 2.1W**
Goggles	**Frame material: Plastic Lens material: Polycarbonate**
Power	**Three lithium-ion batteries (12 V)**

Eleven near-infrared LEDs were implemented in commercial goggles

- **Around the eyes**
  6 placed on both sides of eyelids;
  2 placed on both sides of pupils
  (30°: inside two; 20°: outside two;
  0°: innermost two)
- **Around the nose**
  2 placed on both sides of nose;
  1 placed between eyebrows.

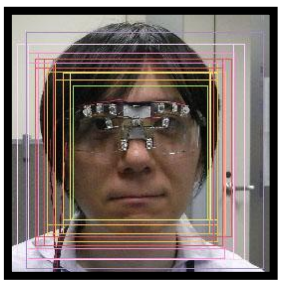
Effect of wearing privacy visor

➡ **Prevents face detection with almost no facial discomfort**

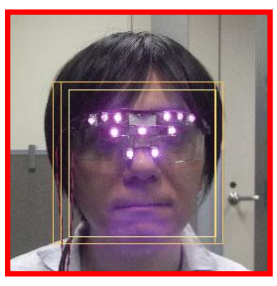
Evaluation experiment

Method:

- Evaluators: 10
- Distance: 1 – 22 m
- Angle: 0°, 10°, 20°
- Number of people detected: 0 – 10 people



M ≥ 2: Face detect



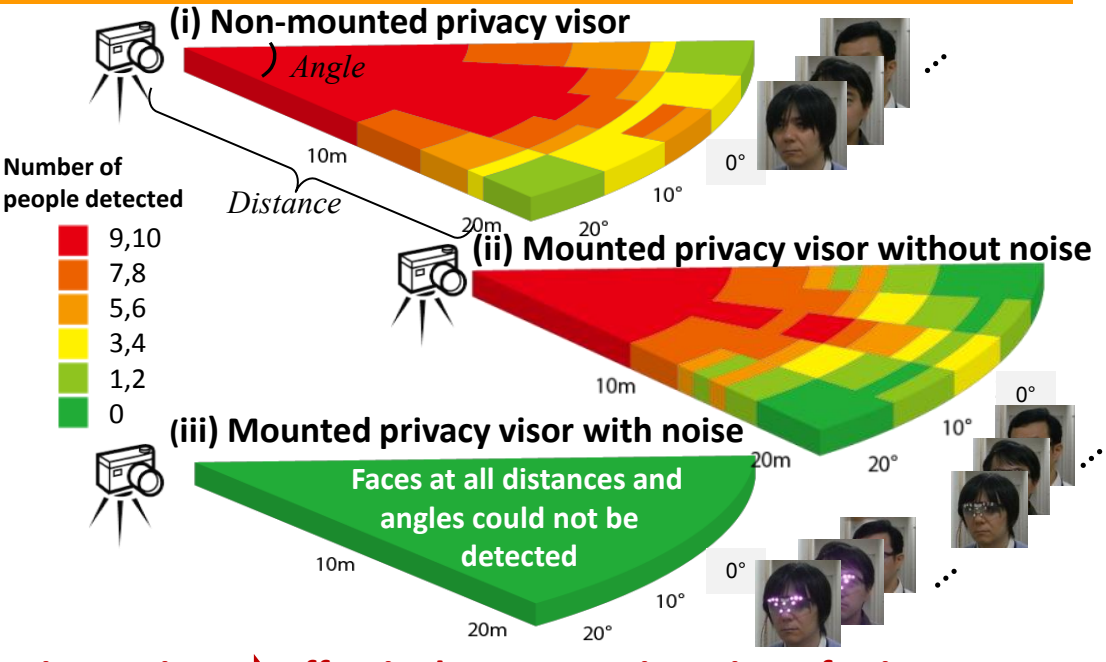
M < 2: Face not detect

Detect face using Open CV algorithm:

- Detection areas which pass all the strong classifier become candidate of a face
- In the area determined as the candidate of a face being contained, detection area (different sizes) M determined as the candidate of other faces being contained is shown as below

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

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



Privacy visor ➡ Effectively prevents invasion of privacy

NII
Contact: Isao Echizen – Associate Professor of Digital Content and Media Sciences Research Division
TEL: +81-3-4212-2516 FAX: +81-3-4212-2120 Email: iechizen@nii.ac.jp