CNN を用いた顔認証システムはプライバシーバイザーに効果があるのか

脇一史

背景

- 顔認証カメラの利用が進んでいる
  - 個人の追跡
  - 防犯や商用に活用[1]
- 追跡回避や削除要求などの課題[2]
  - 顔を隠すことで追跡が停止できると言われている.
- プライバシー保護を目的としたデバイスが商用化

[1]

[2]

[1]朝日新聞，“成田、出国手続きも「顔認証」開始 待ち時間の短縮狙い”，2018-10-03, https://www.asahi.com/articles/ASLB33398LB3UDCB00C.html
[2]朝日新聞，“大阪駅ビル顔で追跡”，2014年1月6日 朝刊 pp.1

研究目的

- プライバシーバイザー[3]は顔認証の精度を低下させる効果はあるのか

プライバシーバイザーは顔の凹凸による明暗差をフィルターによって分析し顔かどうか判別するものである（Haar-like特徴量）

[3]山田隆行，合志清一，越前功“光の反射・吸収特性を利用した撮影画像からの顔検出防止手法”，情報処理学会論文誌Vol.55，No 9，pp.2104-2119，Sep. 2014.

実験目的

1. CNNによる顔認証の精度を明らかにする
   - 口や目で判別する専用識別器では外乱に弱い
   - CNNは画像認識で有用なディープラーニング技術の一つ
2. 素顔を学習したときに識別精度を下げる外乱を明らかにする
   - 素顔
   - プライバシーバイザーOFF（通常）
   - プライバシーバイザーON（保護）
3. 外乱ごと学習したときの外乱の精度を明らかにする
   - 同上

実験内容

1. 顔画像データの取得
2. 顔画像データの拡張
3. CNNの構成
4. 素顔で学習したCNNに対する追跡停止の評価
5. プライバシーバイザーで学習したCNNに対する追跡停止の評価

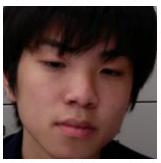
顔画像データの取得

- iMacのwebカメラを使用
- 画面上に枠を出し、その範囲内に収まるように撮影
- CNN作成用データ
  - 被験者　: 20名
  - 撮影枚数/人: 100枚×2日＝ 200枚
- 評価用データ
  - 被験者　: 20名
  - 撮影枚数: 100枚

	CNN作成用データ	評価用データ
被験者	20名	20名
撮影枚数	100枚×2日＝ 200枚	100枚

顔画像データの拡張

- 取得画像を224 × 224にリサイズ
- 右図の9パターンの調整を行った
  - ❑元画像含め2,100枚


元画像


コントラスト 47%

手法	コントラスト調整	左右反転	ガウシアンノイズ
種類	12% 23% 35% 47% 59% 70%	1	2 4
計	6	1	2

CNNの構成

- VGG-16[4]という識別手法を参考にした
  - ❑Fine-tuningを使用
    - » 学習済みのモデルを転用して新たなモデルを生成する
  - ❑Dropout[5]を追加
    - » ニューロンをランダムに消去し過学習を抑制
- 2,100枚 × 20人 ＝ 42,000枚
  - ❑40,000枚を学習データ
  - ❑2,000枚をテストデータ
- 学習回数: 10epoch

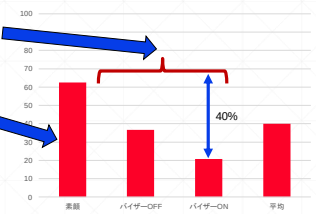
[4] Karen Simonyan and AndrewZisserman(2014):Very Deep Convolutional Networks for Large-Scale Image Recognition, ICLR,2014.
[5]斎藤康毅, “ゼロから作るDeep Learning python で学ぶディープラーニングの理論と実装”, OREILLY, 2016.

CNNでの追跡停止の評価

- 素顔&外乱画像それぞれでCNNを構築
  - ❑3つのCNNを作成
  - ❑それぞれの画像で適合率を計算
  - ❑被験者Aの適合率$P_A = \frac{A\text{と正しく判定した数}}{\text{被験者}A\text{と判定した全ての画像数}}$
  - ❑全員の適合率の平均を比較

素顔で学習したときの結果

- バイザーを加えることで識別率は25-40%低下した
- 素顔が最も高くなった
  - ❑顔全体が露見しているため多くの特徴量から学習できた



外乱画像を学習した結果

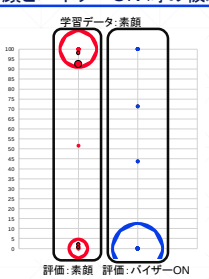
- 学習と評価が同じ組み合わせの中ではバイザーONが一番低かった.
- 学習，評価どちらも平均適合率が最も高かったのはバイザーOFFであった.

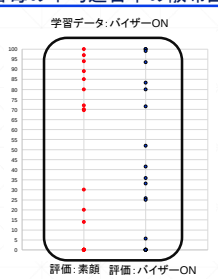
学習＼評価	素顔	バイザーOFF	バイザーON	平均
素顔	62.59	36.67	20.75	40.00
バイザーOFF	27.36	59.37	44.78	43.80
バイザーON	40.34	42.58	42.28	41.73
平均	43.40	46.21	35.90	41.84

- 一般的なサングラスよりもバイザー装着時の方が外乱頑強性が高い。

	2017	2018
手法	独自 CNN(vgg-11)	keras(vgg-16)
外乱	帽子，マスク，サングラス	プライバシーバイザー
精度	54.80	41.73
外乱頑強性	低い	高い

素顔とバイザーON 時の被験者毎の平均適合率の散布図





考察、おわりに

- 素顔の学習に対して、バイザーの評価はほぼ0%であった
  - 素顔の学習は目元の特徴量を多く判断材料にしている可能性がある
- バイザーの学習に対して、素顔の評価に被験者毎の違いがみられた
  - 目元の特徴量に依存しない被験者はバイザーを装着しても識別されてしまう
- CNNを用いた顔認証システムでは，プライバシーバイザーは，顔の認証精度を低下させる効果はあるが，それごと学習されてしまうと，認証精度が向上することを示した

12