

暗証番号入力時における瞳孔の位置情報を利用した非正規ユーザ検知

広島市立大学 大学院情報科学研究科情報工学専攻
稲村 勝樹(代表), 高野 知佐

概要

- 現在の普及している認証コード(記憶情報)を用いた認証
 - ・ 流出、紛失といった問題
 - ・ 入力情報のみでは正規ユーザか判別できない
- 認証コードの入力時の目の動きに注目
 - ・ 専用機器を必要とせず、内部カメラで使用可能なOpenPoseの利用を検討

認証コードが流出した場合でも非正規ユーザを遮断できないか考える必要がある

1.OpenPose

- ・ 骨格を検出する姿勢推定ライブラリ
- ・ 画像や動画から人の関節点を検出、それらを線でつなぎ合わせて骨格を表示 (図1)

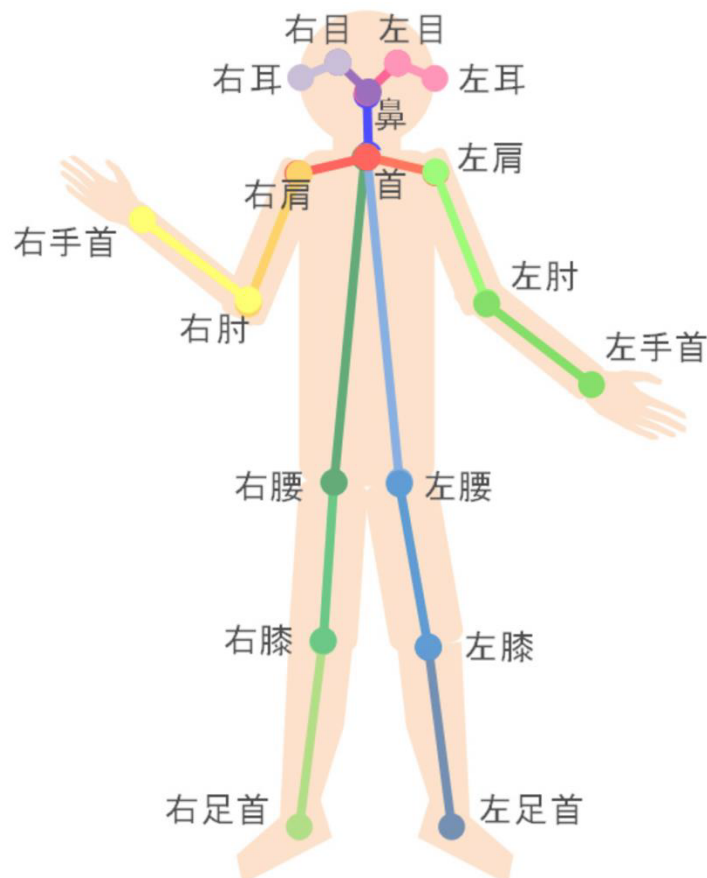


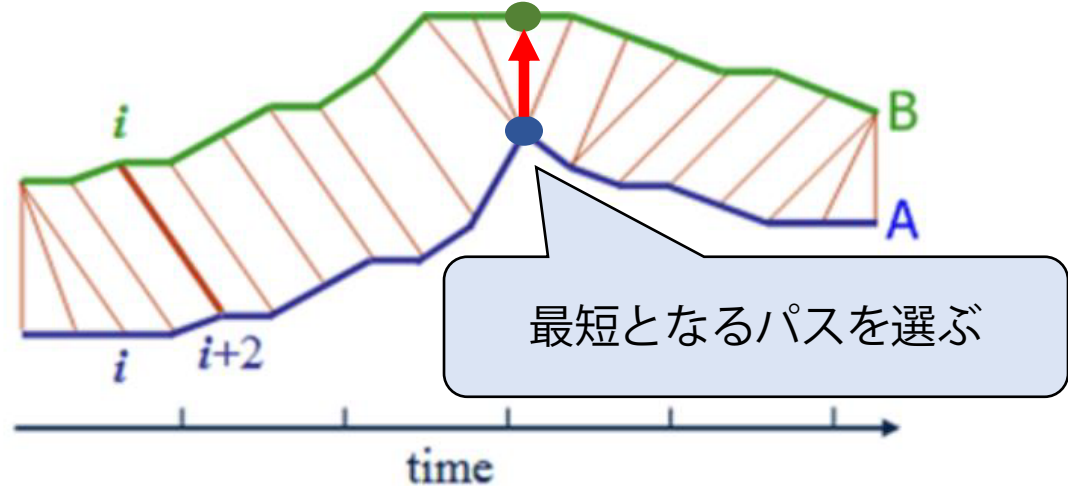
図1 OpenPoseによって求められる関節点

2.調査に用いるデータ

- OpenPose
 - ・ 目の関節点の2次元座標(x,y)の時系列データを調査のためのデータとして利用
- 差分系列
 - ・ 時間的な変化やパターンを捉える際に使われる
 - ・ 1時点前のデータとの差をとった時系列データ
 - ・ 時刻*i* (*i* = 1, 2, 3, ...)に対し現時刻のデータを x_i 時系列データを X_i として

$$X_i = x_{i-1} - x_i$$

- DTW距離
 - ・ 時系列データ同士の類似度を測る手法の1つ
 - ・ 2つの時系列データの各点の距離を総当たりで求め、最短となるパスを見つける
 - ・ その最短のパスの合計によって算出



3.実験の想定状況

- ・ 非正規ユーザが不正ログインしようとする状況
- ・ 認証コードは4種類 (数字：4文字, 6文字 文字：8文字, 16文字)
- ・ 17人の被験者を非正規ユーザとして実験

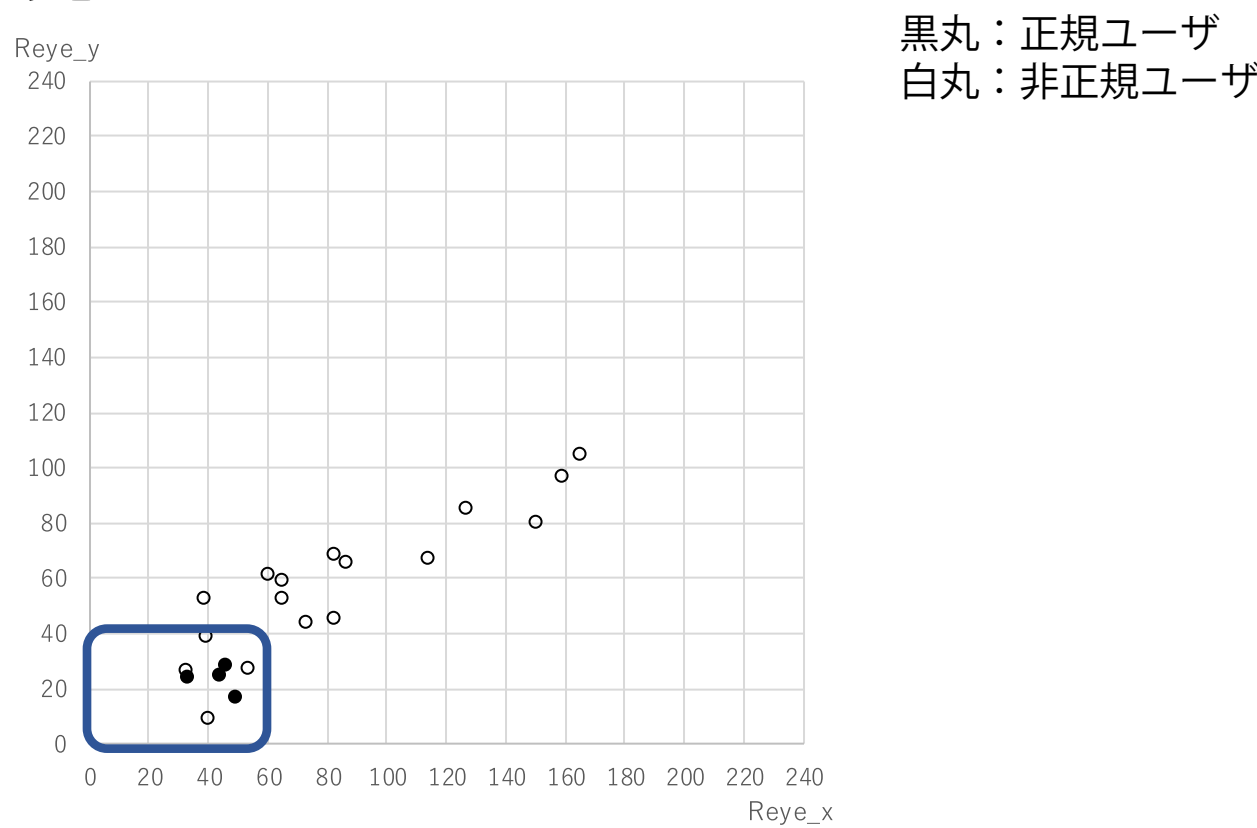
4.実験方法

- 実験手順
 - ・ 被験者(非正規ユーザ)に認証コード(4種類)を書いたメモを渡す
 - ・ 認証コードを入力している様子を撮影
 - ・ OpenPoseを利用して動画から関節点(x,y)を抽出
 - ・ 差分系列からDTW 距離の算出

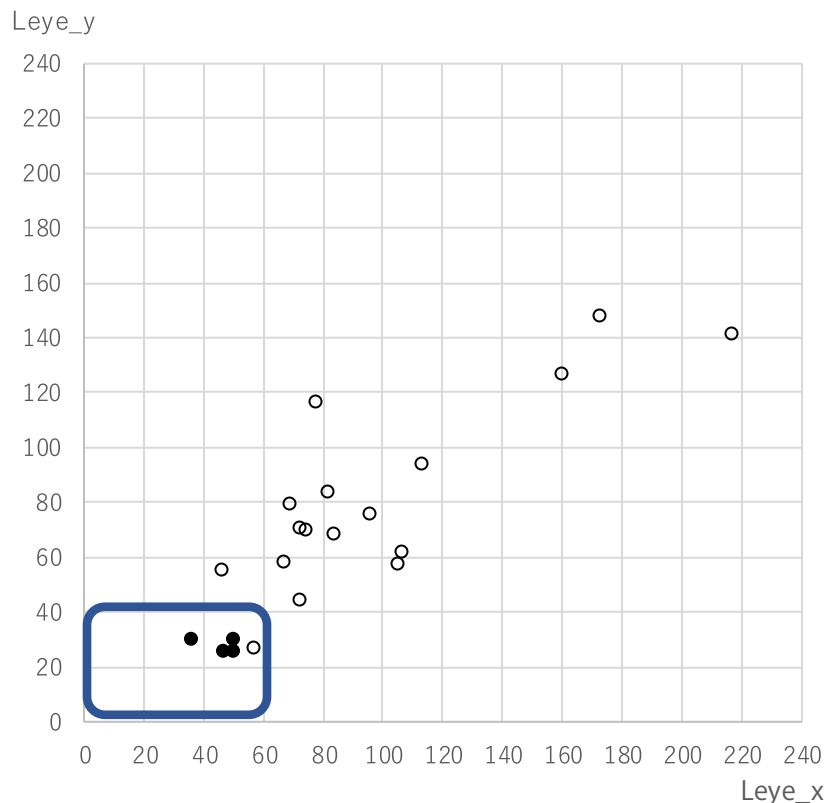
非正規ユーザと正規ユーザの比較したDTW 距離を算出
正規ユーザのデータ同士からもDTW 距離を算出

5.実験結果

- 実験結果
 - ・ 閾値を設けることで正規ユーザと非正規ユーザに概ねグループ分けが可能
 - ・ 正規ユーザと比較したDTW 距離の方が小さい値をとる傾向が見られた



数字4文字の認証コードのDTW距離(右目)



数字4文字の認証コードのDTW距離(左目)

6. 今後の課題

- ・ 非正規ユーザの試行回数を増やした場合の実験
- ・ 精度向上のための検討
- ・ 実用性の検証

7. 参考文献

[1] CMU-Perceptual-Computing-Lab."OpenPose".Github
<https://github.com/CMU-Perceptual-Computing-Lab/openpose/releases>