原著論文 Original Paper

ユーザ敵対型ニューラルネットワーク

ウェアラブルセンサを利用した行動認識におけるユーザ汎化とプライバシーへの配慮のためのユーザ独立な表現の学習手法

User-Adversarial Neural Networks :

Learning User-Independent Features for User-Generalization and Privacy-Protection in Activity Recognition using Wearable Sensors

岩澤 有祐 Yusuke Iwasawa
東京大学大学院工学系研究科技術経営戦略学専攻
Graduate School of Engineering, The University of Tokyo, Japan
iwasawa@weblab.t.u-tokyo.ac.jp

矢入 郁子 Ikuko Eguchi Yairi
上智大学大学院理工学研究科理工学専攻
Graduate School of Science and Technology, Sophia University, Japan
i.e.yairi@sophia.ac.jp

松尾 豊 Yutaka Matsuo
東京大学大学院工学系研究科技術経営戦略学専攻
Graduate School of Engineering, The University of Tokyo, Japan
matsuo@weblab.t.u-tokyo.ac.jp

keywords: user-independent features, user-generalization, privacy-protection, wearable sensors, activity recognition

Summary

This paper proposes a novel neural networks based model for learning user-independent features. In activity recognition using wearable sensors, user-independence of features could provide better user-generalization performance, enhance privacy protection, and both are important for using activity recognition techniques in a real-world scenario. However, designing such features is not an easy task, because it is not clear what kind of features become user-independent, and moreover, poor design of user-independence harms activity recognition performance.

Hear, we propose *User-Adversarial Neural Networks* for automatically learning user-independent features. The proposed model considers an adversarial-user classifier in addition to a regular activity classifier in the training phase, and learn the features that help to distinguish the activities but obstruct to distinguish the users. In other words, the model explicitly penalizes representations for becoming user-dependent, while keeping activity recognition performance as much as possible. Our main result is an empirical validation on three activity recognition tasks regarding wearable sensor based activity recognition. The result shows the proposed model improves independence of features comparing with the regular deep convolutional neural networks in both qualitatively and quantitively. We also summarize future work for better user-generalization and privacy protection from the perspective of the representation learning.

1. は じ め に

ウェアラブルセンサによる人間行動の認識と計測（以降行動認識と呼ぶ）は，高齢者の転倒検出などの見守りシステムやヘルスケアシステムなどの実現のための中心的な技術要素である．画像認識や音声認識などの領域と同様，行動認識においてもディープニューラルネットワーク (DNN) が高い認識精度を示すことが近年の研究で示されている [Hammerla 16, Yang 15, Plötz 11]．行動認識でよく利用される加速度センサやジャイロスコープなどの慣性センサは生データに近く人間による特徴設計が難しいこと，行動認識と一口に言えども認識したい対象はアプリケーションによって異なること，それゆえアプリケーションごとに有効な特徴量は異なることなどから，DNN は今後も重要度を増していくものと考えられる．

本稿では行動認識のための DNN の拡張として，学習する表現のユーザ独立性を高めるモデル User-Adversarial Neural Networks （UANN）を提案する．ここで，表現のユーザ独立性とは，形式的には表現を表す確率変数 R とユーザを表す確率変数 U の独立性であり，ユーザ独立ではない，すなわちユーザ依存であるとは特徴量の値がユーザごとに異なることを意味する．例えば，あるユーザの歩き方のみに強い値を取るような特徴量や，ユーザにより値が異なるような特徴量はユーザ依存な特徴量である．行動認識において，学習される表現 R のユーザ独立性は少なくとも 1. ユーザ汎化性能，2. プライバシーへ

の配慮の 2 つの観点から重要である．

ユーザ汎化性能とは，ある特定のユーザ群のデータで訓練されたモデルが学習時に含まれないユーザに対してどの程度の性能を達成するかという観点である．行動認識では，各ユーザに対するラベルの確保の難しさからユーザごとにモデルを用意することは現実的には難しく，ユーザ汎化性能をいかに高めるかが実用上重要となる．一方，1 つ 1 つの行動の仕方や癖は人によって異なり，ユーザ汎化性能を高めることは難しい問題であることが知られている [Bulling 14]．例えば Lane らは 50 名分の行動データセットを利用した実験を行い，20 代，30 代のデータで訓練したモデルは 20 代，30 代のユーザに対しては 80%から 90%の精度を達成する一方で 65 歳以上に対しては 60%程度であったことを報告している [Lane 11]．また，Weiss らは特定のユーザのデータを使って訓練した個人モデル（personal model）と特定のユーザ以外全員のモデルを使って訓練したモデル（impersonal model）の認識精度を比較し，後者の認識精度が 20%程度低くなることを報告している [Weiss 12]．

ユーザ汎化性能が高まらない要因の 1 つとして，特徴量がユーザ独立になっていないこと，すなわち特徴量が同じ行動でもユーザにより異なる値をとっていることが考えられる．例えば Lane らは上記と同様のデータセットを利用して，20 代，30 代が歩いている時と 65 歳以上の人が歩いている時の特徴量の値がほとんど重ならないことを報告している [Lane 11]．特徴空間 R がユーザに依存している場合，R からラベル空間 Y への写像を与える分類器 $f_y : R \to Y$ が仮に特定のユーザ群によく適合していても，その他のユーザには利用できない可能性がある．

第 2 の観点がプライバシーである．ユーザが身につけるセンサを利用して行動認識を行う場合，収集されたデータは個人に関する情報を含みうるパーソナルデータであり，ユーザの同意に基づいたデータの計測と利用が原則となる．行動認識におけるプライバシー問題の 1 つとして，生データが持つ情報量の大きさとアルゴリズムの進歩による情報暴露 (discrousure）の危険性が指摘され始めている [Raij 11]．例えば，加速度センサは行動の認識に利用可能である一方で，性別や年齢などの属性情報の推論にも可能であることが知られている [Brdar 13]．また，さまざまな研究で疾病状態を予測するためにも利用されている．仮に行動認識のための特徴量としてユーザに依存する歩き方などの利用を許容すると，その背後にあるユーザの属性情報（年齢，性別，疾病の有無など）を暗黙的に収集してしまう可能性がある．この状態は，ユーザ側からすれば同意しない情報を取得されるリスクを，アプリケーション提供者としては意図しない個人情報の取得により無用なプライバシーリスクを負う可能性があり望ましくない．ユーザ独立な特徴を利用すること，ユーザ（あるいはその属性）に依存するような特徴を利用しないように制約をかけることができれば，このようなプライバシー問題を低減することができると考えられる．

ここで，ユーザ独立性を高めることは究極的には行動の予測性能とトレードオフになりうることは重要である．例えば，単純にユーザ独立性を高めるのであれば完全にランダムにデータをマッピングすれば良いが，そのような写像は明らかにデータの持つ重要な性質を取り除いてしまう．すなわち，プライバシーに配慮しながら適切に行動認識を行うためにはユーザ独立性を高めることと行動に関する予測精度を高めるという 2 つの問題を考える必要がある．

本稿ではユーザ独立な特徴を獲得する問題を，特徴量 R のもつ行動 Y に関する情報を最大化しながら，ユーザ変数 U に関する情報を最小化する問題として定式化する．そのうえで，上記の最適化問題を解く方法として敵対的訓練（Adversarial Training）を利用した User-Adversarial Neural Networks （UANN）を提案する．敵対的訓練によるユーザ独立な特徴獲得のアイディアは，特徴量 R からユーザ変数 U を予想しようとする敵対的ユーザ分類器 f_u を騙すように特徴抽出器 $f_f : X \to R$ を学習させることである．すなわち，提案手法では識別器 f_u が R からどの程度 U を予測できるかをユーザ独立性の指標へと利用する．敵対的訓練を利用した DNN の拡張により，DNN による高い識別能力を活用しながらユーザ独立な特徴量を獲得できることが期待される．

本稿では，提案手法によりユーザ独立な表現が獲得できることを，慣性センサを利用したパブリックな行動認識データセット 2 つ（3 つの分類タスク）を利用して検証する．具体的には，行動認識精度とユーザ認識精度の 2 つの観点を用いて，行動認識でよく利用される畳み込みニューラルネットワーク（CNN）と比較して提案手法が行動認識精度を維持しながらユーザ独立な表現を獲得することができることを定量的に検証する．また，学習された特徴空間でのクラスタリングにより得られるクラスタのユーザ独立性を視覚化し，表現のユーザ独立性が改善していることを定性的に確認する．これらの検証を通じて，提案手法により既存の手法と比較してよりユーザ独立な特徴が獲得できることを示す．

本稿の主要な貢献は次の通りである．

- ユーザ独立な特徴を獲得する問題を，行動に関する認識精度を最大化しながらユーザに関する認識精度を最小化する問題として定式化した．その上で，最適化問題を解くニューラルネットワークのモデルを提案した （3 章）．また，情報理論的独立性の指標である相互情報量と提案手法の関係を整理することで，提案手法の妥当性について論じた．
- 実データによる検証により，提案手法が単純な DNN と比較してよりユーザ独立な特徴を確認できることを示した （4 章）．この結果は，敵対的訓練によるユーザ独立性の指標の利用が実際にユーザ独立性を

高めることに貢献することを示したものである．
- 実験により得られた結果から，ユーザ独立性およびユーザ汎化性能を高めるための課題，プライバシーへの配慮をより良く行うための課題をまとめた（5章）．

2. 関 連 研 究

2·1 行動認識とディープニューラルネット

近年，さまざまな研究においてDNNの行動認識における有効性が検証され，DNNは高精度な行動認識実現の上で必須の技術要素となりつつある．行動認識のタスクにおいてDNNが重要な技術要素である理由の1つが特徴設計の難しさである．DNNによりデータから直接に重要な特徴量を獲得することで，時間特徴量や周波数特徴量などの経験的に設計され利用されてきた特徴量のみでは捉えられなかった特徴量を獲得し良い認識精度を達成することができる．

Plötzらは行動認識タスクにおいてDNNをはじめて利用し，従来の特徴設計パイプラインをRestricted Boltzmann Machineや主成分分析で置き換える方法の有効性を4つのデータセットで検証した[Plötz 11]．また，Vollmerらはスパース符号化を利用したニューラルネットワークの有効性を検証している[Vollmer 13]．近年の研究で，Jingらは畳み込みニューラルネットワークが行動認識タスクと親和性が高く，認識精度も高いことを検証した[Yang 15]．また，OrdóñezやHammerlaらがLong Short Term Memoryのように時系列性を考慮したDNNの手法が良い精度を達成することを確認している[Hammerla 16, Ordóñez 16]．これらのように，DNNの行動認識タスクにおける利用は着実に進んでおり，認識精度も改善し続けている．しかし，学習する表現のユーザ独立性に着目した研究は存在せず，提案手法に新規性がある．

2·2 敵 対 的 訓 練

敵対的訓練によるユーザ依存性最小化のアイディアは，特徴量Rからユーザ変数Uを予想しようとする識別器uを騙すように，特徴抽出器$f: X \to R$を学習させることである．すなわち，識別器uがどの程度RからUを予想できるかをRのユーザ依存度の指標へと利用する．

著者らが知るかぎり，敵対的訓練アプローチはSchmidhuberらにより初めて利用された[Schmidhuber 92]．より近年の研究で，Goodfellowらは敵対的訓練による方法を画像生成タスクに利用し[Goodfellow 14]，さまざまな研究による改良がなされている[Denton 15]．提案手法により近い研究として，Ganinがドメイン適応の文脈で提案したDomain-Adversarial Neural Networks（DANN）[Ganin 14]とEdwardsが表現から機微情報を取り除くための手法として開発したAdversarial Learned Fair Representations（ALFR）がある[Edwards 16]．これらはある特徴量Rが何らかの情報S（前者はドメイン，後者は機微情報）に依存しないように学習するという点では提案手法と類似しているが，学習される特徴量のユーザ依存性を低下させることを目的とする本手法とは異なる目的で開発されているものである．

また，これらの研究ではドメインや機微情報Sとして2値を想定しているのに対して，本稿が取り扱うユーザ独立な表現を獲得する問題ではUは一般に多値となるという点でも異なっている．Uが多値になることが引き起こす問題として，1. DANNやALFRはHダイバージェンスという2つの分布（$P_{s=1}(R)$と$P_{s=0}(R)$）の距離を測る指標に理論的に立脚しているが，Hダイバージェンスは多値を直接扱えないため多値にした場合の理論的妥当性が不明である，2. 取り除きたい情報Sが2値の場合と比較して，敵対的分類器と特徴抽出器のバランスをとることが難しくなる，といった問題がある．これらの問題に対して本稿では，1. 独立性の情報理論的な指標である相互情報量と提案手法の関係を整理，2. バランスを取るための技術的対策の提案を行い，その有用性を検証する．

3. User-Adversarial Neural Networks

3·1 定 式 化

前述したとおり，ユーザ独立かつ行動認識に利用できる特徴量を獲得するためには，特徴量RがYに関する情報を持ちながらUに関する情報を持たないようにする必要がある．この問題は，次のような2つの損失関数の同時最適化問題として定式化することができる．

$$\mathrm{L} = \mathrm{L}_y(X,Y) + \lambda \mathrm{L}_u(R,U) \tag{1}$$

ここで，L_yおよびL_uは特徴量が持つラベルYに関する情報の大きさおよびユーザUに関する情報の小ささを表す損失関数である．また，λは相対的な重みである．以降，この最適化問題を順伝播型ニューラルネットワークで解く提案手法，User-Adversarial Neural Networksについて説明する．

3·2 UANN の 構 造

図1にUser-Adversarial Neural Networksの構造を示す．参考までに，通常の順伝播型ニューラルネットワークを横に並べた．図中矢印は，順伝播パスおよび逆伝播パスを意味している．提案手法は，通常のニューラルネットワークが持つ1. 特徴抽出器$f_f: X \to R$，2. 分類器$f_y: R \to Y$に加えて，3. 敵対的ユーザ分類器$f_u: R \to U$の3つのニューラルネットワークにより構成される．ここで，fはそれぞれ任意の構造を持つニューラルネットワークであり，それぞれ$\theta_f, \theta_y, \theta_u$のパラメタを持つ．提案手法では，これらの3つのニューラルネットワークを利用してL_yおよびL_uを定量化する．

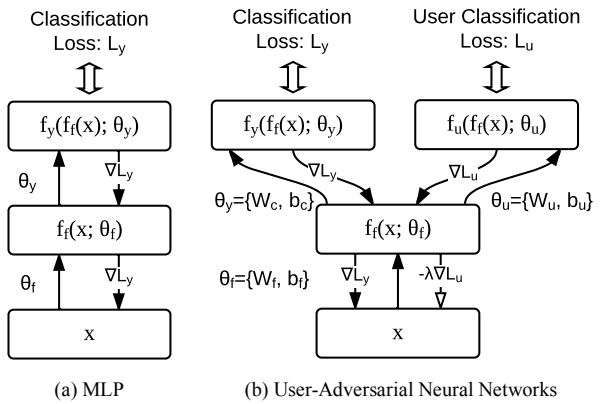


図 1: User-Adversarial Neural Networks の構造と一般的な MLP の比較.

3·3 $\mathrm{L}_y(X,Y)$ の定量化

L_y は，通常のニューラルネットワークと同様の方法で求める．すなわち，X と Y の間で定義される交差エントロピーを最小化することで求める．交差エントロピーによる損失関数は，定式的には次の式のようになる．

$$\mathrm{L}_y = -\frac{1}{N}\sum_{n=1}^{N}\sum_{m=1}^{M} y_{nm}\log f_y(f_f(x_n)) \qquad (2)$$

ここで，N は学習サンプル数，M は分類したいクラスの数，y_{nm} はサンプル n が m 番目のクラスであるかを表す $\{0,1\}$ の値である．特徴抽出器および行動分類器は確率変数 X から Y が予想しやすいようにする．すなわち式 (2) を最小化するようにパラメタ θ_f および θ_y を修正する．

3·4 $\mathrm{L}_u(R,U)$ の定量化

L_u の定量化には敵対的訓練を利用する．具体的にはまず，変数 R から U を予想しようとするような敵対的分類器 f_u を考える．これは，f_u を任意の構造のニューラルネットワークとすると，次の損失関数を最大化することにより実現できる．

$$\mathrm{L}_u = \frac{1}{N}\sum_{n=1}^{N}\sum_{k=1}^{K} u_{nk}\log f_u(f_f(x_n)) \qquad (3)$$

ここで，K はユーザの数，u_{nk} はサンプル n が k 番目のユーザであるかを表す $\{0,1\}$ の値である．ユーザ分類器は，確率変数 R からユーザ U を予測するように関数 f_u を学習する．これは，形式的には特徴抽出器 f_f のパラメタである θ_f を固定した上で，式 (3) を最大化するようにパラメタ θ_u を更新することと対応する．

逆に，特徴抽出器は，敵対的分類器が確率変数 R からユーザ U を学習できないようにする，これは形式的には，敵対的ユーザ分類器 f_u のパラメタ θ_u を固定した上で式 (3) を最小化するようにパラメタ θ_f を更新することで実現できる．また，概念的には特徴 R から U を予想するような敵対者を想定した上で，その仮想的な敵対者が情報を抽出できないように f_f を修正することに対応する．

3·5 最　適　化

まとめると，提案手法は 1. 特徴抽出器 f_f，2. 行動分類器 f_y，3. 敵対的ユーザ分類器 f_u の 3 つの要素から構成され，最終的な最適化問題は式**??**eq:uann-minmax) のようになる．

$$\min_{\theta_f,\theta_y}\max_{\theta_u}[\mathrm{L}_y(X,Y;\theta_f,\theta_y)+\lambda\mathrm{L}_u(R,U;\theta_f,\theta_u)] \qquad (4)$$

全体の最適化問題は明らかに凸でなく，単純な最適化で解くのは難しい．ここでは，[Ajakan 14] や [Edwards 16] に従い確率的最急降下法（SGD）による交互最適化を行った．すなわち，1. L_u を最大化するように θ_u を更新する，2. L を最小化するように θ_f および θ_y を更新するという手続きを交互に繰り返し行った．

敵対的訓練の成否の鍵をにぎる要素の 1 つとして，L に関する最小化と最大化のバランスがあることが知られている [Ajakan 14, Edwards 16, Goodfellow 14]．ここでバランスとは，提案手法の場合敵対的ユーザ分類器が L_u を最大化する能力と特徴抽出器が敵対的ユーザ分類器を騙す能力の均衡のことを意味する．このバランスが崩れると，勾配が十分に伝わらなかったり，おかしな方向に進んだりするおそれがある．特に，今回の場合，敵対的分類器が行うのは多クラス分類となるため，2 値分類である類似研究より敵対的分類器の認識能力が低くなりがちであると予想される．実際，実験的にも初めから L_u を最小化するように特徴抽出器を学習させると過度にユーザ独立にする能力が強くなり，行動の予測精度が上がらない現象が観測された．

この問題を解消するために，λ をはじめは小さな値から始め，エポックが進むごとに徐々に大きくするアニーリングを行った．パラメタ λ のアニーリングを行うことで，ユーザ独立性の観点において特徴抽出器が特に初期フェーズで過剰に強くなるのを抑えることができる．スケジューリングとしては，今回は単純に線形に増やす方法を利用した．本稿の実験で利用した具体的なスケジューリング式は以下のとおりである．ここで，t はエポック数，$\alpha+1$ はアニーリングを開始するエポック，β はアニーリングを終了するエポック，λ は最終的なパラメタの設定値を意味している．

$$\lambda(t) = \begin{cases} 0.0 & (t \le \alpha) \\ (t-\alpha)\cdot\frac{\lambda}{(\beta-\alpha)} & (\alpha \le t < \beta) \\ \lambda & (\beta \le t) \end{cases} \qquad (5)$$

以上をまとめた提案手法の擬似コードは Algorithm1 の通りである．

Algorithm 1 Optimization of the proposed model

Require: Samples $S = \{(x_n, y_n, u_n)\}_{i=1}^{N}$
Require: hyper parameters λ
Ensure: neural network $\{\theta_f, \theta_y, \theta_u\}$
  $\theta_f, \theta_y, \theta_u \leftarrow$ initialize()
  $t \leftarrow 1$
  while training() **do**
    $\lambda(t) \leftarrow Eq.5$
    $\mathrm{L}_u \leftarrow Eq.3\ \forall(x_n, u_n) \in S$
    $\theta_u \leftarrow \theta_u + \frac{\delta L_u}{\delta \theta_u}$ {Update User-Adversarial classifier s.t maximize L_y}
    $\mathrm{L}_y \leftarrow Eq.2\ \forall(x_n, y_n) \in S$
    $\mathrm{L}'_u \leftarrow Eq.3\ \forall(x_n, u_n) \in S$
    $\mathrm{L} = L_y + L'_u$
    $\theta_f \leftarrow \theta_f - \frac{\delta L}{\delta \theta_f}$
    $\theta_y \leftarrow \theta_y - \frac{\delta L_y}{\delta \theta_y}$
    $t \leftarrow t + 1$
  end while

3·6 相互情報量最小化との関係

情報理論的には，確率変数 R が確率変数 U に関する情報を持つかは 2 つの確率変数の独立性により表される．2 つの確率変数の独立性は，次に示す相互情報量により定義することができる．

$$I(U;R) = \sum_{r \in R} \sum_{u \in U} P(u,r) \log \frac{P(u,r)}{P(u)P(r)}$$

$I(U;R)$ は 0 以上の値であり，0 の時に R と U は独立である，すなわち R は U に関する情報を含まないことを意味する．

ここで，L_u と $I(U;R)$ の間には次のような対応関係がある．詳細は付録 A を参照のこと．

$$I(U;R) = N \cdot \mathrm{L}_u - C$$

ただし，C は定数である．すなわち，θ_f を固定して L_u を最大化することは θ_u を相互情報量 $I(U;R)$ を最大化するように更新することを，また θ_u を固定して L_u を最小化することは θ_r を相互情報量 $I(U;R)$ を最小化するように更新することを意味している．

4. 実　　験

4·1 データセット

§1 Opportunity Activity Recognition

データセットとして，最もポピュラーなデータセットの 1 つである Opportunity データセットを利用した．Opportunity データセットは，朝食をシミュレートしたシナリオにおける日常行動を 4 人分（S1–S4）記録したデータセットである．多数の種類の活動者の身体，物体，および環境に設置されたセンサにより行動を計測しており，合計で 72 のセンサ，10 のモダリティを持つデータである（詳しくは，Sagha らの論文の図 1 [Sagha 11] を参照されたい）．結果として，各時刻において 113 の実数値（時刻情報は除く）が記録されている．本稿では，提供されている 3 つのうち Gestures（以降 Opp-G）と Locomotion（以降 Opp-L）による検証を行った．Opp-G は，18 クラス [*1] のより細かな行動を分類するタスクであり，Opp-L は 5 種類のより大局的なユーザの状態を分類するタスクである．分類問題を解くにあたり，一般に利用されるスライディングウィンドウ方式（スライド幅 30，重なり率 0.5）により学習サンプルを生成し，結果として 4 ユーザ合計で約 50,000 のサンプルを得た．

§2 USC-HAD

USC-HAD は，公開されている行動認識データセットの中では比較的大規模な男女 7 名ずつ合計 14 名のデータを含む点が特徴である [**?**]．行動としては，前に歩く，右に曲がる，左に曲がるなどの一般的な生活における最も基本的な 12 種類の行動が記録されている [*2]．データの計測は MotionNode [*3]により行われており，6 次元の系列データである．Opportuniry データセットと同様，スライディングウィンドウ方式により学習サンプルを生成し，結果として 14 ユーザ合計で約 127,000 のサンプルを得た．

4·2 実 験 設 定

図 2 に提案手法を利用した User-Adversarial CNN の具体的なネットワーク構造を示す．敵対的ユーザ分類器を除くと，ネットワーク構造は単純な CNN と同様となる．層の数やフィルタ数などのハイパーパラメタは Opportunity データセットに対して CNN を利用した研究である [Yang 15] を参考に設計した．ここで，図中 $1 \times K$ は畳み込みサイズ（あるいはプーリングサイズ）を，各層の右下に位置する数値は特徴マップ数を意味しているものである．活性化関数としては出力層にソフトマックス関数を利用したほかは，ReLU を利用した．また，各畳み込み層および全結合層のあとにはドロップアウトを行い，過学習を抑制した．最適化には Adam [Kingma 15] を利用し 150 エポック学習させた．学習率は 0.0001 とし，その他のパラメタは推奨パラメタとした．

敵対的ユーザ分類器 f_u としては，図中全結合層における特徴量を入力とする MLP_{800} を利用した．ここで，MLP_{800} とは 800 個の中間ユニット数もつ 3 層ニューラルネットワークを意味している．L_u と L_y を重み付ける

∗1 open door 1, open door 2, close door1, close door 2, open fridge, close fridge, open dishwasher, close dishwasher, open drawer 1, close drawer 1, open drawer 2, close drawer 2, open drawer 3, close drawer 3, clean table, drink cup, toggle switch, and Null
∗2 walking forward, walking left, walking right, walking upstairs, walking downstairs, running forward, jumping, sitting, standing, sleeping, elevator up, elevator down
∗3 http://www.motionnode.com/

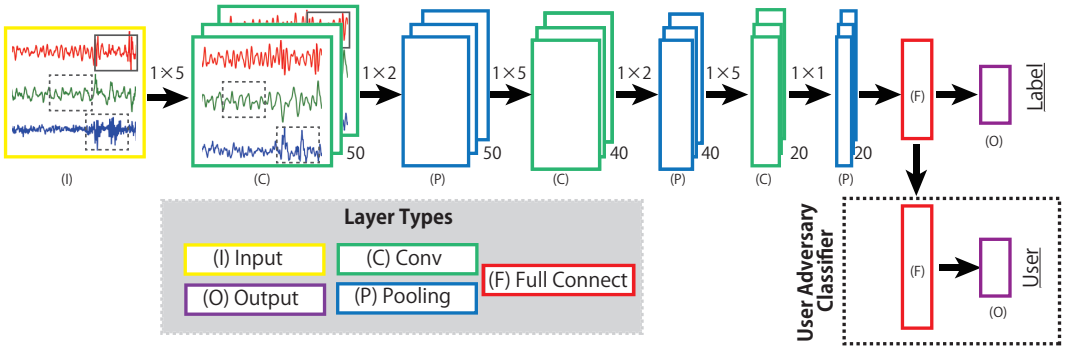


図 2: 実験に利用した提案手法のネットワーク構造.

ハイパーパラメタ λ は他に言及がない限り 0.1 に設定した．また，アニーリングのパラメタ α および β は開始直後と終了直前の 15 エポックずつは固定した λ で学習されるように，それぞれ 15，135 とした．

提案手法の有効性およびパラメタの重要性を検証のため次の 4 つの手法を比較した．1) CNN：提案手法において λ=0.0 とした場合に対応．2) UANN_{LR}：敵対的ユーザ分類器として，MLP_{800} の代わりにロジスティック回帰を利用したものに対応．3) UANN_{MLP}：提案手法においてパラメタ λ のアニーリングを行わない場合に対応．4)$\text{UANN}_{\text{MLPA}}$：敵対的ユーザ分類器として MLP_{800} を利用し，かつアニーリングを行った場合．これらの手法を比較することで，単純な CNN と比較して提案手法群がよりユーザ独立な特徴量を獲得できること，敵対的ユーザ分類器の表現力およびアニーリングの影響を検証する．

4·3 評 価 方 法

各手法の評価は次のような Leave-One-Subject-Out 手続き（LOSO）により行った．LOSO は新規ユーザに対する認識精度を検証するためによく利用される方法であり，ここでは 1. K 人のうちから 1 人テストユーザ i を選択する，2. ユーザ i を除く $K-1$ 人のデータの一部を訓練データとして利用しモデルを訓練する（このとき，80%を訓練データとし残り 20%は検証データとして利用した），3. ユーザ i のデータ（以降テストデータ）を利用して評価を行う，という手続きを K 回にわたり繰り返し行う．このような手続きでは，ユーザ i のデータは各ステップのモデルにおいて訓練に全く利用されないので，学習されたモデルの新規ユーザに対する認識性能を評価することができる．また，テストデータによる評価に加えて，検証データに対する認識精度とテストデータに対する認識精度の差を比較し，学習されたモデルのユーザに関する過学習度合いを評価した．

モデルの評価指標として，行動分類能力に関する指標と表現のユーザ独立性に関する指標の双方を利用して評価を行う．行動分類能力に関する指標としては，正解率および平均 F 値を利用した．正解率および平均 F 値の定義は次のとおりである．

$$accuracy = \frac{1}{N}\sum_{n=1}^{N} 1(\hat{y_n} = y_n),$$

$$Fscore = \frac{1}{|L|}\sum_{l\in L} F^l(\hat{y}, y),$$

ここで，N は全サンプル数，L は行動クラスの集合，y_n と $\hat{y_n}$ は i 番目のサンプルに対する正解ラベルおよび予測ラベル，$F^l(\hat{y}, y)$ は l 番目のクラスに関する F 値を意味する．正解率は全サンプルを均等に扱うのに対して，平均 F 値は少数クラスのサンプルを重要視した指標であるという点で異なる役割を持つ指標である．

ユーザ独立性に関する定量的な指標としては，ユーザの認識精度を利用した．具体的には，モデルを学習後にその特徴量 R からユーザを分類するような分類器 γ を改めて学習させ，その認識精度を計測した．このとき認識精度が高い，すなわち特徴量 R からユーザ U が予測できる場合には独立性が低く，逆に予想できない場合には独立性が高いことを意味する．認識精度は用いる分類器 γ に強く影響されると考えられるため，ここでは γ としてロジスティック回帰（LR），隠れユニット数 50 の 3 層ニューラルネットワーク（MLP_{50}），および隠れユニット数 800 の 3 層ニューラルネットワーク（MLP_{800}）の 3 つを利用した．

ユーザ独立性に関して，定量的な評価に加えてクラスタリングによる定性評価を行った．具体的には，学習されたモデルの特徴量 R をクラスタリングし，クラスタリング結果から算出したユーザ傾向行列 C を可視化した．ここで，C の要素 c_{ij} はクラスタ j においてユーザ i のサンプルが占める割合を示しており，0.0 から 1.0 までの値

を取る．C を可視化することで，特定のユーザに偏ったクラスタが発生しているかどうか，すなわち学習された特徴量が強いユーザ依存性を持つかどうかを可視化した．

4·4 実 験 結 果

§1 行動認識精度とユーザ独立性のバランス

図 3 に，各データセットにおける行動認識精度およびユーザ認識精度を比較した結果を示す．縦軸が行動認識精度を，横軸は分類器としてロジスティック回帰を利用した場合のユーザ認識精度を表しており，左上に行くほどユーザ独立かつ行動の認識精度が高く，右下に行くほど行動の認識精度が低くユーザ独立性も低いことを意味している．各マーカは異なるユーザを表しており，各色がそれぞれ異なる手法に対応している．なお，図中の点線は CNN の行動認識精度を示したものである．

結果として，まずユーザ認識精度に関して，CNN と比較して提案手法群の認識精度が著しく低下していることがわかる．行動認識精度はデータセットにより結果が異なっているものの，Opp-G および Opp-L では提案手法群の認識精度は CNN と同程度かわずかに上回っており，また USC-HAD データセットについても認識精度の低下はユーザ認識精度の改善具合と比較すると軽微であった．この結果は，敵対的訓練を利用した提案手法により行動認識精度とユーザ独立性のより良いトレードオフを実現できることを示唆している．

§2 ユーザ汎化性能に関する結果

表 1 に，各データセットでの行動認識精度の比較結果を示す．表 1-(a) はテストユーザに対する認識精度を，また表 1-(b) は参考までにユーザに関する過学習度合い（テストデータと検証データに対する認識精度の差）を示している．**太字+下線** の項目は認識精度が最も高かったことを，**太字**の項目は 2 番目に高かったことを意味している．

結果として，次のような結果が得られた．まず，CNN と $\mathrm{UANN_{MLPA}}$ を比較すると，新規ユーザに対する認識精度については平均 F 値および正解率双方で Opp-G および Opp-L については $\mathrm{UANN_{MLPA}}$ が優れており，USC については通常の CNN が優れていた．また，ユーザに関する過学習度合いでは USC を含むすべての場合で $\mathrm{UANN_{MLPA}}$ が優れていた．この結果は，提案手法が利用した敵対的訓練は学習時に存在するユーザに対する認識精度を低下させるものの，新規ユーザに対する認識精度はわずかに改善するかあるいは低下する場合でもその低下度合いは学習時に存在するユーザに対するものと比較すると軽微であったことを意味している．

次に，$\mathrm{UANN_{LR}}$ と $\mathrm{UANN_{MLPA}}$ を比較すると，USC データに関するテストユーザに関する認識精度を除くと $\mathrm{UANN_{MLPA}}$ が上回る結果となっていた．また，Wilcoxson の検定を行うとテストユーザに関する認識精度では平均 F 値および正解率それぞれ 0.055，0.061 の p 値となり 5%危険率で有意差は見られなかったが，過学習度合いでは平均 F 値および正解率それぞれ 0.0005，0.0002 の p 値となり有意差が見られた．この結果は，敵対的ユーザ分類器としてより適切な分類器を利用することでユーザに関する過学習を抑制できる可能性を示唆している．最後に $\mathrm{UANN_{MLP}}$ と $\mathrm{UANN_{MLPA}}$ を比較すると，ユーザに関する過学習度合いについては同程度であった一方で，新規ユーザに対する認識精度では $\mathrm{UANN_{MLPA}}$ がすべての場合で上回っていた．この結果は，パラメタのスケジューリングを行うことで過学習を同程度に抑えながらテストユーザに対する認識精度を適切に高めることができることを示唆している．

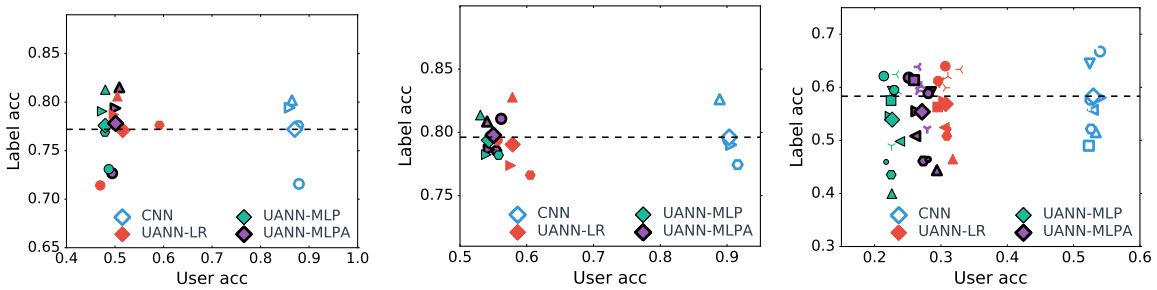
図 4-(a) および (b) に，検証データとテストデータに対する CNN（青線）と $\mathrm{UANN_{MLPA}}$（赤線）の認識精度の推移を比較した結果を示す．ここで，横軸がエポック数，縦軸が正解率である。また，図中の値は Opp-G における 4 回の試行の平均をとったものである．なお，今回の実験では α=15 としたため，15 エポック目までは CNN と $\mathrm{UANN_{MLPA}}$ は同じ損失関数を最適化している．結果として，1) 約 20 エポック目までは両者はほぼ同じ正解率になっていること，2) 20 エポックを超えたあたりから $\mathrm{UANN_{MLPA}}$ が安定的に良い精度になっていること，3) 検証データに関しては 100 エポックを超えたあたりで $\mathrm{UANN_{MLPA}}$ が飽和しているのに対して CNN では更に学習が進んでいること，の 3 点が確認できた．これらの結果は，単純な CNN はユーザに対して過剰に適合する可能性があること，また提案手法により学習ユーザに対する過剰適合を抑制できていることを示唆している．

図 4-(c) に，検証データに対するユーザ分類器の正解率のごとの推移を示す．横軸はエポック数，縦軸は正解率であり，各色が異なる λ に対応している．結果，c-1) CNN（λ=0.0）の場合最終的に 99%程度でユーザ識別が可能になる一方，$\lambda \geq 0.1$ の場合にはユーザ分類器の精度を抑制することができていること，c-2) λ を大きくするほどユーザ分類器の精度は早く低下するが，最終的な認識精度は飽和すること，c-3) 正解率の低下はおおよそ 20 エポック目から始めっており，図 4 においてテストデータに対する認識精度の改善が始まったタイミングとほぼ一致していること，などが確認された．

§3 ユーザ独立性に関する結果

表 2 に，異なるユーザ分類器を利用した場合の認識精度を比較した結果を示す．各行はそれぞれ学習時に利用した敵対的ユーザ分類器 f_u を，各列は評価に利用した分類器 γ の種類を示している．f_u=None は敵対的訓練を行わない場合であり，CNN に対応するものである．また，完全にランダムに予測した場合の予測精度 (Rand) を参考値として示した．特徴量が完全にユーザ独立な場合どのような分類器を利用してもランダム予測となるため，Rand は論理的な限界値を示すものである．

結果としてまず，評価用分類器 γ によらず MLP や LR を利用した敵対的訓練を行う場合に，行わない場合と比



(a) Opp-G (b) Opp-L (c) USC-HAD

図 3: 行動認識精度とユーザ独立性のバランスの比較．各マーカはテストユーザ，各色は手法の違いを表している．また，ダイヤモンドマーカは全ユーザの平均値を表す．

表 1: 行動認識精度に関する比較．

(a) テストユーザに対する認識精度

	平均 F 値				正解率			
	CNN	UANN_{LR}	UANN_{MLP}	$\text{UANN}_{\text{MLPA}}$	CNN	UANN_{LR}	UANN_{MLP}	$\text{UANN}_{\text{MLPA}}$
Opp-G	**0.557**	0.547	0.551	**0.566**	0.772	0.771	**0.776**	**0.778**
Opp-L	**0.794**	0.786	0.781	**0.804**	**0.796**	0.790	0.794	**0.798**
USC	**0.573**	**0.548**	0.501	0.523	**0.583**	**0.568**	0.539	0.554
average	**0.660**	0.643	0.624	**0.644**	**0.735**	**0.724**	0.713	0.721

(b) ユーザに関する過学習度合い

	平均 F 値				正解率			
	CNN	UANN_{LR}	UANN_{MLP}	$\text{UANN}_{\text{MLPA}}$	CNN	UANN_{LR}	UANN_{MLP}	$\text{UANN}_{\text{MLPA}}$
Opp-G	-0.321	-0.333	**-0.319**	**-0.303**	-0.159	-0.161	**-0.151**	**-0.147**
Opp-L	**-0.159**	-0.165	-0.171	**-0.148**	**-0.145**	-0.151	-0.147	**-0.143**
USC	-0.187	-0.149	**-0.104**	**-0.120**	-0.185	-0.139	**-0.094**	**-0.109**
average	-0.234	-0.231	**-0.216**	**-0.205**	-0.161	-0.152	**-0.135**	**-0.136**

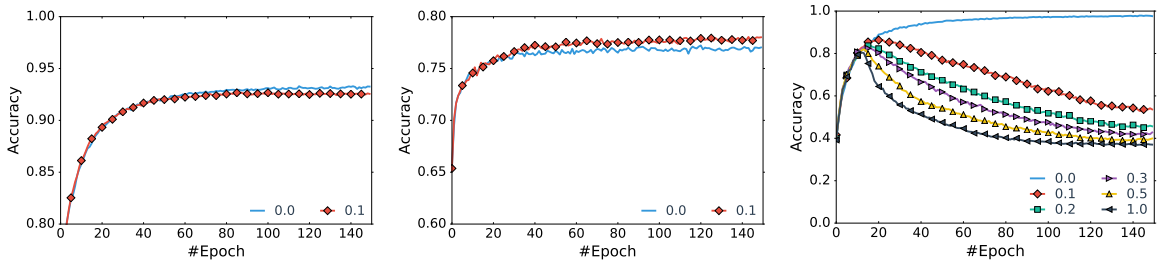
較してユーザ識別性能が低下していることがわかる．この結果は，提案手法により単純な CNN を利用する場合と比較してユーザ独立性の高い表現を学習できていることを示すものである．一方で提案手法の課題として，γ として f_u より強い表現力を利用する場合，敵対的分類器を利用した場合でもユーザ認識精度が低下しにくい傾向が見られた．例えば，Opp-G について，f_u にロジスティック回帰（LR）を，γ に同様の LR を利用した場合には認識精度は 0.579 ポイントと敵対的訓練を利用しない場合（0.903）と比較して 0.30 ポイント以上認識精度を抑制できていたのに対して，γ に MLP_{50} を利用した場合には 0.953 ポイントとなっており，敵対的訓練を利用しない場合（0.966 ポイント）とほとんど変わらない値であった．また，γ として MLP_{800} を利用した場合の結果は各データセットでそれぞれ 0.950，0.957，0.521 であり，ランダムな予測と比べて著しく高かった．

最後に，ユーザ独立性の定性的な評価として図 5 に，CNN および $\text{UANN}_{\text{MLPA}}$ で学習された特徴量のクラスタリングによって得られたユーザ傾向行列 C を可視化した結果を示す．図中青が濃い部分がクラスタに占める特定のユーザの割合が高いことを，白に近いほど低いことを意味している．また，クラスタリング手法としては k 平均法を利用した．結果として，提案手法によりユーザ傾向が低いクラスタができていることが視覚的に確認された．例えば，CNN の場合クラスタ 18 や 19 で S4 の割合が高くなっているのに対して，提案手法では同様の傾向を持つクラスタは存在しなかった．

5. 考　　察

5·1 ユーザ独立性について

実験の結果は，提案手法が行動の認識精度を可能な限り保った上でユーザ独立な特徴量を獲得できることを示唆していた．図 3 の結果は，敵対的訓練を行わない通常の CNN が学習した特徴量と比較して提案手法が学習した特徴量は，行動に関して同程度の予測性能を持つ一方で，ユーザを予測しにくい特徴量となっていることを示している．また，図 5 に示した特徴量のユーザ傾向の可視化結果は，CNN が獲得した特徴量によるクラスタの一部や過度に特定のユーザが固まる傾向にあったのに対して，提案手法が学習した特徴量はすべてのクラスタで特定のユーザが固まるような現象は見られなかった．これらの結果は，敵対的ユーザ分類器を学習時に考慮する提



(a) 行動認識精度（検証データ） (b) 行動認識精度（テストデータ） (c) ユーザ認識精度

図 4: 行動認識精度およびユーザ認識精度のエポックごとの変化.

表 2: 異なるユーザ分類器を利用した場合のユーザ認識精度の比較.

(a) Opp-G

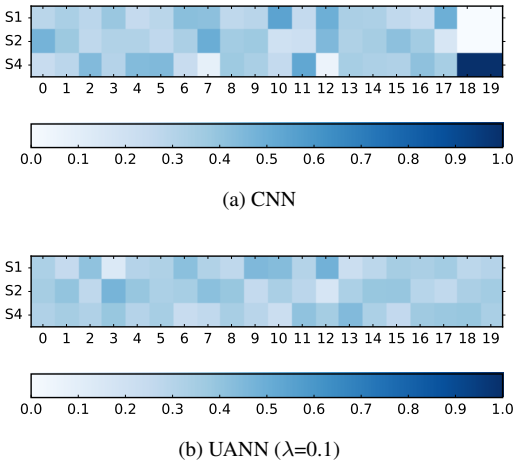
	LR	MLP_{50}	MLP_{800}
None	0.870	0.963	0.983
LR	0.516	0.955	0.981
MLP_{800}	**0.501**	**0.774**	**0.950**
Rand	0.333	0.333	0.333

(b) Opp-L

	LR	MLP_{50}	MLP_{800}
None	0.903	0.966	0.980
LR	0.579	0.953	0.977
MLP_{800}	**0.550**	**0.822**	**0.957**
Rand	0.333	0.333	0.333

(c) USC-HAD

	LR	MLP_{50}	MLP_{800}
None	0.530	0.649	0.770
LR	0.307	0.493	0.636
MLP_{800}	**0.272**	**0.377**	**0.521**
Rand	0.078	0.078	0.078



(a) CNN

(b) UANN (λ=0.1)

図 5: クラスタ数を 20 とした際の Opp-G における各クラスタのユーザ傾向の可視化．a: CNN，b: UANN (λ=0.1).

案手法により，CNN が学習する特徴量のユーザ独立性を高めることができることを意味している．

一方，ユーザ独立性に関する限界として，表 2 に示したように提案手法により得られた表現はランダム予測と比較すると著しく高いユーザ依存性を持っており，完全にユーザ独立な表現を学習しているわけではないという点がある．言い換えれば，本稿での検証により得られた結果は単純な CNN に対する比較優位性を示すものであり，絶対的に十分なユーザ独立性が得られていることを示すものではない点には注意されたい．提案手法の枠組みの中でよりユーザ独立性の高い表現を学習するためには，適切な分類器やハイパーパラメタ λ の選択，敵対的分類器を接続する層の選択，複数の層における敵対的分類器の利用などの方法が考えられる．これらの項目について検証を加えることで，手法の改良を行う必要がある．

5·2 ユーザ汎化性能について

ユーザ独立な特徴量を獲得する動機の 1 つであったユーザ汎化性能については，まず提案手法を利用することで CNN と比較してユーザ過学習度合いを抑制できることが示された（表 1）．この結果は，特徴抽出器の出力のユーザ独立性を高めることにより，行動分類器のユーザ汎用性を高めるという提案手法のアイディアの妥当性を示すものであると考えられる．一方で，平均すると過学習度合いは 3 つのデータセット平均で 0.136 ポイント（F 値では 0.205 ポイント）と依然として大きい値となっていた．この原因としてまず，5.1 節に記述したように提案手法によるユーザ独立性が不十分であったことが考えられる．もう 1 つの可能性として，ある特徴量が与えられたときの行動の真の確率分布 $P(Y|U)$ がユーザによって異なるケースが考えられる．これは，例えばある人が歩くときに生じる観測パターンと他の人が早歩きするときの観測パターンが類似している場合などでが考えられる．このような場合，特徴量がユーザ独立になったとしても予測された結果が正しいかどうかはユーザによって異なることになる．提案手法の限界として，提案手法は特徴量 R のユーザ独立性を高めるためのものであり，ある特徴量が発生したときにどの行動が生じたかの確率分布 $P(Y|R)$ がユーザごとに異なることに伴う認識精度の劣化を考慮することはできない．後者の問題を解決するためには，ユーザ適応など別の方法を適用する必要があると考えられる．

また，提案手法によるもう 1 つの課題として，新規ユーザに対する絶対的な認識精度がデータセットによっては劣化する場合があることが確認された．具体的には，表

1 が示すように，Opp-L および Opp-G については提案手法によりユーザ汎化性能が改善する一方で，USC データセットについては汎化性能が低下していた．

この原因として，次の 2 つが考えられる．第 1 に，モデルの持つ表現力が十分でなかった可能性がある．式 (1) に示したように，提案手法では通常の CNN と比較してより複雑な損失関数を最適化するように学習している．その結果として，モデルの持つ表現力が不足していた可能性が考えられる．紙面の都合上割愛したものの，実際 USC データセットについては訓練データに対する認識精度（正解率）が CNN の 0.776 に対して $\mathrm{UANN}_{\mathrm{MLPA}}$ では 0.666 と著しく低下しており，Opportunity データセットを利用した 2 つの分類タスクについては同様の傾向は見られなかった．また，この差はユーザ汎化性能における差（CNN が 0.583 に対して提案手法が 0.554）の差より著しく大きかった．より多くのパラメタを持つネットワーク構造を利用した場合にユーザ汎化性能が改善するかの検証は今後の課題である．

第 2 に，ユーザ独立な特徴量を学習することに伴う問題として，テストユーザと類似したユーザが学習時に存在する場合にはユーザ独立な特徴量を獲得するよりもその類似ユーザに対して適合した特徴を利用することが認識精度改善に寄与する可能性である．この観点から考えると，学習に利用するユーザ数が増えれば増えるほど新規ユーザと類似した特徴を持つユーザが学習データに含まれる可能性は高まる．一方，学習ユーザが増えれば増えるほど学習が難しくなり，結果として認識精度の改善も限定的である可能性がある．例えば，Ogawa らは学習に利用するユーザ数を増やした際のユーザ汎化性能の変化を検証し，その精度改善が 50 人程度で飽和した報告している [Ogawa 11]．また，今回はデータの都合上 LOSO という新規ユーザが 1 人の場合における検証を行ったが，新規ユーザが増えれば増えるほど学習ユーザに類似しているユーザが含まれる可能性は低下するため，提案手法の有効性が増すと考えられる．より大規模なユーザ数のデータセットによる検証により，どの程度のユーザ数を持つときに提案手法の有効性が強く現れるかの検証が必要と考えられる．

5·3 プライバシー保護について

提案手法により得られる特徴量のユーザ独立性は，1 章にも述べたようにプライバシー保護の観点からも重要となりうる．一方で，一般にセンサデータは長時間にわたって収集されることから，敵対者は複数のウィンドウを予測に利用することでより正確に予測を行える可能性があることには注意が必要である．例えば特徴量からユーザを予測する本稿で扱った例では，図 B.1 に示したように複数のウィンドウの結果を平均化することにより著しく高い精度でユーザを予測することができるようになる（詳細は付録 B を参照のこと）．特徴量が完全に独立になれば複数ウィンドウを利用することは全く意味をなさないため，この問題は特徴量の独立性を高めることにより原理的には解決可能であるものの，本稿で検証したような 1 つのウィンドウに対する特徴量 r からの予測可能性だけでなく，複数のウィンドウを利用した場合の予測性能を考慮した形に手法を拡張することでより優れたプライバシー保護が行える可能性がある．

プライバシー保護の観点から見たときのもう 1 つの課題として，より大規模なデータ，特にユーザ数および含まれる属性が増えた場合での検証が必要である．プライバシー保護の観点からは，ユーザ独自の特徴を利用しないということよりむしろユーザに関する機微情報（例えば病気の有無など）に影響された特徴量にならないことが重要である．ユーザに関する精緻な属性情報を持ったデータベースを利用することでプライバシー保護の観点からの考察を深めることが必要である．

ユーザ数が増えた際の提案手法の問題点として，敵対的ユーザ分類器の学習が難しくなることがある．例えば，今回，最大でユーザ分類器としては 13 人の場合の分類を行ったが，1,000 人のユーザがいる場合に提案手法における敵対的ユーザ分類器は 1,000 クラスの分類を適切に行うように学習する必要がある．このような複雑な分類問題を行うことは技術的に非常に難しい，あるいは学習に相当の時間がかかると考えられる．対応策として，プライバシー保護の領域で利用されている k-匿名性 [Samarati 01, Sweeney 02] や l-多様性 [Machanavajjhala 07]，t-近接性 [Li 07] といった概念が参考になる可能性がある．例えば，1,000 クラス分類を諦め k クラス分類器を複数学習させる方法や，その際に機微情報に関する情報がばらつくように k 人を選定する方法などが考えられる．これらの検証を行うことで，より大規模なユーザが存在する場合にも適用可能なように手法の改良が必要と考える．

6. お わ り に

本稿では，ユーザ独立な表現を獲得するためのディープニューラルネットワークの拡張手法を提案し，その有効性を検証した．ウェアラブルセンサを利用した行動認識において，特徴量のユーザ独立性はユーザ汎化性能およびにプライバシー保護の観点で重要である．しかし，どのような特徴量がユーザに独立になるかは自明ではなく，また特徴量のユーザ独立性は究極的には行動の予測性能を下げる可能性があるものであり，そのような特徴量の人出による設計は難しい．

この問題に対して本稿では，ユーザ独立な特徴量を獲得するためのニューラルネットワークモデル，User-Adversarial Neural Networks を提案した．提案手法は，学習時に自身からユーザに関する情報を抜き出そうとする敵対的ユーザ分類器を考慮し，行動に関する認識性能を最大化するとともに敵対的ユーザ分類器がユーザに関す

る分類を行えないような表現を学習する用に通常の DNN を拡張する方法である．すなわち，自身から情報を抜き出そうとする分類器を学習時から考慮し，その分類器を騙すような特徴量を獲得する機構を追加することにより，特徴量が持つユーザに関する情報を可能な限り低下させる．ウェアラブルセンサを利用した 3 つの行動分類タスクにおいて，1. ユーザ汎化性能，2. ユーザ独立性，3. 行動認識精度とユーザ独立性のバランスの 3 つの観点で評価を行い，提案手法が単純な CNN と比較して定量的・定性的に優れていることを確認した．本手法を発展により，人間の実世界行動をプライバシーに配慮した形で計測する方法の確立に貢献していきたい．

◇ 参 考 文 献 ◇

[Ajakan 14] Ajakan, H., Germain, P., Larochelle, H., Laviolette, F., and Marchand, M.: Domain-adversarial neural networks, in *NIPS Workshop on Transfer and Multi-Task Learning: Theory meets Practice* (2014)

[Brdar 13] Brdar, S., Ćulibrk, D., and Crnojević, V.: Demographic attributes prediction on the real-world mobile data, in *Proc. Mobile Data Challenge by Nokia Workshop, in Conjunction with International Conference on Pervasive Computing* (2013)

[Bulling 14] Bulling, A., Blanke, U., and Schiele, B.: A tutorial on human activity recognition using body-worn inertial sensors, *ACM Computing Surveys (CSUR)*, Vol. 46, No. 3, p. 33 (2014)

[Denton 15] Denton, E. L., Chintala, S., Fergus, R., and al., et : Deep generative image models using a laplacian pyramid of adversarial networks, in *Advances in Neural Information Processing Systems (NIPS)*, pp. 1486–1494 (2015)

[Edwards 16] Edwards, H. and Storkey, A.: Censoring representations with an adversary, in *International Conference on Learning Representation (ICLR)* (2016)

[Ganin 14] Ganin, Y. and Lempitsky, V.: Unsupervised Domain Adaptation by Backpropagation, *arXiv preprint arXiv:1409.7495* (2014)

[Goodfellow 14] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y.: Generative adversarial nets, in *Advances in Neural Information Processing Systems (NIPS)*, pp. 2672–2680 (2014)

[Hammerla 16] Hammerla, N. Y., Halloran, S., and Ploetz, T.: Deep, convolutional, and recurrent models for human activity recognition using wearables, *International Joint Conference on Artificial Intelligence (IJCAI)* (2016)

[Kingma 15] Kingma, D. and Ba, J.: Adam: A method for stochastic optimization, in *International Conference on Learning Representation (ICLR)* (2015)

[Lane 11] Lane, N. D., Xu, Y., Lu, H., Hu, S., Choudhury, T., Campbell, A. T., and Zhao, F.: Enabling large-scale human activity inference on smartphones using community similarity networks (CSN), in *International Conference on Ubiquitous Computing (UbiComp)*, p. 355, New York, New York, USA (2011)

[Li 07] Li, N., Li, T., and Venkatasubramanian, S.: t-closeness: Privacy beyond k-anonymity and l-diversity, in *IEEE International Conference on Data Engineering*, pp. 106–115, (2007)

[Machanavajjhala 07] Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M.: *l*-diversity: Privacy beyond *k*-anonymity, *ACM Transactions on Knowledge Discovery from Data (TKDD)*, Vol. 1, No. 1, p. 3 (2007)

[Ogawa 11] Ogawa, N., Kaji, K., and Kawaguchi, N.: Effects of number of subjects on activity recognition -HASC2010corpus, in *International Workshop on Frontiers in Activity Recognition using Pervasive Sensing (IWFAR)*, pp. 48–51 (2011)

[Ordóñez 16] Ordóñez, F. J. and Roggen, D.: Deep convolutional and LSTM recurrent neural networks for multimodal wearable activity recognition, *Sensors*, Vol. 16, No. 1, p. 115 (2016)

[Plötz 11] Plötz, T., Hammerla, N. Y., and Olivier, P.: Feature learning for activity recognition in ubiquitous computing, in *International Joint Conference on Artificial Intelligence (IJCAI)*, p. 1729 (2011)

[Raij 11] Raij, A., Ghosh, A., Kumar, S., and Srivastava, M.: Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment, in *Annual Conference on Human Factors in Computing Systems (CHI)*, p. 11, New York, New York, USA (2011)

[Sagha 11] Sagha, H., Digumarti, S. T., Millán, J. d. R., Chavarriaga, R., Calatroni, A., Gen, D., and Tröster, G.: Benchmarking classification techniques using the Opportunity human activity dataset, in *INSS*, pp. 36–40 (2011)

[Samarati 01] Samarati, P.: Protecting respondents identities in microdata release, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 13, No. 6, pp. 1010–1027 (2001)

[Schmidhuber 92] Schmidhuber, J.: Learning factorial codes by predictability minimization, *Neural Computation*, Vol. 4, No. 6, pp. 863–879 (1992)

[Sweeney 02] Sweeney, L.: Achieving k-anonymity privacy protection using generalization and suppression, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 05, pp. 571–588 (2002)

[Vollmer 13] Vollmer, C., Gross, H.-M., and Eggert, J. P.: Learning features for activity recognition with shift-invariant sparse coding, in *International Conference on Artificial Neural Networks*, pp. 367–374, Springer (2013)

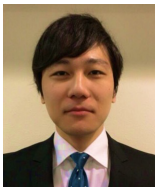
[Weiss 12] Weiss, G. M. and Lockhart, J. W.: The impact of personalization on smartphone-based activity recognition, in *AAAI Workshop on Activity Context Representation: Techniques and Languages* (2012)

[Yang 15] Yang, J. B., Nguyen, M. N., San, P. P., Li, X. L., and Krishnaswamy, S.: Deep convolutional neural networks on multichannel time series for human activity recognition, in *International Joint Conference on Artificial Intelligence (IJCAI)* (2015)

〔担当委員：尾形 哲也〕

2016 年 11 月 25 日　受理

著 者 紹 介



岩澤有祐

2012 年に上智大学理工学部卒業，2014 年に同大学院理工学系研究科修士課程，2017 年に東京大学大学院工学系研究科博士課程修了．博士（工学）．2017 年より東京大学大学院工学系研究科技術経営戦略学専攻 松尾研究室 特任研究員．専門はウェアラブルセンサによる行動認識，障害者支援，機械学習・深層学習応用．



矢入郁子（正会員）

1994 年東京大学工学部卒業．1996 年同大学院工学系研究科修士課程，1999 年同博士課程修了．同年，郵政省通信総合研究所（現 情報通信研究機構）に研究官として入所，2008 年上智大学に転職，現在，理工学部准教授．2006 年ドコモ・モバイル・サイエンス賞社会科学部門奨励賞等を受賞．2012〜2016 年 HI 学会理事，その間 2012〜2014 年度同学会学会誌委員会委員長．ACM，情報処理学会，日本機械学会会員．博士（工学）．



松尾豊（正会員）

1997 年東京大学工学部卒業．2002 年同大学院博士課程修了．博士（工学）．産業技術総合研究所，スタンフォード大学を経て，2007 年より，東京大学大学院工学系研究科技術経営戦略学専攻 准教授．2012 年より本学会理事・編集委員長，2014 年より倫理委員長．人工知能学会論文賞，情報処理学会長尾真記念特別賞，ドコモ・モバイル・サイエンス賞などを受賞．専門は，Web 工学，Deep Learning，人工知能．

♢ 付　　録 ♢

A. 交差エントロピー最大化と相互情報量

$$
\begin{aligned}
I(U;R) &= \sum_{(u,r)} P(U=u,R=r)\log\frac{P(U=u,R=r)}{P(U=u)P(R=r)} \\
&= \sum_{n}^{N}\log\frac{P(U=u_n,R=r_n)}{P(U=u_n)P(R=r_n)} \\
&= \sum_{n}^{N}\log\frac{P(U=u_n|R=r_n)P(R=r_n)}{P(U=u_n)P(R=r_n)}
\end{aligned}
$$

ここで，パラメタ θ_u によるニューラルネットワークの入出力関係 $f_{u_n}(r_n;\theta_u)$ を事後確率 $P(U=u_n|R=r_n)$ のモデルとすると，

$$
\begin{aligned}
I(U;R) &= \sum_{n}^{N}\log\frac{f_{u_n}(r_n;\theta_u)}{P(U=u_n)} \\
&= \sum_{n}^{N}\log f_{u_n}(r_n;\theta_u) - \sum_{n}^{N}\log P(U=u_n)
\end{aligned}
$$

となる．この時，第 2 項目はデータが与えられた上では固定であるから，相互情報量 $I(U;R)$ を最大化することは事後確率の尤度 $\sum_n^N \log f_{u_n}(r_n;\theta_u)$ を最大化することに等しい．

また，式 3 の u_nk は，各サンプルが k 番目のクラスに属するかを示すいずれかが 1 になるような値であるので，$\sum_n^N \log f_{u_n}(r_n;\theta_u)$=$N\cdot \mathrm{L}_u$ となる．

B. 複数のウィンドウを利用した場合のユーザ予測精度に関する検討

図 B.1 に，複数のウィンドウを予測に利用した場合の結果を示す．ここで，複数のウィンドウを予測に利用する方法としては，単純に複数のウィンドウの出力 $P(u|r_i)(i\in 1\cdots w)$ の平均値を取るアンサンブル処理を利用した．横軸は予測に利用したウィンドウ数 w を，縦軸はユーザ予測精度をそれぞれ表している．データセットとしては，表 2 の結果で MLP_{800} を γ として利用した場合に最も CNN と提案手法の差が大きかった USC を利用した．また，他ユーザでも概ね同じ傾向であったため，ここではユーザ ID=1 をテストデータとする Leave-One-Subject-Out イテレーションの結果を示す．結果として，CNN，$\mathrm{UANN}_{\mathrm{MLPA}}$ どちらもウィンドウを大きくすると w=1 の場合と比較して予測精度が高まる傾向にあった．ただし，例えば w=100 の場合には CNN と $\mathrm{UANN}_{\mathrm{MLPA}}$ を比較するとほぼ同程度であるが，CNN は w=10 の時点ですでにほぼ 1.0 であり，依然として提案手法により予測がわずかながら抑制されていることには注意されたい．

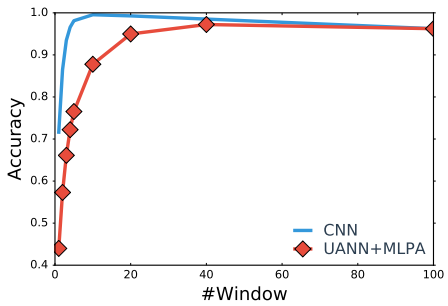


図 B.1: 複数のウィンドウでの出力確率の平均によるユーザ識別性能の変化.