スマートウォッチデータからの感情推定に向けた AutoEncoder を用いて次元圧縮された LDP によるプライバシー保護

小泉 海斗 †　　菊池 浩明 †

明治大学総合数理学部 †

1　はじめに

近年，ウェアラブルデバイスの普及に伴い，心拍や皮膚電気活動などの生体信号を用いたヘルスケア応用が進展している．しかし，これらのデータは個人の身体的特徴だけでなく感情が推定可能．プライバシー情報であり，安全管理が不十分な事業者から漏洩することがないように適切な保護が求められる．

Dwork によって提唱された差分プライバシー (DP) [2] は，数学的に厳密なプライバシー保証を与える枠組みであり，特にデータ収集段階でノイズを加えるローカル差分プライバシー (LDP) は，実社会での導入が進んでいる．

しかし，ヘルスケアデータのような高次元のデータに LDP 適用する場合，次元に比例した大きなノイズを加えると，有用性が損なわれる課題がある．そこで，宮地ら [5] は学習に有効な属性のみを選択することで次元削減を行う手法を提案している．

本研究では，次元圧縮が可能な AutoEncoder[4] を用いて，n 次元データを k 次元の潜在変数 $\boldsymbol{z}$ に集約し，低次元空間内で LDP を適用する手法を提案する．

2　提案手法

2.1　システム構成

本研究の，提案手法「Proposed」の処理フローを図 1 に示す. n 次元の学習データと感情 y について学習した分類器を f_n，k 次元に圧縮したデータについて学習した分類器を f_k とおく．

2.2　AutoEncoder による次元圧縮

AutoEncoder[4] を用い，生体信号の非線形な特徴を低次元に圧縮する．

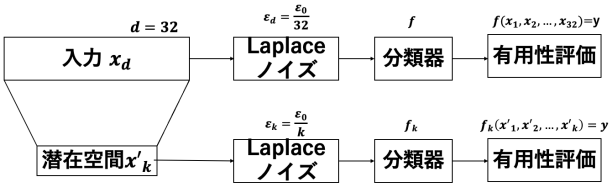

図 1　システム構成図.

入力ベクトル $\boldsymbol{x} \in \mathbb{R}^{32}$ をより低次元の k 個の潜在変数 $\boldsymbol{z} \in \mathbb{R}^k$ に写像する．

学習時には，入力 $\boldsymbol{x}$ と再構成出力 $\hat{\boldsymbol{x}}$ の間の平均二乗誤差 (MSE) を最小化するように，誤差逆伝播法を用いてエンコーダとデコーダの重みを更新する．

学習済みのエンコーダによって得られた潜在変数 $\boldsymbol{z}$ の各要素 z_i に対して，ラプラスノイズ η_i により摂動化する．

$$\tilde{z}_i = z_i + \eta_i, \quad \eta_i \sim \mathrm{Laplace}\left(0, \frac{\Delta f}{\epsilon/k}\right) \quad (i = 1, \ldots, k) \tag{1}$$

分類器 f_k は $\tilde{\boldsymbol{z}}$ について学習する．ここで Δf は感度である．

3　評価実験

3.1　実験設定

オープンデータ WESAD データセット [1] を使用する. 本データセットは手首装着型デバイス (Empatica E4) から取得された BVP, EDA, TEMP, ACC の 4 種類のセンサデータの平均値・標準偏差・最大値・最小値などの統計量に加え，BVP からは心拍変動指標 (HRV)，EDA からは皮膚コンダクタンス反応 (SCR) のピーク数などを算出・結合し，合計 32 次元の特徴量ベクトル $\boldsymbol{x} \in \mathbb{R}^{32}$ から成る．

感情クラス y は表 1 に示される頻度を持つ. Baseline, Stress, Amusement, Meditation の 4 クラス分類とする．

表 1　各感情クラスのデータ数分布

Class	Baseline	Stress	Amusement	Meditation	Total
Count	859	387	109	256	1611

Privacy-Preserving via AutoEncoder-based Dimensionality Reduced LDP toward Emotion Estimation from Smartwatch Data †Kaito Koizumi, Hiroaki Kikuchi, School of Interdisciplinary Mathematical Science, Meiji University.

3.2　実験方法

提案手法の有効性を検証するため，以下の 4 つの条件で比較を行った．なお，LDP 適用後のデータは全て定義域 $[0, 1]$ に収まるようクリッピング処理を施している．

- **Raw Clean**: 生データ（上限値）．
- **AE Clean**: 圧縮のみ行い，ノイズなし．
- **ベースライン**：$\boldsymbol{x}$ ($n = 32$) の各次元に対して，予算 ϵ/n のノイズ加算．
- **提案手法**: 潜在変数 $\boldsymbol{z}$ (k＜32) に圧縮後予算 ϵ/k の小さなノイズを加算．

評価指標には，クラス不均衡の影響を考慮した Macro F1-Score を用いた．プライバシー予算 ϵ を 0.1 から 9 まで変化させ，潜在空間の次元数 k を 1 から 15 まで変化させた際の精度推移を評価した．

3.3　推定精度 の評価

図 2 に，潜在次元数 k と F1-Score の関係を示す．

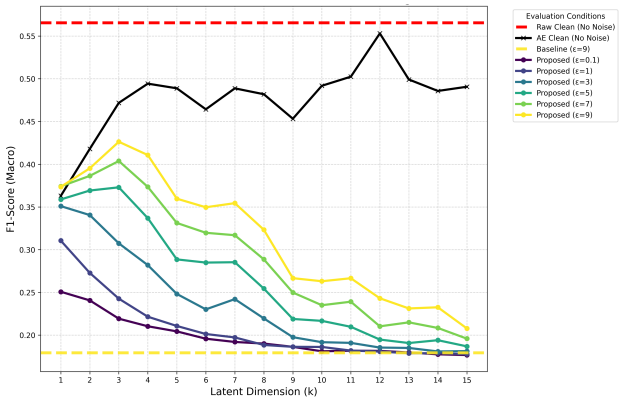

図 2　潜在次元数 k についてのモデル分布推定．

ベースラインとの比較　図 2 の Raw Clean と AE Clean の比較より，次元数 $k \geq 3$ であれば F1-Score を大きく損なわないことが確認できる．これは，32 次元の生体特徴量の多くが冗長であり，低次元空間に効率的に集約可能であることを示唆している．一方，ベースラインは，ϵ に依存せず常に F1-Score が低い．これは，高次元データに対する単純な予算分割 ($n = 32$) により，大きなノイズが加わったためと考えられる．

提案手法の有効性と次元数の影響　提案手法は，いずれの ϵ においてもベースラインを上回る精度を達成した．これは次元圧縮によりノイズを分散させる次元数を減らした効果 ($\epsilon/k > \epsilon/n$) が，情報損失のリスクを上回ったためである．すなわち，高次元のままノイズに埋没させるより，冗長な情報を捨て次元を削減し，個々の特徴量を保つ方が，LDP 環境下では有利であることが示された．また，最適な次元数 k は ϵ に依存する．$\epsilon \geq 5$ の低ノイズ条件下では $k = 3$ が最大精度となり，それ以上の次元増は逆効果であった．対照的に $\epsilon = 1$ の高ノイズ条件下では $k = 1$ が最適となり，次元増に伴い精度は低下した．以上より，データによって最適な次元 k やプライバシ予算 ϵ が存在すると考えられる．

4　おわりに

本研究では，AutoEncoder を用いた次元圧縮により，高次元生体データに対する LDP の課題を解決した．評価実験の結果，生データに直接ノイズを付加するよりも，情報を低次元に集約し，その潜在変数を直接用いることで実用的な推定精度を向上することを示した．この結果は，LDP 環境下の機械学習においては，全次元の情報を保存するよりも，プライバシー予算に応じて情報の「選択と集中」を行うことが重要であることを示唆している．

参考文献

[1] P. Schmidt et al., Introducing WESAD,"*ICMI*, pp. 400–408, 2018.

[2] C. Dwork, Differential Privacy,*ICALP*, pp. 1–12, 2006.

[3] C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, *Foundations and Trends in TCS*, vol. 9, no. 3–4, 2014.

[4] G. E. Hinton et al., Reducing the dimensionality of data with neural networks, *Science*, 2006.

[5] 宮地，高橋，WANG，山月，三本，LDP を用いた機械学習フレームワーク, コンピュータセキュリティシンポジウム *2022* 論文集 *(CSS2022)*, pp. 848–855, 2022.