基于相关性的 Swarm 联邦降维方法

李文平 [1] 杜 选 [1]

摘 要 联邦学习 (Federated learning, FL) 在解决人工智能 (Artificial intelligence, AI) 面临的隐私泄露和数据孤岛问题方面具有显著优势. 针对联邦学习的已有研究未考虑联邦数据之间的关联性和高维性问题, 提出一种基于联邦数据相关性的去中心化联邦降维方法. 该方法基于 Swarm 学习 (Swarm learning, SL) 思想, 通过分离耦合特征, 构建典型相关分析 (Canonical correlation analysis, CCA) 的 Swarm 联邦框架, 以提取 Swarm 节点的低维关联特征. 为保护协作参数的隐私安全, 还构建一种随机扰乱策略来隐藏 Swarm 特征隐私. 在真实数据集上的实验验证了所提方法的有效性.

关键词 隐私保护, Swarm 学习, 联邦学习, 典型相关分析

引用格式 李文平, 杜选. 基于相关性的 Swarm 联邦降维方法. 自动化学报, 2024, **50**(9): 1866−1876

DOI 10.16383/j.aas.c220690

Swarm Federated Dimensionality Reduction Method Based on Correlation

LI Wen-Ping[1] DU Xuan[1]

Abstract Federated learning (FL) has significant advantages in solving the problems of privacy disclosure and data islands faced by artificial intelligence (AI). Previous studies on federated learning do not consider the problems of relevance and high dimensionality of data distributed among different federations. Based on the relevance of federated data, a decentralized federated dimensionality reduction method is proposed. This method draws on the idea of Swarm learning (SL). Based on the separation of coupling features, a Swarm federated framework for canonical correlation analysis (CCA) is constructed to extract the low dimensional correlation features of Swarm nodes. In order to protect the privacy of collaboration parameters, a random disturbance strategy is also constructed to hide the privacy of Swarm features. Experiments on real data sets verify the effectiveness of the proposed method.

Key words Privacy protection, Swarm learning (SL), federated learning (FL), canonical correlation analysis (CCA)

Citation Li Wen-Ping, Du Xuan. Swarm federated dimensionality reduction method based on correlation. *Acta Automatica Sinica*, 2024, **50**(9): 1866−1876

随着 5G 和物联网等数字技术的兴起, 各行各业收集了丰富的数据. 为有效挖掘数据中蕴含的知识, 数据持有者希望相关行为主体之间能共享数据[1]. 然而数据共享导致的安全隐患令人担忧, *Nature* 杂志上发表的一项评论曾指出, 数据科学可以聚合公开可用的数据, 这会对隐私安全造成威胁[2]; 一项发表在 *Science* 杂志上的评论认为, 数据的隐私保护是人工智能 (Artificial intelligence, AI) 实用化不可回避的关键问题[3]. 尽管近年来 AI 技术进步显著, 然而驱动 AI 的数据的隐私问题未得到考虑. 有研究指出, AI 中隐私数据的使用可能触犯道德和法律问题[4]. 还有证据表明, AI 中的隐私泄露问题凸显[5]. 可见 AI 的应用亟需解决隐私问题[6].

联邦学习 (Federated learning, FL) 技术的兴起可望成为应对 AI 中隐私威胁的有效解决方案[7], 该技术将数据存储和模型训练阶段转移至本地, 仅与中心服务器交互模型, 既能提升模型性能, 又具有隐私保护功能[8]. FL 的发展方向可以归纳为 4 类, 其一是研究既有 AI 模型的联邦算法, 其二是探索联邦学习的实现载体, 其三是发展针对特殊数据的联邦学习方法, 其四是开展联邦学习技术的应用探索.

既有 AI 模型的联邦算法研究, 主要任务是将基于集中式架构的 AI 模型扩展至联邦场景[9]. 决策树算法和神经网络模型的联邦实现已得到了学者们的关注, 郭艳卿等[10] 借助直方图存储结构和混淆布隆过滤器, 将基于集中式架构的决策树算法推广至数据非共享场景下的联邦应用, 在金融数据集上的

收稿日期 2022-09-01 录用日期 2023-04-12
Manuscript received September 1, 2022; accepted April 12, 2023
教育部人文社会科学研究规划基金 (23YJAZH068), 嘉兴市科技特派员专项项目 (K2022A015) 资助
Supported by Humanity and Social Science Planning Foundation of Ministry of Education of China (23YJAZH068) and Jiaxing Science and Technology Commissioner Special Project (K2022A015)
本文责任编委 赫然
Recommended by Associate Editor HE Ran
1. 嘉兴学院信息科学与工程学院 嘉兴 314001
1. College of Information Science and Engineering, Jiaxing University, Jiaxing 314001

实验结果显示, 其联合建模的分类准确率接近于集中式架构下的精度, 有效解决了决策树算法的隐私泄露问题; 最近, 张泽辉等[11] 开发一种深度神经网络模型在联邦场景下的训练技术, 其方法通过同态加密保护协同训练的网络参数, 获得了计算量小和保护性高的双重效果.

探索联邦学习的实现载体是联邦学习的研究热点, 其中在区块链上的尝试是目前学界的主攻方向. 为解决异步联邦学习的可信性和隐私问题, 高胜等[12] 基于共识算法、指数机制和双因子调整策略, 构建一种区块链上的联邦学习方案, 在解决单点失效和隐私泄露方面具有较好效果. 朱建明等[13] 的研究更加集中于区块链本身, 模型参数记录和验证都由区块链来实现, 通过惩罚机制约束自利性, 具有参数噪声适时调整和模型适应性聚合能力.

针对特殊数据的联邦学习, 既要满足非共享合作的联邦场景, 又要兼顾数据的特殊性对模型训练的需求, 研究较有挑战性. 冯霁等[14] 针对训练阶段攻击问题, 通过扩展 DeepConfuse 方法生成对抗训练数据, 提出一种联邦 AI 框架, 结果显示出联邦学习系统的隐私脆弱性. 非独立同分布数据的联邦学习最近得到张泽辉等[15] 的关注, 其研究引入混沌系统和同态加密技术, 提出一种联邦局部模型的自适应聚合框架, 获得了较好的精度和较高的训练效率.

联邦学习技术的应用探索较有吸引力, 朱静等[16] 从联邦生态的角度出发, 提出一种名为联邦控制的新型控制理论, 深刻论述了联邦控制原理及其广泛应用前景, 为联邦学习技术的应用开辟了一个全新视野. 方晨等[17] 的研究结合区块链, 将联邦学习应用于边缘计算场景, 通过动态监测隐私损失, 构建自适应差分隐私机制, 获得了较好的模型精度和较高的隐私保护度. 张沁楠等[18] 针对数字经济背景下的安全数据交易需求, 基于区块链和贝叶斯博弈论, 提出一种联邦激励机制, 对解决数据交易的供给不足问题较有参考价值.

上述方法主要基于中心服务器聚合模型参数, 未考虑中心服务器的不可信问题. Warnat 等[19] 前不久在 *Nature* 杂志上报道的 Swarm 学习 (Swarm learning, SL) 架构采用去中心化方案, 不需要模型聚合服务器, 通过 Swarm 网络共享学习参数, 并在各个 Swarm 边缘节点的私有数据上独立构建模型, 在新型冠状病毒 (COVID-19)、结核病、白血病和肺部病变数据集上的分类结果验证了 SL 架构的高可用性. SL 架构原本是基于 Swarm 网络的一种联邦技术, 但其实现可以是多种载体, 其本质在于去中心化. 本文借鉴 SL 思想, 提出一种去中心化联邦场景下的数据协同降维方法.

联邦参与方之间协作学习的目的除了保护数据隐私外, 还希望获得较单方数据更好的模型[20]. 已有研究发现, 当参与方之间的数据具有较好关联性时, 联邦协作学习获得的模型识别率更高[21]. 由此可见, 如何有效利用联邦数据之间的关联性提高模型精度或训练效率, 是联邦计算的一个关键科学问题. 此外, 联邦学习中常用的数据往往是高维的[22], 例如图像、视频、音频、基因序列、蛋白质结构数据等的维度往往都较高, 联邦学习如何解决高维数据下的协作效率是一个亟需攻克的重要课题.

尽管联邦数据之间的关联性和高维性可以单独选择不同的技术进行解决, 但是采用同时兼顾二者的集成化方案有望能使问题简单化. 典型相关分析 (Canonical correlation analysis, CCA) 理论[23] 有望成为解决此问题的有效工具. CCA 具有坚实的数学理论基础, 是一种成熟的多元统计方法, 能检测多维变量之间的相关性, 同时也是一种基于相关性的降维方法, 已在广泛领域得到了成功应用, 关于 CCA 较全面的综述建议读者参阅文献 [24]. 已有 CCA 方法主要是基于单节点的计算架构, 即 CCA 所需的数据集需放到同一个计算节点上, 不适用于联邦场景, 而且参加计算的是原始数据, 隐私问题未得到考虑.

针对联邦数据的关联性和高维性, 本文基于 SL 思想, 提出一种名为 SCCA (Swarm CCA) 的协作降维方法, 在去中心化的 Swarm 场景下, 构建支持隐私保护的 CCA 求解算法. 创新性工作如下:

1) 剖析 CCA 隐私泄露的根源在于协方差矩阵需要协作方提供原始数据;

2) 分析经典 CCA 不适用于 Swarm 场景的原因是互协方差的耦合导致的, 据此推演出耦合特征的分离解析式;

3) 构建 CCA 求解的 Swarm 协作框架, 提出 SCCA 的求解算法;

4) 对 SCCA 的隐私性进行分类, 据此提出一种 SCCA 的特征隐私保护策略;

5) 开展 SCCA 的仿真实验研究, 在真实数据集上评估 SCCA 算法的有效性, 并给出其在图像分类上的应用实例.

1 问题描述

记 Swarm S_1和 S_2采集的数据集分别为 $X=\{x_1, x_2, \cdots, x_p\}$ 和 $Y=\{y_1, y_2, \cdots, y_q\}$, 其中 p 和 q 分别为 S_1 和 S_2 所采集数据的维度或属性个数; $x_i=[x_{1i}, x_{2i}, \cdots, x_{ni}]^{\mathrm{T}} \in \mathbf{R}^{n\times 1}$, $i=1, \cdots, p$; $y_j=[y_{1j}, y_{2j},$

$\cdots, y_{nj}]^{\mathrm{T}} \in \mathbf{R}^{n\times 1},\ j=1,\cdots,q;\ n$为样本容量. CCA的目标是寻找实向量$\alpha$和$\beta$, 使得$X$和$Y$分别在其上的投影的相关性最大. CCA形式化描述为[23]

$$\begin{aligned}&\arg\max_{\alpha,\beta}\ \rho=\alpha^{\mathrm{T}}C_{12}\beta\\&\text{s.t. }\alpha^{\mathrm{T}}C_{11}\alpha=1,\ \beta^{\mathrm{T}}C_{22}\beta=1\end{aligned}\tag{1}$$

式(1)中, $C_{12}=C_{21}$为X与Y的互协方差矩阵, C_{11}和C_{22}分别为X和Y的自协方差矩阵, ρ为投影向量之间的相关系数. 作旋转坐标变换

$$\alpha=C_{11}^{-\frac{1}{2}}u_1,\ \beta=C_{22}^{-\frac{1}{2}}v_1\tag{2}$$

其中, u_1和v_1分别为P的左、右奇异向量. 由拉格朗日乘子法可得式(1)的SVD (Singular value decomposition)解[25]

$$\begin{bmatrix}-\rho\mathbf{1} & P\\ P^{\mathrm{T}} & -\rho\mathbf{1}\end{bmatrix}\begin{bmatrix}u_1\\ v_1\end{bmatrix}=\mathbf{0}\tag{3}$$

式(3)中, $P=C_{11}^{-1/2}C_{12}C_{22}^{-1/2}$, P关于u_1和v_1的奇异值ρ恰为式(1)中的皮尔逊相关系数值, 即典型相关系数. 对P进行奇异值分解

$$P=U\Sigma V^{\mathrm{T}}\tag{4}$$

可获得式(1)的全部解[26], 其中非零奇异值$\Sigma=\mathrm{diag}\{\rho_1,\rho_2,\cdots,\rho_d\},\ \rho_1\geq\rho_2\geq\cdots\geq\rho_d>0$, 第$i$个奇异值$\rho_i$对应第$i$个典型相关系数, 对应的奇异向量为

$$U=[u_1,u_2,\cdots,u_d],\ V=[v_1,v_2,\cdots,v_d]$$

按式(2)变换即为式(1)的典型向量

$$A=[\alpha_1,\alpha_2,\cdots,\alpha_d],\ B=[\beta_1,\beta_2,\cdots,\beta_d]$$

观察矩阵C_{12}, 若数据X和Y已中心化, 则$C_{12}=X^{\mathrm{T}}Y$, 由此可见, 需要Swarm S_1和S_2提供原始数据X和Y, 才能获得$P=C_{11}^{-1/2}C_{12}C_{22}^{-1/2}$的SVD解, 数据隐私遭到暴露. 这显然不是一个Swarm计算问题, 缺乏隐私保护能力. Swarm计算的基本前提是参与方不提供原始数据, 而仅共享学习参数, 以达到隐私安全的协作计算目的.

如何将式(4)分解为Swarm协作计算是拟解决的关键问题, SCCA的核心任务包括:

1) 式(4)的SVD过程应分解为两个Swarm节点协作计算完成, 而非单独由一方计算, 也不需要中心服务器参与, 前者是与经典CCA的区别, 后者是与传统联邦计算方法的差异;

2) Swarm协作的共享参数应该是隐私安全的, 协作时交互的是过程参数, 既不共享原始数据, 也不加密共享参数, 共享原始数据适用于经典CCA, 而加密参数适用于多方计算, 都不满足Swarm场景.

2 SCCA

2.1 特征分离

为获得CCA在Swarm场景下的解, 需先将式(3)中的矩阵P分解为仅与X和Y自身有关的两部分, 以实现特征分离.

定理 1. 式(3)中X和Y的协方差矩阵耦合的矩阵$P=C_{11}^{-1/2}C_{12}C_{22}^{-1/2}$可分解为分别仅与$X$和$Y$有关的两矩阵$M_x$和$M_y$的乘积.

证明. 对X和Y分别进行QR分解

$$X=Q_xR_x,\ Y=Q_yR_y\tag{5}$$

不妨设数据X和Y已中心化, 则

$$C_{12}=X^{\mathrm{T}}Y=R_x^{\mathrm{T}}Q_x^{\mathrm{T}}Q_yR_y$$

$$C_{11}=X^{\mathrm{T}}X=R_x^{\mathrm{T}}Q_x^{\mathrm{T}}Q_xR_x=R_x^{\mathrm{T}}R_x$$

同理$C_{22}=R_y^{\mathrm{T}}R_y$, 所以式(3)中的矩阵$P$为

$$P=(R_x^{\mathrm{T}}R_x)^{-\frac{1}{2}}R_x^{\mathrm{T}}Q_x^{\mathrm{T}}Q_yR_y(R_y^{\mathrm{T}}R_y)^{-\frac{1}{2}}$$

记

$$M_x=Q_xR_x(R_x^{\mathrm{T}}R_x)^{-\frac{1}{2}}$$

$$M_y=Q_yR_y(R_y^{\mathrm{T}}R_y)^{-\frac{1}{2}}$$

则有

$$M_x^{\mathrm{T}}M_y=P=U\Sigma V^{\mathrm{T}}\tag{6}$$

式(6)的意义在于实现了耦合特征的分离, M_x仅与X有关, M_y仅与Y有关, 于是式(4)的SVD问题变为式(6)的两乘积矩阵$M_x^{\mathrm{T}}M_y$的SVD问题. □

2.2 协作过程

为实现式(4)在Swarm场景下的SVD分解, 需将其分解为两个Swarm节点在不传送原始数据的前提下的协作计算过程.

定理 2. 式(4)的SVD分解可在不传送原始数据的前提下, 由两个Swarm节点通过共享Swarm参数完成协作求解.

证明. 由定理1得知, 矩阵P可分解为式(6)所示的乘积矩阵$P=M_x^{\mathrm{T}}M_y$. 根据矩阵论的SVD理论可有, 乘积矩阵$M_x^{\mathrm{T}}M_y$的精确解可以通过PSVD[27] (Product-induced SVD)算法实现, 其流程为: 1) $\Delta_x=\mathrm{diag}\{\|m_1\|_2,\|m_2\|_2,\cdots,\|m_n\|_2\}$, $G_1=\Delta_x^{\dagger}M_x$, $H_2=\Delta_xM_y$; 2) 计算H_2^{T}的QR分解$H_2^{\mathrm{T}}=Q_2R_2$; 3) 计算$F=G_1^{\mathrm{T}}R_2^{\mathrm{T}}$; 4) 计算$F$的QR分解$F=Q_fR_f$; 5) 计算$R_f$的SVD分解$\Sigma=V_f^{\mathrm{T}}R_fW_f$; 6) $M_x^{\mathrm{T}}M_y=(Q_fV_f)\Sigma(Q_2W_f)^{\mathrm{T}}$. 其中$\|m_i\|_2$是$M_x$的第

i 个行向量的 L_2 范数, $\Delta_x^{\dagger}$ 是 Δ_x 的 Moore-Penrose 广义逆. 据此可得式 (6) 中 $U = Q_f V_f$, $V = Q_2 W_f$. 两个 Swarm 节点按如下流程协作, 首先由 Swarm S_1 向 Swarm S_2 传递 Δ_x, S_2 节点计算出 R_2 后传递给 S_1, 再在 S_1 端执行 3)、4)、5) 步运算, 最后 S_1 将 $\mathrm{diag}\{\Sigma\}$ 和 W_f 传递给 S_2, 按此协作过程, Swarm 节点间不需要传递原始数据且可获得式 (4) 的解.□

定理 2 的证明过程描述了 SCCA 的协作流程, 其协作序列如图 1(a) 所示.

2.3　SCCA 算法描述

SCCA 协作过程见算法 1 和算法 2. 在 Swarm S_1 端执行算法 1, 在 Swarm S_2 端执行算法 2.

算法 1. SCCA-S1

输入. Swarm S_1 端的原始数据 $X \in \mathbf{R}^{n\times p}$.

输出. 典型相关系数向量 ρ, 典型向量构成的矩阵 A.

1) 数据中心化 $X \leftarrow X - \overline{X}$;

2) 执行 QR 分解 $X = Q_x R_x$;

3) 求矩阵乘积 $M_x = Q_x R_x (R_x^{\mathrm{T}} R_x)^{-1/2}$;

4) 求矩阵 $\Delta_x = \mathrm{diag}\{\|m_1\|_2, \|m_2\|_2, \cdots, \|m_n\|_2\}$;

5) 将 Δ_x 发送给 Swarm S_2;

6) 等待 Swarm S_2 运行, 直到其返回矩阵 R_2;

7) 求矩阵乘积 $G_1 = \Delta_x^{\dagger} M_x$;

8) 求矩阵乘积 $F = G_1^{\mathrm{T}} R_2^{\mathrm{T}}$;

9) 执行 QR 分解 $F = Q_f R_f$;

10) 执行 SVD 分解 $\Sigma = V_f^{\mathrm{T}} R_f W_f$;

11) 置 $\rho = \mathrm{diag}\{\Sigma\}$;

12) 将 ρ 和 W_f 发送给 Swarm S_2;

13) 求矩阵乘积 $U = Q_f V_f$;

14) 计算典型向量构成的矩阵 $A = C_{11}^{-1/2} U$;

15) 返回 ρ 和 A.

算法 2. SCCA-S2

输入. Swarm S_2 端的原始数据 $Y \in \mathbf{R}^{n\times q}$.

输出. 典型相关系数向量 ρ, 典型向量构成的矩阵 B.

1) 数据中心化 $Y \leftarrow Y - \overline{Y}$;

2) 执行 QR 分解 $Y = Q_y R_y$;

3) 求矩阵乘积 $M_y = Q_y R_y (R_y^{\mathrm{T}} R_y)^{-1/2}$;

4) 等待 Swarm S_1 运行, 直到接收到矩阵 Δ_x;

5) 求矩阵乘积 $H_2 = \Delta_x M_y$;

6) 执行 QR 分解 $H_2^{\mathrm{T}} = Q_2 R_2$;

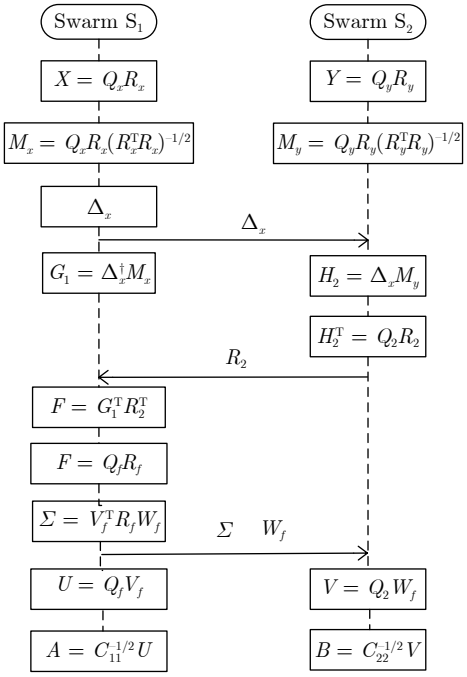
7) 将 R_2 发送给 Swarm S_1;

8) 等待 Swarm S_1 运行, 直到收到向量 ρ 和矩阵 W_f;

9) 求矩阵乘积 $V = Q_2 W_f$;

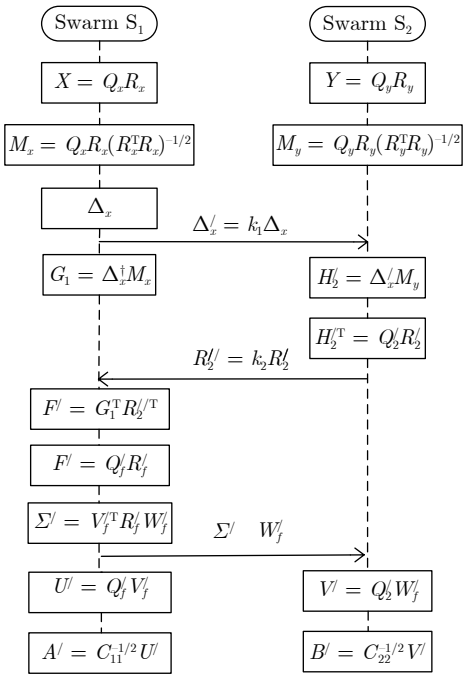
10) 计算典型向量构成的矩阵 $B = C_{22}^{-1/2} V$;

11) 返回 ρ 和 B.



(a) 基本协作序列

(a) The basic collaboration sequence



(b) 隐私保护协作序列

(b) Collaboration sequence with privacy preserving

图 1　SCCA 协作序列

Fig. 1　Collaboration sequences of the SCCA

2.4　参数传递量分析

Swarm S_1 和 S_2 采集的原始数据集 X 和 Y 分别是 $n \times p$ 维和 $n \times q$ 维矩阵. S_1 需向 S_2 传递典型相关系数向量 ρ、参数 Δ_x 和 W_f, 其中 ρ 仅需取前 d 个

非零奇异值, $d = |\rho| \leq \min\{p, q\}$,而 $\Delta_x = \mathrm{diag}\{\|m_1\|_2, \|m_2\|_2, \cdots, \|m_n\|_2\}$ 只需传递 n 个对角元素$\|m_i\|_2$, $i = 1, 2, \cdots, n$ 即可, 与 d 个非零奇异值对应的右奇异向量 W_f 的元素个数为$n \times d$, 因此 S_1 向 S_2 传递的参数量为$nd + n + d$.

Swarm S_2 向 S_1 传递的参数为R_2, 这是一个 $n \times q$ 维的矩阵, 传递的参数量为$n \times q$. 当$p < q$时, Swarm 双方互换所执行的算法可使参数量降为np, 这只需将算法 SCCA-S1 和 SCCA-S2 都布置到 Swarm 双方, 协作计算开始时, Swarm 双方向对方互发所感知的数据维数 p 和q, 据此选择参数量较小的方案运算. 所以 SCCA 需传递的参数量为$np + nd + n + d$.

经典 CCA 需将参与双方的数据汇集到单机上执行. 设$p < q$, S_1将数据传给S_2, 在S_2 上运行, 需传递的原始数据量为np; S_2 将运算结果传给S_1, 含 d 个典型相关系数值和nd 个典型向量. 所以单节点的经典 CCA 需传递的参数量为$np + nd + d$.

总之, SCCA 求解时所需传递的参数量, 比将数据汇集到单节点下运算的经典 CCA 所需的传递量多 n, 这与参与运算的原始数据集 X 和 Y 的数据量 $n \times p$ 和 $n \times q$ 相比, 其增加量并不显著.

3 SCCA 的隐私保护

3.1 隐私界定

求解 SCCA 过程中, 哪些信息属于隐私范畴, 即隐私界定, 是隐私性分析及隐私保护的前提. Swarm S_1和 S_2 协作过程中, 本文做如下三点界定:

1) 数据集 X 和 Y 之间的典型相关系数 $\rho = \mathrm{diag}\{\Sigma\}$ 是共性需求, 不属于隐私范畴;

2) 数据集 X 和 Y 是 Swarm 参与双方各自的数据资产, 属于高度敏感的隐私信息;

3) SCCA 协作过程中传递的参数携带了特征级的隐私信息.

本文将隐私分为两类, 即数据隐私和参数隐私, 前者指原始数据的隐私, 后者指协作参数的隐私. 为此, 涉及数据和参数两类隐私性.

数据隐私性, 是指 Swarm 参与方基于所接收到的协作参数复原对方原始数据的能力, 即, S_2 复原出 X 的可能性以及S_1复原出Y 的可能性.

参数隐私性, 是指 Swarm 参与方向协作对方传递的参数表征自身隐私信息的水平, 表征水平越强, 参数隐私性越强, 反之则越弱.

3.2 隐私性分析

1) 数据隐私性

数据隐私性分析的本质是考察原始数据的复原可能性.

首先考察 S_2 复原 X 的可能性. S_2 接收到S_1传入的参数是 Δ_x 和W_f, 对角矩阵Δ_x 的对角元素 $\|m_i\|_2 = \left(\sum_{k=1}^{n} (M_x(i, k))^2\right)^{1/2}$ 是 M_x 的第 i 个行向量的 L_2 范数, 显然由$\|m_i\|_2$求解每个元素 $M_x(i, k)$, $k = 1, 2, \cdots, n$ 是一个不可解问题; 同理由W_f 求解 M_x 也是不可解问题. 可见S_2 复原 X 是不可行的.

其次考察S_1复原 Y 的可能性. S_1接收到S_2传入的参数是 R_2, 而 R_2 由 H_2^{T} 进行 QR 分解 $H_2^{\mathrm{T}} = Q_2 R_2$ 得到, 因为S_1并不知晓Q_2, 仅由因子 R_2 构造 H_2^{T} 不可行.

由此可知, SCCA 协作过程中, 数据未遭到隐私泄露, 数据隐私性是安全的.

2) 参数隐私性

首先考察 Swarm 参与方S_1向S_2传递的可能携带特征隐私的参数 Δ_x 和W_f 的特征级隐私性. 对于参数 W_f, S_1 生成矩阵 U 不需要W_f 的参与, 同时也无法由 W_f 复原G_1, 因此W_f 对S_1而言是特征级安全的. 然而 Δ_x 则是不安全的, 矩阵Δ_x 的对角元素$\|m_i\|_2$是 M_x 的第 i 个行向量的 L_2 范数, 此参数携带了 M_x 的范数的隐私信息, 基于范数的运算将泄露S_1的范数特征级隐私.

再考察 S_2 向 S_1 传递的参数 R_2 的特征级隐私性. 基于 QR 分解原理, 通过平方根滤波法可以去掉正交矩阵Q_2的影响, 这只需注意到 $H_2 H_2^{\mathrm{T}} = R_2^{\mathrm{T}} R_2$, 尽管由 $R_2^{\mathrm{T}} R_2$ 求解平方根矩阵 H_2^{T} 的精确值是不可解的, 然而 R_2 携带了 M_y 平方层面的隐私信息, 基于平方或绝对值的运算都将泄露S_2的平方特征级隐私.

综上可知, SCCA 的参数隐私性是不安全的, 因为 Swarm 参与方向协作对方传递的参数是由自身数据中提取的结构信息, 对自身信息都具有一定的表征能力, 只是表征水平不同而已.

由此可见, 保护 Swarm 参数的隐私安全是必要的, 需要进一步探讨 Δ_x 和 R_2 的隐私保护策略.

3.3 SCCA 的特征隐私保护

由第 3.2 节得知, Swarm 参与方在协作过程中数据隐私性是安全的, 而参数 Δ_x 和 R_2 的特征级隐私被暴露, 因此 SCCA 的隐私保护任务是实现参数 Δ_x 和 R_2 的隐匿. 为保护Δ_x 和R_2 的特征级隐私, 本文提出一种随机扰乱策略, 如图 1(b) 所示, 其中任意标有上角标"/"的量表示隐私保护后的量.

Swarm 特征隐私保护策略: Swarm 参与方每次向对方传递参数 Δ_x 和 R_2 之前, 各自生成一个随机正实数 k_1 和 k_2 对传递参数进行乘性随机扰乱, 传

递的参数变为 $\Delta_x^{/}=k_1\Delta_x$ 和 $R_2^{//}=k_2R_2^{/}$.

首先, 考察此保护策略对协作参数 Δ_x 和 $R_2^{/}$ 保护的有效性. 观察 $\Delta_x^{/}=k_1\Delta_x$ 和 $R_2^{//}=k_2R_2^{/}$, 因为 k_1 和 k_2 为随机正实数, 显然由 $\Delta_x^{/}$ 分离出 Δ_x 以及由 $R_2^{//}$ 构造出 $R_2^{/}$ 都是不可解问题, 因此上述保护策略能有效保护参数的隐私安全.

其次, 证明此保护策略的正确性, 即 CCA 结果的一致性.

定理 3. 用随机正实数 k_1 和 k_2 扰乱协作参数 Δ_x 和 $R_2^{/}$, 用保护后的参数 $\Delta_x^{/}=k_1\Delta_x$ 和 $R_2^{//}=k_2R_2^{/}$ 作为协作参数, 则图 1 所示的两类协作过程结果等价, 即, $A^{/}=A$, $B^{/}=B$ 且 $\Sigma^{/}=k_1k_2\Sigma$.

证明. 根据图 1, 由 $\Delta_x^{/}=k_1\Delta_x$ 得 $H_2^{/}=k_1H_2$, 由 Q_2 和 $Q_2^{/}$ 单位正交性得 $H_2H_2^{\mathrm{T}}=R_2^{\mathrm{T}}R_2$ 和 $H_2^{/}H_2^{/\mathrm{T}}=R_2^{/\mathrm{T}}R_2^{/}$, 据此有 $R_2^{/}=k_1R_2$, $Q_2^{/}=Q_2$. 同理可得 $R_f^{/}=k_1k_2R_f$, $Q_f^{/}=Q_f$. 当 W_f 取单位化奇异向量时, 由 $R_f^{\mathrm{T}}R_f=W_f\Sigma^2W_f^{\mathrm{T}}$ 和 $R_f^{/\mathrm{T}}R_f^{/}=W_f^{/}\Sigma^{/2}W_f^{/\mathrm{T}}$ 可得 $\Sigma^{/}=k_1k_2\Sigma$ 且 $W_f^{/}=W_f$. 同理可得 $V_f^{/}=V_f$. 据此有 $A^{/}=A$, $B^{/}=B$ 且 $\Sigma^{/}=k_1k_2\Sigma$. □

定理 3 表明, 上述乘性随机扰乱策略能保证 CCA 结果的正确性.

首先, 观察典型向量 A 和 B, 用随机正实数 k_1 和 k_2 扰乱协作参数 Δ_x 和 $R_2^{/}$ 后, 所得的典型向量 A 和 B 的结构得到了完整保留而未遭到破坏, 这对于 Swarm 降维和 Swarm 特征聚合等基于特征的挖掘或学习任务是有益的.

其次, 考察典型相关系数 $\rho=\mathrm{diag}\{\Sigma\}$ 的结构, ρ 被放大了 $k_1\times k_2$ 倍, 因此隐私保护后不宜直接应用于 Swarm 相关性检测, 然而在 Swarm 降维和 Swarm 特征聚合等场景中仍然可以作为主特征量选取的依据. 记 $\rho_1>\rho_2>\cdots>\rho_d>0$ 和 $\rho_1^{/}>\rho_2^{/}>\cdots>\rho_d^{/}>0$ 分别为 $\rho=\mathrm{diag}\{\Sigma\}$ 和 $\rho^{/}=\mathrm{diag}\{\Sigma^{/}\}$ 降序排列的前 d 个非零值, 因为 $\Sigma^{/}=k_1k_2\Sigma$, 所以它们具有一致的比值, 即 $\rho_1:\rho_2:\cdots:\rho_d=\rho_1^{/}:\rho_2^{/}:\cdots:\rho_d^{/}$, 这表明典型相关系数的结构得到了保持.

4　实验结果及分析

4.1　数据集及实验设置

实验采用 UCI 机器学习库的数据集 HAPT[28] (Human activities and postural transitions) 来评估算法的有效性. HAPT 数据集记录了受试 6 项基本活动信息, 包括 3 种静态姿势 (站、坐、卧) 和 3 种动态活动 (步行、下楼和上楼). HAPT 包括传感器值和特征数据, 传感器值由智能手机内嵌的加速度计和陀螺仪收集的 3 轴线性加速度值和 3 轴角速度值组成, 特征数据通过低通滤波和快速傅里叶变换分别获得时域和频域共 561 个特征, 本文的实验在特征数据上进行. HAPT 的特征数据共含 10 929 条记录, 其中选取 7 767 条记录作为训练数据, 约占 70%, 其余 3162 条记录作为测试数据, 约占 30%.

实验还采用了另一个数据集 IMDB-WIKI[29] 作为 SCCA 的应用示例. IMDB-WIKI 是带有性别和年龄标签的人脸图像数据集, 图 2 是其部分人脸图像示例, 包括彩色图和灰度图. IMDB-WIKI 数据集包括 IMDB 和 WIKI 两部分, 本文仅使用来自 WIKI 的人脸图像和元数据.

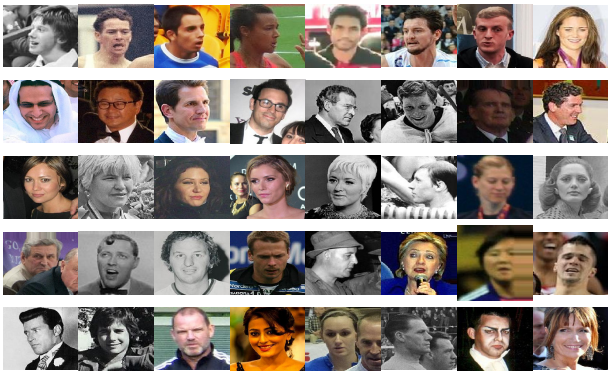


图 2　来自 IMDB-WIKI 的图像示例

Fig. 2　The sample images selected from IMDB-WIKI

实验在配置有 32 GB RAM 的单台 PC 机上仿真完成.

4.2　主向量的影响评估

SCCA 获得的典型相关系数值是递减的, 即, 越靠前的典型相关系数值越大, 越靠后的系数越小. 典型相关系数值越大, 典型向量携带的信息越重要. 本文将预设的典型相关系数值对应的主要典型向量称为主向量. 如何选取主向量是 SCCA 应用的关键.

与 IMDB-WIKI 数据集相比, HAPT 数据集的复杂度低. 为降低实验复杂度, 主向量的影响评估在 HAPT 数据集上进行.

实验假设 Swarm 协作一方持有加速度计采集的特征数据 (简记为 Acc), 而协作另一方持有陀螺仪采集的特征数据 (简记为 Gyro), 由加速度值采集方 Swarm 1 和陀螺仪值采集方 Swarm 2 协作完成 CCA, 这是一个典型的 Swarm 学习问题.

实验的目的在于, 以 Acc 和 Gyro 作为原始数据, 通过 SCCA 提取低维特征, 在低维特征上实现 Swarm 协作学习 (分类), 以考察主向量的影响.

后文所提的原始数据是指 HAPT 中时域及频

域特征 Acc 和 Gyro, 而特征数据是指 SCCA 获得的低维特征, 即原始数据在典型向量上的投影值.

实验 1. 主向量对相对分类精度的影响

本实验考察不同典型相关系数阈值对应的主向量对分类精度的影响. 选择 k-近邻分类器, 取 $k=1$; 训练数据和测试数据取自 HAPT 数据集的原分割.

实验分为两步, 首先 Swarm 参与方各自在训练数据集上协作训练 SCCA 模型, 其中一方使用 Acc 训练, 另一方使用 Gyro 训练, 双方各自获得自身的典型向量集; 其次从典型向量集中选取典型相关系数大于设定阈值的主向量, Swarm 协作方分别将各自持有的 HAPT 训练数据和测试数据投影到主向量方向, 获得 Swarm 特征数据, 各自以 Swarm 特征数据作为 k-近邻分类器的训练和测试语料.

为将焦点聚集在对主向量的选取上, 分类精度采用相对精度来刻画, 比较基准是 k-近邻分类器在原始数据上的分类精度. 不妨记在 Swarm 特征数据上获得的分类精度为 $KAcuSwarm$, 而比较基准对应的分类精度记为 $KAcuOrg$, 则相对精度定义为 $100\% \times KAcuSwarm/KAcuOrg$.

以 0.05 作为步长, 典型相关系数阈值从 0.95 依次降低到 0.15, 获得的相对分类精度如图 3 中圆圈图例 Acc 和菱形图例 Gyro 标记的曲线所示, 其中相对分类精度的最大值以红色实心方框标注, 其典型相关系数阈值与绿色线对应.

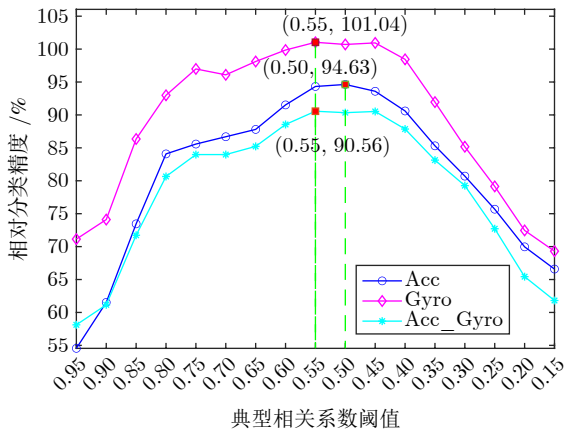


图 3 主向量对分类精度的影响

Fig. 3 Influence of the principal vectors on classification accuracy

典型相关系数阈值降低, 表明选取的主向量增多. 相对精度曲线呈现出钟形变化趋势, 即, 主向量数目增加的过程中, 相对分类精度先增大后减小. 这表明选取适度量的主向量是必要的, 但是主向量数目并不是越多越好, 这是一个朴素认知之外的有趣现象, 朴素观点认为, 特征越多越好 (精度越高).

为考察相对精度曲线的钟形趋势是否是分割数据 (Acc 和 Gyro) 独有的, 实验进一步将 Swarm 参与双方由 Acc 和 Gyro 各自获得的 Swarm 特征通过拼接方式进行特征聚合, 同时将对应的 SCCA 典型向量拼接获得聚合模型, 考察聚合特征 (记为 Acc _ Gyro) 上的主向量选取对相对分类精度的影响, 结果如图 3 中星号图例标记的曲线所示. 聚合特征上的结果仍然显示出相对精度曲线的钟形趋势, 这进一步表明选取适量的主向量是必要的.

当比较分割特征 Acc 及 Gyro 上的相对精度与聚合特征 Acc_Gyro 上的相对精度的关系时发现, 除了典型相关系数阈值大于 0.9 的区域外, 聚合特征上的相对分类精度比分割特征上的相对分类精度低. 一个让人诧异但极具说服力的结果, 来自典型相关系数阈值等于 0.55 (对应 37 对主向量) 时分割特征 Gyro 与聚合特征 Acc_Gyro 对应的相对分类精度值, 前者的相对分类精度超过 101%, 而后者不足 91%, 二者相差接近 10%、差异明显, 表明合适的主向量选取可以获得较原数据上更高的分类精度.

实验 2. 主向量对数据量的影响

前面的实验结果表明, 适量的主向量选取可获得较高的相对分类精度, 说明通过 SCCA 获得的协作模型可用性较好. 事实上, Swarm 特征的应用大幅降低了注入 k-近邻分类器的数据量. 选取的主向量数增加的过程中, 用 k-近邻分类器进行训练和测试时, Swarm 特征的总数据量相对于原数据总量比值的变化趋势如图 4 所示.

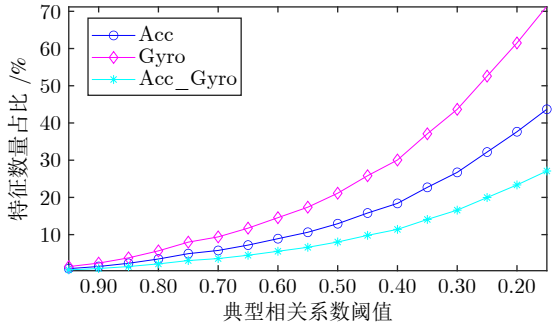


图 4 主向量对数据量的影响

Fig. 4 Influence of the principal vectors on data size

图 4 呈现出两个现象, 其一是典型相关系数阈值降低 (主向量数相应增加) 过程中, 数据量快速增加; 其二是典型相关系数阈值大的区域是低数据量的聚集区, 例如结合图 3 的钟形曲线, 若取 0.75 作为典型相关系数阈值, 在 Gyro 上能获得超过 95% 的相对分类精度, 然而所需的数据量占比却不足 10%, 由此表明 SCCA 降维是可用和有效的.

4.3　Swarm 联邦降维在图像分类上的应用

实验目的. 本组实验考察经过 Swarm 联邦协作降维获得的低维特征在分类任务上的可用性, 一方面观察基于低维特征的分类精度较原始数据上的分类精度的损失情况, 另一方面比较两者之间的效率. 实验采用 IMDB-WIKI 图像数据集.

研究假设. 两个 Swarm 参与协作图像分类, 每个 Swarm 各自持有自身的图像数据, 双方通过 SCCA 协作, 获得低维特征模型 (即主向量), 各自再基于低维主特征在本地完成图像的性别分类.

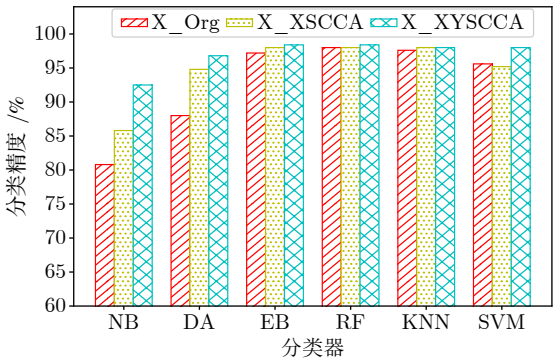
数据质量分析. IMDB-WIKI 数据集包含性别元数据, 与本实验目的契合度较好. 该数据集是通过维基百科收集的人脸图像, 是一种众包方式收集的数据集, 其优点是来源于现实环境, 但是其数据质量不及实验环境下采集的人脸数据. 分析发现, 该数据集复杂性较高, 除了图像大小和图像清晰度不一致外, 还体现在背景复杂、部分图有多张人脸、性别标注缺失和标注争议、存在部分非人脸图像等方面. 为提高考察针对性, 有必要进行数据预处理.

图像预处理. 实验选取脸部得分不低于 3 的高质量图像 (数据集元数据标记了脸部得分, 介于 1 至 7 之间), 并去除年龄标记有歧义 (年龄为负或大于 100) 的图像, 获得男性人脸图像 17 182 张, 女性人脸图像 7 285 张. 为获得大小一致的图像并降低存储开销, 实验将彩色图像转换为灰度图, 再通过图像金字塔下采样技术获得 64×64 的规整图像, 其滤波器设置为 3×3 的二维高斯滤波. 最后按行优先的顺序将采样图像拉直为行向量, 获得 4 096 个属性特征.

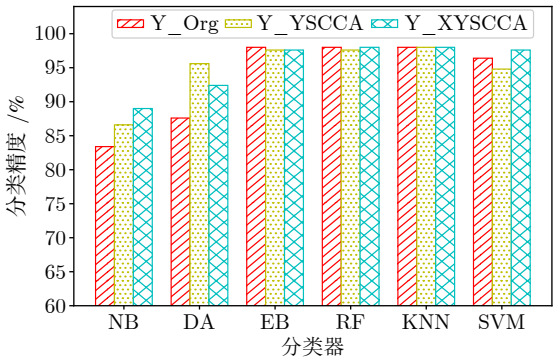
分类算法选择. 在 Swarm 1 端和 Swarm 2 端, 分别采用多个分类器进行性别分类, 分类算法包括朴素贝叶斯 (Naive Bayes, NB)、判别分析 (Discriminant analysis, DA; 决策类型参数 type = 'pseudolinear')、集成学习 (Ensembles for boosting and bagging, EB; 方法参数 method = 'AdaBoostM1')、随机森林 (Random forest, RF; 决策树数目参数 nTree = 10)、k-近邻 (k-nearest neighbor, KNN; 参数 $k = 1$)、支持向量机 (Support vector machine, SVM) 共 6 个分类器.

实验 3. 性别协作识别精度比较

从男、女图像中人工挑选出质量较好的图像各 7 150 张, 混合后分别随机选取 6 500 张图的采样数据作为 Swarm 1 的训练数据 X 和 Swarm 2 的训练数据 Y, 测试数据分别选取 650 张图的采样值. SCCA 协作端各自选取分位数大于 0.65 的主典型相关系数值对应的 1 434 个主向量作为低维特征生成模型. 实验重复了 10 次, 精度和时间取均值. 性别协作识别精度的比较结果如图 5 所示.



(a) Swarm 1 端的分类精度
(a) Classification accuracy on Swarm 1



(b) Swarm 2 端的分类精度
(b) Classification accuracy on Swarm 2

图 5　性别识别精度
Fig. 5　Recognition accuracy for gender

图 5 中的前缀 X_* 和 Y_* 分别表示 Swarm 1 端和 Swarm 2 端的采样数据; 后缀 *_Org 表示原图像, 后缀 *_XSCCA 和 *_YSCCA 表示 Swarm 端仅使用自身的主向量, 而后缀 *_XYSCCA 表示 Swarm 端使用了协作双方的聚合主向量 (将两主向量拼接聚合得 2 868 个主向量).

从三个方面分析分类结果, 首先比较原数据与 SCCA 降维特征上的分类结果发现, 后 4 个分类器 (EB、RF、KNN、SVM) 上的分类差异不大, 而在前两个分类器 (NB、DA) 上, SCCA 低维特征的分类精度较原数据优势明显, 这表明基于低维特征的分类精度较原始数据上的分类精度损失较小, 在有的分类器上还能获得高于原始数据的分类精度.

其次通过比较分类器之间的分类精度得知, 不同分类器的分类结果有差异, 此结果提示选择合适的分类器对于提高 SCCA 协同降维后的低维特征应用效果是有益的.

最后观察聚合特征上的分类精度可见, 与单一特征相比, 并非聚合后的精度都得到提高, 大部分

聚合特征上的分类精度与单个 Swarm 上的分类精度几乎持平 (EB、RF、KNN), 而且还存在精度降低的情况 (Swarm 2 端的 DA 分类器下), 这说明对 SCCA 获得的协作降维特征进行聚合也许是没有必要的, 这可能与 CCA 已提取出最大相关成分有关.

实验 4. 训练时间比较

实验记录了创建 SCCA 模型的运行时间和每类特征的训练时间. 图 6 为 Swarm 1 端的平均训练时间比较, 图例符号含义与图 5 中一致.

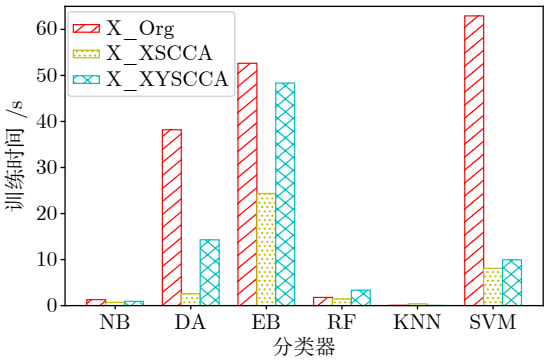


图 6 训练时间比较

Fig. 6 Comparison of training time

生成 SCCA 主向量耗时 88.135 s, 图 6 中的值未包括 SCCA 模型生成时间. 基于 SCCA 的分类任务需要训练两个模型, 其一是获得 SCCA 的主向量, 其二是训练分类器模型. 如果从总时间来看, SCCA 需要额外的低维模型生成时间, 但是 SCCA 本质上是一种协同降维工具, 本文关注的是降维后低维特征的有效性, 因此后续分析中剔除 SCCA 主向量的生成时间.

比较原始值与自身低维特征上的训练时间得知, 在 SCCA 的低维关联特征上获得的效率优势是明显的, 尤其是在 DA、EB 和 SVM 分类器上更显著, 其中 DA 上的训练时间降低了约 20 倍.

尽管 KNN 上的训练时间较少, 但是其呈现出一个奇异现象, 在原数据、自身低维特征和聚合特征上的训练时间依次为 0.071 s、0.391 s 和 0.051 s, 即在 SCCA 低维关联特征上的训练时间比在原始数据上的训练时间长. 初看这是让人诧异的结果, 但是这并不值得惊异, 相反这是 SCCA 低维关联特征在分类器的适应性上呈现出的一个特殊现象, 其原因可能是在 SCCA 低维关联特征上对应分类器收敛性降低导致的, 这暗示能否用 SCCA 的低维协作特征评估分类器的收敛性可能是一个值得探索的课题, 不过这已超出本文的研究范围.

比较不同分类器的训练时间可见, SCCA 的低维特征在不同分类器下的训练时间差异明显, 这提示 SCCA 特征应用对分类器的选择是必要的. 结合图 5 的分类精度来看, 在 WIKI 数据集的性别分类任务中, 与另外 5 个分类器相比, DA 分类器在 SCCA 低维特征上表现出既快又好的适应性.

实验 5. 不同降维方法的对比分析

实验考察了 SCCA 与主成分分析 (Principal component analysis, PCA) 和经典 CCA 两种主流降维方法应用到分类任务上的差异, 结果如图 7 所示, 其中图 7(a) 为不同降维方法对应的分类精度, 图 7(b) 为使用的低维特征数目.

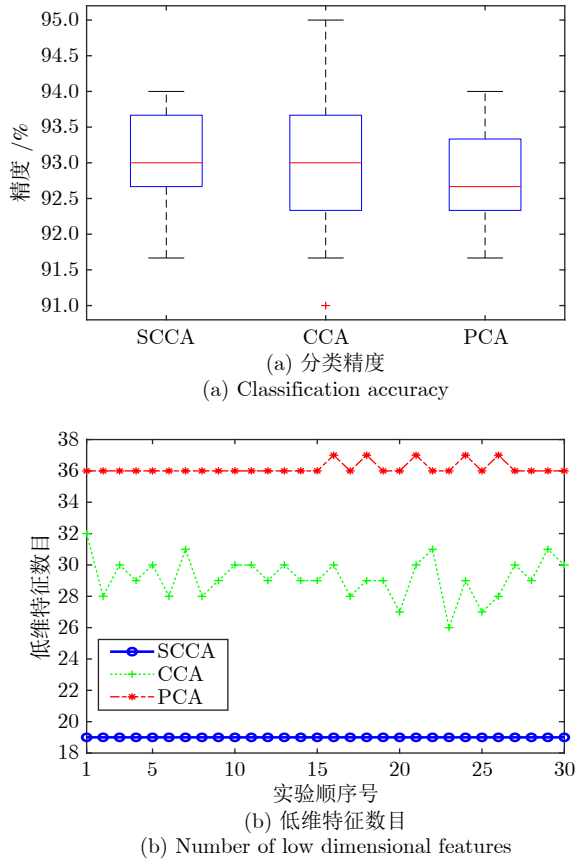


图 7 降维方法比较

Fig. 7 Comparison of dimension reduction methods

由于 CCA 和 PCA 的降维数据需存储在单端, 不适用于 Swarm 协作降维场景, 因此实验在单个 Swarm 节点上执行 CCA 和 PCA, 其中 CCA 将单个节点的数据集均分为两部分作为输入. SCCA 在两个 Swarm 节点上获得主向量, 再将主向量应用于运行 CCA 和 PCA 的节点对应的数据集上.

由于 CCA 和 PCA 在高维情况下易出现协方差矩阵非正定而导致结果异常, 实验通过金字塔下采样技术生成 16×16 的稀疏图, 获得 256 个特征.

实验载入 14300 张图, 分为两组, 一组含 13000 张图作为训练备选集, 其余图像作为测试备选集. 实验进行了 30 次, 每次从备选集中随机选取图片进行降维, 并基于低维特征进行分类. 每次训练数据为 3000 条, 测试数据为 300 条. 采用 DA 分类器.

图 7(a) 的箱盒图呈现了分类精度的分布情况, 第一, 就中位数而言, SCCA 略高于 PCA, 表明前者的平均精度优于后者; 第二, 就四分位间距而论, SCCA 的上四分位 Q3 和下四分位 Q1 的距离小于 CCA, 表明前者的分布较集中; 第三, 从最值来看, 三者的最小值接近, SCCA 的最大值小于 CCA, 表明 SCCA 的波动性较小; 第四, 考察异常值发现, SCCA 未显现出离群值, 说明 SCCA 的稳定性较好.

每次实验从 256 个图像特征中获得的低维特征数目如图 7(b) 所示. 低维特征的选择方法是, SCCA 和 CCA 选择前 15% 典型相关系数对应的主向量, 而 PCA 选择方差累积解释率大于 95% 的主成分. 图 7(b) 表明, SCCA 所使用的特征数低于 CCA 和 PCA, 结合图 7(a) 发现, SCCA 用较少数目的低维特征即可获得与比较算法接近的分类结果; 此外, SCCA 的低维特征数目稳定, CCA 和 PCA 使用的低维特征数目却存在波动, 尤其 CCA 更明显.

实验 6. 性别识别示例

随机挑选 40 张图观察分类效果, 采用 DA 分类器, SCCA 主向量和 DA 分类器模型用实验 3 中最后一次训练结果. 识别情况如图 8 所示, 图 8(a) 为原图片的灰度图, 图 8(b) 为金字塔下采样图及分类错误标记, 红色长方形标注的图表示分类错误. 有 3 张图分类错误, 正确率为 92.5 %, 与实验 3 的分类精度基本接近. 分类错误的 3 张图的共同特点是一图有多张人脸, 说明 SCCA 对复杂图像的降维能力有改进空间.

综上所述, 上述实验结果验证了本文所提方法的有效性.

5　结束语

作为去中心化的联邦技术, Swarm 学习是解决联邦计算中中心服务器不可信问题的良好框架. 本文基于 Swarm 学习思想, 针对联邦之间数据的关联性和高维性问题以及联邦数据的隐私保护需求, 提出一种支持隐私保护的 Swarm 联邦降维方法. 本文在耦合特征分离的基础上, 通过构建典型相关分析的 Swarm 联邦框架, 经由随机扰乱策略来隐藏 Swarm 特征隐私, 在 Swarm 节点本地提取低维特征, 并在真实数据集上进行仿真实验, 结果验证了所提方法的有效性, 同时尝试在图像协作分类中开展示例性应用.

(a) 原图片的灰度图
(a) The grayscale version of original images

(b) 金字塔下采样图及分类错误标记
(b) Pyramid down-sampling images and classification error marks

图 8　分类实例

Fig. 8　An instance of classification

实验结果发现的一个有趣现象是, 在主向量数目增加的过程中, 相对精度曲线呈现出钟形变化趋势, 这提示适当数目的主向量选取是必要的. 如何选取主向量是值得深入探索的科学问题, 因为 Swarm 协作效率和低维关联特征的可用性都会受其影响, 下一步将展开此内容的研究工作.

References

1　Kels C G. HIPAA in the era of data sharing. *Journal of the American Medical Association*, 2020, **323**(5): 476−477

2　Raymond N. Reboot ethical review for the age of big data. *Nature*, DOI: https://doi.org/10.1038/d41586-019-01164-z

3　Taddeo M, Floridi L. How AI can be a force for good. *Science*, 2018, **361**(6404): 751−752

4　Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 2019, **1**(9): 389−399

5　Stahl B C, Wright D. Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, 2018, **16**(3): 26−33

6　Stadler T, Troncoso C. Why the search for a privacy-preserving data sharing mechanism is failing. *Nature Computational Science*, 2022, **2**(4): 208−210

7　Wu C H, Wu F Z, Lyu L J, Huang Y F, Xie X. Communication-

efficient federated learning via knowledge distillation. *Nature Communications*, 2022, **13**(1): Article No. 2032

8 Nguyen D C, Ding M, Pathirana P N, Seneviratne A, Li J, Poor H V. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2021, **23**(3): 1622−1658

9 Liang Feng, Yang En-Yue, Pan Wei-Ke, Yang Qiang, Ming Zhong. Survey of recommender systems based on federated learning. *Scientia Sinica Informationis*, 2022, **52**(5): 713−741
(梁锋, 羊恩跃, 潘微科, 杨强, 明仲. 基于联邦学习的推荐系统综述. 中国科学: 信息科学, 2022, **52**(5): 713−741)

10 Guo Yan-Qing, Wang Xin-Lei, Fu Hai-Yan, Liu Hang, Yao Ming. Federated decision tree algorithm for privacy security. *Chinese Journal of Computers*, 2021, **44**(10): 2090−2103
(郭艳卿, 王鑫磊, 付海燕, 刘航, 姚明. 面向隐私安全的联邦决策树算法. 计算机学报, 2021, **44**(10): 2090−2103)

11 Zhang Ze-Hui, Fu Yao, Gao Tie-Gang. Research on federated deep neural network model for data privacy preserving. *Acta Automatica Sinica*, 2022, **48**(5): 1273−1284
(张泽辉, 富瑶, 高铁杠. 支持数据隐私保护的联邦深度神经网络模型研究. 自动化学报, 2022, **48**(5): 1273−1284)

12 Gao Sheng, Yuan Li-Ping, Zhu Jian-Ming, Ma Xin-Di, Zhang Rui, Ma Jian-Feng. A blockchain-based privacy-preserving asynchronous federated learning. *Scientia Sinica Informationis*, 2021, **51**(10): 1755−1774
(高胜, 袁丽萍, 朱建明, 马鑫迪, 章睿, 马建峰. 一种基于区块链的隐私保护异步联邦学习. 中国科学: 信息科学, 2021, **51**(10): 1755−1774)

13 Zhu Jian-Ming, Zhang Qin-Nan, Gao Sheng, Ding Qing-Yang, Yuan Li-Ping. Privacy preserving and trustworthy federated learning model based on blokchain. *Chinese Journal of Computers*, 2021, **44**(12): 2464−2484
(朱建明, 张沁楠, 高胜, 丁庆洋, 袁丽萍. 基于区块链的隐私保护可信联邦学习模型. 计算机学报, 2021, **44**(12): 2464−2484)

14 Feng Ji, Cai Qi-Zhi, Jiang Yuan. Towards training time attacks for federated machine learning systems. *Scientia Sinica Informationis*, 2021, **51**(6): 900−911
(冯雯, 蔡其志, 姜远. 联邦学习下对抗训练样本表示的研究. 中国科学: 信息科学, 2021, **51**(6): 900−911)

15 Zhang Ze-Hui, Li Qing-Dan, Fu Yao, He Ning-Xin, Gao Tie-Gang. Adaptive federated deep learning with Non-IID data. *Acta Automatica Sinica*, 2023, **49**(12): 2493−2506
(张泽辉, 李庆丹, 富瑶, 何宁昕, 高铁杠. 面向非独立同分布数据的自适应联邦深度学习算法. 自动化学报, 2023, **49**(12): 2493−2506)

16 Zhu Jing, Wang Fei-Yue, Wang Ge, Tian Yong-Lin, Yuan Yong, Wang Xiao, et al. Federated control: A distributed control approach towards information security and rights protection. *Acta Automatica Sinica*, 2021, **47**(8): 1912−1920
(朱静, 王飞跃, 王戈, 田永林, 袁勇, 王晓, 等. 联邦控制: 面向信息安全和权益保护的分布式控制方法. 自动化学报, 2021, **47**(8): 1912−1920)

17 Fang Chen, Guo Yuan-Bo, Wang Yi-Feng, Hu Yong-Jin, Ma Jia-Li, Zhang Han, et al. Edge computing privacy protection method based on blockchain and federated learning. *Journal on Communications*, 2021, **42**(11): 28−40
(方晨, 郭渊博, 王一丰, 胡永进, 马佳利, 张晗, 等. 基于区块链和联邦学习的边缘计算隐私保护方法. 通信学报, 2021, **42**(11): 28−40)

18 Zhang Qin-Nan, Zhu Jian-Ming, Gao Sheng, Xiong Ze-Hui, Ding Qing-Yang, Piao Gui-Rong. Incentive mechanism for federated learning based on block-chain and Bayesian game. *Scientia Sinica Informationis*, 2022, **52**(6): 971−991
(张沁楠, 朱建明, 高胜, 熊泽辉, 丁庆洋, 朴桂荣. 基于区块链和贝叶斯博弈的联邦学习激励机制. 中国科学: 信息科学, 2022, **52**(6): 971−991)

19 Warnat-Herresthal S, Schultze H, Shastry K L, Manamohan S, Mukherjee S, Garg V, et al. Swarm learning for decentralized and confidential clinical machine learning. *Nature*, 2021, **594**(7862): 265−270

20 Sun C, Wu S T, Cui T. User selection for federated learning in a wireless environment: A process to minimize the negative effect of training data correlation and improve performance. *IEEE Vehicular Technology Magazine*, 2022, **17**(3): 26−33

21 Uddin M P, Xiang Y, Lu X Q, Yearwood J, Gao L X. Mutual information driven federated learning. *IEEE Transactions on Parallel and Distributed Systems*, 2021, **32**(7): 1526−1538

22 Gao Y, Zhang G M, Zhang C C, Wang J K, Yang L T, Zhao Y L. Federated tensor decomposition-based feature extraction approach for industrial IoT. *IEEE Transactions on Industrial Informatics*, 2021, **17**(12): 8541−8549

23 Hotelling H. The most predictable criterion. *Journal of Educational Psychology*, 1935, **26**(2): 139−142

24 Yang X H, Liu W F, Liu W, Tao D C. A survey on canonical correlation analysis. *IEEE Transactions on Knowledge and Data Engineering*, 2021, **33**(6): 2349−2368

25 Ewerbring L M, Luk F T. Canonical correlations and generalized SVD: Applications and new algorithms. *Journal of Computational and Applied Mathematics*, 1989, **27**(1−2): 37−52

26 Uurtio V, Monteiro J M, Kandola J, Shawe-Taylor J, Fernandez-Reyes D, Rousu J. A tutorial on canonical correlation methods. *ACM Computing Surveys*, 2018, **50**(6): Article No. 95

27 Drmač Z. Accurate computation of the product-induced singular value decomposition with application. *Siam Journal on Numerical Analysis*, 1998, **35**(5): 1969−1994

28 Reyes-Ortiz J L, Oneto L, Sama A, Parra X, Anguita D. Transition-aware human activity recognition using smartphones. *Neurocomputing*, 2016, **171**: 754−767

29 Rothe R, Timofte R, Gool L V. Deep expectation of real and apparent age from a single image without facial landmarks. *International Journal of Computer Vision*, 2018, **126**(2): 144−157

李文平 嘉兴学院信息科学与工程学院副教授. 主要研究方向为隐私保护技术. 本文通信作者.
E-mail: liwenping@hrbeu.edu.cn
(**LI Wen-Ping** Associate professor at the College of Information Science and Engineering, Jiaxing University. His main research interest is privacy protection. Corresponding author of this paper.)

杜 选 嘉兴学院信息科学与工程学院副教授. 主要研究方向为隐私保护技术. E-mail: duxuan@zjxu.edu.cn
(**DU Xuan** Associate professor at the College of Information Science and Engineering, Jiaxing University. His main research interest is privacy protection.)