

联邦可视化：一种隐私保护的可视化新模型

魏雅婷, 王智勇, 周舒悦, 陈为

(浙江大学计算机辅助设计与图形学国家重点实验室, 浙江 杭州 310058)

摘要: 概述了联邦可视化的概念、框架、方法与应用。联邦可视化框架能够在不进行数据整合的情况下, 针对具体任务和特定场景进行加密训练, 得出反映全体数据特征的可视化模型。联邦可视化是联邦学习框架在可视化领域的拓展应用, 主要强调在保障数据隐私的前提下, 互利共赢的联邦协作方式在对多数据源数据进行可视分析方面的应用, 以打破各领域、各行业的数据壁垒, 实现数据与知识的共享。

关键词: 联邦学习; 数据隐私; 视觉特征; 数据可视化; 人工智能

中图分类号: TP183

文献标识码: A

doi: 10.11959/j.issn.2096-6652.201946

Federated visualization: a new model for privacy-preserving visualization

WEI Yating, WANG Zhiyong, ZHOU Shuyue, CHEN Wei

State Key Lab of CAD&CG, Zhejiang University, Hangzhou 310058, China

Abstract: The concept, architecture, methods and applications of federated visualization were introduced. The federated visualization framework is capable of encrypting and training a visual model that reflect the characteristics of the entire data for specific tasks and scenarios. The federated visualization framework is an extension and application of federated learning, which emphasized using mutual benefit and win-win federal cooperation to visually analyze multi-source data under the premise of ensuring data privacy, towards breaking down data barriers in various fields and industries and realizing the sharing of data and knowledge.

Key words: federated learning, data privacy, visual feature, data visualization, artificial intelligence

1 引言

近年来, 在大多数行业中, 行业之间的竞争、行政手续、数据隐私安全等问题, 使得数据是以孤岛的形式存在的, 甚至有时同一个公司的不同部门之间也无法实现数据互通。这一困境严重阻碍了各类数据科学技术的落地。

数据的全面与否将直接影响数据可视化分析结果的准确性。使用片面的数据进行可视分析往往会使结果和真实情况大相径庭。尤其是当前数据可视化在安防、交通、金融等领域扮演着十

分重要的角色, 分析结果的偏差可能会带来严重损失。

与此同时, 通过数据整合的方式来解决数据孤岛问题逐渐变得不可行。一方面, 随着大数据的进一步发展, 人们越来越重视数据隐私和数据安全, 保障用户数据隐私是企业获得用户信任的前提。用户数据的每一次泄露都会引起媒体和公众的极大关注, 如 Facebook 的数据泄露事件引发了大范围的抗议行动。另一方面, 各国也在通过法律手段加强对数据隐私和数据安全的保护。2018年5月25日欧盟开始实施《通用数据保护条例》(general data

收稿日期: 2019-10-18; 修回日期: 2019-11-21

通信作者: 陈为, chenvi@zju.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61772456)

Foundation Item: The National Natural Science Foundation of China (No.61772456)

protection regulation, GDPR)》, GDPR 旨在保护用户的个人隐私和数据安全,它要求经营者必须使用清晰、明确的语言来表述自己的用户协议,同时用户拥有抹除数据的权利,即用户可以要求企业删除其个人数据并停止利用其个人数据进行建模,违背该条例的企业将面临巨额罚款。同样,我国在 2017 年起实施的《中华人民共和国网络安全法》和《中华人民共和国民法总则》也指出,网络运营者不得泄露、篡改、毁坏其收集的个人信息,并且与第三方进行数据交易时需确保拟定的合同明确约定拟交易数据的范围和数据保护义务。

在机器学习领域,学者面临着相似的困境。表现良好的模型背后往往需要数量大、维度高的优质数据,而在实际产业界中,除了有限的几个行业,很多领域存在着数据有限且质量较差的问题,其拥有的数据不足以支撑人工智能技术的实现。因此,联邦学习应运而生,它能够在保障数据安全的前提下,打破数据孤岛。

受到联邦学习的启发,本文提出一个框架,能够在保障数据隐私的前提下,对分布在不同机构的数据进行可视化,即联邦可视化。在传统的数据可视化流程中,视觉编码决定需要的特征数据,并从数据库中读取这些数据。而在联邦可视化中,可视化的特征数据将不再通过查询数据库直接获取,而是通过由各方机构共同完善的模型计算得到。

2 相关工作

2.1 隐私保护

在隐私保护的数据挖掘领域,句法匿名模型和差异隐私模型是 2 种常用的隐私模型,它们从不同的角度解决隐私问题。 k -匿名模型^[1]是语法匿名模型的代表之一,其目标是通过链接公共数据库和私有数据库中共存的准标识符防止重新标识,使 k 条记录彼此相同,防止身份泄露(因为攻击者无法识别特定的个人),但是, k -匿名模型在防止属性泄露方面有其缺点:如果具有相同准标识符的个人也具有相似甚至相同的敏感属性值,则某些敏感信息仍然可能泄露。随后,研究人员提出了 l -多样性模型^[2]和 t -紧密度模型^[3]来分析隐私保护泄露数据挖掘中的属性公开风险。差异隐私模型主要用于匿名化查询响应^[4],是通过

将从确定的分布中选择的随机噪声添加到真实查询结果中的方式实现的。

在隐私保护数据可视化领域,研究人员已经对数据挖掘社区的模型进行了修改和扩展,以在匿名可视化表示中的隐私与实用性之间取得平衡。参考文献[5]讨论了当使用平行坐标表示多维数据时,应用语法匿名化方法(即 k -匿名性和 l -多样性)的策略。参考文献[6]将重点放在事件序列数据上,为数据所有者提供视觉界面,检查潜在的隐私问题并根据算法建议和自己的判断微调结果。参考文献[7-8]着眼于多属性表格数据匿名化和图数据隐私保护,设计一种可以辅助用户定制既能保护隐私,又能降低实用性损失的隐私保护方案,但是需要用户进行一些复杂的交互。参考文献[9]利用屏幕空间的不确定性来防御攻击。参考文献[10-11]在系统后端已经拿到各方数据的基础上,通过向可视化图表中加入不确定性来保护隐私。

本文从数据层面出发,提出不同于传统可视化的新框架,使攻击者完全触碰不到原始数据,而且数据持有者不需要进行复杂的交互即可定制隐私保护方案。

2.2 AI 与可视化

将可视化与传统机器学习技术结合以构建人在回路(human in the loop)分析流水线,一直是视觉分析的核心目标^[12]。AI 模型的“黑匣子”特性推动了用于揭示 AI 模型内部运行机制的可视化技术的出现,即 AI 可解释性可视化^[13]。参考文献[14-15]全面介绍了当前的研究。研究人员提出了许多可视化技术从不同方面解释各种类型的 AI 模型,如 Tree Boosting 方法^[16]、卷积神经网络(CNN)^[17-18]、循环神经网络(RNN)^[19]、生成对抗网络(GAN)^[20]、深度强化学习网络(DQN)^[21]以及深度生成模型^[22]。这些工作本质上是利用可视化技术解释、优化 AI 模型,即用可视化技术解决 AI 中的问题(VIS for AI)。与之相反,本文提出的联邦可视化框架是利用 AI 模型(联邦学习模型)解决可视化中存在的隐私保护问题,即用 AI 技术解决可视化中的问题(AI for VIS)。

AI for VIS 这个概念目前被很多领域专家认可,是可视化领域一个非常有发展前景的方向。近几年,在可视探索^[23-24]、图绘制^[25-27]、可视化图表推荐与自动生成^[28-30]等领域出现许多优秀

的研究工作，它们使用 AI 模型解决可视化中存在的各种问题。

2.3 联邦学习

联邦学习的概念最早于 2016 年由 Google 公司提出^[31]，用于解决 Android 手机终端用户在本地更新模型方面的问题。最近，研究人员研究了联邦优化^[32]、隐私增强^[33-34] 以及各种实际应用场景^[35-36]，当多个数据拥有方（如企业） $F_i (i=1, \dots, N)$ 想要联合其他数据拥有方的数据 D_i 训练机器学习模型时，传统做法是把数据整合到其中一方，利用数据 $D=\{D_i, i=1, \dots, N\}$ 进行训练，并得到模型 M_{sum} 。但是，这种做法在没有得到用户同意的情况下是违反隐私和数据安全的相关法律的，通常难以实施。因此联邦学习应运而生，在联邦学习中，数据拥有方 F_i 可以在不给出己方数据 D_i 的情况下进行模型训练，得到模型 M_{fed} ，并能够保证模型 M_{fed} 的效果 (V_{fed}) 与模型 M_{sum} 的效果 (V_{sum}) 的差距足够小，即 $|V_{\text{fed}} - V_{\text{sum}}| < \delta$ ，其中 δ 是任意小的一个正值。

杨强^[37]教授根据参与训练的数据分布情况将联邦学习分为 3 类：横向联邦学习（horizontal federated learning）、纵向联邦学习（vertical federated learning）和联邦迁移学习（federated transfer learning, FTL），如图 1（a）所示。联邦学习框架如图 1（b）所示，各客户端在不上传本地数据的前提下，训练本地模型，并将梯度值上传到服务端；服务端将所有梯度值平均分发到各客户端；客户端更新本地模型，这个迭代过程持续到模型收敛或人为结束训练。

3 联邦可视化框架

本文借鉴联邦学习框架提出适用于可视化领域的联邦可视化框架，解决可视化分析中的数据孤岛问题。联邦可视化框架的核心思想是得到一个反映全体数据特征的可视化模型，在各个数据拥有方的数据不离开本地的情况下进行加密训练。

3.1 可视化模型

可视化映射是信息可视化的核心步骤，指将数据信息映射成可视化元素，映射结果通常表达直观，易于理解和记忆。可视化元素由 3 方面组成：可视化空间、标记和视觉通道。数据由属性和值构成，属性与标记对应，值与视觉通道对应。其中，标记是数据属性到可视化元素的映射，用以直观地

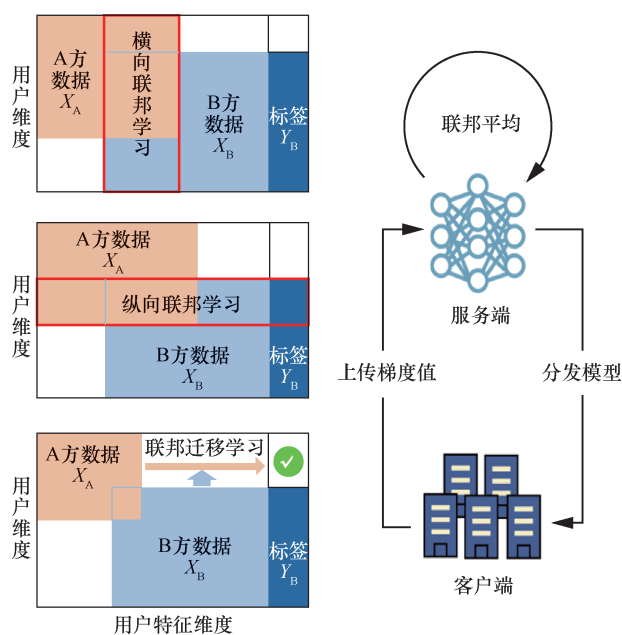


图1 联邦学习

表示数据的属性归类，如点、线、面、体等；视觉通道是数据属性的值到标记的视觉呈现参数的映射，用于控制标记的视觉特征，通常可用的视觉通道包括标记的位置、大小、形状、方向、色调等，标记和视觉通道的结合可以完整地将数据信息进行可视化表达。

假设 V 是一个可视化图表，一般地，可以将其分解成多个视觉特征集，表示为 $V=\{VF_1, VF_2, \dots, VF_n\}$ ，其中， $VF_i=\{vf_{i1}, vf_{i2}, \dots, vf_{in}\}$ 是一个视觉特征集，由多个视觉特征组成。例如，直方图只有一组视觉特征，每个视觉特征的作用是编码柱子的高度（如图 2（a）所示）；热力图也只有一组视觉特征，每个视觉特征的作用是编码每个小方格的颜色（如图 2（b）所示）。

3.2 框架架构

本文以包含 3 个数据拥有方（即企业 A、B、C），且每个数据拥有方有相同的用户特征和不同的用户（即横向联邦学习）的场景为例，介绍联邦可视化的框架（对该框架的细节设置进行调整，即可扩展至更加复杂的数据分布情况）。这些企业仅使用各自拥有的数据进行数据分析。假设这 3 家企业想联合起来看整体数据的数据分布特点，出于数据隐私保护和安全考虑，3 家企业无法直接进行数据整合，但是可以使用联邦可视化框架建立可视化模型，使各个企业看到近似的数据全貌。联邦可视化的框架与运行机制如图 3 所示。

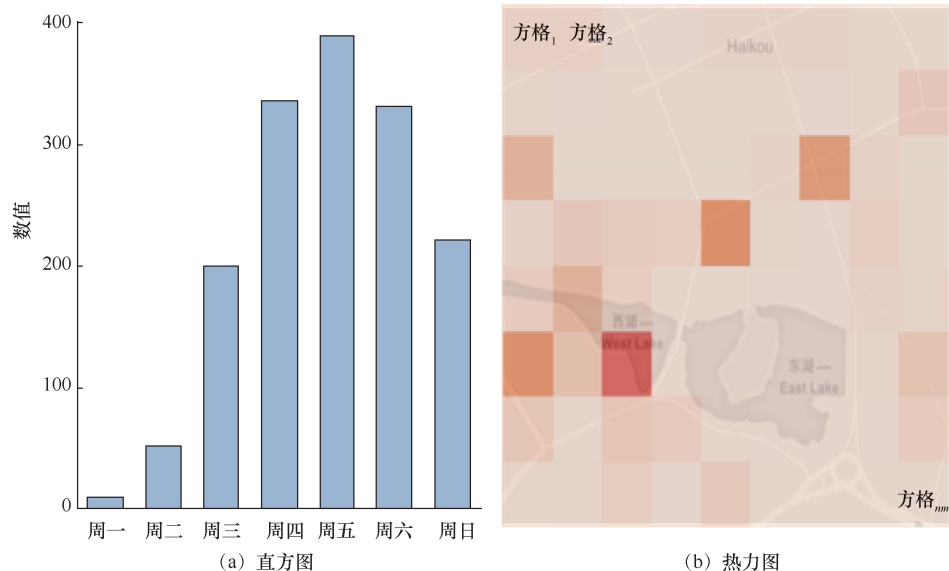


图2 视觉特征集示例

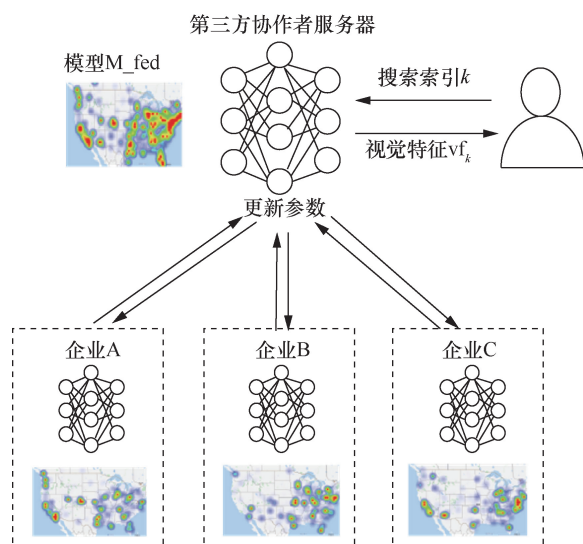


图3 联邦可视化的框架与运行机制

为保证训练过程中数据的保密性，需要借助第三方协作服务器（Server）进行加密训练。以热力图为例，训练过程可分为以下4步。

- 数据预处理。各个企业将本地的地理数据根据经纬度统一用 $n \times m$ 的网格进行划分，并对每个网格中的数据点进行计数。

- 初始模型分发。基于联邦学习，Server端初始化一个模型 M_fed ，将参数发送至各个企业。如在热力图的实例中，模型 M_fed 的输入为一组经纬度对应的网格索引，输出为该网格中的数据点统计量。

- 加密模型训练。各个企业获取 Server 端发

来的参数，根据本地数据计算梯度值，并加密发送给 Server 端。Server 端对各个企业发来的梯度值进行加权平均，更新参数后再次发送给各个企业。

- 可视图表绘制。经过多次迭代，模型逐渐精确。在各个企业本地，对于 $n \times m$ 的地理网格，将每个网格的搜索索引 k 作为模型 M_fed 的输入，可以得到对应网格的数据点统计量，即 vf_k ，最终以热力图的形式将 $n \times m$ 的网格数据可视化地表示出来。

在训练过程中，各个企业没有进行本地数据传输，数据隐私得到了保障，同时也使得各个企业可以看到数据全貌，有利于企业间的合作，并且可以辅助企业做出更加有效的决策。

4 实验

基于上述联邦可视化框架架构，本文使用数百万条海口出租车订单数据（包括经纬度信息）做了一个简单的实验，来验证框架的有效性。

4.1 数据预处理

为了模拟多家企业，本文将一份数据集随机分为3份非独立同分布的数据集，对数据进行以下处理。

- 将海口划分为 360×180 的网格，用 (x, y) $\{x \in [1, 360], y \in [1, 180]\}$ 表示。
- 对每个网格里的数据进行计数，获得数据 $(x, y, \text{count}) \{x \in [1, 360], y \in [1, 180]\}$ 。

4.2 技术实施

针对上述3份数据,借助联邦平均算法对3个客户端进行加密训练,并拟合整合后的数据,以此保证各方的数据隐私。

在联邦平均算法的配置方面,使用Python的SocketIO开源数据库进行服务器与客户端之间的通信。所有客户端均参与每轮训练,每个客户端训练一轮。

在神经网络设置方面,输入为经纬度索引 (x, y) ,输出为对应网格的计数结果。使用5层宽度为96的全连接层,每层均使用线性整流函数(rectified linear unit, ReLU)作为激活函数,优化器采用Adadelta算法,批尺寸设为32。

4.3 实验结果

随着迭代次数的增加,模型输出结果的相对误差的变化情况如图4所示,在训练前期,相对误差降低得较快,在达到一定训练次数后,相对误差的变化速度变慢,需要增加多次迭代才能获得更准确的结果。经过20 000次迭代后,相对误差降到了4.9%,所获得的热力图已经接近将3份数据直接整合的效果。进一步优化训练方法,结果会更加逼近数据直接整合的结果。

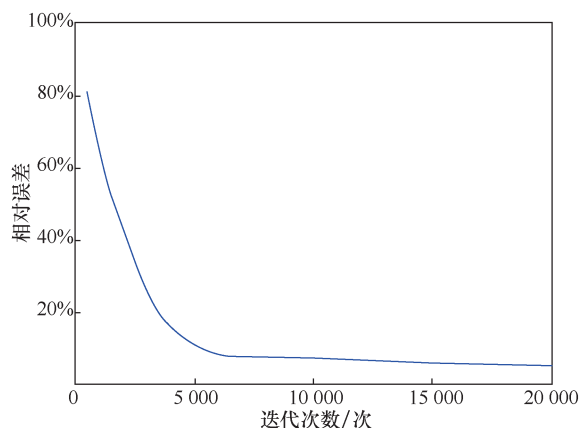


图4 相对误差随迭代次数的变化曲线(平滑后)

与现有的可视化领域隐私保护方法^[1-3, 10-11]相比,本文的方法不需要提前整合多个客户端的原始数据,各个客户端的数据不会离开本地,这从根本上保护了数据隐私,并且可以通过控制迭代的次数得到不同精确度的聚合结果。

5 结束语

数据的孤岛分布以及相关部门对数据隐私监管力度的加强是研究领域面临的主要问题。联邦学

习的出现为人工智能领域打破数据屏障及人工智能领域的进一步发展提供了新的思路。本文基于联邦学习的思想,提出了联邦可视化框架,用于解决可视化领域的数据孤岛问题。联邦可视化框架的核心思想是将可视化当作模型,在保证数据不离开数据拥有方本地的前提下,加密训练出反映全体数据特征的可视化模型。本文使用简单的实验验证了联邦可视化框架的有效性,即能够帮助多个数据拥有方打破数据壁垒,进行协作分析。

联邦可视化的研究仍处于发展阶段。在隐私性方面,本文提出的联邦可视化方法能够有效避免隐私数据的泄露;在准确性方面,当需要拟合的特征数据小于10 000时,准确率能在数千次迭代后过拟合,而更多的特征数据则需要更多的迭代次数;在通用性方面,本文的方法只考虑了表格型数据,可以绘制常见的可视化图表,比如柱状图、饼图、热力图等。联邦可视化是联邦学习在可视化领域的应用,具有重要的、前瞻性的实际意义,是打破数据壁垒的有效途径,具有巨大的应用前景,同时,更加复杂的应用场景也值得学者们进一步研究。

参考文献:

- [1] SWEENEY L. K-anonymity: a model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557-570.
- [2] MACHANAVAJJHALA A, GEHRHE J, KIFER D, et al. L-diversity: privacy beyond k-anonymity[J]. ACM Transactions on Knowledge Discovery from Data, 2006, 1(1):3.
- [3] LI N H, LI T C, VENKATASUBRAMANIAN S. T-closeness: privacy beyond k-anonymity and l-diversity[C]// 2007 IEEE 23rd International Conference on Data Engineering, April 15-20, 2007, Istanbul, Turkey. Piscataway: IEEE Press, 2007: 106-115.
- [4] COMAS J S, FERRERT J D. Differential privacy via t-closeness in data publishing[C]// 2013 Eleventh Annual Conference on Privacy, Security and Trust, July 10-12, 2013, Tarragona, Spain. Piscataway: IEEE Press, 2013: 27-35.
- [5] DASGUPTA A, KOSARA R. Adaptive privacy-preserving visualization using parallel coordinates[J]. IEEE Transactions on Visualization and Computer Graphics, 2011, 17(12): 2241-2248.
- [6] CHOU J K, WANG Y, MA K L. Privacy preserving visualization: a study on event sequence data[J]. Computer Graphics Forum, 2018.
- [7] WANG X M, CHEN W, CHOU J K, et al. GraphProtector: a visual interface for employing and assessing multiple privacy preserving graph algorithms[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 25(1): 193-203.
- [8] WANG X M, CHOU J K, CHEN W, et al. A utility-aware visual approach for anonymizing multi-attribute tabular data[J]. IEEE Transactions on Visualization and Computer Graphics, 2017, 24(1): 351-360.
- [9] DASGUPTA A, KOSARA R, CHEN M. Guess me if you can: a visual uncertainty model for transparent evaluation of disclosure risks in privacy-preserving data visualization[C]// The 16th IEEE Symposium on Visualization for Cyber Security, October 23, 2019, Vancouver, Canada. Piscataway: IEEE Press, 2019.
- [10] OKSANEN J, BERGMAN C, SAINIO J, et al. Methods for deriving and calibrating privacy-preserving heat maps from mobile sports

- tracking application data[J]. Journal of Transport Geography, 2015, 48: 135-144.
- [11] DASGUPTA A, KOSARA R. Adaptive privacy-preserving visualization using parallel coordinates[J]. IEEE Transactions on Visualization and Computer Graphics, 2011, 17(12): 2241-2248.
- [12] AMERSHI S, CAKMAK M, KNOX W B, et al. Power to the people: the role of humans in interactive machine learning[J]. AI Magazine, 2014, 35(4): 105-120.
- [13] TZENG F Y, MA K L. Opening the black box-data driven visualization of neural networks[C]// IEEE Visualization, October 23-28, 2005, Minneapolis, USA. Piscataway: IEEE Press, 2005: 383-390.
- [14] JAEGUL C, LIU S X. Visual analytics for explainable deep learning[J]. IEEE Computer Graphics and Applications, 2018, 38(4): 84-92.
- [15] HOHMAN F M, KAHNG M, PIENTA R, et al. Visual analytics in deep learning: an interrogative survey for the next frontiers[J]. IEEE Transactions on Visualization and Computer Graphics, 2018.
- [16] LIU S X, XIAO J N, LIU J L, et al. Visual diagnosis of tree boosting methods[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 24(1): 163-173.
- [17] ALSALLAKH B, LOURABLOO A, YE M, et al. Do convolutional neural networks learn class hierarchy[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 24(1): 152-162.
- [18] LIU M C, SHI J X, LI Z, et al. Towards better analysis of deep convolutional neural networks[J]. IEEE Transactions on Visualization and Computer Graphics, 2016, 23(1): 91-100.
- [19] MING Y, CAO S Z, ZHANG R X, et al. Understanding hidden memories of recurrent neural networks[C]// 2017 IEEE Conference on Visual Analytics Science and Technology, October 1, Phoenix, USA. Piscataway: IEEE Press, 2017: 13-24.
- [20] KAHNG M, THORAT N, CHAU DHP, et al. Gan lab: understanding complex deep generative models using interactive visual experimentation[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 25(1): 1-11.
- [21] WANG J, GOU L, SHEN H W, et al. Dqnviz: A visual analytics approach to understand deep q-networks[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 25(1): 288-298.
- [22] LIU M C, SHI J X, CAO K, et al. Analyzing the training processes of deep generative models[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 24(1): 77-87.
- [23] HUANG Z S, ZHAO Y, CHEN W, et al. A natural-language-based visual query approach of uncertain human trajectories[J]. IEEE Transactions on Visualization and Computer Graphics, 2020, 26(1): 1256-1266.
- [24] YU B W, SILVA C T. FlowSense: a natural language interface for visual data exploration within a dataflow system[J]. IEEE Transactions on Visualization and Computer Graphics, 2019.
- [25] ZHENG J X S, PAWAR S, MATTHEW G D F. Graph drawing by stochastic gradient descent[J]. IEEE Transactions on Visualization and Computer Graphics, 2018: 1-1.
- [26] WANG Y, JIN Z H, WANG Q W, et al. DeepDrawing: a deep learning approach to graph drawing[J]. IEEE Transactions on Visualization and Computer Graphics, 2019, 26(1): 676-686.
- [27] KWON O H, MA K L. A deep generative model for graph layout[J]. arXiv preprint, 2019, arXiv:1904.12225.
- [28] CHEN Z T, WANG Y, WANG Q, et al. Towards automated infographic design: deep learning-based auto-extraction of extensible timeline[J]. IEEE Transactions on Visualization and Computer Graphics, 2019, 26(1): 917-926.
- [29] CUI W, ZHANG X, WANG Y, et al. Text-to-viz: automatic generation of infographics from proportion-related natural language statements[J]. IEEE Transactions on Visualization and Computer Graphics, 2019, 26(1): 906-916.
- [30] WANG Y, SUN Z, ZHANG H, et al. DataShot: automatic generation of fact sheets from tabular data[J]. IEEE Transactions on Visualization and Computer Graphics, 2019, 26(1): 895-905.
- [31] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. International Conference on Artificial Intelligence, 2017, 20(22): 1273-1282.
- [32] KONECHY J, MCMAHAN H B, RAMAGE D, et al. Federated optimization: distributed machine learning for on-device intelligence[J]. arXiv preprint, 2016, arXiv:1610.02527.
- [33] MCMAHAN H B, RAMAGE D, TALWAR K, et al. Learning differentially private recurrent language models[J]. arXiv preprint, 2017, arXiv:1710.06963.
- [34] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: a client level perspective[J]. arXiv preprint, 2017, arXiv:1712.07557.
- [35] HUANG L, LIU D B. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records[J]. Journal of Biomedical Informatics, 2019, 99: 103291.
- [36] HUANG L, YIN Y F, FU Z, et al. LoAdaBoost: loss-based AdaBoost federated machine learning on medical data[J]. arXiv preprint, 2018, arXiv:1811.12629.
- [37] 杨强. GDPR 对 AI 的挑战和基于联邦迁移学习的对策[J]. 中国人工智能学会通讯, 2018, 8:1-8.
- YANG Q. The challenge of GDPR to AI and the countermeasures based on federal immigration learning[J]. China Artificial Intelligence Society Newsletter, 2018, 8:1-8.

[作者简介]



魏雅婷（1994—），女，浙江大学计算机辅助设计与图形学国家重点实验室博士生，主要研究方向为可视分析、可视设计、感知、认知。



王智勇（1996—），男，浙江大学计算机辅助设计与图形学国家重点实验室硕士生，主要研究方向为可视分析、机器学习。



周舒悦（1996—），女，浙江大学计算机辅助设计与图形学国家重点实验室硕士生，主要研究方向为可视化、可视分析、感知认知。



陈为（1976—），男，博士，浙江大学计算机辅助设计与图形学国家重点实验室教授，博士生导师，CCF 高级会员，主要研究方向为可视化、可视分析、大数据分析、人机混合智能。