虚拟现实中空间可导航性差异带来的隐私问题

预印本，编译于2023年2月7日

Aryabrata Basu [1], **Mohammad Jahed Murad Sunny** [1], **及 Jayasri Sai Nikitha Guthula** [1]

[1]阿肯色大学小石城分校计算机科学系

arXiv:2302.02525v1 [cs.HC] 6 Feb 2023

摘要

当前的虚拟现实（VR）输入设备使用户能够在虚拟环境中移动，并记录有关用户动作和特定行为习惯的沉浸式个性化数据，这使用户隐私问题成为关注焦点。在本文中，作者提出研究由机器学习驱动、旨在与人类用户协同学习的算法。这些算法可用于应对虚拟现实中现有的隐私问题，也可以扩展到增强现实（AR）平台。

1 引言

空间导航是一种具身体验。在虚拟现实环境中进行空间导航，需要借助听觉、视觉和/或触觉感知来探索虚拟空间，同时完成相关任务。虚拟现实设备拓展了该环境中的交互维度。最新的动作捕捉设备，例如索尼的 Mocopi [1], , 能够通过人体四肢在现实世界中的动作，在虚拟现实环境中捕捉并驱动三维虚拟形象，同时实时跟踪和转换这些动作，且所需的设备布置极为简单。当前虚拟现实输入设备跟踪技术的影响巨大，并能降低长期使用虚拟现实的门槛。与此同时，人们也担忧这些追踪数据集存在以不同方式推断信息的风险，可能侵犯用户隐私，造成身体伤害 [2][3]；还可能导致身体伤害 [4], , 以及操纵和破坏沉浸式体验[5] [6]。

如果虚拟现实系统存在安全漏洞，就可能利用虚拟现实可用性数据为用户制造恶意软件，使他们面临严重风险 [7]。随着技术领域以极快的速度发展，对虚拟现实技术中的数据流施加控制已变得至关重要。Meta旗下一个名为 Horizon Worlds 的知名平台，在用户参与各种有趣的虚拟现实活动时，会积极记录用户行为数据，包括音频日志，并将其纳入数据保留政策。然而，利用社交媒体网站上的信息来揭露用户的私生活，这种行为被称为“人肉搜索”。人们可能会利用元宇宙获取有关某人的更多隐私信息，例如其习惯和身体特征 [8]。本文的 [3] 和 [4] 章节将通过示例说明为何应提高对虚拟现实安全性的重视。

2 背景

获取有关用户的个性化信息，可能会被用来影响他们与任何信息资源的互动方式。通常，保存的用户信息称为用户模型或档案。用户建模是人工智能研究中一个成熟的领域。许多自适应或个性化系统都内置了用户模型，并以此为基础提供定制化推荐等特征。这种策略存在若干局限，其中一点是应用开发者必须自行创建并维护用户模型。由于这些局限，堡垒之夜 [9], 这款热门电子游戏利用了隐私漏洞，利用数字行为模式收集13岁以下儿童的信息，且未征得其父母的同意。其母公司 Epic Games 因侵犯隐私而与美国联邦贸易委员会达成和解[10]。

根据Kanoje等人的说法，用户画像是指查找有关用户兴趣领域的信息。系统可以利用这些数据进一步了解用户，并运用这些认知改进信息检索，从而令用户满意[11]。Farid等人 [12], 在另一篇关于用户画像的文章中指出，用户建模过程采用了两种方式：为新用户创建初始用户档案，以及持续更新档案信息，以适应用户兴趣、偏好和需求的不断变化。创建用户档案是用户画像中的一大难题，因为要准确呈现用户偏好并不容易。然而，尽管这会侵犯隐私，这类数据仍在被研究。因此，为了进一步了解用户画像，我们考虑了一个测试案例，以识别其中一些可能具有剥削性质的隐藏维度。

特征	定义
行进距离	它是……的总长度 所经过的路径 两个位置之间。
覆盖范围	单位立方体的总数 覆盖范围（面积）。
到达的决策点数量	决策点总数 覆盖的 迷宫中的 .
位置曲率	曲率的有符号 角度 之间 two 连续的 位置向量。
头部旋转量	无符号头部旋- 转角度之间 两个连续的旋转 变换 .

表1：从用户深度探索的轨迹数据中提取的特征及其对应定义。

Preprint doi

*通讯：abasu@ualr.edu

3 测试案例场景：单层迷宫

设计了一个简单的（单层）三维迷宫，用于观察受试者的导航能力，同时收集了一组实证数据，例如轨迹数据、头部旋转和身体旋转 [图1]。迷宫体验以 2×2研究设计的形式部署。因子 2×2 设计是一种实验设计，使研究人员能够了解两个自变量（各有两个水平）对单个因变量产生的效应。

4 测量指标

为全面分析轨迹数据，我们定义了一组适用于每条轨迹的数学推导特征。这些特征包括行进距离、在迷宫内到达的决策点（节点）数量、头部旋转量、位置曲率以及迷宫覆盖范围。表 1 展示了其中一些轨迹特征。位置曲率特征指的是逐帧计算的连续位置向量之间轨迹的曲率。旋转量特征指的是逐帧计算的、连续头部旋转变换之间的无符号夹角，这些旋转变换以四元数形式存储。覆盖范围特征则是指用户逐帧覆盖的单位立方体数量（面积）。我们结合使用 R 和 SPSS 对轨迹数据进行了分析。

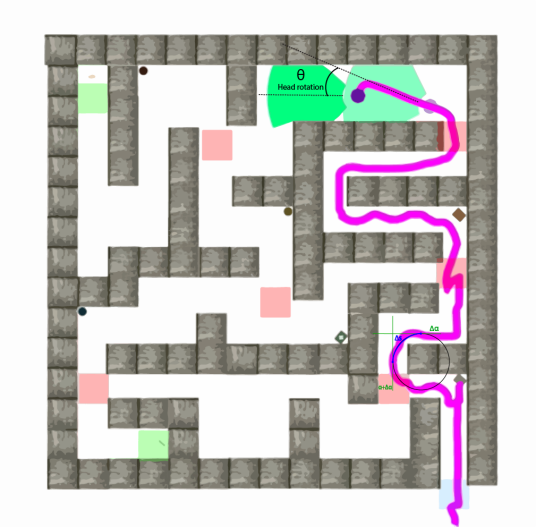

图 1：单层迷宫研究——两个轨迹特征的可视化：位置曲率和头部旋转量。

5 机器学习隐私方法——LSTM框架

深度学习是一种利用数据进行操作的动态工具。使用循环神经网络（RNN）构建深度学习（DL）模型，是处理序列数据的理想选择之一。在迷宫求解游戏范式中，人们通常会利用以往的记忆，迅速做出空间决策。无论是电子游戏玩家还是非电子游戏玩家，通常都会利用已有的信息来解开虚拟迷宫。比如，如果有人走进死胡同，他们可能会试着回忆自己在迷宫中走过的路线，回到一个可以选择另一条路并避开死胡同的位置。这种策略的关键在于记住不同时期的不同状态。长短时记忆（LSTM）模仿了类似的推理框架。LSTM 是一种特殊类型的循环神经网络，传统上包含循环结构，将前一时间步的网络激活作为输入馈送给网络，从而影响当前时间步的预测[13]。长短期记忆网络的输出取决于数据类型。根据问题的不同，每个时间步的输出表现也会有所不同。在机器人学中，长短期记忆网络已被用于处理复杂数据，并成功验证了可变运动模式，这与人体运动类似。预测人类动作或具有高度自由度的人体运动时面临的挑战，包括从实时序列中估算时产生的不准确和缺陷[14]。长短期记忆网络具备理解序列数据上下文的关键能力。无论数据规模如何，它都能通过复制网络层，学习更新和估算代表内部状态的相对权重，从而评估预测结果[15]。由于循环连接会使输入的影响呈指数级变化，传统循环神经网络的上下文信息有限，这种现象被称为梯度消失问题。在这方面，长短期记忆型循环神经网络也不例外，但由包含多个内部单元的子网络构成的自连接层有助于解决这一问题。乘法门使信息能够更轻松地长期存储和读取。这类网络有助于创建算法，在处理序列数据时，将信息判定为即时记忆的一部分，并决定是将其移除还是继续保留[16]。

长短期记忆网络可以通过控制这些门（即输入门、遗忘门和输出门），从一段时间内的数据中学习（很像人脑）。这些门的作用相当于对记忆单元进行写入、读取和重置。在长短期记忆网络中，记忆单元彼此相连，因此一个状态的输出可以作为下一个单元的输入。长短期记忆网络的示意架构见图2。这个简化的示意图展示了长短期记忆网络的第t个单元，它接收前一个单元的细胞状态C_{t-1}，表示截至前一个$(t-1)$步所掌握的信息。每个长短期记忆单元接收输入x_t，作为序列中的第t个样本，同时接收前一状态的输出h_{t-1}，并处理得到输出值h_t以及更新后的细胞状态C_t。该长短期记忆网络的门在计算过程中能够建立相关性，并帮助信息在后续单元中被“遗忘”或“传递” [15]。

输入门i_t和输出门o_t分别控制输入和输出信息：

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i); [input\ gate]$$
$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o); [output\ gate]$$

W 和 b 表示参数的权重和偏置，它们用于控制信息流。

新的t时刻的值将通过以下公式更新：

$$C_t = f_t * C_{t_1} + i_t * C_{t_*}$$

C_{t_*} = 当前步骤的计算状态 x_t 以及先前的输出 h_{t-1}

$$C_{t_*} = tanh(W_C.[h_{t_1}, x_t] + b_C)$$

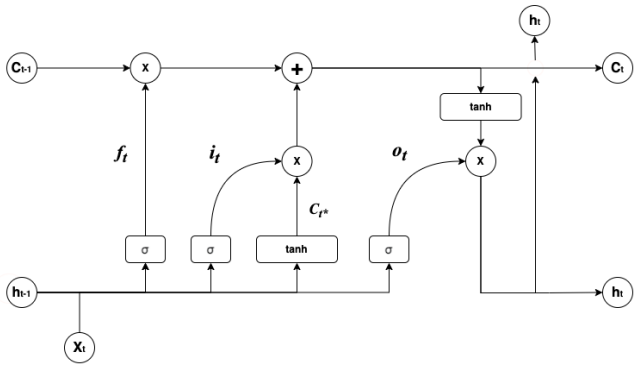

图2：长短期记忆网络单个细胞示意图。C_{t-1} 表示前一个$t-1$步的细胞状态，h_{t-1} 表示前一个$t-1$步的输出。x_t 表示序列中的第t个样本，C_t 和h_t 分别表示更新后的细胞状态和输出。i_t 、o_t、f_t 分别表示输入门、输出门和遗忘门[17]。

步骤的最终输出值由以下公式表示：

$$h_{t_*} = o_t * tanh(C_t)$$

遗忘门 f_t 帮助网络遗忘不再需要的信息：

$$f_t = \sigma(W_f.[h_{t-1}, x_t] + b_f)$$

6 隐私风险

虚拟现实的可用性能够拓展各类活动的能力；然而，这也增加了潜在风险[18]。从隐私、安全性、福祉等不同角度来看，虚拟现实中的风险管理仍缺乏用户的信任 [5]。增强现实领域也在探讨类似问题 [19]。然而，隐私与安全措施的问题仍未得到解答。所有选择通过虚拟现实与增强现实平台获得沉浸式体验的用户（包括游戏玩家和非游戏玩家），都可能不了解自己正在泄露多少信息。通过虚拟现实或增强现实收集的信息，可能成为模仿特定任务相关动作、视觉或情绪模式的资源。例如，个人可以利用从某人的虚拟现实体验中获取的实际数据，在没有经过训练的人工智能模型协助的情况下执行深度人脸验证程序[20]。

业界已开始使用“合成数据”，这种数据可以通过简化的数据生成，并非真实数据。然而，它仍能产生与真实数据相似的数学模式[21]。合成数据旨在保护隐私，但也可用于其他目的。当今最强大的工具之一——机器学习，能够轻易地从这类输入中提取非常准确的预测数据。苹果公司使用 TrueDepth 验证 FaceID。要解锁手机，TrueDepth 会采用注意力感知技术[22]。当有人睁着眼睛、专注地看着智能手机时，FaceID 会检测相关信息。因此，未经许可解锁他人的设备会更困难。不过，如果有人利用某些信息来模仿这种注意力模式，就可能解锁设备并利用这些知识。这很可能会成为长远的发展趋势。同样，沉浸式迷宫解谜电子游戏的测试案例也能提供足够的数据，以可行的效率预测后续步骤。

目前提出了许多策略，以缓解元宇宙中的隐私问题。用户可以为自己的虚拟化身克隆体创建一个附加副本，从而能够转移位置并改变外观。虚拟化身可以通过传送生成多个自身副本，用来阻止跟踪。智能合约应加入防范措施，以应对试图不道德地跟踪用户的公司。

目前正在研究电子游戏画像分析，以提升玩家表现和游戏体验。然而，如果玩家的游戏画像公开了某些内部信息，其隐私可能会受到损害 [23]。游戏开发者的观点可能更为积极，但如果遭到滥用，情况可能会更糟。

7 未来工作

互联网隐私已是一个重大问题，却尚未得到充分解决 [24]；此外，VR应用的安全性问题也显著增加。在VR环境中度过几个小时，就能为开发者提供训练数据，用于创建将身体属性与后续行为相匹配的算法。可以针对VR修改伦理准则[5], ，也可以扩大用户对数据共享的授权范围，但算法仍需以更通用的方式实现。如前所述，机器学习是一项强大的技术，可用于按预期方式创建算法。机器学习应谨慎运行，或许可以将可被利用的数据与可用性数据分开。机器学习在衍生数据中识别出某种模式后，可以征求用户许可，以保留或删除该模式。这相当于在进行任何医疗程序之前征求同意，无论患者是否愿意在死后捐献身体器官。

8 结论

智能手机面临的许多问题，如今也延伸到了面向普通用户的增强现实/虚拟现实可穿戴设备。这些设备的一项共同关键问题是，它们能够轻而易举地拍摄图像、录制视频并追踪其他可能的可用性数据，却无需经过适当审查。智能手机摄像头的出现引发了人们对参与这一过程的第三方的担忧，也引发了人们对拍摄旁观者有多么容易的隐私顾虑。鉴于虚拟现实/增强现实显示设备尚属新兴事物，且普遍缺乏基于伦理的实践标准，机器学习驱动的方法必须重视可用性数据，以进一步增强信任并促进这项技术的健康使用。

参考文献

[1] Steve Dent。索尼凭借“mo-copi”动作追踪系统进军元宇宙。https://tinyurl.com/5n6pb233，2022年。[2] Fiachra O’Brolcháin、Tim Jacquemard、David Monaghan、Noel O’Connor、Peter Novitzky 和 Bert Gordijn。

虚拟现实与社交网络的融合：对隐私和自主权的威胁。Science and Engineering Ethics，22:1–29，2016年。[3] Franziska Roesner、Tadayoshi Kohno 和 David Molnar。增强现实系统的安全与隐私。Commun. ACM，57(4):88–96，2014年4月。ISSN 0001-0782。doi: 10.1145/2580723.2580730。URL https: // doi.org/10.1145/2580723.2580730。[4] Sue Valerie Gray Cobb、Sarah Nichols、Amanda Ramsey 和 John R. Wilson。虚拟现实诱发症状与效应（vrise）。Presence: Teleoperators & Virtual Environments，8:169–186，1999年。[5] Devon Adams、Alseny Bah、Catherine Barwulor、Nureli Musabay、Kadeem Pitkin 和 Elissa M. Redmiles。伦理新议题：虚拟现实中的隐私与安全感知之探究。载于第十四届 USENIX 可用隐私与安全会议论文集，SOUPS '18，第443–458页，美国，2018年。USENIX Association。ISBN 9781931971454。[6] Orin S. Kerr。虚拟世界中的刑法。Cyberspace Law eJournal，2008年。[7] Store Help Center。Meta Horizon Worlds 常见问题：您是否正在录制 Meta Horizon Worlds 中发生的事情？[8] Pınar Kürtünlüo ̆glu、Beste Akdik 和 Enis Karaarslan。元宇宙中虚拟现实身份验证方法的安全性：概述。arXiv 预印本 arXiv:2209.06447，2022年。[9]维基百科。堡垒之夜。https://en.wikipedia.org/ wiki/Fortnite，2023年。[10] BloombergLaw。《堡垒之夜》诉讼案：美国联邦贸易委员会。https://tinyurl. com/bdds25ye，2022年。[11] Sumitkumar Kanoje、Sheetal Girase 和 Debajyoti Mukhopadhyay。用户画像趋势、技术与应用。arXiv 预印本 arXiv:1503.07474，2015年。[12] Marina Farid、Rania Elgohary、Ibrahim Moawad 和 Mohamed Roushdy。用户画像方法、建模与个性化。载于第十一届国际信息学与系统会议（INFOS 2018）论文集，2018年。[13] Marleen C. Tjepkema-Cloostermans、Rafael C.V. de Carvalho 和 Michel J.A.M. van Putten。利用深度学习检测头皮脑电图记录中的局灶性癫痫样放电。Clinical Neurophysiology，129(10):2191–2196，2018年。ISSN 1388-2457。doi: https://doi.org/10.1016/j.clinph.2018.06.024。URL https://www.sciencedirect.com/science/article/pii/S1388245718311465。[14] Jae Sung Park、Chonhyon Park 和 Dinesh Manocha。I-planner：利用基于学习的人体运动预测进行意图感知运动规划。The International Journal of Robotics Research，38(1):23–39，2019年。doi: 10.1177/ 0278364918812981。URL https://doi.org/10.1177/ 0278364918812981。[15] Ian Goodfellow、Yoshua Bengio 和 Aaron Courville。深度学习。MIT Press，2016年。

[16] Rafael Rêgo Drumond、Bruno Augusto Dorta Marques、Cristina Nader Vasconcelos 和 Esteban Walter Gonza- lez Clua。《Peek：一种基于稀疏数据进行动作分类的长短期记忆循环网络》。载于 VISIGRAPP，2018年。[17]Christopher Olah。《理解长短期记忆网络》，2015年。网址：http://colah.github.io/posts/2015-08-Understanding-LSTMs/。[18] Ian. Warren、Darren. Palmer 和澳大利亚犯罪学研究所。《三维虚拟环境中的犯罪风险》/ Ian Warren 和 Darren Palmer。澳大利亚犯罪学研究所，澳大利亚首都领地堪培拉，2010年。[19] Tamara Denning、Zakariya Dehlawi 和 Tadayoshi Kohno。《与增强现实眼镜旁观者的实地研究：对录制和隐私调节技术的看法》。载于《SIGCHI计算机系统人为因素会议论文集》，CHI '14，第2377–2386页，美国纽约州纽约市，2014年。计算机协会。ISBN 9781450324731。doi：10.1145/2556288.2557352。网址：https://doi.org/10. 1145/2556288.2557352。[20] Yaniv Taigman、Ming Yang、Marc'Aurelio Ranzato 和 Lior Wolf。《DeepFace：在人脸验证方面达到人类水平性能》。载于《2014年IEEE计算机视觉与模式识别会议》，第1701–1708页，2014年。doi：10.1109/CVPR.2014.220。[21] Brian Eastwood。《什么是合成数据——它如何助你在竞争中胜出？》https://tinyurl.com/ 55k8ekwe，2023年。[22] 苹果公司。《关于 Face ID 先进技术》。https://support.apple.com/en-us/HT208108，2022年。[23] Emmanuel Guardiola 和 Stephane Natkin。《用于生成玩家心理画像的游戏设计方法》，第363–380页。Springer International Publishing，瑞士尚，2015年。ISBN 978-3-319-05834-4。doi：10.1007/978-3-319-05834-4_16。网址：https://doi. org/10.1007/978-3-319-05834-4_16。[24] Annie I. Anton、Julia B. Earp 和 Jessica D. Young。《自2002年以来互联网用户的隐私关注如何演变》。IEEE安全与隐私，8(1):21–27，2010年。doi：10.1109/ MSP.2010.38。