

机器学习在生物医学工程的应用与挑战

梁聪岳

东北大学 医学与生物信息工程学院 辽宁 沈阳 110167

摘要:随着人工智能技术的迅猛发展,机器学习在生物医学工程中的应用日益广泛,已成为推动医疗智能化转型的重要动力。本文系统梳理了机器学习在医学图像处理、生物信号分析、临床辅助诊断等主要子领域的应用,分析了生物医学数据的复杂性与伦理敏感性带来的挑战,探讨了大模型、联邦学习等前沿技术的发展趋势,并展望其在精准医疗和个性化健康管理中的广阔前景。文章旨在为该领域的研究与实践提供理论支持与方向参考。

关键词:机器学习;生物医学工程;医学人工智能;数据融合;伦理挑战

引言:

随着计算能力的飞速提升和大数据技术的广泛应用,机器学习作为人工智能的重要分支,已经成为现代科技发展的前沿领域。机器学习通过自动从数据中学习规律和特征,实现预测、分类和决策等功能,极大地推动了众多行业的智能化进程。

生物医学工程作为一个融合了医学、工程学和计算科学的交叉学科,致力于解决医学中的复杂问题,促进医疗技术与设备的发展。随着医疗数据的爆炸式增长,如医学影像、生物信号、基因组数据等,传统的分析方法已难以满足高效、精准诊断和治疗的需求。

在此背景下,机器学习技术因其强大的数据处理和模式识别能力,逐渐成为生物医学工程领域的重要工具。它不仅在疾病诊断、治疗方案设计和医疗设备智能化方面展现出广阔的应用前景,还为个性化医疗和智慧医疗的发展提供了坚实的技术支撑。

本文梳理了机器学习在生物医学工程中的现状,探讨其面临的挑战,并展望未来的发展趋势,以期为该领域的研究和应用提供参考与启示。

1 机器学习在生物医学工程的应用现状

近年来,随着生物医学工程与人工智能的深度融合,机器学习在多个核心子领域中展现出强大的应用潜力。从医学影像处理到生物信号分析,从个性化治疗到临床决策支持,机器学习正不断重塑传统医疗工程的研究与实践方式。以下将从五个代表性方向进行系统分析。

1.1 医学影像处理与辅助诊断

医学影像是生物医学工程最核心的数据来源之一,具有非侵入性、可视化的优势,广泛应用于临床诊断与治疗评估中。传统影像分析依赖人工经验,效率低且主观性强。而机器学习,特别是深度学习(如CNN卷积神经网络)的引入,使得医学影像分析实现了从“规则驱动”到“数据驱动”的飞跃。

以肺结节检测为例,研究人员利用卷积神经网络对低剂量CT图像进行特征提取和分类,实现了早期肺癌的自动识别。在乳腺癌筛查中,基于机器学习的模型已可在Mammogram图像中达到媲美放射科医生的识别准

确率。此外,分割模型如U-Net在肿瘤轮廓标注、器官分割方面也表现优异。

目前,医学影像AI系统已在部分医院落地,用于辅助病灶识别、影像质控与诊断建议。然而,该领域仍面临多中心数据差异、模型可解释性差和医生信任度不高等挑战。

1.2 生物信号分析与疾病预测

生物信号,如心电图(ECG)、脑电图(EEG)、肌电图(EMG)等,是反映人体生理状态的重要动态数据。与图像数据不同,生物信号具有强烈的时序性和非线性特征。机器学习特别是时间序列建模方法,如支持向量机(SVM)、随机森林、长短期记忆网络(LSTM)等,在信号降噪、特征提取、异常检测等方面发挥着关键作用。

在心电信号分析中,深度神经网络已被广泛应用于心律失常分类、房颤检测等任务,并在PhysioNet等公共数据集上获得高度准确率。在脑电信号领域,研究

者开发出可通过 EEG 识别癫痫发作前兆、睡眠阶段分布等的模型，为智能监测与干预提供了新手段。

此外，融合多个传感器信号（如心率 + 呼吸 + 皮肤电）进行多模态健康评估也是当前研究热点。值得注意的是，信号数据常受干扰和个体差异影响，因此提升模型的泛化能力和鲁棒性仍是研究重点。

1.3 个性化医疗与智能治疗系统

个性化医疗旨在根据个体的基因、生活方式和环境等因素制定精准的诊疗方案。机器学习在处理高维基因组数据、挖掘疾病亚型、预测治疗反应方面展现出巨大潜力。

在基因层面，研究人员利用聚类分析、LASSO 回归等方法进行生物标志物筛选，用于癌症亚型识别、药物靶点预测。例如，利用机器学习模型对乳腺癌患者的基因表达谱进行分析，可实现对 HER2 阳性、三阴性等不同亚型的精准分类。

在智能治疗方面，脑机接口（BCI）结合深度学习算法，使得脑电信号可以驱动假肢或辅助设备运动，实现瘫痪患者的运动控制。此外，可穿戴设备收集的生理信号经机器学习分析后，可用于慢病管理和治疗方案优化。

1.4 医疗大数据与临床决策支持

随着电子病历系统（EMR/EHR）的普及，海量临床数据成为推动智能医疗的重要资源。机器学习技术被广泛应用于诊疗路径预测、疾病风险评估、临床决策支持等方向，助力实现基于数据的精准医学。

例如，研究者利用自然语言处理（NLP）技术对电子病历进行信息抽取，将非结构化的临床描述转化为结构化信息，用于疾病分类和疗效预测。在 ICU 临床风险预测中，基于 XGBoost、RNN 等模型开发的系统可对患者在未来 24 小时内的危重状态进行预测，帮助医生提前干预。

临床路径优化方面，一些医院引入机器学习系统，对治疗方案与历史病历数据进行分析，辅助制定标准化流程，提升资源利用效率与治疗效果。

2 当前研究面临的技术与伦理挑战

尽管机器学习在生物医学工程领域展现出强大的潜力和广阔的应用前景，但其在现实临床和科研环境中的推广仍面临诸多挑战。这些挑战不仅体现在技术层面，如数据获取、模型泛化、可解释性与安全性问题，还涉

及伦理、法律与社会责任的复杂议题。系统识别并应对这些挑战，是推动人工智能从实验室成果走向临床实践的关键一步。

2.1 技术挑战

2.1.1 高质量医疗数据的获取与共享困难

高质量医疗数据的获取与共享是当前亟待突破的瓶颈。机器学习模型依赖大规模、结构化的数据进行训练，但医疗数据通常具有强烈的异构性，包括图像、文本、生理信号、遗传信息等多个模态，不同医院、设备、采集协议间的差异导致数据标准不统一。此外，在疾病分布上，诸如罕见病或特定人群（如婴幼儿、高龄群体）的样本稀缺，训练数据呈现出显著的不均衡性，严重影响模型对“弱类”样本的识别能力。更重要的是，受限于隐私法规和伦理审批，真实、丰富的医疗数据往往难以在机构间共享，导致多数研究依赖少数公开数据集（如 MIMIC-III、PhysioNet 等），这些数据虽然便于复现，但其代表性与现实适应性仍存较大差距。

2.1.2 模型泛化能力和鲁棒性不足

当前机器学习模型的泛化能力与鲁棒性仍显不足。在训练集上表现优异的模型，往往在跨设备、跨区域或跨种族人群的场景中出现性能骤降，这一问题在医学图像诊断和生物信号分析中尤为突出。此外，许多模型对输入扰动高度敏感，例如微小噪声、图像模糊或信号伪影都可能导致错误诊断。更为严峻的是，模型往往依赖大量人工预处理与特征工程，这不仅加重临床应用负担，也限制了端到端模型的泛化能力。因此，如何构建具备迁移学习、领域自适应与多模态融合能力的通用型模型，成为当前研究的重要方向。

2.1.3 可解释性与信任机制缺乏

医学决策高度依赖对病理机制的理解与专业判断，而传统深度学习模型普遍存在“黑箱”特征，即难以解释其预测结果的逻辑依据。这种不透明性使得医生在实际诊疗中难以放心采纳模型建议，也增加了患者对智能医疗的质疑。近年来，诸如 Grad-CAM、SHAP、LIME 等可解释 AI 方法被广泛应用，用于揭示模型关注区域或重要特征，尽管取得一定成效，但其解释往往缺乏临床语义的严谨性，难以转化为可靠的医学依据。此外，当前多数解释方法仍以图像为主，对于文本、时序信号等数据的解释机制尚不成熟。

2.1.4 安全性与对抗攻击风险

研究发现,深度学习模型对对抗样本极其敏感,即通过微小、不可察觉的输入扰动即可误导模型做出错误判断。若此类攻击被应用于自动诊断或辅助决策系统,可能导致严重的医疗事故。如何构建具备防御机制的安全模型、在系统级别保障诊疗流程的鲁棒性与可信度,是当前AI医疗工程化必须解决的问题。

2.2 伦理与法律挑战

2.2.1 患者隐私保护与数据安全

医疗数据本身涉及患者身份、病史、基因、心理状态等高度敏感信息,在数据采集、存储、传输和使用的各个环节中,均面临潜在的泄露风险。尽管近年来《个人信息保护法》《数据安全法》等法律法规不断完善,对医疗数据处理设定了更严格的边界,但在技术实践中仍存在诸多挑战。例如,部分医院缺乏统一的数据安全规范,第三方平台处理数据时未充分加密,甚至出现通过模型反推训练样本的反演攻击行为。因此,在推动数据共享和模型训练的同时,必须同步加强加密技术、访问控制与审计机制的建设。

2.2.2 知情同意与算法透明度

当前,越来越多的医院开始尝试将AI系统引入辅助诊疗环节,但患者是否知晓其医疗决策受到机器模型影响?是否拥有拒绝算法参与的权利?在诊断出现差异时,患者该听从医生还是AI?这些问题尚无统一答案。在医疗伦理框架下,保障患者对算法过程的“可感知”

与“可追责”显得尤为重要,这也要求构建一种“人机共治”的医疗决策协作机制。

2.2.3 算法偏见与歧视问题

如果训练数据中某类人群(如女性、少数族裔、老年人)样本不足或标签偏倚,模型就可能在潜移默化中放大这种不公。例如,心血管疾病预测模型在男性群体中的准确率往往高于女性,在面部识别任务中白人样本的识别准确率远超其他人种。这种算法歧视不仅会导致诊疗差异化,甚至可能影响患者的就医选择与生存机会,违背了医疗公平的基本伦理。

2.2.4 责任归属与医疗事故界定不清

当AI辅助系统参与诊疗决策后,一旦发生误诊、漏诊或医疗事故,责任应由谁承担?是模型开发者、系统集成商,还是最终采纳建议的临床医生?若医生未采纳模型建议而错失诊断,是否意味着过失?反之,若过度依赖模型导致失误,又是否可以将责任转嫁给算法?当前我国尚缺乏专门针对医疗人工智能系统的责任认定法律框架,相关司法解释和行业规范有待完善。

尽管机器学习技术在生物医学工程领域已取得阶段性成果,但其广泛应用仍需跨越技术与伦理两道门槛。从提升模型性能到规范技术边界,从构建信任机制到完善法律保障,只有在多学科、多主体的协同治理下,人工智能技术才能真正服务于医学实践,造福于广大患者。

结 语:

随着信息技术的迅猛发展,机器学习作为人工智能的重要分支,正在深刻地重塑生物医学工程的研究范式与应用格局。从传统的医学图像处理、信号分析到精准医疗、智能诊断,再到远程健康管理和个性化治疗,机器学习技术正以前所未有的速度渗透至医疗系统的每一个角落。在疾病早筛、治疗优化、公共卫生监测等多个层面,它不仅提高了效率与准确性,也为医学研究提供了新的思路和工具。

然而,机遇之中也蕴含挑战。当前机器学习在医学中的广泛应用仍面临诸多技术瓶颈与伦理难题,如数据异质性、样本偏倚、模型可解释性不足、隐私泄露风

险及临床落地难度等。这些问题的存在提醒我们,生物医学工程领域对AI技术的引入不应仅限于算法的“迁移”,更应关注系统性的“融合”与“适配”。唯有在坚持多学科协同、加强监管体系建设和完善伦理机制的基础上,方能实现技术的可持续与高质量发展。

参考文献:

- [1] 王需虹. 生物大数据: 现状、挑战与未来发展 [J]. 解放军医学院学报. 2025,46(01)
- [2] 吴俊. 人工智能背景下影像图像分析与应用研究 [J]. 佳木斯大学学报(自然科学版). 2023,41(02)
- [3] 龙细连. 听力障碍儿童对情绪面孔的加工特点研究 [J]. 佳木斯大学学报(自然科学版). 2023,41(02)