doi:10.3969/j.issn.1003-3106.2025.11.017
引用格式:戴锐,张洪欣.低空脑机接口人机融合技术的安全性研究[J].无线电工程,2025,55(11):2290-2298.[DAI Rui, ZHANG Hongxin, et al. Research on Security of Low-altitude Brain-Computer Interface and Human-Machine Integration Technology [J]. Radio Engineering, 2025, 55(11): 2290-2298.]

低空脑机接口人机融合技术的安全性研究

戴　锐[1],张洪欣[2]
(1.中国人民公安大学 治安学院,北京 100038;
2.北京邮电大学 电子工程学院,北京 100876)

摘　要:探究了脑机接口(Brain-Computer Interface,BCI)和人机融合技术在无人机操控及反制设备使用领域的应用价值,分析了该技术面临的问题,并提出了针对性的解决策略,以推动其在低空经济发展及安全保卫中的合理应用。通过分析 BCI 技术在提升无人机操控效率、增加反制设备使用精准度等方面的作用,结合其为低空经济发展型塑的新应用场景和创造的低空安全保卫新形态,梳理该技术面临的人机融合技术自身缺陷、信息安全风险及其对低空安全造成的影响等问题,进而提出应对策略。BCI 技术在无人机操控和反制设备使用领域作用显著,能够提升无人机操控效率、增加反制设备使用的精准度,基于该技术与人机融合技术为低空经济发展型塑了新的应用场景,创造了低空安全保卫的新形态。

关键词:脑机接口人机融合技术;低空安全;无人机操控与反制
中图分类号:TN273.5　　**文献标志码**:A　　**开放科学(资源服务)标识码(OSID)**:
文章编号:1003-3106(2025)11-2290-09

Research on Security of Low-altitude Brain-Computer Interface and Human-Machine Integration Technology

DAI Rui[1], ZHANG Hongxin[2]
(1. *School of Public Security*, *People's Public Security University of China*, *Beijing* 100038, *China*;
2. *School of Electronic Engineering*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

Abstract: The application value of Brain-Computer Interface (BCI) and human-machine integration technology in the fields of UAV control and countermeasure equipment operation is explored, the problems faced by these technologies are analyzed, and targeted solutions are proposed to promote their rational application in the development of the low-altitude economy and security protection. By analyzing the role of BCI technology in improving UAV control efficiency and enhancing the accuracy of countermeasure equipment operation, and combining the new application scenarios that BCI technology shapes for the low-altitude economy and the new form of low-altitude security protection it creates, the problems faced by these technologies are sorted out, such as inherent defects of human-machine integration technology, information security risks, and their impacts on low-altitude security, and corresponding countermeasures are further put forward. BCI technology plays a significant role in the fields of UAV control and countermeasure equipment operation: it can improve UAV control efficiency and enhance the accuracy of countermeasure equipment operation. Based on BCI and human-machine integration technology, new application scenarios for the low-altitude economy have been shaped, and a new form of low-altitude security protection has been created.

Keywords: BCI and human-machine integration technology; low-altitude security; UAV control and countermeasures

收稿日期:2025-04-12
基金项目:中国人民公安大学治安学双一流专项(2023SYL01);2024 北京市高等教育学会面上课题(MS2024070);北京邮电大学 AI4S 探索计划项目(2025AI4S04)
Foundation Item: Double-First-Class Discipline Project of Public Security Science at People's Public Security University of China (2023SYL01); 2024 Beijing Association of Higher Education General Research Project (MS2024070); Beijing University of Posts and Telecommunications AI4S (Artificial Intelligence for Science) Exploration Initiative Project (2025AI4S04)

0 引言

BCI 人机融合技术面临诸多问题,包括人机融合技术本身的缺陷及其对低空安全造成的影响、人机融合技术中的信息安全风险及其对低空安全造成的影响。有关 BCI 技术在无人机反制和操控领域的运用的研究还有待深入。近年来,随着神经科学、人工智能和生物工程的快速发展,BCI 技术逐渐从科幻变为现实,成为新一代人机交互和人机混合智能的核心技术。目前,基于 BCI 的无人机操控与反制技术还存在一些安全挑战,面临信息安全风险,操控方面也存在信息安全问题,相关法律规定还不健全,本文将针对这些问题提出一些解决对策。

1 BCI 人机融合技术现状

BCI 技术旨在实现人脑与计算机或其他设备之间的直接通信,从而打破传统的人机交互方式。BCI 技术通过采集、分析和解码大脑的神经信号,将其转化为指令来控制外部设备。近年来,随着神经科学、人工智能和生物工程的快速发展,BCI 技术逐渐从科幻变为现实,成为新一代人机交互和人机混合智能的核心技术。

1.1 BCI 技术及其实现

BCI 技术是一种在脑与外部设备之间建立直接通信渠道的技术。它通过捕捉大脑的电信号,并将这些信号转换为控制命令,从而实现对外部设备的控制。其技术核心在于从神经信号中提取有效信息并转化为控制指令,其实现依赖于信号处理算法和分类模型的深度结合。BCI 技术主要分为侵入式、非侵入式和半侵入式 3 种。侵入式 BCI 是指通过外科手术将电极植入大脑皮层,能够记录高精度的神经信号,但手术风险较高。非侵入式 BCI 是指通过头皮表面的电极记录脑电信号,操作简单,但信号质量相对较低。半侵入式 BCI 介于侵入式和非侵入式之间,通常将电极放置在颅骨表面或硬脑膜上。

BCI 的实现涉及信号采集、信号处理、特征提取、分类算法等多个关键技术。信号采集是通过电极采集大脑的脑电图(Electronencephalogram,EEG)、脑磁图(Magnetoencephalogram,MEG)和功能性核磁共振成像(Functional Magnetic Resonance Imaging,fMRI)等神经信号;信号处理是利用放大器和滤波器对采集到的微弱信号进行放大和过滤,以去除噪声和干扰;特征提取是从处理后的信号中提取有用的特征,如脑电信号的频率特征和时域特征;分类算法是将提取的特征输入到分类算法中,如支持向量机(Support Vector Machine,SVM)、深度学习算法等,以实现对特定任务的分类和控制。

1.2 BCI 信号采集与预处理

BCI 系统主要采集 EEG 信号,即通过电极阵列捕捉皮层神经元活动引发的电位变化。由于 EEG 信号微弱,在对其进行信号特征提取之前通常进行噪声抑制、滤波等预处理工作,结合滤波与独立成分分析算法等提升信噪比。主要包括:

(1)时域滤波:使用无限冲激响应(Infinite Impulse Response,IIR)或有限冲激响应(Finite Impulse Response,FIR)滤波器带通滤波器去除肌电(Electromyography,EMG)、眼电(Electrooculography,EOG)和工频干扰噪声。

(2)空域滤波:通过共同空间模式(Common Spatial Pattern,CSP)算法对多个电极信号进行空间滤波,增强运动相关节律(如 μ 波和 β 波)的能量差异,同时抑制无关噪声。

(3)小波变换:采用 db4 或 Coiflet 小波进行多尺度分解,提取特定频段信号并去噪。

1.3 EEG 特征提取

脑电信号具有非平稳性特性,需结合自适应滤波与动态特征选择技术进行信号分析。考虑到个体差异性,常采用迁移学习或个性化微调策略,利用预训练模型与少量用户数据快速适配。

(1)时频域特征提取

在时域、频域和时频域常用的特征提取方法有:功率谱密度(Power Spectral Density,PSD),利用 Welch 方法计算运动想象时不同频段(如 8~12 Hz、15~30 Hz 等)的能量变化,进行 PSD 计算得到 PSD 特征。时域统计指标通过提取信号的均方根(Root Mean Square,RMS)、波幅、积分肌电(Integrated Electromyography,iEMG)等统计量得到时域统计指标。时频联合分析,利用短时傅里叶变换(Short-Time Fourier Transform,STFT)或小波包分解(Wavelet Packet Transform,WPT)生成时频图,捕捉非平稳信号的瞬态时频特征[1]。CSP 特征通过优化空间滤波矩阵,将多通道 EEG 信号投影到特征空间,最大化 2 类运动想象信号的方差比。利用传感器阵列信号的协方差矩阵提取信号的空间分布特征,结合特征值分解提升分类效果。

(2)信号分类模型

脑电信号的分类模型有:线性判别分析(Linear Discriminant Analysis,LDA),即利用投影最大化类间距离与最小化类内距离进行信号分类,适用于低维特征分类。SVM 通过非线性核函数构建高维分

类超平面对信号进行分类,对高噪声数据的鲁棒性好。

随机森林(Random Forest,RF)通过集成多棵决策树,自动生成特征重要性评估对信号进行分类,减少过拟合风险。卷积神经网络(Convolutional Neural Network,CNN)通过处理时频图的空间-频率信息,利用多层卷积提取局部特征对信号进行分类。循环神经网络(Recurrent Neural Network,RNN)或者长短期记忆网络(Long Short Term Memory,LSTM)通过捕捉 EEG 信号的时序依赖性对信号进行分类,这种方法具有时间维度上的动态变化特性。时空图卷积网络(Spatial Temporal Graph Convolutional Networks,STGCN)结合图结构建模各通道信号的空间关系与时间序列特征,提升多通道信号的关联性分析。增量学习(Incremental Learning,IL)通过动态更新分类器参数对信号进行分类,适应用户因疲劳或环境变化导致的信号漂移。域自适应(Domain Adaptation,DA)通过对抗训练对齐训练集与实时信号的分布差异对信号进行分类,减少个体间特征差异的影响。

(3)BCI 实时系统设计

通常采用滑动窗口机制对 BCI 实时系统设计,例如以 500~2 000 ms 窗口分段 EEG 信号,确保实时性和时序连续性[2]。在系统模型优化中,常采用轻量化模型进行优化。BCI 实时系统采用反馈闭环架构,分类结果通过解码器生成控制指令,并实时反馈给用户进行闭环优化[3]。

在运动想象 BCI 中,用户想象左手/右手运动时,EEG 信号经 5~30 Hz 的带通滤波去除基线漂移和工频干扰,通过 CSP 提取空间特征,计算 μ 波(8~12 Hz)和 β 波(15~30 Hz)频段的能量比作为输入特征,最后由 LDA 或 CNN 模型分类并输出控制指令。近年来,如 CSP+LSTM 等混合模型和端到端深度学习逐渐成为研究热点,推动 BCI 系统向更高准确率和更自然交互方向发展[4]。

基于 BCI 的人机融合技术在多个领域展示了广泛的应用前景。在医疗领域,BCI 技术不依赖于正常的外周神经和肌肉系统,为神经系统疾病患者提供了新的康复手段,同时为健康人群提供了增强认知和感知能力的可能性[5]。如通过 BCI 控制外骨骼帮助截瘫患者行走。对于丧失语言能力的患者,BCI 技术可以通过解码脑信号生成语音,帮助他们重新获得交流能力。在生活领域,BCI 技术可以实现智能家居设备的控制,提高生活便利性;在教育领域,BCI 技术可以帮助学生更高效地学习和记忆;在飞行领域,BCI 技术被用于提高飞行员的反应速度和操作精度,增强操作效能。BCI 技术与人工智能、深度学习等技术的融合将进一步提高系统的准确性和可靠性。

1.4 BCI 人机融合技术

BCI 技术旨在实现人脑与计算机或其他设备之间的直接通信,从而打破传统的人机交互方式。BCI 技术通过采集、分析和解码大脑的神经信号,将其转化为指令来控制外部设备。近年来,随着神经科学、人工智能和生物工程的快速发展,BCI 技术逐渐从科幻变为现实,成为新一代人机交互和人机混合智能的核心技术。在无人机操控和反制设备使用领域,BCI 技术都能够发挥重要作用。

第一,BCI 技术可以提升无人机操控效率。BCI 系统通过非侵入式电极(如 EEG 头戴设备)或侵入式植入装置实时采集操作员的运动想象或视觉诱发电位信号,解码后转化为无人机控制指令(如起飞、转向、悬停)。结合 BCI 与手势、语音控制,实现更自然的人机多模态交互[6]。例如,通过想象“加速”配合手势划动,提升复杂任务的操作流畅度。利用 BCI 监测操作员的专注度与疲劳状态,动态调整无人机响应灵敏度,降低人为失误风险。

第二,BCI 技术可以增加反制设备使用的精准度。BCI 系统可增强操作员对低空威胁的神经敏感性。例如,当操作员视觉注意到非法无人机时,脑电信号中与注意力相关的 P300 成分可被检测并触发自动反制程序(如启动无线电干扰)[7]。通过机器学习分析操作员的神经信号模式,预测其意图并推荐选择导航诱骗或激光打击最优反制策略,缩短响应时间。操作员通过 BCI 直接操控激光发射器等高精度定向能武器,瞄准目标无人机摄像头或电池等关键部件,实现精准打击。在反无人机蜂群场景中,BCI 支持多操作员神经信号同步,协调分布式反制设备形成联合防御网。

2 BCI 人机融合技术对低空经济和安全的影响

基于 BCI 和人机融合技术为低空经济发展型塑了新的应用场景,创造了低空安全保卫的新形态。

2.1 BCI 人机融合技术托举低空经济发展

低空经济作为一种新型经济形态,主要依托于低空空域内的飞行活动,涵盖有人驾驶和无人驾驶航空器,典型产业代表是无人机。中国正在通过体制机制改革,建立与低空经济发展相匹配的生产关系和管理体系,包括适航审定、飞行活动审批和运营监管等方面,以实现科学、高效的管理[8]。适用于

低空新经济的BCI和人机融合技术本身是新型经济形态的重要形式。BCI技术近年来取得了显著进展。Neuralink公司在侵入式BCI技术方面取得了重大突破,通过神经手术机器人植入微电极,实现了高效的大脑信号读取。此外,Facebook资助的UCSF研究也在非侵入式BCI技术上取得了进展[9]。基于BCI的人机融合智能研究旨在结合人类智能和机器智能,形成一种新的智能形式。这些技术的发展推动了低空产业新赛道的出现,为低空经济发展拓宽了新领域。

2.2 BCI人机融合技术保障低空安全

低空经济的发展依赖于飞行控制系统、通信技术、感知与导航技术、信息技术、数据处理技术及人机融合等核心技术。随着低空经济的突飞猛进以及BCI技术的广泛应用,与之相关的网络安全与数据安全风险亦日益显著,具体有安全监管不完善、数据高度敏感、设备广泛联网以及对数字技术高度依赖等问题。而基于BCI的人机融合智能面临的主要挑战包括人机认知差异化、意向化与形式化以及伦理性问题。当前,信息安全研究主要集中在计算机网络信息技术方面,涉及云计算、大数据、物联网等新兴技术[10]。未来,随着技术迭代与法规完善,BCI人机融合技术的安全防范或将成为低空安全治理的核心问题之一。有必要结合BCI人机融合技术的具体应用中的问题,探究发掘有针对性的对策。

3 低空BCI人机融合技术的安全问题

本节总结了BCI人机融合技术面临的具体问题。

3.1 人机融合技术本身的缺陷及其对低空安全造成的影响

3.1.1 人机融合技术自身缺陷

第一,人机融合面临信号干扰问题。信号干扰包括环境噪声、设备间的电磁干扰以及人机交互过程中产生的各种干扰信号。这些干扰信号会影响系统的准确性和稳定性,从而降低人机融合系统的整体性能。人机交互系统容易受到来自手机、电脑、电源等设备电磁干扰的影响,例如在存在电磁干扰的情况下,人机交互系统的信号质量会下降40%~60%,导致其解码精度下降20%~30%。此外,电磁干扰还会导致人机交互系统的功耗增加10%~20%。电磁干扰会影响人机交互系统的信号质量和解码精度,从而降低系统的性能和可靠性。

第二,人机融合面临稳定性问题。稳定性存在问题会影响系统的长期运行性能、响应速度以及在不同环境条件下的适应能力。在使用BCI系统进行人机交互时,系统的准确率平均为80%,而稳定性的标准差为10%。这意味着系统的准确率可能会在70%~90%波动,影响其可靠性和一致性。导致系统性能下降,准确率降低,甚至出现系统崩溃或无法正常工作的情况。这将严重影响人机融合系统的长期运行性能和响应速度,限制其在实际应用中的推广和使用。

第三,人机融合面临环境适应性问题。基于BCI的人机融合技术,在不同环境条件下的适应性表现不一致,例如,用户在嘈杂的环境中使用基于BCI的人机融合系统,系统的识别准确率可能会下降,导致用户体验不佳。如果系统在特定环境下表现不稳定,可能会影响其整体可靠性,可能导致用户对系统的信任度下降,系统可能需要更长的时间来适应和调整,从而影响操作效率。BCI系统在业务训练、户外运动等室外环境中的应用面临着环境噪声、电磁干扰、温度变化等挑战。这些因素可能会影响BCI系统的信号采集、处理和解码性能,从而降低其环境适应性。在室外环境中使用BCI系统进行运动控制时,系统的准确率平均为75%,而环境适应性的标准差为15%,这可能会影响其室外应用的可靠性和一致性,影响人机融合系统的性能,甚至导致系统崩溃。

第四,人机融合还存在准确性和实时性方面的问题。自然人机交互技术主要研究人和计算机之间如何用自然的方式进行交互[11]。但该技术在实际应用中系统的实时性和准确性仍然受到一些挑战[12]。在使用BCI系统进行VR人机交互时,系统的响应时间平均2 s,而准确率平均为70%。这意味着系统的实时性和准确性还有待提高。此外,在不同用户个体和不同VR环境条件下,系统的实时性和准确性也会受到影响。

第五,人机融合自身的安全性也面临一些问题。人机交互安全性包括物理安全性和感知安全性。物理安全性主要关注交互过程中避免对用户造成物理伤害,例如在机器人与人类协作的场景中,确保机器人不会碰撞到人类。感知安全性则关注用户在使用交互系统时的心理感受,包括舒适性、可预测性、控制感和信任等。在使用BCI系统进行VR人机交互时,有20%的用户报告了晕动症,有15%的用户报告了视觉疲劳。此外,有10%的用户报告了由于系统故障或误操作导致的晕动症或视觉疲劳。基于BCI的人机融合系统在虚拟现实中的感知安全性问题,会导致用户在虚拟环境中的体验下降,影响其实

时性和准确性。此外,感知安全性问题还会增加用户的恐惧感和不信任感,降低其使用系统的积极性。

3.1.2 基于 BCI 的无人机操控与反制技术的安全挑战

人机交互技术自身的缺陷对无人机操控与反制技术带来了负面影响。

第一,基于 BCI 的无人机操控安全风险。此类技术存在以下安全隐患:一是通信链路劫持,通过无线电频率干扰或协议漏洞,攻击者可劫持无人机控制信号,导致无人机失控或执行恶意指令;二是导航系统欺骗,GPS/北斗信号易受欺骗攻击,虚假定位信息可误导无人机偏离航线,甚至引发碰撞事故;三是 BCI 操控漏洞,基于 BCI 的无人机操控系统若未加密神经信号,可能被恶意截取或篡改,威胁操作安全。

第二,基于 BCI 的无人机反制安全风险。一是无线电干扰,通过发射大功率干扰信号阻断无人机与控制端的通信,迫使其迫降或返航。但此类设备若未严格管控,可能干扰合法通信频段,影响低空产业正常运营。二是导航诱骗,向无人机发送虚假导航信号,诱使其降落在指定区域。然而,技术滥用可能导致合法无人机被劫持,甚至用于犯罪活动。三是激光、微波等定向能设备,高能激光或微波可通过烧毁电路或干扰传感器直接摧毁无人机,但此类武器能量扩散可能误伤周边设备或人员,需严格限制使用场景。

3.2 人机融合技术中的信息安全风险及其对低空安全造成的影响

3.2.1 人机融合技术中的信息安全风险

第一,脑电信号泄露风险。首先,脑电信号可能被恶意软件拦截或篡改,导致用户的思维和指令被泄露或被误导。其次,BCI 设备可能受到对抗性攻击,使得设备输出错误的指令或翻译错误的语言,从而对用户造成危害。

第二,控制指令篡改风险。一是外部恶意攻击造成的指令篡改,主要表现为黑客或恶意软件通过多种方式篡改控制指令。例如,通过入侵系统的通信信道,截获并修改传输中的指令。二是系统内部的错误或故障造成的指令篡改,主要表现为系统的软件或硬件故障导致控制指令被篡改。例如,软件中的漏洞或硬件的故障可能导致指令在传输或执行过程中被错误地修改。控制指令的篡改可能导致系统行为异常,甚至造成严重的安全事故。

3.2.2 基于 BCI 的无人机操控与反制技术的信息安全问题

第一,GPS 欺骗与信号干扰。无人机依赖卫星导航系统实现精准定位,但 GPS 信号易受欺骗攻击。攻击者可生成虚假信号覆盖真实信号,使无人机偏离航线或进入禁飞区。

第二,数据链路劫持。无人机与控制端的数据链路若未加密,可能被中间人攻击劫持。采用量子通信或区块链技术可增强链路安全性,确保指令不可篡改。

第三,系统入侵与攻击风险。在无人机人机交互系统中,系统入侵与攻击风险是指未经授权的访问、数据篡改、服务中断等安全威胁。根据不同的攻击方式和目标,人机交互系统入侵与攻击风险可以分为以下几类。一是设备接口攻击:如 HID-USB 设备可能被用于注入恶意代码或窃取数据。二是生物识别攻击:包括指纹识别、语音识别和人脸识别等技术的攻击,如指纹伪造、声音模仿和照片欺骗。三是网络攻击:通过网络监听、中间人攻击等方式获取用户隐私和敏感数据。

3.2.3 技术漏洞与系统可靠性问题

第一,存与算法的协同风险。BCI 依赖高精度硬件(如忆阻器神经形态器件)与实时解码算法。天津大学与清华大学的实验中,尽管实现了百倍效率提升,但硬件故障或算法偏差仍可能导致无人机失控,尤其在复杂电磁环境下更容易由于电磁干扰导致无人机失控。

(1)在实验设计中,首先明确实验的目标,例如评估忆阻器神经形态器件在实时解码算法中的性能表现,或者探索特定算法对不同脑电信号的适应性。然后,选择合适的实验方法,如离线分析和在线测试。离线分析用于初步验证算法的有效性,而在线测试则用于评估实时系统的性能。进一步确定数据采集的方式和设备,包括 EEG 或其他类型的生物信号采集设备。确保采集的数据质量高且具有代表性。

(2)在样本选取中,根据统计学原则确定足够的样本量,以确保实验结果的统计显著性。选择具有代表性的受试者群体。例如,可以考虑不同年龄、性别、健康状况等因素的影响。如果实验涉及对照组和实验组,则需要随机分配受试者以减少偏差。

(3)在变量控制中,明确实验中的自变量,如不同的解码算法或不同的硬件配置。定义因变量,即实验中要测量的结果指标,如解码准确率、响应时间等。识别并控制可能影响结果的其他变量,如环境噪音、受试者的疲劳程度等。

(4)实验步骤包括:① 预处理阶段,对收集到的数据进行预处理,包括去除噪声、标准化等步骤。

② 算法开发与训练阶段,开发或选择合适的解码算法,并使用训练集进行训练。③ 在测试与验证阶段,使用测试集对算法进行验证,并记录各项性能指标。④ 在结果分析阶段,分析实验结果,评估算法性能,并讨论可能的影响因素。

第二,长时程交互的稳定性问题。实验显示,脑机协同性能随时间推移可能会出现波动(如初期依赖机器解码,后期大脑适应性增强),因此需动态调整系统参数,如果未能实时校准,可能引发操作延迟或错误导致无人机失控。

(1)在实验设计中,明确实验的目标,例如评估BCI系统在不同时间点的性能波动,或者探索用户适应性对系统性能的影响。采用纵向研究设计,即在多个时间点上重复测量同一组受试者的性能。这可以包括离线分析和在线测试,以便全面评估系统的稳定性。

(2)在数据采集中,确定数据采集的方式和设备,确保在不同时间点上采集的数据具有可比性。例如,使用相同的EEG设备和相同的实验环境。根据统计学原则确定足够的样本量,以确保实验结果的统计显著性。考虑到长期研究的复杂性,可能需要更多的受试者。选择具有代表性的受试者群体。例如,可以考虑不同年龄、性别、健康状况等因素的影响,以及不同技术水平的用户。如果实验涉及对照组和实验组,则需要随机分配受试者以减少偏差。此外,可以考虑在不同时间点上对同一组受试者进行多次测量。

(3)在变量控制中,明确实验中的自变量,如时间点、用户的适应性水平等。定义因变量,即实验中要测量的结果指标,如解码准确率、响应时间等。识别并控制可能影响结果的其他变量,如环境噪音、受试者的疲劳程度、情绪状态等。此外,需要确保在不同时间点上使用相同的实验条件和设备。

(4)实验步骤包括:① 在实验的预处理阶段,对收集到的数据进行预处理,包括去除噪声、标准化等步骤。确保在不同时间点上使用的预处理方法一致。② 在算法开发与训练阶段,开发或选择合适的解码算法,并使用训练集进行训练。确保在不同时间点上使用的算法和训练方法一致。③ 在测试与验证阶段,使用测试集对算法进行验证,并记录各项性能指标。在不同时间点上重复测试,以评估系统性能的波动。④ 分析实验结果,评估系统性能随时间的波动情况,并讨论可能的影响因素。可以使用统计方法(如方差分析、时间序列分析等)来量化性能波动。

第三,自主权与知情同意的冲突。BCI可能会影响用户自主决策能力,例如通过“情感计算”调节情绪或覆盖记忆就会对自主决策造成严重影响。因此,增强型应用(如注意力调节)需要严格限制,确保用户知情权[13]。同时,当前各国对BCI的伦理标准不一,例如美国倾向于在打击功能领域探索,而中国更注重医疗修复[14]。全球亟需类似国际原子能机构的监管框架,防止技术滥用并协调责任划分。

3.2.4 责任模糊问题

技术应用中的责任界定模糊。如果脑控无人机因信号干扰或算法错误导致误伤,则责任归属将难以界定。脑机协同演进技术虽提升了操控效率,但是“脑学习”与“机学习”的动态责任划分仍需法律规范。

4 低空BCI人机融合技术的安全问题的对策

4.1 加强弥补人机融合技术自身的缺陷,应对基于BCI的无人机操控与反制技术的安全挑战

第一,加强弥补人机融合技术自身的缺陷。一是针对信号干扰问题,应利用信号处理技术来识别不同类型的干扰源,分类采取对策。通过卡尔曼滤波、自适应滤波等信号处理算法和先进的滤波技术,以及优化设备设计和布局来减少干扰,采用差分编码、扩频技术等降低信号的干扰,通过合理布局天线、屏蔽干扰源等措施,减少环境噪声对信号的影响。二是针对稳定性问题,可以通过优化系统设计和算法,提高系统的稳定性和响应速度。采用自适应控制算法和机器学习技术来动态调整系统参数,以适应不同的工作条件。采用双机热备、多模冗余等技术等设计冗余系统结构,提高系统的容错能力,确保在部分硬件故障时仍能维持基本功能。三是针对环境适应性问题,在强电磁干扰、高噪声环境等不同环境条件下进行系统性能测试,发现并解决环境适应性问题。利用数字孪生技术构建极端场景模拟平台,通过对抗训练提升系统鲁棒性。四是针对自然人机交互技术还存在准确性和实时性方面的问题,通过深度学习的语音识别、图像识别和手势识别等技术使得人机交互系统能够更好地理解用户的意图[15],从而提高交互的准确性。通过GPU加速、FPGA加速硬件优化和剪枝、量化算法优化,提升计算能力,提高交互实时性,实现计算能力的提升和算法的改进,提升人机交互实时性。五是在安全性方面,可以使用弹性材料连杆机构、柔性电子材料以及事前预防主动控制等方法,以提高在人机交互过程

中的安全性。此外,发展 HID-USB、指纹识别、语音识别和人脸识别等多种交互方式的安全攻防技术,提升攻防效益。

第二,在完善 BCI 技术基础上,针对无人机操控与反制技术的安全挑战作出应对。结合 BCI 技术,可开发智能化反制系统。一方面利用实时态势感知技术,通过 BCI 增强操作员对低空威胁的感知能力,快速识别非法无人机并启动反制措施。另一方面,利用自适应干扰算法,通过机器学习优化无线电干扰策略,精准压制目标频段,减少对合法通信的影响。

4.2 解决无人机操控与反制技术的信息安全问题

第一,处理人机融合技术中的信息安全风险。一是针对脑电信号泄露风险,不断完善和提出加密以及信息隐藏方法。例如,基于 WPT、奇异值分解和 Logistic 算法的脑电信号信息隐藏算法,能够在保证较好的感知保真度的同时,隐藏更多的信息。采用数字水印、隐写术等信息隐藏技术,在保证信号质量的前提下,隐藏脑电信号信息,提高信号的安全性。二是针对控制指令篡改的风险,可以通过对称加密、非对称加密等加密技术保护指令在传输过程中的安全性,以及通过基于机器学习的异常检测、基于规则的异常检测等异常检测技术识别潜在的篡改行为。

第二,解决基于 BCI 的无人机操控与反制技术的信息安全问题。针对无人机数据链路劫持风险,可以采用量子通信或区块链技术增强链路安全性,确保指令不可篡改;采用区块链技术,确保数据链路的安全性和可追溯性。为了应对无人机系统入侵与攻击风险,可以发展以下防御策略和方法:① 设备认证与访问控制:加强设备认证,使用安全固件,并对 USB 设备进行严格的访问控制。② 多因素认证与实时监控:采用多因素认证,增强图像处理算法以降低伪造指纹的识别率,并实时监控和检测异常登录行为。③ 网络安全防护:采用安全的网络协议和加密技术,加强网络防火墙和入侵检测系统建设,定期进行网络安全审计和漏洞扫描。

4.3 完善顶层设计,加快基于 BCI 人机融合技术安全、信息安全的法律政策制定

第一,制定 BCI 技术应用安全规范。国家科技伦理委员会人工智能伦理分委员会研究编制了《脑机接口研究伦理指引》,旨在指导 BCI 研究合规开展,防范 BCI 研究与技术应用过程中的科技伦理风险[16]。该指引提出了保障健康、提升福祉,尊重被试、适度应用,坚持公正、保障公平,风险管控、保障安全,信息公开、知情保障,支持创新、严格规范等基本原则[17]。应当依据该规范,制定无人机领域的 BCI 技术规范、标准,规范前述的一系列安全问题[18]。

第二,加强 BCI 技术在无人机操控和反制设备使用方面的规范化管理。一是建立分级分类规范。开发智能防御系统,融合 BCI 与人工智能技术,实现威胁自动识别与分级响应,降低人为操作风险。二是明确反制设备使用标准。制定无线电干扰功率、激光能量阈值等参数标准,防止滥用导致次生危害。建立反制许可制度,仅在授权场景使用高能武器,避免民用领域误用。

第三,加强人机融合信息安全法律法规建设。规定无人机操控和反制设备使用的相关频率、链路数据的管理主体,发送、传输、接受规则,监督管理机制以及违反相关规则的法律责任。

此外,提升公众的信息安全意识与素养也是关键,需要通过教育和宣传,增强公众对无人机操控和反制设备使用中信息安全的认识和理解。

4.4 加强数据隐私与网络安全、强化技术可靠性

第一,加强神经信号动态加密技术。开发基于量子加密或神经动态特征的实时加密算法,确保脑电信号传输全程端到端加密。例如利用脑电波信号的个体唯一性生成动态密钥,可以防止中间人攻击。

第二,引入区块链技术分布式存储脑数据。方便实现数据访问权限可追溯,避免中心化数据库被集中破解。

第三,采用生物数据最小化原则。仅采集运动意图等与功能直接相关的必要脑信号以减少数据量,并通过边缘计算在本地完成数据处理,减少原始数据外传风险。同时,建立“动态脱敏”机制,对存储的脑数据进行去标识化处理,并设置自动销毁,如欧盟 GDPR 的“数据生命周期管理”等。

第四,采取技术可靠性强化方案。设计硬件冗余与容错架构,采用 FPGA+ASIC 组合等双核异构处理器,确保在部分硬件故障时仍能维持基本功能。开发“神经信号-机械指令”交叉验证算法,当脑信号与预设行为模式偏差超过阈值时,自动切换至人工接管模式。

第五,加强复杂环境适应性训练。利用数字孪生技术构建电磁干扰、高噪声等环境极端场景模拟平台,通过对抗训练提升系统鲁棒性。建立 BCI 失效应急协议,例如无人机失控时启动预设安全航线并触发物理断连开关,从而在复杂环境中训练无人机的自适应能力。

4.5 加强社会协同与全球化治理

第一,加强公众参与技术监督。建立 BCI 技术透明化平台,公开项目的技术路线与安全测试结果,接受公众质询。推广“伦理渗透测试”(Ethical Penetration Testing),鼓励白帽黑客发现系统漏洞,并及时反馈修正。

第二,建立跨国技术标准联盟。例如,由中国、欧盟等牵头成立“全球脑机接口标准委员会”,统一数据格式、安全协议与测试规范,避免技术碎片化。对发展中国家实施技术援助与伦理能力建设,防止低标准应用引发全球性风险。

5 结束语

本文系统地探讨了低空 BCI 人机融合技术的安全性问题及其应对策略。创新性地提出从技术改进角度优化信号处理算法、强化加密技术、开发冗余架构与容错机制;从法律政策层面制定安全规范与伦理指引,建立分级管理及国际公约;从数据隐私与网络安全角度采用量子加密、区块链技术、生物数据最小化原则;从社会协同治理层面推动公众参与技术监督、构建跨国标准联盟、设立伦理审查机制。

未来,低空 BCI 人机融合技术将在智能化与精准化方向持续突破,但其安全治理需兼顾技术创新与伦理约束,完善法律法规与技术标准,构建“人机融合、攻防一体”的低空安全体系。从技术发展来看,需进一步优化脑信号解码精度与抗干扰能力,推动边缘计算与自适应算法在实时交互中的应用;在安全体系构建方面,需建立“人机融合、攻防一体”的低空安全框架,整合智能化反制系统与动态防御机制;在全球治理方面,亟需国际协作以统一技术标准与伦理规范,限制打击功能滥用,平衡技术红利与人类自主性;从公众参与角度,应该通过教育与透明化平台提升社会认知,形成多方协同的技术监督生态[19]。

参考文献

[1] YANG C, ZHANG H X, ZHANG S G, et al. The Spatio-Temporal Equalization for Evoked or Event-related Potential Detection in Multichannel EEG Data [J]. IEEE Transactions on Biomedical Engineering, 2019, 67(8): 2397-2414.

[2] 张洪欣,王俊淞,杨晨. 面向 SSVEP-BCI 的最大后验准则异步检测算法[J]. 北京邮电大学学报 2023, 146(6): 15-19.

[3] YANG C, YAN X Y, WANG Y J, et al. Spatio-Temporal Equalization Multi-window Algorithm for Asynchronous SSVEP-based BCI [J]. Journal of Neural Engineering, 2021, 18: 0460b7.

[4] 张舒玲,杨晨,张洪欣,等. 一种多码元时分编码 SSVEP-BCI 少训练检测算法[J]. 北京邮电大学学报, 2022, 12, 45(6): 40-46.

[5] 黄超. 自然人机交互相关技术研究与系统实现[D]. 上海:上海交通大学, 2010.

[6] 李家伟,张洪欣,徐瑞林. 基于脑机接口的无人机编队控制系统设计[J]. 航空科学技术, 2023, 34(2): 104-110.

[7] ZHANG Y F, ZHANG H X, GAO X R, et al. UAV Target Detection for IoT via Enhancing ERP Component by Brain-Computer Interface System [J]. IEEE Internet of Things Journal. 2023, 10(19): 17243-17253.

[8] 孔得建,袁泽. 低空经济政策法律体系的现状、经验与展望[J]. 北京航空航天大学学报(社会科学版), 2024, 37(5): 84-95.

[9] 刘菁,刘丹阳,李梦婷,等. 脑机接口的发展和监管挑战[J]. 中国医疗器械信息, 2024, 30(19): 7-10.

[10] 王雪影,高国柱,古利兰,等. 促进我国低空经济发展的法规体系研究[J]. 信息通信技术与政策, 2024, 50(11): 48-53.

[11] 赵霞,高源,李之红,等. 城市交通枢纽行人异常行为分析研究综述[J]. 市政技术, 2024, 42(7): 124-132.

[12] 黄超. 自然人机交互相关技术研究与系统实现 [D]. 上海:上海交通大学, 2010.

[13] 杨文杰,南文雅,龚安民,等. 神经反馈调节健康个体注意力的研究进展[J]. 中国生物医学工程学报, 2022, 41(3): 351-359.

[14] 朱依娜,卢阳旭. 中国人工智能伦理治理实践与挑战—基于三期交叠视角[J]. 中国科技论坛, 2025(1): 148-153.

[15] MA W X, SONG G, ZENG Q T, et al. FFCSLT: A Deep Learning Model for Traffic Police Hand Gesture Recognition Using Surface Electromyographic Signals [J]. IEEE Sensors Journal, 2024, 24, (8): 13640-13655

[16] 林水强. 自然人机交互关键技术研究及其应用 [D]. 绵阳:西南科技大学, 2015.

[17] 陈燕军,汪地,杨浩,等. 基于 Kinect 的手术辅助系统研究[J]. 计算机技术与发展, 2014, 24(9): 81-83.

[18] 刘菁,刘丹阳,李梦婷,等. 脑机接口的发展和监管挑战[J]. 中国医疗器械信息, 2024, 30(19): 7-10.

[19] 刘永博,张洪欣,杨晨. 基于分布式架构的脑机接口教学系统设计与实现[J]. 信息通信技术与政策, 2025, 51(3): 2-10.

作者简介

戴 锐 男,(1980—),博士,副教授。主要研究方向:治安学、低空安全

张洪欣 男,(1969—),博士,教授。主要研究方向:电磁信息安全、脑机接口与人机交互。