文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

大模型驱动的人工智能在智能安防场景中的深度应用与优化

周旭[1] 王玮[2] 县泽宇[1]
1 联通数字科技有限公司宁夏回族自治区分公司 2 宁夏汉林德电子科技有限公司
DOI:10.12238/acair.v3i2.13503

[摘 要] 在科技飞速革新的当下,智能安防作为社会安全保障的关键领域,正经历着深刻变革。大模型驱动的人工智能技术凭借其卓越的数据处理、深度分析与自主学习能力,为智能安防带来了前所未有的发展契机。本文深入剖析大模型支撑下人工智能在智能安防场景中的核心运作原理与独特优势,全方位阐述其在视频监控、入侵预警、身份识别、安防数据分析等多元场景中的深度应用,并创新性地提出一系列涵盖模型性能、数据管理、安全防护、协同运作等层面的优化策略,旨在深度挖掘人工智能在智能安防领域的潜力,显著提升安防系统的智能化水平与安全性,为社会安全稳定筑牢坚实防线,推动智能安防行业向更高质量、更具创新性的方向迈进。
[关键词] 大模型驱动；人工智能；智能安防场景
中图分类号：TP18 文献标识码：A

Deep application and optimization of large model-driven artificial intelligence in intelligent security scenarios

Xu Zhou[1] Wei Wang[2] Zeyu Xian[1]
1 Unicom Digital Technology Co., LTD. Ningxia Hui Autonomous Region Branch
2 Ningxia Hanlind Electronic Technology Co.,LTD

[Abstract] In the rapid innovation of science and technology, intelligent security, as a key area of social security, is undergoing profound changes. Large model-driven artificial intelligence technology, with its excellent data processing, deep analysis and autonomous learning capabilities, has brought unprecedented development opportunities for intelligent security. This paper analyzes the core operating principles and unique advantages of artificial intelligence in intelligent security scenarios supported by large models, comprehensively describes its deep application in video surveillance, intrusion warning, identity identification, security data analysis and other multiple scenarios, and innovatively proposes a series of optimization strategies covering model performance, data management, security protection, collaborative operation and other levels. It aims to deeply tap the potential of artificial intelligence in the field of intelligent security, significantly improve the intelligence level and security of the security system, build a solid defense line for social security and stability, and promote the intelligent security industry to a higher quality and more innovative direction.
[Key words] large model driven; Artificial intelligence; Intelligent security scenario

随着数字化与智能化进程的加速,社会对安全保障的需求呈现出爆发式增长。传统安防体系在面对日益复杂的安全威胁、海量且多样的数据以及动态变化的应用场景时,逐渐暴露出效率低下、精准度欠佳等局限性。大模型驱动的人工智能技术应运而生,为智能安防领域注入了强大动力。通过构建超大规模、结构复杂的神经网络模型,对海量安防数据进行系统性学习与深度挖掘,人工智能能够精准洞察安防场景中的复杂模式与潜在风险,实现对各类安全事件的高效预警与精准处置。这一技术革新不仅大幅提升了安防系统的智能化程度,更从根本上改变了安防行业的运作模式,成为智能安防领域实现跨越式发展的核心引擎。

1 大模型驱动人工智能在智能安防中的核心原理与优势

大模型驱动的人工智能依托深度学习架构,构建包含海量参数的神经网络,对大规模、多模态的安防数据开展无监督或有监督学习。在智能安防场景中,丰富的数据来源包括监控视频中的图像序列、各类传感器收集的环境数据以及文本形式的安防记录等。人工智能借助卷积神经网络(CNN)对图像和视频数据进

行处理,通过层层卷积与池化操作,精准提取图像中的关键特征,如人物的外貌特征、行为动作模式、物体的形状与结构等。循环神经网络(RNN)及其变体长短时记忆网络(LSTM)则擅长处理具有时间序列特性的数据,能够有效分析安防事件在时间维度上的演变规律,例如对监控视频中连续帧所呈现的行为变化进行动态分析。

其优势极为显著,具体表现为:强大的泛化能力使得人工智能无需针对每个特定安防场景进行繁复的定制化开发,而是通过对大量不同场景下安防数据的深度学习,掌握通用的安防模式与特征,从而在全新、未知的场景中也能快速、准确地进行识别与判断。高度的准确性源于对海量数据的深度挖掘,能够捕捉到极其细微的特征差异,在目标识别、行为分析等关键任务中展现出远超传统安防技术的精度。以人脸识别为例,人工智能大模型能够在不同光照、姿态以及部分遮挡等复杂条件下,精确识别出人员身份,极大提高了身份识别的准确率。良好的扩展性保障了随着安防数据的持续积累与更新,模型能够通过在线学习或增量学习的方式不断优化与升级,实时适应不断变化的安防需求与威胁态势。

2 大模型驱动人工智能在智能安防多元场景的深度应用

2.1智能视频监控分析

在智能视频监控领域,大模型驱动的人工智能发挥着核心作用。通过对监控视频流的实时分析,人工智能能够精准识别各类目标物体,涵盖人员、车辆、可疑物品等。利用先进的目标检测算法,模型可迅速定位视频画面中的目标,并准确判断其类别。在人员检测方面,不仅能够识别人员的存在,还能深入分析人员的行为,诸如行走、奔跑、徘徊、打斗等异常行为模式。通过对连续视频帧的追踪分析,人工智能能够精确描绘目标物体的运动轨迹,实现对人员或车辆的实时动态跟踪。这对于监控重要区域的人员流动态势、精准监测交通流量以及高效追踪犯罪嫌疑人等具有不可替代的重要意义。例如,在公共场所的监控场景中,人工智能模型能够实时监测人群密度,一旦检测到人员聚集程度超过预设阈值,便立即发出预警信号,有效预防拥挤踩踏等安全事故的发生。

2.2入侵预警与风险评估

在入侵预警与风险评估方面,人工智能展现出强大的能力。通过对安防传感器数据、环境数据以及历史事件数据的综合分析,模型能够深度学习正常状态下的环境特征与行为模式。一旦监测到数据偏离既定的正常模式,人工智能可迅速判断是否存在入侵行为或潜在安全风险。以周界防范系统为例,模型整合红外传感器、震动传感器等多源数据,精准分析是否有非法闯入者翻越围栏、破坏围墙等入侵行为。在风险评估环节,人工智能依据历史数据和实时监测数据,对不同区域在不同时间段的安全风险等级进行科学预测,为安防资源的合理调配提供精准依据。在大型活动安保场景中,模型结合场地周边环境、人员流量预测数据以及以往类似活动的安全事件记录,提前评估可能出现的安全风险,如恐怖袭击风险、火灾风险等,助力制定针对性强、高效的安保措施。

2.3身份识别与访问控制

身份识别是智能安防的关键环节,大模型驱动的人工智能在人脸识别、指纹识别、虹膜识别等生物特征识别技术中扮演着核心角色。在人脸识别领域,人工智能通过对海量人脸图像的深度学习,提取人脸的独特特征向量,构建超高精度的人脸识别模型。该模型能够在复杂环境下,如不同光照强度、不同姿态角度、部分面部遮挡等情况下,准确识别出人员身份。在门禁系统、考勤系统以及重要场所的人员出入管理中,人工智能驱动的人脸识别技术极大地提高了身份识别的效率与准确性,有效杜绝非法人员进入。在指纹识别与虹膜识别领域,人工智能同样借助对指纹纹路细节、虹膜纹理特征的深度分析,实现对人员身份的精准确认,为访问控制提供可靠保障。

2.4智能安防数据分析与决策支持

大模型驱动的人工智能能够对海量的安防数据进行深度分析,为安防决策提供强有力的支持。通过数据挖掘与机器学习算法,模型可以从大量的监控视频、报警记录、人员信息等数据中挖掘出潜在的关联与规律。例如,分析不同时间段、不同区域的犯罪类型分布规律,以及犯罪行为与人员属性、环境因素之间的内在联系。基于这些深度分析结果,安防部门能够制定更具针对性、科学性的安保策略,实现安防资源的合理、高效分配。在城市安防规划中,人工智能模型根据历史安防数据和城市发展规划,预测未来可能出现安全隐患的区域,为城市基础设施建设、安防设施布局提供科学依据。在突发事件发生时,通过对安防数据的实时分析,人工智能能够快速生成最佳应对方案,显著提高应急处理效率。

3 大模型驱动人工智能在智能安防应用中的优化策略

3.1模型性能强化

为显著提升人工智能模型于智能安防领域的性能表现,需持续且深入地优化模型架构。积极探索融合新型理念的神经网络结构,例如将具备独特优势的结合注意力机制的Transformer架构创新性地引入安防场景,凭借其对关键信息强大的聚焦与精准捕捉能力,助力模型在复杂安防数据中快速锁定核心要素。在模型训练进程中,引入自适应学习率调整算法,使模型宛如具备自主感知能力,能够依据数据特征的动态变化,自动且精准地调整学习率。这一机制可极大地加速模型的收敛进程,显著提升训练效率,缩短训练周期。同时,采用先进的模型压缩技术,诸如剪枝、量化等方法,在确保模型性能不受显著影响的严格前提下,大幅削减模型参数数量,有效降低模型存储所需空间与复杂的计算复杂度,从而显著提升模型在资源受限的边缘设备上的运行效率,使其能够在各类安防终端高效运作。此外,定期收集新的安防数据对模型进行更新与优化,借助增量学习机制,使模型能够敏锐且及时地适应不断涌现的新安防场景与潜在威胁,始终保持卓越的性能状态[1]。

3.2数据管理精细

强化安防数据的质量管理至关重要，需制定极为严格的数据采集标准与规范，从源头上确保采集到的数据具备高度的准确性、完整性与一致性。运用前沿的数据清洗技术，对采集到的数据进行深度处理，去除其中混杂的噪声、冗余的重复数据以及错误的标注信息，以此显著提高数据质量，为后续模型训练与分析奠定坚实基础。构建功能强大的安防数据湖，将多源异构数据，如丰富多样的视频数据、各类传感器采集的环境数据以及文本形式记录的安防数据等进行有机整合，实现数据的集中存储与统一管理，便于高效调用与分析。借助先进的数据加密技术，对包含敏感信息的安防数据进行加密处理，构建严密的数据安全防护网，切实保障数据安全。采用科学的数据脱敏技术，在不干扰模型训练效果的前提下，对涉及个人隐私的数据进行脱敏操作，在合理利用数据的同时保护个人信息安全。建立完善且精细的数据生命周期管理机制，对数据从采集、存储、使用到最终销毁的全流程环节进行精细化管控，确保数据在各个阶段都能得到合理利用且处于安全可控状态[2]。

3.3安全防护加固

加强人工智能模型在智能安防应用中的安全防护工作刻不容缓。采用对抗训练技术，精心模拟各种复杂的对抗攻击环境，让模型在其中进行针对性训练，以此大幅提升模型的鲁棒性，使其能够有效抵御各类恶意攻击，如极具隐蔽性的对抗样本攻击、可能导致数据污染的数据投毒攻击等。搭建专业的模型安全监测系统，实时且全面地监测模型的运行状态，运用先进的监测算法与数据分析技术，及时精准地发现异常行为与潜在安全风险。对模型的访问权限实施极为严格的管理，运用先进的身份认证、访问授权等技术，构建严密的访问控制体系，确保仅有经过授权的人员能够安全地访问和使用模型。强化对数据传输过程的加密保护，采用高强度的加密算法，防止数据在传输过程中被不法分子窃取或篡改。制定完善且周全的应急预案，在模型遭受攻击或出现故障时，能够迅速且有序地切换至备用模型或采取有效的应急措施，全力保障安防系统的持续稳定运行，维护社会安全[3]。

3.4多模态融合增效

大力推动多模态数据融合在智能安防中的广泛应用，将视频图像数据、音频数据、传感器数据等多种模态的数据进行深度且有机的融合分析。通过构建创新的多模态融合模型，充分挖掘不同模态数据之间潜在的互补信息，打破数据壁垒，使各类数据相互补充、协同作用，以此显著提高安防系统的准确性与可靠性。在安防系统内部，积极促进不同组件与模型之间的协同工作，实现视频监控系统、入侵预警系统、身份识别系统等关键组成部分的无缝对接与高效协同运行。通过制定统一且规范的数据接口与通信协议，消除系统间的数据交互障碍，实现各系统之间的数据共享与流畅交互，全面提升安防系统的整体运行效率与响应速度，打造高效智能的安防体系[4]。

3.5边缘-云协同优化

采用边缘计算与云计算协同的创新架构，对人工智能模型在智能安防中的部署与运行模式进行深度优化。在边缘设备层面，充分利用其低延迟特性，对实时性要求极高的安防任务，如视频监控中的目标检测与行为分析，进行快速且精准的响应，能够在第一时间捕捉到安防场景中的关键信息与异常情况。将复杂且对计算资源需求巨大的模型训练与深度数据分析任务部署在云端，充分借助云计算强大的计算资源与存储能力，确保模型训练的高效性与数据分析的全面性。通过边缘计算与云计算的紧密协同运作，实现数据的分级处理与模型的分层部署，既能满足安防系统对实时性的严格要求，又能有效降低数据传输压力，避免网络拥堵，同时提升系统的整体性能与可扩展性，以适应不断增长的安防需求与复杂多变的安防场景[5]。

4 结语

大模型驱动的人工智能在智能安防场景中的深度应用，正引领智能安防行业步入智能化、高效化、精准化的崭新时代。通过深入理解其核心原理与独特优势，并将其广泛应用于多元安防场景，人工智能为安防工作提供了强大的技术支撑。通过实施模型性能强化、数据管理精细、安全防护加固、多模态融合增效、边缘-云协同优化等一系列创新优化策略，能够进一步挖掘人工智能在智能安防中的巨大潜力，显著提升安防系统的整体效能与安全性。这不仅对维护社会安全稳定、保障人民生命财产安全具有重要意义，更将推动智能安防行业的技术创新与产业升级，在科技与安全的深度融合中，为社会进步注入强大动力，开创智能安防领域发展的全新格局。

[参考文献]

[1]李文军.众智公司智能安防业务竞争战略研究[D].贵州大学,2022.

[2]关健荣.基于物联网技术的智能安防领域的运用[J].信息与电脑(理论版),2022,34(01):189-191.

[3]黄亨斌.智能安防巡检机器人的人脸检测与识别方法研究[D].湖南大学,2021.

[4]张书伟.面向智能安防场景的人体行为识别算法研究及应用[D].西安电子科技大学,2021.

[5]肖秋语.AJ公司智能安防门禁系统营销策略研究[D].华侨大学,2020.

作者简介：

周旭(1992--),男,汉族,宁夏人,本科,人工智能与机器学习方向。

王玮(1994--),女,汉族,宁夏人,本科,人工智能与机器学习方向。

县泽宇(1991--),男,汉族,宁夏人,硕士研究生,人工智能与机器学习方向。