

智能识别技术在校园一卡通系统中的应用

李 伟

(桂林电子科技大学, 广西 桂林 541002)

摘 要 智能识别技术在校园一卡通系统中的应用, 对提升校园管理效率与服务质量意义重大。常见智能识别技术如人脸识别、指纹识别等, 以其独特原理, 正不断革新校园一卡通的应用模式。该技术与一卡通系统融合, 优化了系统架构, 拓展了身份验证、消费支付等功能模块, 增强了与校园其他信息系统的兼容性, 提升了身份识别的准确性和便捷性, 加快了校园管理的信息化进程, 应用效果显著, 但也面临隐私保护、技术稳定性等潜在风险。本文认为通过制定严格的数据保护策略、持续技术优化升级等措施, 能有效应对风险。

关键词 智能识别技术; 校园一卡通系统; 基础功能模块; 校园信息系统

中图分类号: TP18

文献标志码: A

DOI: 10.3969/j.issn.2097-3365.2025.24.007

0 引言

在数字化浪潮的席卷下, 校园管理模式正经历着深刻变革, 对高效、智能管理体系的需求愈发迫切。校园一卡通系统作为校园信息化建设的关键组成部分, 承载着身份识别、消费支付、门禁管理等诸多功能, 在师生的校园生活中扮演着不可或缺的角色。传统校园一卡通系统在身份验证环节存在效率较低、准确性有限等问题, 难以满足日益增长的校园管理需求。智能识别技术的兴起, 为人脸识别、指纹识别、虹膜识别等精准、高效的识别方式走进校园提供了可能。将智能识别技术深度融入校园一卡通系统, 有望突破传统模式的局限, 提升校园管理效率, 优化师生校园体验, 为构建智慧化校园奠定坚实的基础。

1 智能识别技术概述

1.1 常见智能识别技术类型

智能识别技术包含多种类型, 其中生物特征识别利用人体固有的生理或行为特征来验证身份, 如指纹识别, 凭借指纹的唯一性和稳定性, 在门禁系统、电子设备解锁等场景广泛应用; 人脸识别通过分析面部特征进行身份识别, 在安防监控、支付认证领域发挥关键作用。图像识别技术专注于让计算机理解图像内容, 如物体检测可精准识别图片或视频中的物体类别和位置, 在自动驾驶中助力车辆识别行人、交通标志等。语音识别技术将语音信号转化为文本或指令, 智能音箱、语音助手借此实现人机交互, 极大地便利了人们的生活与工作。

1.2 技术原理深度剖析

从原理层面深入剖析, 智能识别技术的运作有着严谨且复杂的流程。首先, 数据收集是基础环节, 收

集的数据丰富多样, 涵盖图像、音频、文本等多种格式。以人脸识别为例, 需借助摄像头等设备采集清晰的人脸图像; 语音识别则依赖麦克风获取准确的语音信号。进入预处理阶段, 通过滤波等手段去除数据中的噪声干扰, 并对数据格式进行标准化处理, 让数据契合后续处理要求。其次, 运用特定算法精准提取数据关键特征, 人脸识别时, 会着重提取面部轮廓、五官间距等极具代表性的特征。随后, 利用机器学习或深度学习算法对模型展开训练, 让模型充分学习特征与目标之间的内在关联, 不断优化各项参数以提高识别精度。最后, 将训练成熟的模型应用到实际场景, 输入新数据进行识别并输出结果, 实现身份判断、物体识别等功能^[1]。

1.3 技术发展趋势展望

在科技迅猛发展的浪潮下, 智能识别技术正朝着更为多元和深入的方向大步迈进。未来, 其在算法领域的创新步伐将持续加速, 新型深度学习模型会如雨后春笋般不断涌现, 针对光线昏暗、人员遮挡等复杂场景, 进一步提升识别准确率与效率。在多模态融合层面, 不再局限于单一维度识别, 而是有机融合图像、语音、文本等多模态信息, 以实现更为全面、精准的身份判定。例如: 在智能安防领域, 将人脸识别与语音识别深度结合, 进一步加强身份确认, 降低误判风险。随着物联网的蓬勃发展, 边缘计算与智能识别技术的融合会更加紧密, 大量数据于边缘设备本地处理, 有效减少传输延迟, 满足实时性需求, 如智能摄像头可在本地实时分析画面, 及时捕捉异常情况。此外, 鉴于数据安全的重要性日益凸显, 对数据隐私和安全的重视程度会不断提升, 进而促使加密、匿名化等保

护技术持续发展,为智能识别技术的广泛应用筑牢安全防线。

2 校园一卡通系统架构与功能

2.1 校园一卡通系统整体架构解析

校园一卡通系统架构是支撑其高效运作的关键。从技术层面看,采用分层架构设计,最底层为数据层,涵盖用户基本信息、消费记录、门禁权限等各类数据,存储于数据库中,保障数据安全与持久化。中间层是业务逻辑层,负责处理各类业务规则,如消费扣款逻辑、身份认证流程等。最上层是应用层,直接面向用户,以APP、刷卡终端、自助服务机等形式呈现。从部署架构来讲,基于校园网络,在校园数据中心集中部署核心服务器,确保系统稳定运行;同时,借助分布式缓存和负载均衡技术,应对高并发访问,提高系统响应速度^[2]。

2.2 基础功能模块详解

校园一卡通系统凭借其丰富且实用的基础功能,深度融入校园生活的方方面面。身份识别模块作为核心,利用卡片内置芯片或二维码,在门禁、考勤、图书借阅等关键场景中,迅速与后台数据库进行信息比对,精准确认师生身份,有力保障校园安全与管理秩序。消费支付模块功能强大,广泛覆盖食堂用餐、校内购物、水电费缴纳等各类消费场景,依托先进的支付技术,实时完成金额扣除与数据记录。并且,该模块支持与银行卡关联,让充值变得轻松便捷,一键操作即可完成资金注入。信息查询模块则为用户贴心服务,提供账户余额、消费明细、门禁记录等详尽信息的查询服务,用户只需通过专属APP或校园内的自助查询机,就能随时掌握一卡通使用情况,方便核对与管理,极大地提升校园生活的便捷性。

2.3 与校园信息系统的融合要点

校园一卡通系统与校园信息系统融合是提升校园管理效率的重要方向。与教务系统融合,可实现学生选课、考试签到等功能,学生用一卡通即可完成操作,简化流程,同时教务系统能实时获取学生考勤等信息,便于教学管理。与图书馆系统融合,一卡通充当借书证,实现图书借阅、归还、超期提醒等功能,还可将借阅信息同步至一卡通系统,方便学生统一查看。在融合过程中,要统一数据标准,确保不同系统间数据格式、编码一致;还要构建安全可靠的数据交互接口,采用加密传输、身份验证等技术,保障数据传输安全,避免信息泄露。

3 智能识别技术与校园一卡通系统的融合

3.1 融合的必要性及优势

在以往的校园管理体系中,传统校园一卡通系统主要依赖卡片识别方式,然而这种方式存在诸多弊端。卡片容易出现丢失情况,给师生带来不便与财产风险,一旦被盗用,更是会造成安全隐患,并且其识别速度相对迟缓,准确性也大打折扣,难以满足校园日益增长的管理需求。因此,智能识别技术与校园一卡通系统的融合势在必行^[3]。融合之后,师生无需再时刻携带实体卡,通过刷脸、指纹识别等方式就能让他们在门禁、消费等场景中快速通行,极大地提升了身份认证的便捷性。从安全性角度出发,智能识别技术依托的生物特征具有唯一性且难以伪造,能有效降低身份冒用风险,为校园安全保驾护航。在管理效率方面,系统可自动采集、分析各类数据,为校园管理决策提供有力的数据支持,例如通过深度剖析学生消费数据,精准把握学生饮食偏好,从而优化食堂菜品供应,提升校园服务质量。

3.2 融合实现的技术路径

在智能识别技术与校园一卡通系统融合的过程中,硬件与软件层面的优化升级必不可少。在硬件方面,迫切需要全面升级校园一卡通系统终端设备。例如:在门禁、消费机以及图书馆借阅设备上,都要集成先进的人脸识别、指纹识别模块,从硬件基础上确保设备能精准、高效地采集生物特征数据。软件层面同样关键,要全力开发适配智能识别技术的算法接口,以此实现与一卡通系统后台数据的顺畅对接与实时交互。同时,搭建统一身份认证平台意义重大。通过整合校园各类身份信息,保障智能识别与原有卡片识别在系统中的良好兼容性,让用户在不同场景下能自由、灵活地选择认证方式,并且确保数据实时同步,彻底避免信息不一致问题,为校园一卡通系统的高效运行筑牢根基^[4]。

3.3 融合过程中的关键问题及解决策略

在智能识别技术与各类系统的融合过程中,隐私保护无疑是最为关键的问题之一。智能识别技术在运作时会采集大量个人生物特征数据,如指纹、人脸信息等,这些数据一旦泄露,将对个人隐私和安全造成难以估量的严重后果。为有效应对此问题,可采用先进的加密存储技术,在数据采集后立即加密处理,并且在访问时设置多重授权验证,层层把关。同时,严格规范数据使用流程,清晰界定数据使用权限与范围,从源头杜绝数据滥用。此外,技术稳定性也不容忽视,

环境因素如光线强弱、温度高低等，都可能影响智能识别的准确率。通过持续优化算法，提升其对复杂环境的适应性；并部署备用识别设备，当主设备识别异常时能自动无缝切换，全方位保障系统正常运行。

4 智能识别技术在校园一卡通系统中的应用效果评估与潜在风险应对

4.1 应用效果的多维度评估指标

从识别效率来看，考量智能识别技术在校园一卡通系统中身份验证的速度，如在上下课、就餐等人员流动高峰期，系统完成一次身份识别所需的平均时间，时间越短，表明能更快地服务师生，减少排队等待现象，提升校园运转效率。在准确性上，关注识别准确率，统计识别错误的次数占总识别次数的比例，较低的错误率可确保系统判断无误，防止非授权人员进入校园或造成消费、权限管理的混乱。此外，系统稳定性也至关重要，统计一定时间段内系统出现卡顿、崩溃等异常情况的次数，以此衡量系统能否持续稳定运行，为师生提供不间断的服务。

4.2 可能面临的潜在风险分析

在隐私安全层面，智能识别技术在校园一卡通系统的应用中，涉及海量师生个人生物特征数据，这些数据包含指纹、人脸、虹膜等敏感信息。一旦在数据存储环节的加密算法强度不足，或者传输时网络防护存在漏洞，数据就极有可能泄露，这不仅会严重侵犯师生隐私权，更会引发师生对校园信息安全的信任危机，导致对一卡通系统的抵触^[5]。

技术故障风险同样不容小觑，人脸识别在光线昏暗、强光直射、面部有口罩帽子等遮挡时，指纹识别在手指受伤、有污渍、蜕皮等情况下，都会极大地影响识别准确性，甚至出现无法识别的状况，致使系统无法正常使用，给师生校园生活带来诸多不便^[6]。

此外，系统兼容性问题也频频出现。智能识别技术与校园一卡通系统原有模块、校园其他信息系统对接时，常因接口标准不同、数据格式不一致、通信协议不匹配等，造成数据交互受阻、功能难以正常实现，严重阻碍校园信息化建设进程。

4.3 风险应对措施与保障机制

在智能识别技术与校园一卡通系统融合过程中，应对各类风险十分关键。针对隐私安全风险，采用先进且高强度的加密算法，从数据采集伊始便对数据进行加密处理，确保在传输、存储、调用等各个环节的数据安全性，让数据泄露风险降至最低。同时，明确

数据使用权限，仅授权专业、经过严格审查的特定人员访问关键数据，并建立起严格的数据访问审计制度，详尽记录所有数据操作细节，以便在出现异常时精准追溯。面对技术故障，提前建立完备的应急预案，例如设置传统刷卡、密码验证等备用识别方式，以便在主识别技术因环境干扰或设备故障失效时能迅速切换，不影响正常使用^[7]。定期对智能识别设备进行全面维护和校准，及时跟进并更新技术版本，不断提高识别性能。为解决兼容性问题，在系统开发阶段就开展充分的兼容性测试，提前与校园内各相关系统深入沟通协调，统一数据标准和接口规范，全方位保障系统间的无缝对接。

5 结束语

智能识别技术与校园一卡通系统的融合，是校园信息化发展的重要突破。从硬件升级到软件优化，从多维度应用到风险防控，这一融合全面革新了校园管理模式。在身份识别上，其便捷性与安全性远超传统卡片识别；在消费支付、信息查询等功能上，也带来了更流畅、高效的体验。尽管在数据隐私保护、技术稳定性方面仍面临挑战，但随着加密技术、算法优化不断推进，这些问题正逐步得到解决。未来，随着科技持续进步，智能识别技术有望在校园实现更深度的应用，与教学、科研等场景紧密结合，为校园智慧化建设注入源源不断的动力，助力校园管理朝着更智能、更人性化的方向发展。

参考文献：

- [1] 张则青,黄莹,耿孝敏,等.视觉识别技术在板材智能分拣系统中的应用研究[J].现代信息科技,2025,09(02):139-144.
- [2] 杜成菲.智能语音识别技术在车机交互系统中的应用[J].电视技术,2024,48(04):217-219.
- [3] 郭南.生物识别技术在高校校园门禁系统中的应用[J].电子产品世界,2024,31(11):8-10.
- [4] 崔伟欣.智能语音识别技术在金融交易系统中的应用研究[J].电声技术,2024,48(12):70-72.
- [5] 张亮.人工智能技术在计算机网络安全中的应用[J].计算机应用文摘,2025,41(02):82-84.
- [6] 温俊元,陈威.计算机人工智能识别技术在教育管理系统中的应用研究[J].中文科技期刊数据库(全文版)教育科学,2024(10):73-76.
- [7] 范远芳.人脸识别技术在高校中的研究与应用[J].信息记录材料,2025,26(03):114-116.