项目结题验收单

专家验收表

项目名称	高校图书馆人脸识别海量数据传输存储技术探讨		
主持人	马可	职务/职称	馆员
所在单位	江南大学图书馆		
专家意见	专家组认真审阅了课题研究报告，形成如下鉴定意见： 人脸识别技术应用于图书馆门禁系统、身份验证等是智慧图书馆发展的必然。为保障读者海量信息传输存贮的安全性，课题组对高校图书馆人脸识别海量数据传输存储技术进行研究，选题新颖。 课题探索加密过程内存消耗低、加密速度快、密钥强度高的 AES 算法在人脸识别中的应用，探索去中心化分布式数据存储技术解决集中式存储方式中数据安全、可靠性和可扩展性问题，以防止数据被篡改或者破坏，论证较为科学合理。 提出高校图书馆人脸识别海量数据传输存储系统架构设计，包括采集模块、传输模块、存储模块、应用模块，探索AES 加密算法在数据传输加密、数据存储加密中的应用、元数据的分布式数据存储技术方法的应用，具有一定的应用参考价值。 专家组认为，该课题研究完成了预定的研究目标，同意结题。建议课题组后续开展更加深入的理论与应用研究，获得更多研究成果。 （如需要可增加页数）		
专家签字			
职务/职称			

项目编号：2023035

CALIS 全国农学文献信息中心研究项目

结题报告

项目名称：高校图书馆人脸识别海量数据传输存储技术探讨

项目关键词：人脸识别、数据传输、分布式存储

项目单位（盖章）：

通信地址：（详细地址含邮编）江苏省无锡市蠡湖大道 1800 号江南大学图书馆

邮编 214122

项目主持人：马　可

联系电话：17766475261

电子邮件：1759541970@qq.com

提交日期：2024 年 5 月 10 日

高校图书馆人脸识别海量数据传输存储技术探讨

关键词：人脸识别，数据传输，分布式存储

1、研究的背景、目的及意义

1.1 研究背景

人脸识别是基于人的脸部特征信息进行身份识别的一种生物特征识别技术，经历了基于几何特征的人脸识别算法、基于模板的人脸识别算法和基于深度神经网络的人脸识别算法 3 个历程[1]。人脸识别技术因其唯一性、便捷性、无接触性、并发性等特点，在高校身份验证、出入门禁、考勤签到、消费支付等方面得到广泛应用，有效改善了高校管理效率和服务质量，提升了信息化建设水平[2]。

在智慧图书馆建设的大背景下，以人脸识别为代表的人工智能技术已逐渐成为我国图书馆的信息化研究热点。2017 年，浙江理工大学图书馆应用人脸识别技术实现读者入馆验证及自助借阅服务，受到广大读者的青睐，获得了良好的使用效果[3]。国内其他的高校图书馆，也陆续推出了人脸识别服务项目，这使得该项技术的应用性更是进一步的广泛起来。

1.2 研究目的及意义

人脸识别技术凭借精确性、高效性、便捷性等优点加速推进了智慧图书馆的建设与发展。特别是前几年新冠疫情在全球范围内肆虐情况下，人脸识别因其不需与终端设备接触、避免病毒或细菌接触传播的优点，实际应用价值得以体现出来。

随着人脸识别技术的日渐完善，各高校图书馆陆续把人脸识别应用到图书馆管理范畴中。自 2017 年开始，哈尔滨工业大学、华中科技大学、海南大学、上海交通大学、中国计量大学、天津大学、西安外国语大学等高校的图书馆都已在保留原有传统的校园卡门禁系统的基础上增设了刷脸进出馆方式，相对于刷卡进馆方式，人脸识别门禁的接受度更快，且能提高读者的进馆效率，这对图书馆后续向智慧图书馆转型具有重要意义[4]。

然而，在享受人脸识别技术带给高校图书馆各种便捷管理的同时，也要严密防范人脸识别随之带来的一系列风险隐患，特别是运用中需要加强海量信息传输存储技术的支撑，因为海量读者个人信息隐私保护显得尤为重要，须严防泄密；同时，集中式存储系统已无法适应海量数据的存储需求。因此，需要设计一种去中心化的广域分布式数据储存与共享模型，以保证区块信息具有一致性和数据的严格完整性，防止关键信息被恶意节点篡改。所以，在智能化时代，如何保障读者海量信息安全的情况下，最大限度满足各高校图书馆人脸识别相

关数据传输存储的需求，解决海量、多类型数据传输存储问题以及提高数据的共享性，是亟待解决的一大难题。

2、研究思路、方法及具体内容

2.1 主要研究思路：

为更好地保障读者海量信息传输存贮的安全性，需对高校图书馆人脸识别海量数据传输存储技术进行研究，根据现代信息技术成果为依托，打造基于物理层数据传输安全模块和去中心化分布式数据存储及共享模块的平台。项目负责人将探讨高校图书馆人脸识别海量数据传输存储技术的应用与实践。首先，对现有的海量数据传输存储技术进行梳理和分析，以便为后续的研究提供理论基础。然后，研究高校图书馆人脸识别海量数据的传输存储技术，以期为我国高校图书馆的智能化发展提供有益的参考。

2.2 研究方法

在研究方法方面，我们在广泛收集资料的基础上，将采用文献分析法、案例分析法和逻辑推理法相结合的方式进行研究。文献分析法主要用于收集和整理相关领域的文献资料，以便对海量数据传输存储技术有一个全面的了解；案例分析法主要用于分析高校图书馆人脸识别海量数据传输存储技术的具体应用情况，以便为后续研究提供实践参考；逻辑推理法主要根据现有的理论基础对高校图书馆人脸识别海量数据传输存储技术进行研究整合，以推断出该领域的发展与前景。

2.3 研究的具体内容

2.3.1 AES 加密算法简介

高校图书馆作为现代图书馆的重要组成部分，其人脸识别技术在提高图书馆管理效率、保障读者隐私安全等方面具有重要作用。高级加密标准 AES 算法是一种广泛应用于数据加密领域的安全算法，以其强大的加密能力和高效的数据处理能力而备受推崇。AES（Advanced Encryption Standard）是一种带有可变块长和可变密钥长度的迭代分组加密算法。该算法的分组大小为 128 位，密钥长度有三种，分别是 128、192 和 256 位[5]。根据密钥长度的不同，相应的加密轮数分别为 10、12、14。AES 算法因其加密过程内存消耗低、加密速度快、密钥强度高而成为当前流行的国际加密标准。

在数据传输过程中，采用 AES 加密算法可以有效保障人脸识别数据的隐私性。具体而言，在数据传输过程中，可以将人脸识别数据通过 AES 算法进行加密，依托秘钥将密文形式的数据传输，从而有效防止数据在传输过程中被窃取与篡改[6,7]。

在数据存储过程中，同样可以利用 AES 加密算法进行加密。由于人脸识别数据的敏感性，采用 AES 加密算法对数据进行加密可以有效保护数据的安全。

此外，AES 加密算法的可变块长和可变密钥长度特点，可以针对不同场景和需求进行灵活设置，提高数据加密的安全性和实用性。

为了提高 AES 加密算法的性能，还需探讨其在并行计算环境下的应用。并行计算作为一种高效计算技术，可以有效提高加密算法的运行速度。采用 AES 加密算法进行人脸识别数据的加密传输与存储，可以有效保障数据的隐私性和安全性，为高校图书馆人脸识别技术的发展提供有益参考。

AES 算法加密过程首先将 128 位的明文数据划分为 16Bit，然后将其依次复制到 4×n 阶状态矩阵上。矩阵的行数为 4，列数 n 根据不同的密钥长度分别为 4、6、8。AES 每轮加密循环均包含 4 个阶段：字节替代变换、行位移变换、列混淆变换和轮密钥加变换。

字节替代变换阶段，采用 8 位 S 盒替换表将矩阵中每个字节 $a_{i,j}$ 替换成另一个字节 $S(a_{i,j})$。S 盒的构造是算法安全的关键，结合了有限域 $GF(2^8)$上乘法逆元及可逆的仿射变换矩阵共同建构而成。

行位移变换阶段，将变换后的状态矩阵每一行周期性地位移某偏移量。第 1、2、3 和 4 行分别循环左移 0、1、2、3 位。行位移变换避免了列线性独立，在这种情况下，AES 简化成四个独立的分组密码。

列混淆变换阶段，状态矩阵的每一列的四个字节通过线性变换互相结合后即为有限域 GF (2^8)中的多项式系数，接着将此多项式和一个固定的多项式 a(x) 进行模多项式 $m(x)=x^2+1$ 的乘法运算。几轮行位移变换和列混淆变换后，所有的输出均与所有的输入相关，密码系统扩散性更强。

轮密钥加变换阶段，在加密循环时，初始密钥通过固定变换得到每一轮的子密钥。该步骤就是将状态矩阵与子密钥矩阵的对应字节做异或运算。轮密钥加变换非常简单，却影响着状态中的每一位。

AES 加密算法因其强大的加密能力和高效的数据处理能力，通过合理利用，可有效保护海量数据的传输存储安全，以确保高校图书馆的人脸识别技术能够健康、安全地运行。

2.3.2 去中心化分布式存储技术概述

随着海量数据传输和存储的需求日益增加，传统的集中式存储方式已经无法满足需求，因此去中心化分布式存储技术应运而生[8]。去中心化分布式存储技术是一种新型的数据存储方式，可以有效地解决集中式存储方式中数据安全、可靠性和可扩展性问题。去中心化分布式存储技术的基本原理是将数据分散存储在多个节点上，每个节点都可以存储一部分数据[9]。在数据传输时，数据会被切分成多个块，每个块都会经过多个节点的验证，只有所有节点都确认无误后，数据才会被写入节点。这种方式可以有效地防止数据被篡改或者破坏。同时，由于数据是分散存储在多个节点上，因此即使某个节点出现问题，也不会影响整个系统的正常运行。

去中心化分布式存储技术可以有效地解决数据安全问题，还可以实现数据的可靠性和可扩展性。由于数据是分散存储在多个节点上，不会因某个节点出现问题而影响整个系统的正常运行，同时，还可以随时添加或者删除节点，实现了数据的可靠性和可扩展性。

高校图书馆采用去中心化分布式存储技术可解决人脸识别海量数据传输和存储的问题。

2.3.3 高校图书馆人脸识别海量数据传输存储系统架构设计

为了更好地实现人脸识别技术在高校图书馆的应用，需要设计一个高效、稳定、安全的人脸识别海量数据传输存储系统架构。

该系统架构应包括以下几个模块：

一. 采集模块

采集模块是整个系统的入口，其主要作用是将人脸识别系统采集到的人脸信息进行采集、处理和存储。采集模块应包括摄像头、人脸识别算法、人脸特征提取算法、人脸图像压缩和传输等功能。其中，摄像头用于捕捉人脸图像，人脸识别算法用于识别人脸，人脸特征提取算法用于提取人脸特征，人脸图像压缩和传输功能则将人脸图像压缩后进行传输和存储[10]。

二. 传输模块

传输模块是整个系统的传输部分，其主要作用是将采集模块采集到的人脸信息进行传输。传输模块应包括人脸信息压缩和传输算法、人脸信息加密和传输算法、人脸信息传输协议和传输网络等功能。其中，人脸信息压缩和传输算法用于将人脸信息压缩后进行传输，人脸信息加密和传输算法用于保证人脸信息的传输安全，人脸信息传输协议和传输网络用于保证人脸信息的传输效率和可靠性。

三. 存储模块

存储模块是整个系统的存储部分，其主要作用是将采集模块采集到的人脸信息进行存储。存储模块应包括人脸信息存储算法、人脸信息存储协议和存储网络等功能。其中，人脸信息存储算法用于将人脸信息进行存储，人脸信息存储协议用于保证人脸信息的存储安全，人脸信息存储网络用于保证人脸信息的存储效率和可靠性。

四. 应用模块

应用模块是整个系统的应用部分，其主要作用是将存储模块存储的人脸信息进行处理和应用。应用模块应包括人脸信息处理算法、人脸信息分析算法、人脸信息查询算法和应用界面等功能。其中，人脸信息处理算法用于对存储模

块存储的人脸信息进行处理，人脸信息分析算法用于分析人脸信息，人脸信息查询算法用于查询人脸信息，应用界面用于用户操作。

2.3.4 AES 加密算法在系统中的实现与应用

高校图书馆是一个重要的学术机构，需要处理大量的人脸识别数据。这些数据需要进行传输和存储，以确保安全和隐私。AES 加密算法是一种非常安全的加密算法，可以在系统中对人脸识别数据进行加密。

AES 加密算法是一种对称密钥加密算法，它使用相同的密钥对数据进行加密和解密[11, 12]。AES 加密算法的密钥长度可以长达 256 位，这使得它具有非常高的安全性。AES 加密算法还可以实现密钥交换，使得密钥在传输过程中更加安全。因此，在高校图书馆人脸识别海量数据传输存储技术中，AES 加密算法是一种非常优秀的加密算法。

在高校图书馆人脸识别海量数据传输存储技术中，AES 加密算法的应用主要包括以下几个方面：

一. 数据传输加密

在高校图书馆人脸识别海量数据传输过程中，AES 加密算法可以对传输数据进行加密，确保数据在传输过程中的安全性。例如，当人脸识别设备采集到人脸信息后，可以将这些信息通过网络传输到服务器上。在这个过程中，AES 加密算法可以依托秘钥对传输数据进行加密，防止数据在传输过程中被窃取或篡改[6]。

二. 数据存储加密

在高校图书馆人脸识别海量数据存储过程中，AES 加密算法可以对存储数据进行加密，确保数据的隐私和安全[13]。当人脸识别设备采集到人脸信息后，可以将这些信息存储在服务器上的数据库中。在此过程中，AES 加密算法可以对存储数据进行加密，防止海量海量数据被非法访问或窃取。

AES 加密算法在高校图书馆人脸识别海量数据传输存储技术中的应用可以有效地保护人脸识别数据的安全性和隐私性。

2.3.5 基于元数据的分布式数据存储技术方法

为了保证海量数据的存储效率和安全性，基于元数据的分布式数据存储技术方法成为了高校图书馆人脸识别海量数据传输存储技术探讨的重要内容。

基于元数据的分布式数据存储技术方法是一种将数据存储在多个节点上的方法，每个节点都存储着不同的数据，并且节点之间通过元数据进行连接[14]。元数据是描述数据属性和关系的一种信息，包括数据的名称、类型、大小、位置、创建时间、修改时间等信息。

基于元数据的分布式数据存储技术方法具有以下优点：

一. 可扩展性好：基于元数据的分布式数据存储技术方法可以轻松地扩展存储容量，只需要添加更多的节点即可。

二. 数据安全性高：每个节点都存储着不同的数据,并且节点之间通过元数据进行连接，可以有效地防止数据泄露。

三. 数据管理方便：基于元数据的分布式数据存储技术方法可以通过元数据进行数据的查询、修改、删除等操作，方便数据管理。

高校图书馆需要存储大量的人脸识别数据，这些数据不仅包括人脸图像本身，还包括人脸识别结果、人脸特征等信息。基于元数据的分布式数据存储技术方法可以将这些数据存储在多个节点上，并且每个节点都可以通过元数据查询到其他节点的数据，从而提高数据的存储效率和安全性[14]。

3、结论、建议与展望

3.1 结论

在当前人脸识别技术逐渐普及的背景下，高校图书馆如何有效地进行海量数据的传输、存储保护显得尤为重要。

高校图书馆人脸识别海量数据传输存储技术探讨，是一项涉及人脸识别技术、海量数据传输技术和海量数据分布式存储技术的综合性研究，需要综合考虑人脸识别算法的准确性、数据压缩和加密的效率和安全性等因素。

高校图书馆人脸识别数据的传输和存储还面临着一系列挑战，如数据量巨大、数据安全问题、算法准确性问题等。为了解决这些问题，基于 AES 加密算法、分布式存储等技术，提出了一种高效、安全、准确的数据传输和存储方案。

总之，高校图书馆人脸识别数据的传输和存储是一个涉及多个学科的综合性问题，需要综合考虑人脸识别技术、数据传输技术和数据存储技术等多个方面的因素。

3.2 建议与展望

针对高校图书馆人脸识别海量数据的传输，特提出以下几点建议。首先，应该采用加密技术进行数据传输，以保证数据的机密性；其次，应采用高效的数据压缩技术，以降低数据传输过程中的延迟和带宽占用；然后，还可以考虑采用边缘计算技术，将数据处理和分析的工作量分散到数据采集设备上，以降低中心服务器的负载压力。

对于高校图书馆人脸识别海量数据的存储，提出以下几点建议。首先，应采用分布式存储技术，以保证数据的可靠性和安全性；其次，应采用高效的数

据管理技术，以降低数据存储和管理的工作量；然后，还可以考虑采用数据备份和恢复技术，以保证数据的安全性和完整性。

高校图书馆人脸识别海量数据的传输与分布式存储保护是一个复杂且重要的问题。对其研究需要从多方面入手，并加强跨学科的融合与创新。项目负责人针对现有技术提出了一些建议和展望，希望能够为高校图书馆的数据管理提供一些参考。随着技术的不断发展和变化，相信高校图书馆人脸识别海量数据传输存储技术也将不断更新和完善。因此，我们需要持续关注和研究这一领域，以适应未来的发展需求。

4、项目成果

（1）形成研究报告;（2）进一步完善研究内容，争取形成学术期刊论文。

5、参考文献

[1] 刁胜先, 姜音. 论人脸识别信息的法律保护-兼评我国“人脸识别第一案”[J].重庆科技学院学报(社会科学版), 2022, 277(6): 19-31.

[2] 李东风.人脸识别技术在智慧校园中的安全应用研究[J].现代信息科技, 2023,7(24):152-156.

[3] 李宇.图书馆人脸识别技术应用研究[J].图书馆工作与研究,2023,332(10):57-62.

[4] 耿雅玲, 袁申, 徐向阳. 人脸识别技术在高校智慧图书馆建设中的应用研究[J].电脑知识与技术, 2023, 19(17):30-32+35.

[5] 何信一, 何磊, 白韦娟. 基于优化 S 盒的 AES 算法的北斗短报文加密方案[J].网络安全技术与应用, 2023, 276(12):29-32.

[6] 宋阳,果福明.计算机网络中数据加密技术应用[J].集成电路应用, 2023, 40(11):100-101.

[7] 贺家兴, 贾湘琳. 基于智慧校园的职业本科大数据治理中的信息安全应对策略[J].信息与电脑(理论版), 2023, 35(23):231-233+241.

[8] 魏若愚.分布式存储系统中故障节点修复及数据更新方法研究[D].桂林电子科技大学,2022.

[9] 申高.基于云计算的分布式存储技术分析[J].集成电路应用,2023,40(08):38-40

[10]程雨芊.高校图书馆人脸识别技术应用的调查与研究-以山东大学(威海)为例[J].内蒙古科技与经济,2022,496(06):125-127.

[11]范海峰.数据加密技术在计算机网络安全中的应用[J].信息记录材料,2023,24(06):58-60.

[12]邱丹青.大数据背景下信息通信网络安全管理措施探讨[J].中国新通信,2023,25(23):10-12.

[13]翟羽佳.智慧图书馆环境下的个性化适应性服务研究[J].科技资讯,2023,21(23):239-241.

[14]郝琨,信俊昌,黄达,王国仁.去中心化的分布式存储模型[J].计算机工程与应用,2017,53(24):1-7+22.