2025 年　第 3 期

江苏省计算机学会

COMMUNICATIONS OF THE JSCS

——攻克低空智联网关键技术，服务低空经济国家战略

以科技为盾，守护软件系统安全

——在安全测评技术研究中砥砺奋进创新

江苏省计算机学会常务理事单位

南京工业大学计算机与信息工程学院（人工智能学院）简介

计算机与信息工程学院（人工智能学院）前身源于南京化工学院 1994 年成立的自动化与计算机系，2001 年原南京化工大学与南京建筑工程学院合并组建了新的南京工业大学，2002 年由原两校的相关专业成立了信息科学与工程学院，2008 年更名为电子与信息工程学院，2015 年因学校学部制改革更名为计算机科学与技术学院，2023 年更名为计算机与信息工程学院（人工智能学院）。学院现有计算机科学与技术系、电子信息工程系、通信工程系、智能科学与技术系、基础教学部和实验教学中心。2025 年入选江苏省省级人工智能学院。

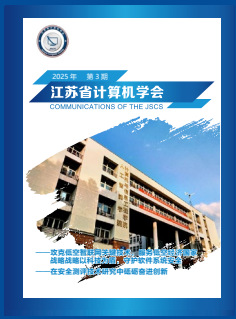
学院拥有一支结构合理、以中青年教师为主的高水平师资队伍。现有教职工 124，其中专任教师 93。教职工中，具有高级职称 61 人，具有博士学位的 62 人，拥有省部级高层次人才 10 余人。

学院现有计算机科学与技术、电子信息工程、通信工程、人工智能四个本科专业，其中计算机科学与技术专业、电子信息工程专业为国家级一流本科专业建设点，通信工程专业为省级一流本科专业建设点，人工智能专业为 2020 年新申办专业。计算机科学与技术、电子信息工程专业通过了教育部专业认证。目前，各专业本科生 2500 余人，研究生 340 余人。学院始终坚持立德树人根本任务，紧紧围绕学校建设国内一流国际知名创业型大学建设目标，强化教育教学管理，积极探索创新、创业和创造型人才培养模式，努力培养会认知、能做事、善合作、谋发展的复合型高素质人才。近年来，学院学生在“挑战杯”中国大学生创业计划大赛、中国大学生计算机设计大赛、全国大学生电子设计大赛、全国大学生嵌入式芯片与系统设计竞赛、ACM 国际大学生程序设计竞赛、全国大学生数学竞赛等重大赛事中获得 400 余项全国级奖项。

学院现有计算机科学与技术一级学科硕士点（学术型）、智能科学与技术一级交叉学科硕士点（学术型）和电子信息类硕士点（专业型），共建“智能制造技术与工程”、“低空技术与工程”交叉学科博士点。学科方向主要为网络与云计算、智能感知与信息处理、数据科学与智能计算、生物信息与医疗大数据、软件理论与方法和人工智能等。建有网络与云计算技术研究所、计算机应用研究所、人工智能研究所、信号处理与智能传感研究所和数字城市与智能建筑研究所等。学院坚持理论研究和实际应用并重，坚持与学校化工、生物、安全等优势学科的交叉研究和协同创新，坚持产学研结合，与华为公司、江苏省未来网络创新研究院等建立了深度的合作关系。近几年，承担了国家自然科学基金、江苏省重点研发计划、江苏省自然科学基金等国家和省部级项目 40 余项，科研到款 8000 多万，授权发明专利 100 余项。一些研究成果发表在本学科的高水平期刊或会议上，获得江苏省科学技术奖一等奖等科学技术奖 10 余项。

江苏省计算机学会通讯

COMMUNICATIONS OF THE JSCS



地　址：中国江苏省南京市栖霞区仙林大道 163 号

邮　编：210023

电　话：025-89680909

邮　箱：jscs@njn.edu.cn

编译中国芯 · 铸匠神威梦——面向国产申威编译器的编译原理教学改革与实践

——江南大学方伟教授

一、成果简介

编译原理是计算机类专业的核心课，主要讲授编译各阶段主要原理及编译器设计的实现方法。针对“学生针对国产编译器实现原理的系统思维难建立”、“学生的编译实践与国产 CPU 平台难适配”、“学生面向自主指令集的理论分析与工程实践难协同”等教学痛点，提出“六联三通”、“双师双平台”、“三堂三真” 的创新方法。通过与课程共建的龙头信创企业国家超算无锡中心、无锡先进技术研究院产教协同，建成双网四库教学资源 200 余项，提出基于数字一体化平台实时反馈的逐级递进全流程编译实验教学新体系，依托省级产教融合重点基地等 4 个教研平台和 30 余个校企实践基地，围绕信创生态全面激发学生学习实践动力，有效提升学生系统思维和编译器设计能力。

立德树人成效突出，学生参与全国大学生计算机系统能力大赛编译系统设计赛（华为毕昇杯）获全国总决赛二等奖、学生设计专用 SoC 获“挑战杯”铜奖，与合作单位共同指导的本科生大创团队对申威处理器进行代码优化，在全球公认的 SPEC CPU 评测中综合提升比 6.17%，有效提升了申威处理器的运算性能。

近三年，编译原理获批省级一流课程，课程团队主持省部级教改 5 项，出版省级高等学校重点教材 1 部，获校级教学成果奖 3 项，获校级讲课比赛三等奖 1 项；向申威生态企业输送毕业生中十余名成为骨干；形成的“产教协同、理实共驱”创新教学方案在全国编译课程教学研讨会、编译课程虚拟教研室等进行报告分享；实践案例获开源创新大赛编译原理教学实践赛二等奖。本专业已正式成立“申威创新班”，并于 2024 年 9 月开始招生；申威创新班的创建是学校深化教育改革的尝试，也是推进产教融合的里程碑。

二、成果主要解决的教学问题及解决教学问题的方法

2.1 主要教学问题

当前信创产业紧缺计算机基础型人才，对编译器研发、国产化适配、处理器性能优化提出了迫切的人才需求。然而，传统校内教学仅学通用编译算法，编译实验主要运行在 Intel 等国外 CPU 平台架构上，缺乏针对国产自主指令集的编译优化。对应以下三个痛点问题：

（1）学生针对国产编译器实现原理的系统思维难建立

（2）学生的编译实践与国产 CPU 平台难适配

（3）学生面向自主指令集的理论分析与工程实践难协同

2.2 解决方法

方伟提出“六联三通”、“双师双平台”、“三堂三真”的创新方法，赋能中国芯，培养信创人才。

2.2.1 面向国产申威编译器三维育人

（1）校企“六联”全周期协同育人

方伟提出校企六联全周期协同育人。六联指校企“联合制定大纲、设计课程内容、开展现场教学、实践指导、实践评价、以及指导编译器适配与优化项目”。强化“需求引领”，推进“资源整合”，加强“协同联动”。

（2）校企“三通”深化产业知识内容

知识内容方面，提出横向连通、纵向贯通、全面融通的校企三通深化产业知识内容。围绕编译器从源程序到目标程序的翻译过程，将编译原理的主要理论知识进行横向连通；结合申威编译器的产业知识，在每个章节，将通用编译器和国产申威编译器的知识点实现纵向贯通；从而全面建立学生基于通用编译理论的申威编译器实现的系统思维，做到全面融通。达到“通用融合专用，自主并且可控”。

图 1 “六联三通”产教融合育人模式示意图

（3）信创战略融入课程思政

此外，结合合作企业的信创特点，将信创战略融入课程思政，学生通过芯片“卡脖子”背景、接触国产申威编译器的研发历史、熟悉申威处理器信创生态，从而接触到信创产业对编译人才的急迫需求，激发学生的工匠精神、科技报国信念、责任担当和家国情怀。激励学生“学好中国芯，编译好中国话”。

2.2.2 面向申威编译实践重塑实验体系

图 2 校企协同的“双师双平台”编译实践教学架构示意图

（1）双师双平台构建逐级递进实验模式

编译实验复杂度高、编译优化又依托目标 CPU 平台。因此，依托产教融合，通过双师双平台实现了面向国产 CPU 平台的实践资源创新。首先，重塑实验内容体系，构建工具使用、算法实践、通用编译器实现到申威编译器优化的逐级递进实验模式，符合学生学习和实践认知规律。通用编译部分，由校内教师主导、依托自建通用数字一体化平台开展实践；申威编译优化部分，由企业导师主导、依托申威云平台开展实践。

（2）数字一体化赋能校企实践指导

实践平台结合大模型技术，提供 AI 课程助教，实时回答学生提问。实践题库为每道编程题预置了多组测试样例，支持编程实践自动评测，学生实时获得正确性反馈。合作企业将前沿工程问题以探索任务的形式发布在论坛，学生可选择感兴趣的问题在申威云平台进行探索和实践。目前已共建 35 个实践任务库和 51 个论坛互动主题。

2.2.3 校企优势互补建立联动机制

（1）三堂三真以产促教

教学理念方面，将传统课堂教学延伸到校内实践第二课堂、企业实践第三课堂，形成三堂联动。校内实践课堂通过校企合作设计申威编译创新课题，激发学生创新意识。企业实践课堂为有能力有兴趣的学生提供申威编译器的实践和研究课题，提供挑战度。再将学生实践中解决的真实问题引入课堂教学案例，面向全体学生讲解，以产促教，提升教学高阶性。

通过产教融合，以产业的真实任务、真实场景、真实考核方式来充分培养学生的自主实践能力。例如和先研院围绕申威处理器中特有的乘法加法优化技术设计了大创课题，发布真实任务。学生通过大创研究积累了申威编译优化经验，在企业真实场景中，学生通过实践发现，申威指令集中的乘加指令能有效提升目标代码的执行速度。通过企业导师的真实考核，发现这一优化，确实能提升申威处理器运行复杂数学运算的性能，因此我们将乘加优化这一案例补充到了教学案例库中，企业将这一方法引入到了产业技术库。通过三堂三真，形成了产教融合闭环。

图 3 “三堂三真”校企协同育人模式

（2）产学研深度融合共建教研实践平台

为了形成可持续产教融合，与国家超算、先研院共建江苏省先进计算与控制产教融合重点基地、创新实践基地、江苏省工信厅人工智能信创实验室等教研实践平台，从企业师资、国产硬件资源、实践课题等各方面为学生参与产业的课程学习和实践提有力保障。

2.2.4 校企协同改革教学评价体系

课程评价方面，在各过程性环节融入企业导师考核，特别在编译实践环节，有 20 分的配额给企业导师，充分结合企业工程师在编译优化方面的工程经验，对学生开展的申威编译器优化实践进行性能达标、实践答辩、优化性能 pk 进行量化考评。性能达标和实践答辩主要围绕完成以往案例来考核，这属于被动需求；而优化性能 PK 是开放性实践题目，由学生在产业导师指导下开展创新探索，并在数字化平台上提交编译优化结果进行 PK，直接由性能决定成绩，实现编译优化技术创新的主动出击，为国产编译优化提供新的思路。

三、成果的创新点

通过学校和企业优势互补，与国家超算无锡中心、无锡先进技术研究院围绕计算机专业核心课编译原理开展产教融合教学改革和创新实践，形成教学成果创新点如下：

（1）内容创新方面

从育人模式、知识内容、课程思政三个维度面向国产申威编译器三维育人，提出“六联三通”创新方法。校企从教学大纲制定环节到编译器实践项目指导等六个环节联合设计教学内容，校企“六联”全周期协同育人。将编译原理主要理论围绕编译过程横向联通、将编译器通用知识与申威编译器产业知识进行纵向贯通，从而建立起全面融通的计算机系统思维。此外，将国产编译相关的案例引入课程思政，激发学生的工匠精神、科技报国信念、责任担当和家国情怀。

（2）资源创新方面

校企合作重塑实践内容体系，提出“双师双平台”创新方法，实现面向国产 CPU 平台的实践资源创新。校内教师的优势在于通用编译技术的理论教学、合作企业国家超算是申威处理器落地应用单位，有丰富的申威工程应用经验、先研院则是申威编译器研发单位，在申威编译优化方面积累了丰富的前沿技术，能提供真实实践任务并进行实践考核。建成的申威云平台由三台本地部署的申威高性能服务器和 70 台申威 PC 一体机构成，能够支持在国产申威处理器上开展编译实践；依托希冀自建的数字一体化平台则能够支持通用编译实践的在线评测、在线答疑、实时反馈，通过双师双平台保障学生随时、随地学。

（3）理念创新方面

拓宽教学空间、拓展教学形式，提出“三堂三真，以产促教”。将传统课堂教学延伸到校内实践第二课堂、企业实践第三课堂，形成三堂联动。以产业的真实任务、真实场景、真实考核方式来充分培养学生的自主实践能力，形成产教融合闭环。

四、成果的推广应用效果

通过开展产教融合的教学创新，我校编译原理课获评第二批江苏省一流课程、江苏省教创赛产教融合赛道特等奖。教学成果推广应用效果包括：

（1）学生创新实践能力不断提高

在本科生参与的企业实践课题中，针对申威处理器进行代码优化，在全球公认的 CPU 性能评测中，部分课题提升比达到2%~6%，学生的实践创新能力获得信创企业认可，近三年有 15 人入职申威生态企业开展国产编译器研发。

（2）师生合作开发开源教学案例

授课教师与研究生、本科生合作开发的编译实践案例获中国计算机学会开源创新大赛编译原理教学实践赛二等奖，包含 5 个实践实验部署在头歌平台，提供公开访问。

（3）会议论坛分享教育教学理念

课程团队积极参与经验交流，通过全国编译课程教学研讨会、编译课程虚拟教研室研讨会、省信创人才论坛等分享课程产教融合经验，方伟组织举办了 CCF 自主可控算力与人工智能大模型发展大会，推广分享自主可控理念。

图 4 自主可控算力与人工智能大模型发展大会

图 5 成立计算机科学与技术申威卓越创新班

（4）成立申威卓越创新班辐射全国招生

在编译原理课程的产教融合示范下，我校计算机专业专门成立了申威卓越创新班，辐射全国招生。为我国信创产业培养紧缺的计算机人才，从用别人的计算机，到造自己的计算机。

教育部解读数字化赋能教师发展行动：六大举措全面提升教师数字素养

来源：教育部
http://www.moe.gov.cn/jyb_xwfb/s271/202507/t20250707_1196786.html

近日，教育部办公厅印发《关于组织实施数字化赋能教师发展行动的通知》（以下简称《通知》）。教育部教师工作司负责人就《通知》相关问题回答了记者提问。

1. 问：《通知》出台有什么背景和意义？

党中央、国务院一直高度重视教育数字化工作，党的二十大报告首次将“推进教育数字化”写进了党代会的报告。2023 年，习近平总书记在中共中央政治局第五次集体学习时指出：“教育数字化是我国开辟教育发展新赛道和塑造教育发展新优势的重要突破口”。实施数字化赋能教师发展行动主要基于以下三方面考虑。

一是落实国家战略。国家教育数字化战略行动于 2022 年启动并深入推进。2024 年，中共中央、国务院印发的《教育强国建设规划纲要（2024—2035 年）》将教育数字化作为重要内容进行了部署。教师是推进教育数字化的关键，教师的数字素养水平深刻影响着教育数字化战略的成色。

二是服务教师发展。数字化的深入推进为教育带来了前所未有的机遇，也对教师教育教学带来新的挑战。如何更好适应数字化条件下的教学，获得更优质的数字化教育教学工具、资源支持，促进教育教学改革和个人发展，是教师的迫切需求。

三是推进实践探索。近年来，我部陆续开展了中小学教师信息技术应用能力提升工程、人工智能助推教师队伍建设试点、国家智慧教育公共服务平台教师研修、《教师数字素养》标准制定等一系列工作，为推进教师发展数字化打下良好基础，也迫切需要相关举措的整合、升级优化。

实施数字化赋能教师发展行动，是深入贯彻习近平总书记关于教育的重要论述、人工智能发展的重要指示精神，落实国家教育数字化战略行动，推进新时代高水平教师队伍建设的重要举措，对夯实教育强国人才培养根基具有深远意义。

2. 问：《通知》的总体思路和主要内容是什么？

落实国家教育数字化战略的总体部署，按照“应用为王、服务至上、简洁高效、安全运行”的基本原则，以提高教师数字素养为关键，以数字技术、人工智能技术融合创新应用为牵引，扩大优质资源和服务供给，开辟教师发展新赛道、塑造教师发展新优势。

具体通过六大行动推进数字赋能。

一是聚焦重点环节，实施教师数字素养提升行动。完善教师数字素养标准体系，修订教师专业标准、师范生教师职业能力标准。出台教师数字素养提升指南，多种方式推进教师数字素养培训全覆盖。持续开展测评，支持有条件的地区汇聚教师发展大数据，探索数据驱动的教师数字素养提升路径。

二是突出应用驱动，实施数字赋能教育教学改革行动。支持地方、学校结合实际建设智慧校园、升级教师智能研训室和智慧教育中心，助力教师开展数字化教学、数字化学习。协同企业、科研院所研发教师智能助手，推动教师教学理念、方法和模式转型。加大宣传推广力度，推广数字应用先进经验。

三是推动培养转型，实施教师发展模式数字转型行动。推进师范生培养、教师研训的数字化转型，推进教师的数字化学习。完善教师自主学习机制，利用人工智能和大数据技术精准推送学习资源，建立教师终身学习积分应用机制。强化名师领学领研领教，实施“数字支教”活动，促进优质资源均衡共享。

四是强化资源支撑，实施教师发展数字资源供给行动。组织力量开发重点领域的精品资源，建立资源建设长效机制和资源使用激励机制。创新教师发展资源形态，组织编写人工智能教师读本，开发多模态数字教材、学科知识图谱、沉浸式师训系统等新型资源，提高资源的智能性和实用性。

五是推动治理升级，实施教师发展数字治理行动。依托国家智慧教育公共服务平台，建强教师发展综合服务管理功能，建立教师教育大模型，优化教师教育专业设置，强化师范专业的规范管理和动态调整。完善教师资格制度，将数字素养纳入中小学教师资格考试的考察范畴，高校教师资格认定中要将数字素养作为教育教学能力的重要方面进行考察，推动数据支撑的教师评价改革。强化数字化安全与规范，研制教师生成式人工智能应用指引。

六是深化国际交流，实施数字教育教师国际合作行动。用好世界数字教育大会等高水平对话交流平台，建好全球教师发展学院平台，开展教师人工智能培训、数字化协同教研和“人机共育”等方面的国际合作，积极参与相关国际标准制定，贡献中国数字教育的智慧和力量。

3. 问：如何抓好《通知》贯彻落实？

组织实施数字化赋能教师发展行动，是回应人工智能时代教师关心关切和期盼的关键之举，更是顺应时代发展趋势和办好人民满意的教育的应有之义。教育部将加强文件解读，做好动员部署和实施过程中的业务指导等工作，压实各方责任，确保《通知》贯彻落实。

一是在组织机制上，加强政府统筹力度，建立分区域专家指导机制，强化实施过程中的针对性研究、指导、跟踪和督促。推动各地各校将数字化赋能教师发展纳入教育数字化和教师队伍建设的重要议事日程，建立多部门协同工作机制，制定专门工作方案，确保各项任务目标如期完成。

二是在示范引领上，推进“百区千校万师”建设，推出百个数字化赋能教师发展特色区，千所数字化赋能教师特色校，万名数字化发展名师，加强对地方和学校的引领，强化典型经验的总结凝炼和典型案例的宣传推广，发挥示范带动作用，进一步释放数字技术对教育高质量发展的倍增效应。

三是在投入保障上，持续健全数字化赋能教师发展的保障体系，提升保障能力。指导、推动地方和高校优化支出结构，创新投入机制，拓展经费来源，推动财政投入、技术研发、产业开发、学校应用的协同联动，强化社会多元参与，提高经费使用效益，促进《通知》高效、高质量落实。

教育部语言文字信息管理司负责人就《教育部 国家语委 中央网信办关于加强数字中文建设 推进语言文字信息化发展的意见》答记者问

来源：教育部：
http://www.moe.gov.cn/jyb_xwfb/s271/202503/t20250331_1185550.html

近日，教育部、国家语委、中央网信办印发了《关于加强数字中文建设 推进语言文字信息化发展的意见》（以下简称《意见》）。教育部语言文字信息管理司负责人就《意见》相关问题回答了记者提问。

一、请介绍《意见》出台的背景。

答：党的十八大以来，习近平总书记深刻把握信息化发展大势，提出“没有信息化就没有现代化”“教育数字化是我国开辟教育发展新赛道和塑造教育发展新优势的重要突破口”等重大论断，深刻阐明了信息化在社会主义现代化建设全局中的重要地位和作用。习近平总书记高度重视语言文字工作，指出“语言是人类交流思想的工具、传承文明的载体、增进理解的桥梁。中文承载着中华民族数千年的文明智慧，是中国贡献给世界的重要公共文化产品。”《教育强国建设规划纲要（2024—2035 年）》就语言文字工作作出新部署。语言文字信息化是经济社会信息化的重要组成部分，是数字中国建设的基础性工作，是把握新一轮科技革命和产业变革深入发展机遇、促进语言文字事业改革发展的重要举措。

进入新时代，语言文字信息化在健全规章制度、完善标准体系、促进创新应用、建设优质资源等方面取得长足进步，有力服务了教育、科技、文化等各领域的发展。近年来，数字中国建设加速演进，以自然语言处理技术为基础的生成式人工智能创新发展态势和竞争格局加速形成，但语言文字信息化还存在政策引导力度不足、基础要素配置薄弱、协同创新发挥不够、技术赋能有待提升等短板弱项，并且中文在全球数字空间、网络空间以及生成式人工智能等关键应用场景中内容占比低、影响力受限，与我国的国际地位不符。为加快推进以信息化促进语言文字事业高质量发展，以数字化赋能语言文字更好服务全面建设社会主义现代化国家，教育部、国家语委、中央网信办在实地调研、部门会商和专家论证的基础上研制了《意见》，明确要深入推进信息技术与语言文字深度融合，以加强数字中文建设为重点全面推进语言文字信息化发展，全方位释放语言文字的数据要素价值、全环节发挥语言文字资源优势、全领域赋能经济社会发展。

二、请介绍《意见》的主要内容。

答：《意见》主要包括 5 个部分。

一是明确语言文字信息化总体要求。《意见》以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大和二十届二中、三中全会精神，贯彻落实全国教育大会精神，按照“坚持需求导向、支撑战略”“坚持融合发展、突破创新”“坚持突出重点、协同推进”三个基本原则，明确了 2027 年国家数字中文建设行动取得重要成效、2035 年语言文字信息化整体水平位居世界前列的目标。

二是推进语言文字信息化加快发展。明确语言文字信息化对语言文字事业全面深化改革、实现高质量发展和服务经济社会发展的重大意义和深远影响。部署数字中文建设，着力推进中文数字化与数据中文化、创新应用与规范安全、新型中文服务体系构建与语言文字治理体系完善。

三是加强语言文字信息化体系建设。提出完善规范标准体系、健全资源服务体系、建强人才培养体系、构建协同创新体系、强化安全保障体系等语言文字信息化体系建设的 5 项主要任务，对建设语言文字信息化基础支撑能力作出系统部署。

四是提升语言文字信息化服务水平。强调以“实”的任务带动战线广泛参与，明确实施数字化示范项目，打造数字化引领品牌，特别是实施数字中文服务教育发展、助力科技创新、赋能文化传承、推动产业升级、促进社会进步等 5 项行动，既是加强数字中文建设的工作抓手，也是推进语言文字信息化发展的关键任务。

五是切实强化语言文字信息化实施。明确工作机制，提出加强组织领导、条件保障、宣传引导等措施。

三、《意见》有哪些主要创新点？

答：《意见》是贯彻落实全国教育大会精神和《教育强国建设规划纲要（2024—2035 年）》的关键举措，《意见》明确“融”的核心导向，推进语言文字与信息技术深度融合；突出“新”的任务体系，一体推进语言文字信息化发展体系建设，实施数字中文专项行动；细化“实”的工作举措，聚焦具体目标打造数字化引领品牌，实施 30 余项数字化示范项目。

一是全面谋划数字中文建设。数字中文建设是服务数字中国建设的重要任务和全面推进语言文字信息化发展的突出重点。加强数字中文建设，要推进语言文字与信息技术深度融合，全方位释放语言文字数据要素价值，着力推进中文数字化和数据中文化、创新应用与规范安全、新型中文服务体系构建与语言文字治理体系完善，既要实现规范、有效、批量地将中文资源信息转化为智能数据，也要促进中文数据的规模生产、优质集成、规范治理和复用增效，提升中文在全球数字空间、网络空间以及生成式人工智能等关键场景中的使用占比和价值引领作用。

二是系统构建语言文字信息化体系。在新时代以来语言文字信息化工作成果的基础上，《意见》首次凝练语言文字信息化建设体系的概念，明确以规范标准体系为基础、资源服务体系为重点、人才培养体系为支撑、协同创新体系为方法、安全保障体系为底线，推进语言文字信息化发展。特别提出，创新应用自然语言处理、大语言模型、多模态信息处理、知识图谱、语料加工等五项前沿技术，重点服务大语言模型等人工智能技术创新应用“制高点”、夯实国家关键语料基础设施“新基建”。

三是积极推动赋能经济社会发展全局。充分发挥语言文字作为国家重要教育资源、科技资源、文化资源、经济资源、安全资源和战略资源的功能作用，实施数字中文服务教育、科技、文化、产业、社会等重点领域的五项专项行动，助力中文发挥立德树人的基础作用、推进科技创新的支撑作用、传承中华文化的根脉作用、赋能产业升级的关键作用和服务社会需求的民生作用。

四、《意见》的工作导向是什么？

答：今年是贯彻全国教育大会精神、落实《教育强国建设规划纲要（2024—2035 年）》的关键之年，也是“十四五”收官和“十五五”谋划之年，更是面向十年建成教育强国全面布局、高位推进之年。语言文字信息化作为服务教育强国建设的重要工作，要展望十年、谋划五年、立足三年，把握赋能全局高度、加快试点先行进度、激发协同创新力度，在落实重点任务上下大功夫。

一是坚持国家战略需求牵引。加快建设国家语言文字大数据中心、国家关键语料库和国家战略语言资源信息库，为国家语言能力建设提供数字化支撑。二是深化语言文字与信息技术融合。探索自然语言处理、大语言模型等技术创新和应用，推动科研成果落地见效。持续支持面向重点行业、战略区域和关键学科等的垂直领域大语言模型建设与应用。三是充分发挥语言文字资源功能。通过组织开发、征集遴选、集成汇聚等方式，鼓励并支持各地各校分类建设基础性、应用性、战略性、特色性语言资源。四是有效释放语言文字数据要素价值。支持语言文字信息技术新产品、新职业和新业态发展，培育基于中文数据的新型语言产业。五是坚持全局赋能经济社会。要通过科教融汇、产教融合、校企合作、校际合作等方式，构建全局化、精准化、特色化的语言服务体系，以数字中文建设“新作为”赋能经济社会高质量发展。

五、请谈谈《意见》如何贯彻落实。

答：健全政府主导、部门协同、社会参与、共建共享的语言文字信息化推进机制。一是加强组织管理。教育部、国家语委、中央网信办会同语委委员单位统筹推进全国语言文字信息化工作，加强工作监督检查，推进工作落实见效。充分发挥语委委员单位、各级各类学校、研究机构和社会组织等多方作用，指导各单位将语言文字信息化纳入工作规划，因地制宜制定专项方案。特别是支持有条件地区建设数字中文建设试验区。二是加强条件保障。要加大统筹力度，优化支出结构，加强语言文字信息化工作经费保障。健全多渠道投入机制，鼓励社会力量参与，形成共建共享机制。三是加强宣传引导。及时总结工作中的好经验好做法，加大宣传推广力度，征集并发布数字中文建设案例，营造多部门参与、多方面支持、多层级联动的良好氛围。

学会动态

“江苏省师范类高校人工智能通识教育教学改革与创新研讨会”在江苏师范大学召开

6 月 29 日，“江苏省师范类高校人工智能通识教育教学改革与创新研讨会”在江苏师范大学召开。来自南京大学、北京师范大学、南京师范大学等多所高校的 70 余位教育专家、人工智能专业学科带头人及一线教师齐聚，共同为师范类高校人工智能通识教育教学改革与创新寻求新思路、探索新路径。

面向 Android 应用的跨设备自动适应技术研究

——2024 年江苏省计算机学会优秀博士论文

作者：李聪

单位：南京大学

指导老师：许畅、蒋炎岩

论文摘要

安卓（Android）碎片化是一把双刃剑，深度定制安卓系统和设备模型的多样性，纵然为消费者提供了更多选择，促进了安卓生态的繁荣发展，但也给安卓开发者带来了沉重的负担。为提升用户体验，本文发现安卓开发者一般遵循应用开发流程，采取以下三个措施确保应用能正确适配各种流行的安卓设备、避免适配问题（如兼容性问题和逻辑错误等）：编写设备适配代码或重新设计开发应用；不运行应用，利用静态检测工具（如 LINT），提前检测适配问题；运行应用程序，利用测试用例动态检查运行时适配问题。

本文关注跨设备自动适应技术，一类协助安卓应用正确适配各种安卓设备的自动化技术。实践中，这类技术能够利用程序合成、静态或动态程序分析等方法，自动合成适配代码、检测适配问题，以降低开发和测试成本，带来更好的开发体验。虽然已有许多工作关注这类技术，但本文发现，尚未有工作对何为“正确适配不同的安卓设备”进行诠释，也未有工作对如何辅助开发者自动化该过程进行系统性理解，以探讨和解决其面临的问题、挑战和机遇。

为此，本文提出设备适应性（device adaptability）的概念和面向 Android 应用的跨设备自动适应技术框架。该框架综合已有工作，根据开发者适配应用的三个措施，将对设备适应性及其自动化的研究系统地分为三个问题：跨设备应用的自动合成、跨设备应用的静态测试和跨设备测试的自动合成。进一步地，本文提出一组面向安卓应用的跨设备自动适应技术，分别用于解决这三个问题所面临的技术挑战，包含如下三方面的研究工作：

针对跨设备应用开发难的问题，即，技术框架中的第一个问题“跨设备应用的自动合成”，提出了一种面向新兴设备的应用自动合成技术：基于程序合成（基于样例编程和约束求解）的应用自动合成技术 Jigsaw，在以智能手表这种新兴设备对实验对象的实验评估中，成功为 16 个现实中存在的、流行的开源安卓应用，自动合成了可安装、界面正确且功能可用的智能手表适配版，弥补了已有工作在该问题上的研究缺失。此外，对于合成后界面、功能不正确的应用，开发者只需付出极低的代价便可修复 Jigsaw 合成的应用程序代码，进而完成应用的合成。

针对兼容性问题静态检测精度低的问题，即，技术框架中的第二个问题“跨设备应用的静态测试”，提出了一种跨设备兼容性问题检测的静态测试技术：基于调用路径敏感型静态分析的 ELEGANT，能有效检测 22 个流行安卓应用中存在的、因设备适配引发的兼容性问题，相比已有工作，ELEGANT 显著降低了这类问题检测的误报率，降

低幅度达 70%，解决了已有工作面临的技术挑战，即，受限的静态分析和第三方库带来的误报。

针对跨设备测试用例普遍缺乏的问题，即，技术框架中的第三个问题“跨设备测试的自动合成”，提出了一个简单实用、面向真实场景的测试用例跨设备自动合成框架：基于响应式和空间局部性设计的 Rx，在为三台广泛使用的安卓设备和 21 个现实中存在的、流行的开源安卓应用，完成 603 个测试用例合成任务时，在仅付出 0.2 个额外事件和 7.31% 运行时搜索开销的前提下，成功完成了其中 498 个，成功率达 82.6%，填充了已有工作的研究空白。此外，Rx 还在知名软件中找到了前所未知的缺陷。

此外，本文也关注适配后的应用能否在底层运行时中可靠运行。具体包括，编译上述应用的编译器工具链中是否存在可靠性问题，及运行上述应用的运行时中是否存在可靠性问题：

针对编译工具链中的可靠性问题，提出了一种基于大模型的模糊测试变异算子自动生成技术：借助大语言模型的 MetaMut，以每个变异算子仅 0.5 美元的成本，为模糊测试工具 CFuzz 自动生成了 118 个变异算子，帮助其在编译安卓应用所使用的编译器 Clang 中找到 81 个可靠性问题，并在世界最广泛使用的编译器之一 GCC 中找到 50 个可靠性问题，值得一提的是，其中 129 个可靠性问题已被相应开发者确认或修复。

针对应用运行时中的可靠性问题，提出了一种对优化、退优化敏感的编程语言虚拟机测试技术：基于编译空间探索的 Artemis，借助多样化的即时编译代码结构，在安卓应用运行时 Android Runtime 中找到 16 个可靠性问题，也在世界最广泛使用的 Java 运行时 HotSpot 和 OpenJ9 中找到 69 个可靠性问题，值得一提的是，其中 53 个可靠性问题被相应开发者确认或修复。

专家推荐语

移动终端应用是数字经济的重要载体，其生态基础已被苹果和 Android 两大阵营瓜分。我国终端操作系统正蓬勃发展，其生态建设任务艰巨。李聪博士的学位论文通过软件自动化技术拓展移动终端应用生态发展，做出了多项代表性工作，包括：

移动应用自动向新兴小屏幕设备的迁移技术，通过版本空间代数实现实现已有终端应用向智能手表迁移的“零代码”自动开发。

移动应用响应式交互模式的自动识别和应用方法，在小 / 大屏终端手机和平板界面具备迥然差异的情况下，实现事件序列的自动迁移，并在世界范围内首次实现了 Microsoft Word、Microsoft Outlook、YouTube 等重量级应用的支持。

上述系统性研究工作产生了系列国际领先的研究成果，发表 ICSE'22、ESEC/FSE'22 等旗舰会议论文和多项发明专利，形成了国家自然科学基金重点项目在多变环境中软件自主适应和可靠运行能力方面的核心技术，受到国内领先厂商公司的关注并已形成积极合作。

李聪博士在该方面的工作也聚焦于安卓运行时系统的可靠性问题：

他提出了世界上首个对优化、退优化敏感的编程语言虚拟机测试技术，先后得到世界应用最广泛编程语言虚拟机团队 Eclipse/OpenJ9、Oracle/OpenJDK 的邮件致谢，并受到 Oracle 公司 Java 平台技术小组首席架构师 Mark Reinhold 关注。该工作发表于 SOSP'23，并获得会议成立 56 年以来中国大陆首个最佳论文奖。

他也在积极探索大语言模型在运行时支撑系统可靠性问题中的应用，提出了世界上首个基于大模型的模糊测试

变异算子自动生成技术，基于该技术生成的变异算子及其配套工具，成功在世界应用最广泛的编译器 GCC/LLVM 中找到上百个缺陷。该工作发表于 ASPLOS'24。

论文看点

2011 年，Android（简称安卓）一跃成为世界上最流行的移动操作系统，并于近些年飞速发展。据统计，截至 2023 年，安卓移动操作系统已占据超过 70% 的市场份额，且 Google Play 移动应用程序商店——安卓官方、最大的移动应用程序商店——中已上架超过 260 万个安卓移动应用程序。伴随着安卓移动操作系统和安卓移动应用程序的蓬勃发展，安卓移动设备的种类亦越来越多：超过 20 家安卓移动设备制造厂商（如三星、小米和华为）已累计向全球发布了超过 24,000 种型号不一的安卓移动设备，包括但不限于智能手机、智能平板和智能手表，并且这个数字仍在快速增长。

安卓碎片化是一把双刃剑，深度定制安卓系统和设备模型的多样性，纵然为消费者提供了更多选择，促进了安卓生态的繁荣发展，但也给安卓开发者带来了沉重的负担。为提升用户体验，本文发现安卓开发者一般遵循应用开发流程，采取以下三个措施确保应用能正确适配各种流行的安卓设备、避免适配问题（如兼容性问题和逻辑错误等）：编写设备适配代码或重新设计开发应用；不运行应用，利用静态检测工具（如 LINT），提前检测适配问题；运行应用程序，利用测试用例动态检查运行时适配问题。

安卓应用

本文重点关注跨设备自动适应技术，一类协助安卓应用正确适配各种安卓设备的自动化技术。实践中，这类技术能够利用程序合成、静态或动态程序分析等方法，自动合成适配代码、检测适配问题，以降低开发和测试成本，带来更好的开发体验。虽然已有许多工作关注这类技术，但本文发现，尚未有工作对何为“正确适配不同的安卓设备”进行诠释，也未有工作对如何辅助开发者自动化该过程进行系统性理解，以探讨和解决其面临的问题、挑战和机遇。

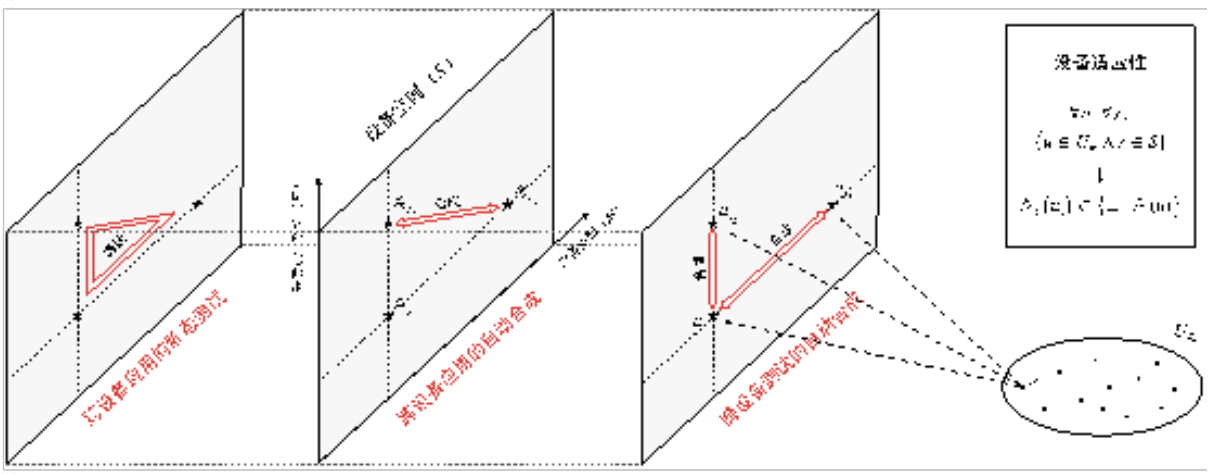


图 1. 面向 Android 应用的跨设备自动适应技术框架

为此，本文提出设备适应性（device adaptability）的概念和面向 Android 应用的跨设备自动适应技术框架（图 1）。该框架综合已有工作，根据开发者适配应用的三个措施，将对设备适应性及其自动化的研究系统地分为三个问题：跨设备应用的自动合成、跨设备应用的静态测试和跨设备测试的自动合成。进一步地，本文提出一组面向安卓应用的跨设备自动适应技术，分别用于解决这三个问题所面临的技术挑战，包含如下三方面的研究工作：

跨设备应用开发难 . 针对跨设备应用开发难的问题，即，技术框架中的第一个问题“跨设备应用的自动合成”，提出了一种面向新兴设备的应用自动合成技术 Jigsaw（图 2）。

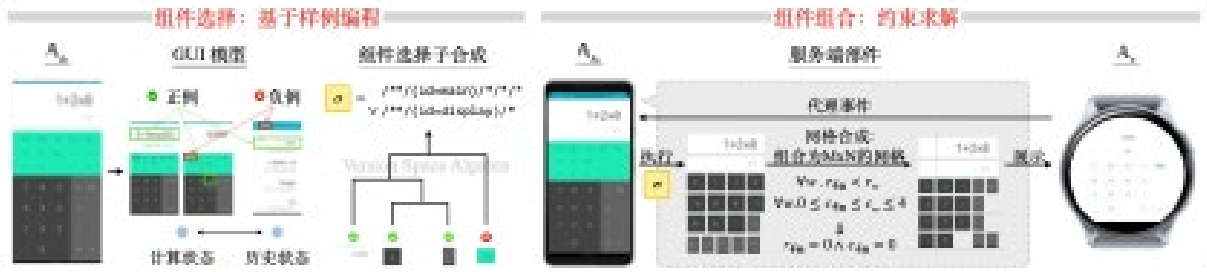


图 2. Jigsaw：面向新兴设备的应用自动合成技术 (ICSE’22)

Jigsaw 以新兴设备为研究对象，以 GUI 合成为主要目标，基于一个安卓应用的某一智能手机适配版本 A1，为其合成新兴设备的适配版本 A2。以智能手表为例，概念上，Jigsaw 为 A1 合成的智能手表应用适配版本 A2 的运行模式类似于一个 A1 安装在智能手表上的远程代理：

· 当 A2 在智能手表上被启动后，它总会与智能手机上正在后台运行的 A1 同步。这种同步会自动迁移 A1 上的一部分组件到智能手表上，并将它们渲染成适合智能手表屏幕尺寸的 GUI 布局。

· 智能手表用户可以与迁移后的组件进行交互。所有用户与智能手表的交互操作（如点击）都会被委托到智能手机上的后台应用 A1，以触发 A1 的 GUI 变化。这种 GUI 变化将再次同步给智能手表以触发 A2 的 GUI 变化。

为此，Jigsaw 将 GUI 合成分为两步：组件选择和组件组合。具体而言，Jigsaw 提出了一种名为组件选择子的领域特定语言（domain-specific language）。基于该语言，Jigsaw 使用基于样例的编程（programming by examples）范式和开发者标记的少量组件进行组件选择子的合成。合成后的组件选择子将被用于标记剩余未被标记的组件，其中，被标记为正的组件会被 Jigsaw 选择。之后，Jigsaw 将为被选择组件创建一组线性的位置约束，并使用约束求解（constraint solving）计算出每个被选择组件适合渲染在智能手表屏幕上的位置坐标，Jigsaw 利用这些坐标完成组件组合，合成适合渲染在智能手表上的 GUI。合成 GUI 后，Jigsaw 会将合成的 GUI 发送给智能手表，作为 A2 的一个 GUI 界面进行渲染。Jigsaw 会实时监控用户与 A2 发生的交互事件。每当监控到新的用户事件，Jigsaw 会将它们即时发送给正在智能手机后台运行的 A1 进行处理，这将触发新一轮的 GUI 合成和事件监控。

基于程序合成（基于样例编程和约束求解）的应用自动合成技术 Jigsaw，在以智能手表这种新兴设备对实验对象的实验评估中，成功为 16 个现实中存在的、流行的开源安卓应用，自动合成了可安装、界面正确且功能可用的智能手表适配版，弥补了已有工作在该问题上的研究缺失。此外，对于合成后界面、功能不正确的应用，开发者只需付出极低的代价便可修复 Jigsaw 合成的应用程序代码，进而完成应用的合成。

兼容性问题静态检测精度低 . 针对兼容性问题静态检测精度低的问题，即，技术框架中的第二个问题“跨设备应用的静态测试”，提出了一种跨设备兼容性问题检测的静态测试技术 ELEGANT。

具体地，ELEGANT 选择了安卓碎片化引发的兼容性问题（FIC 问题）为研究对象，提出了一个二阶段的静态测试方法，这包括一个预处理阶段和一个问题定位阶段。在预处理阶段，ELEGANT 使用白名单增强（whitelist-enhanced）技术或代码混淆不敏感（obfuscation-insensitive）技术来隔离适配应用中的第三方库。在问题定位阶段，ELEGANT 利用一个三步静态检测算法来提高静态分析的精度：

· 第一步，ELEGANT 构建了一个被测应用的调用树来表示某个 FIC 问题的所有潜在调用路径；

· 第二步，ELEGANT 对构建的调用树进行剪枝，以消除假阳性（false positive）的调用路径，提高分析的精度；

· 第三步，ELEGANT 利用调用树生成一份问题报告来提供详细的 FIC 问题信息，以帮助开发者定位 FIC 问题的发生地点。

基于调用路径敏感型静态分析的 ELEGANT，能有效检测 22 个流行安卓应用中存在的、因设备适配引发的兼容性问题，相比已有工作，ELEGANT 显著降低了这类问题检测的误报率，降低幅度达 70%，解决了已有工作面临的技术挑战，即，受限的静态分析和第三方库带来的误报。

图 3. Rx：面向真实场景的测试自动合成技术 (ESEC/FSE’ 22)

跨设备测试用例普遍缺乏 . 针对跨设备测试用例普遍缺乏的问题，即，技术框架中的第三个问题“跨设备测试的自动合成”，提出了一个简单实用、面向真实场景的测试用例跨设备自动合成框架 Rx（图 3）。

具体地，给定能够在适配版本 A1 运行的测试用例 u1 和待合成的适配版本 A2，Rx 可以自动合成能够在 A2 运行的测试用例 u2。传统的方法是使用基于搜索的合成方式，如基于深度优先搜索的方法和基于模型的方法。尽管这些方法理论上具备合成 u2 的可能性，但传统的基于搜索的方法在工业级的大规模安卓应用（如 Microsoft Word）和实际使用场景中的可扩展性有限、性能较差，因为状态空间的搜索需要频繁执行昂贵的回溯操作，甚至应用重启操作。

Rx 框架利用了 LSP 原则（the least surprise principle）来约减搜索空间，加快搜索。在 GUI 设计领域，LSP 原则可以带来如下观察：

· GUI 组件具有空间局部性（spatial locality），功能相关的 GUI 组件在 GUI 界面和 GUI 树中的空间位置是相邻的；

· 跨设备模型的 GUI 变更通常遵从一组有限的响应式模式（responsive patterns），用于指导人类进行高效的 GUI 探索。

据此，Rx 为 u1 中的每个事件 e 一一合成其等价的事件（序列），最后将这些事件序列进行连接（concatenation）。具体地，Rx 框架使用了一个贪心的方法来为每个事件 e 合成其等价事件（序列），这个合成过程无需回溯或应用重

启操作即可完成：

· 执行界面分割将当前界面分为多个界面块，从而使空间上相邻的组件被划分到同一界面块，之后，执行界面块匹配，以确定事件 e 的接收组件所在的界面块；

· 尝试执行一系列可逆的响应式动作，直到 e 的接收组件出现，若所有响应式动作的尝试都失败，则执行该它们的逆动作来抵消副作用。

基于响应式和空间局部性设计的 Rx，在为三台广泛使用的安卓设备和 21 个现实中存在的、流行的开源安卓应用，完成 603 个测试用例合成任务时，在仅付出 0.2 个额外事件和 7.31% 运行时搜索开销的前提下，成功完成了其中 498 个，成功率达 82.6%，填充了已有工作的研究空白。此外，Rx 还在知名软件中找到了前所未知的缺陷。

安卓运行时系统

此外，本文也关注上述适配后的应用能否在底层运行时中可靠运行。具体包括，编译上述应用的编译工具链中是否存在可靠性问题及运行上述应用的运行时中是否存在可靠性问题：

编译工具链的可靠性 . 针对编译工具链的可靠性问题，提出了一个基于大型语言模型的模糊测试变异算子自动生成技术 MetaMut（图 4）。

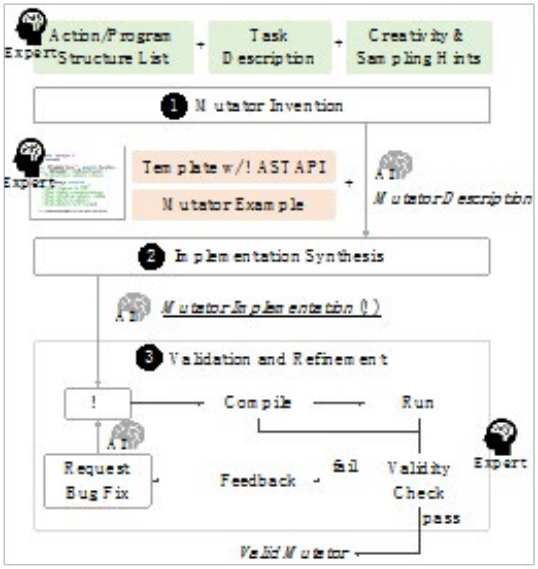


图 4. MetaMut：面向编译工具链的可靠性问题检测 (ASPLOS’24)

具体地，MetaMut 将编译器模糊测试变异算子的生成问题细化为以下三个阶段：：

变异算子构造：MetaMut 引导大模型，通过一系列动作和程序结构，生成用自然语言描述的变异算子。

算子实现合成：在上述自然语言描述和精心设计的变异算子实现模板（包含辅助指令及用于上下文学习的示例）基础上，MetaMut 指导大模型输出可能含有语法、语义错误的变异算子实现代码。

验证和优化：MetaMut 对生成的实现代码进行编译，并利用大模型生成的一组单元测试来检验代码的有效性。对于检测到的语法、语义错误，MetaMut 会将错误信息反馈给大模型，以实现对变异算子实现代码的修正和优化。

遵循这个工作流程，借助大语言模型的 MetaMut，以每个变异算子仅 0.5 美元的成本，为模糊测试工具 CFuzz

自动生成了 118 个变异算子，帮助其在编译安卓应用所使用的编译器 Clang 中找到 81 个可靠性问题，并在世界最广泛使用的编译器之一 GCC 中找到 50 个可靠性问题，值得一提的是，其中 129 个可靠性问题已被相应开发者确认或修复。

应用运行时的可靠性 . 针对运行时中的可靠性问题，本文提出了一个对优化、退优化敏感的编程语言虚拟机测试技术 Artemis（图 5）。

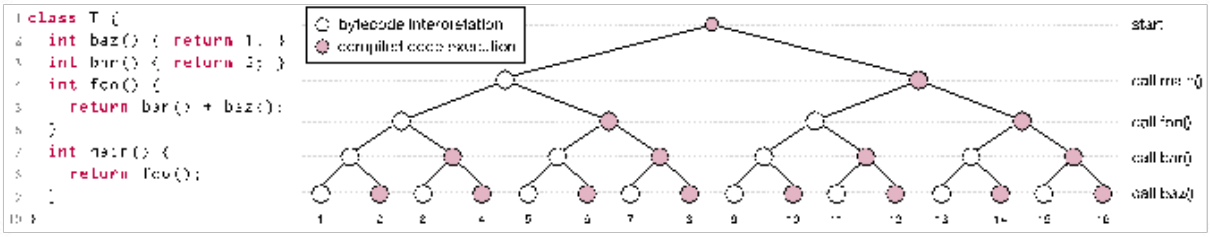


图 5. Artemis：面向安卓运行时的可靠性问题检测 (SOSP ’ 23)

具体地，本文创新地引入了“编译空间”的概念和“编译空间探索”的方法，旨在为安卓运行时虚拟机以及其他现代编程语言虚拟机中的即时（JIT）编译器提供一个系统全面的可靠性验证框架。对于单个程序而言，编译空间表达了一运行时虚拟机系统对其所有可能的 JIT 编译策略，这些策略可以相互验证，确保 JIT 编译的正确性。

然而，编译空间中 JIT 策略的数量庞大（指数级）；在运行时虚拟机系统内实现 JIT 策略的灵活切换，需要庞大的工程投入；不同运行时的策略切换实现也互不兼容。为了在不依赖特定运行时的前提下，以轻量化且系统化的方式快速探索编译空间，本文创造性地对测试程序进行变异处理，引入了与 JIT 紧密相关而语义保持不变的代码结构，从而生成能产生多样化 JIT 编译策略的变异程序，实现对编译空间的间接探索。

基于编译空间探索的 Artemis，借助多样化的 JIT 代码结构，在安卓应用运行时 Android Runtime 中找到 16 个可靠性问题，也在世界最广泛使用的 Java 运行时 HotSpot 和 OpenJ9 中找到 69 个可靠性问题，这些问题中有 53 个被相应开发者确认或修复。特别值得一提的是，所有 Artemis 发现的可靠性问题均涉及运行时系统中处于比较深层的 JIT 编译器，我们甚至收到了来自 HotSpot 和 OpenJ9 开发者的感谢。

本文主要贡献

·提出了设备适应性的概念和定义，进一步提出了面向 Android 应用的跨设备自动适应技术框架，该框架对与“安卓应用正确适配安卓设备”相关的已有工作进行了全面梳理，并尝试对设备适应性及其自动化研究进行系统性理解，以发掘其面临的各类问题、挑战和机遇。

· 针对技术框架中的第一个问题“跨设备应用的自动合成”，即，如何自动地为一些安卓设备生成可适配的应用版本，提出了一种面向新兴设备的应用自动合成技术 Jigsaw。以智能手表为例，Jigsaw 为 16 个现实中存在的、流行的开源安卓应用，自动合成了可安装、界面正确且功能可用的智能手表适配版，弥补了已有工作在该问题上的研究缺失。

· 针对技术框架中的第二个问题“跨设备应用的静态测试”，即，如何在不运行应用的前提下自动地检测应用中因设备适配导致的兼容性问题，提出了一种跨设备兼容性问题检测的静态测试技术 ELEGANT。在 22 个现实中存在的、流行的开源安卓应用中，ELEGANT 的 FIC 问题检测误报率相比已有工作降低了 70%。

· 针对技术框架中的第三个问题“跨设备测试的自动合成”，即，如何自动地为一些设备生成可运行的测试用例集合以方便动态测试，提出了一个简单实用、面向真实场景的测试用例跨设备自动合成框架 Rx。在为三台广泛使用的安卓设备，完成 21 个现实中存在的、流行的开源安卓应用中的 603 个测试用例合成任务时，Rx 的成功率达到 82.6%，填充了已有工作在该场景下的研究空白。

· 针对编译工具链中的可靠性问题，提出了一个基于大模型的模糊测试变异算子自动生成技术 MetaMut。以每个变异算子仅 0.5 美元的成本，MetaMut 为模糊测试工具 CFuzz 自动生成了 118 个变异算子，帮助其在编译安卓应用所使用的编译器 Clang 中找到 81 个可靠性问题。

针对应用运行时中的可靠性问题，提出了一种对优化、退优化敏感的编程语言虚拟机测试技术 Artemis。Artemis 在应用运行时 Android Runtime 中找到 16 个可靠性问题。

作者简介

李聪 (1996-)，男，博士，CCF 专业会员，主要研究领域为安卓应用和运行时系统。

许畅 (1977-)，男，博士，教授，博士生导师，CCF 高级会员，主要研究领域为软件测试与分析、自适应软件系统。

蒋炎岩 (1988-)，男，博士，CCF 专业会员，主要研究领域为操作系统和系统软件

面向复杂场景的行为识别方法研究

——2024 年江苏省计算机学会优秀博士论文

作者：严锐

单位：南京理工大学

指导老师：唐金辉

个人简介

随着信息存储技术和互联网基础设施的不断完善，视频数据成为智能算法研究的主要对象和应用场景。人体行为识别作为视频内容理解的一项基础课题，近年来受到学者们越来越多的关注。该任务的本质是一个分类问题，即识别给定视频中人物所做的行为。现有研究主要关注一些简单场景下的行为识别，例如单人手势、单人行为和（两人）交互行为等。而本文则聚焦于复杂场景下的行为识别，即（多人交互的）群体行为和（人 - 物交互的）组合行为。复杂场景下的行为识别要求算法不仅能够理解单人手势 / 行为、两人间的交互，还需理解多人、多物体之间的复杂依赖关系。面向复杂场景的行为识别技术在智能监控、智能文娱和智能零售等应用中扮演着不可或缺的角色。本文从两个具体问题（群体行为识别和组合行为识别）出发，研究复杂场景下的行为识别问题。群体行为识别的主要挑战在于：场景内人物间交互关系复杂且冗余；场景内细粒度标注成本高昂不利于算法落地。组合行为识别的主要挑战在于：现有的深度视频特征存在严重的表观归纳偏差，致使其在未见的“行为 - 物体”组合样本上的泛化能力明显下降。本文围绕着上述这些问题，展开如下研究：

提出参与度敏感的群体行为识别方法。该算法可从多人场景中筛选出群体行为的关键参与者（即长时行为和瞬时行为），并将其行为特征动态地聚合为群体行为表示。即 1）根据个体行为的运动强度从高到低依次将个体行为特征进行序列关联建模，以使得（高运动强度的）长时行为信息为后续序列建模提供更多的参考；2）基于个体的行为特征相似性和空间位置信息构建群体内上下文交互，以挖掘交互相关的瞬时行为；3）在个体行为特征融合为群体特征过程中，利用可学习的权重挖掘与群体行为语义相关的瞬时行为。

提出基于层级式交叉推理的群体行为识别方法。为了充分挖掘群体场景中的多层级信息（例如肢体局部、个体人物和群体行为）间的潜在时空依赖关系，本文首先设计了一种通用交叉推理块。该推理块可同时捕获 1）每个特征间的空间依赖（例如人物肢体局部之间）和 2）某个特征节点在时序上的依赖（例如某个人的行为随时间的演变）。交叉推理块被应用于捕获肢体局部间或个体人物间的时空依赖关系。该方法无需个体行为标签，依然能够在流行基准数据集上获得不错的表现。这使得该方法更容易应用于人群密集的实时场景（因为无法提供每个人的行为类别标签）。

提出基于交互自适应的弱标注群体行为识别方法。为群体行为识别问题引入了一种新颖的弱标注设置（即仅提供视频级标签）。基于弱标注设置以极低成本采集了一个更大规模更具挑战性的数据集。为缓解弱标注给模型训练带来的不准确监督问题，基于“关键实例往往是彼此密切相关的”这一假设，提出一种交互自适应模块来自动挖掘有效人物和视频帧特征。

提出基于渐进式实例感知的组合行为识别方法。该方法将实例信息（位置和身份）逐步注入到视频特征提取的多个阶段以理解组合行为。具体包括：1）位置感知的表观特征提取：借助视觉实例的运动轨迹，从视频中提取以实例为中心的表观特征；2）身份感知的特征交互：借助于身份信息，在每个实例级特征间进行差异化上下文建模；3）语义感知的实例位置预测：从语义特征中预测实例未来运动轨迹，以促进模型感知实例运动的能力。

提出基于视觉 - 语言联合理解的组合行为识别方法。重新梳理了组合行为识别问题，并提出更实际的组合划分策略和更合理的评估指标。基于此，提出了一个新颖的 `` 少看多想 " 学习框架：1）在视觉表示空间内，基于实例的对视频进行突变来构建反例，以打破物体视觉外观和行为语义间的潜在归纳偏差；2）在语言表示空间内，基于对比学习机制挖掘视觉实例与行为标签间的常识性关联。

专家推荐语

这篇论文选题明确，具有较高的研究价值和实际应用意义，围绕复杂场景中的行为识别问题展开深入探讨。论文通过对国内外研究现状的全面分析，揭示了当前领域的研究成果和存在的挑战，展示出作者对研究方向的全面理解和精准把握。

论文提出了多种创新性的工作，集中解决复杂场景下行为识别的难题：提出了参与度敏感的群体行为识别方法，可有效筛选出关键参与者的行为特征并聚合为更具判别性的群体行为表示；提出了层级式交叉推理群体行为识别方法，可充分挖掘复杂场景内多层级信息间潜在时空依赖关系；提出了交互自适应模块来自适应地挖掘复杂场景内有效人物和视频帧表示，较好地解决了弱标注群体行为识别这一新问题；提出了基于渐进式实例感知的组合行为识别方法，将实例信息逐步融合到行为特征学习的多个阶段中，提升了识别精度；提出了视觉 - 语言联合理解的组合行为识别方法，在视觉表示空间内有效抑制了物体视觉外观和行为语义间的潜在归纳偏差，在语言表示空间内有效挖掘了视觉实例与行为标签之间的常识性联系。

论文结构严谨，逻辑清晰，研究方法与实验设计层次分明，充分体现了作者对相关领域知识的扎实掌握。通过理论推导、算法设计与实验验证，文章内容丰富且逻辑性强，论证有力，展示出良好的学术水平。总的来说，论文研究内容具备较高的创新性，理论与应用结合紧密，体现了作者在行为识别领域的深入思考和系统知识体系。

论文看点

本文从两个任务出发，围绕三个具体挑战，展开面向复杂场景下的行为识别研究。即（多人）群体场景下的群体行为识别和（人 - 物）组合场景下的组合行为识别。群体行为识别的主要挑战在于：如何从冗余多变的可视信息中挖掘关键人物表示，并减少对细粒度监督信息的依赖；组合行为识别的主要挑战在于：如何缓解深度模型在训练阶段对视觉表观信息的归纳偏差，使其能够更好地泛化于未见“行为 - 物体”组合样本上。本文围绕着这些问题，展开如下研究（如图 1.1）：

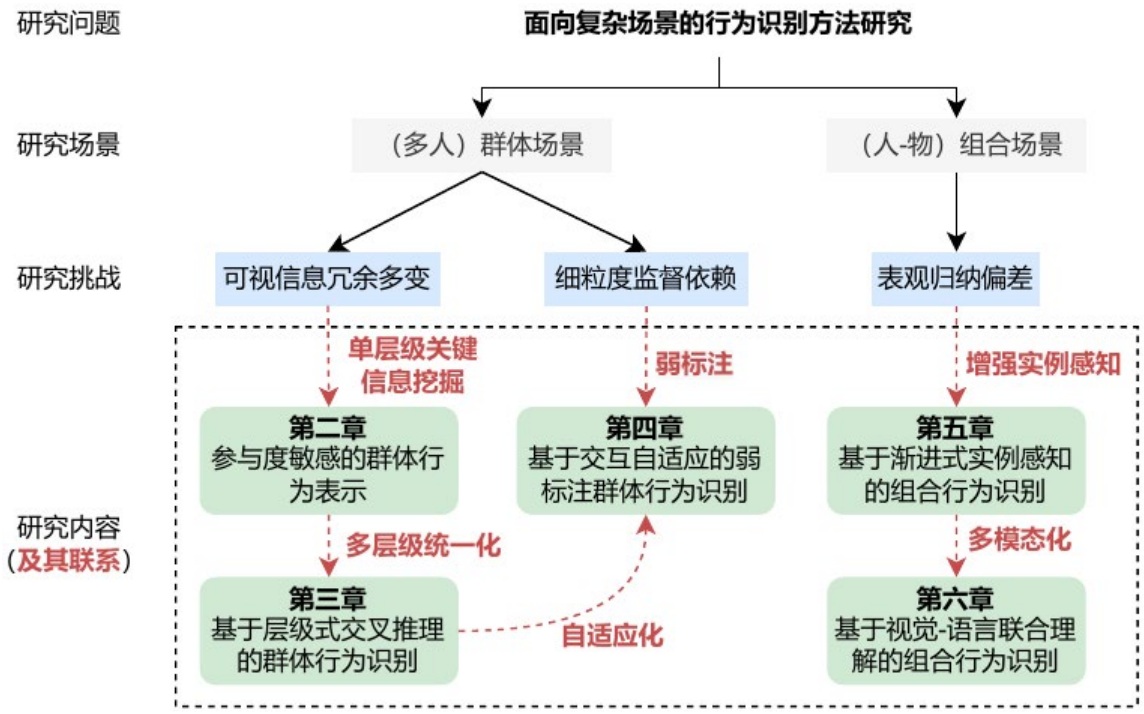


图 1.1 本文研究脉络

成果 1: 参与度敏感的群体行为识别

研究动机：现有的群体行为识别方法大致可以概括为两个关键步骤：1）独立地识别场景中每个人物的行为并提取个体行为特征；2）将若干个体行为特征融合为群体行为特征，并基于此推断出场景对应的群体行为类别。第一步的本质是一个简单的单人行为分类问题，其中基于深度神经网络的方法明显优于非深度方法。在第二步中，现有方法采用简单的池化操作将个体特征汇聚为群体表示，也有方法利用图模型或循环神经网络来探索场景中人物间的深层语义关系。然而，这些方法都基于一种不恰当的假设，即场景内所有人物对群体行为都产生了贡献。

实际上，场景内某些人物与群体行为的发生是无关的。换句话说，场景中只有少数人物会实际参与到群体行为中。因此，寻找到那些关键参与者是理解群体行为的核心所在。通过对大量实际样本进行观察，本章认为关键参与者应该是在整个行为过程中保持稳定运动或者在某一时刻有显著运动的人物。本章以排球比赛为例来说明群体行为中的关键参与者所具备的特征，如图 2.1 所示。在“右传”场景中，人物 A 在整个过程中奔着“排球”移动，并最终参与了群体行为“右传”，本章将这类行为称作长时个体行为。此外，人物 B 在某一瞬间做了一个突然的“垫球”行为，虽然短暂但与群体行为“右传”密切相关，对周边其他人物的影响也很大。本章将这类行为称作瞬时个体行为。相比于其他人物，人物 A 和 B 的行为状态为理解群体行为“右传”提供了最为关键的线索。

方法简介：为此，本章提出了一种基于参与度敏感的群体行为识别方法，以筛选出关键参与者的行为特征并聚合为更具判别性的群体行为表示。即根据其运动强度从高到低的顺序将个体行为特征聚合，以尽可能地保留长时行为；基于个体行为特征与空间位置信息构建群体内上下文交互以挖掘交互相关的瞬时行为；在个体行为特征聚合过程中，利用可学习的注意力权重挖掘与群体行为语义相关的瞬时行为。

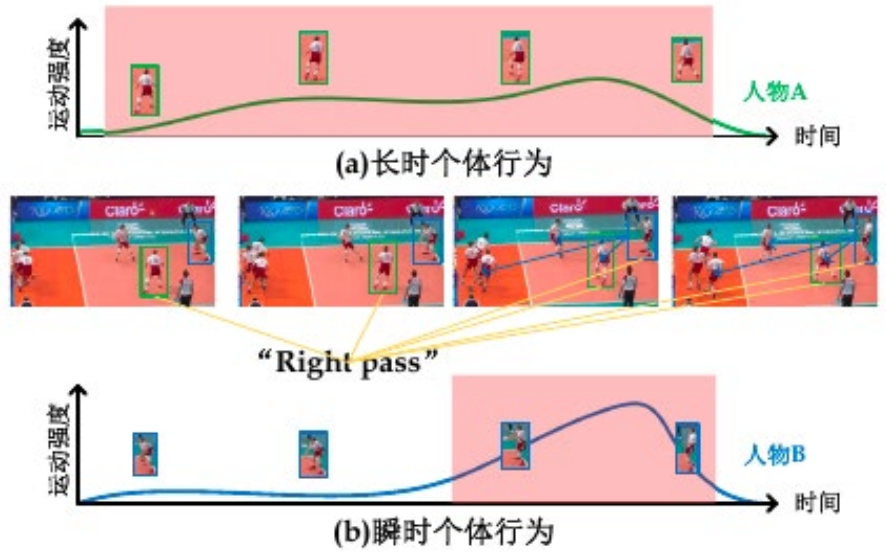


图 2.1 排球比赛中群体行为“右传”的关键参与者示意图

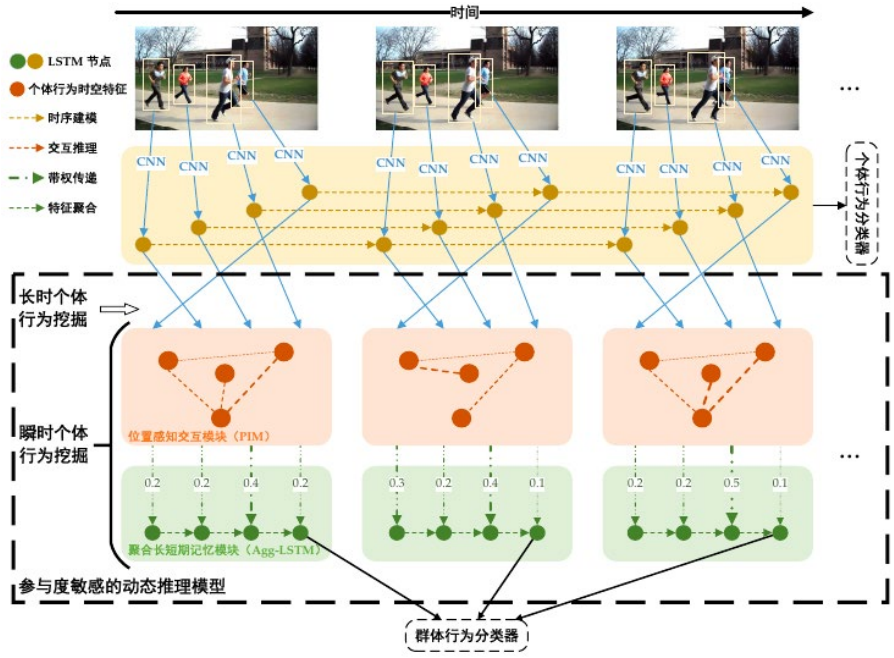


图 2.2 参与度敏感的时序动态模型框架图

具体而言，如图 2.2 所示，本章方法首先使用 CNN+LSTM 结构提取场景中每个人物的时空行为特征。然后，通过挖掘长时或瞬时个体行为特征并以不同程度将其聚合为群体表示。本章方法由两个模块组成，即位置感知交互模块（Position-aware Interaction Module，PIM） 和 聚合长短期记忆模块（Aggregation LSTM，Agg-LSTM）。具体来说，PIM 基于特征相似性和空间位置信息捕获与周围人群密切相关的关键个体行为特征。接着将 PIM 输出特征按其运动强度从大到小依次输入到 Agg-LSTM 中。Agg-LSTM 旨在用可训练的时变注意力权重将这些潜在特征融合成群体表示，挖掘与群体行为语义（标签）密切相关的个体行为特征。最后，Agg-LSTM 输出序列的最后一个节

点特征被视为帧级群体表示，后接一个 Softmax 归一化层计算得分以作分类判别。

成果 2: 基于层级式交叉推理的群体行为识别

研究动机：现有的群体行为识别研究多采用分步法：1）独立地根据所提供的人物轨迹提取个体行为特征； 2）在某个时间步构建个体人物之间的空间上下文交互特征； 最后 3）将这些特征表示拼接聚合为最终的群体行为特征以作预测。这种流程是很实用的，但它忽略了群体行为的时空共现问题，即每个层级（个体和群体）中的运动是相互联系相互影响的。为了更好地解释这一点，本节以排球比赛的场景为例说明。 如图 3.1 所示，一个球员在 `` 接球 " 的时候，他不仅需要调整自己的四肢以完成预定的“接球”行为，还会时刻注意周围队友的运动情况以调整自身行为的执行。尽管 `` 接球 " 行为由单个球员来执行，但这个执行过程涉及了若干人物在多个层级间的同步协作，包括他们的肢体局部运动、个体运动及其间的相互依赖。

然而，过去的方法多是分阶段理解个人和群体行为。具体地，这类方法 1）首先根据给定的人物框从原始视频中裁剪出个体行为序列并提取特征，用以个体行为分类；2）再将若干个体行为特征聚合为单一向量以做最终的群体行为分类。这种两阶段方法严重打破了上述不同层级信息间的潜在时空依赖关系，正如图 3.1 中所标识的蓝色虚线和实线。 此外，现有的方法通常以个体人物为最小单元构建视觉表示，而不考虑肢体局部之间潜在的时空依赖性 ~（即图 3.1 中的橙色虚线和实线），这在一定程度上限制了个体表征的学习。

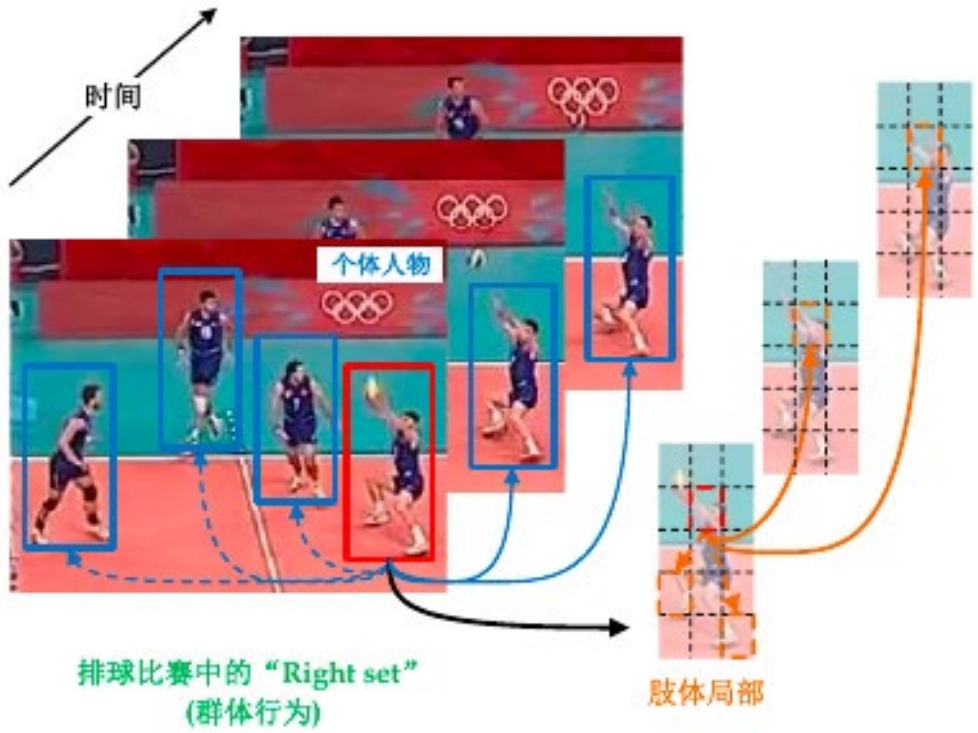


图 3.1 群体行为中多层级时空共现信息的示意图

方法简介：为了充分挖掘场景内多层级信息间的潜在时空依赖关系，本文首先提出了一种通用且高效的交叉推理块（Cross Inference Block，CIB）。 更具体地说，CIB 可以同时捕获 1）空间域中，每个特征节点之间的空间依赖关系（例如，人物肢体局部之间的空间关系）和 2）时间域中，某个特征节点的时序依赖关系（例如，某个人的

行为随时间演变）。 CIB 模块的输入 / 输出维度相同，因此它可被轻松插入现有的模型结构中以探索各种时空依赖关系。对于群体行为识别而言，CIB 可用于捕获肢体局部间或个体人物间的时空依赖关系。

基于 CIB，本章提出了一个简单而统一的群体行为识别框架，即层级式交叉推理网络（Hierarchical Cross Inference Network，HCIN）。本方法集成了多层级信息（例如，肢体局部、个体人物和群体行为），并通过两个核心模块以端到端方式推理这些信息间的相互依赖关系。本章首先设计了一个肢体局部推理模块（Body-regions Inference Module，BIM）来充分挖掘肢体局部特征间的时空依赖性以提取更精细的个体行为特征。此外，本章方法还提出了一个人物推理模块（Person Inference Module，PIM） 来进一步探索个体行为特征之间的时空依赖关系，可以同时建模特征间的空间交互和时序动态演变。值得注意的是，BIM 和 PIM 都是构建于 CIB 之上的。所提出的 HCIN 框架可以兼容各种主流骨干网络结构并以端到端的方式进行优化。此外，本方法在不需要个体行为标签的情况下仍然能够在流行的基准数据集上获得不错的性能。这大大节约了数据标注成本，也使得本方法更容易被应用到人群密集的实时场景中。

具体而言，如图 3.2 所示，给定一个视频序列和每个人物的边界框（又称轨迹），本章方法从多个不同层级信息中构建群体行为表示。首先，考虑到肢体局部特征之间固有的时空依赖性，本章设计了一个基于 CIB 的肢体局部推理模块（Body-region Inference Module，BIM） 来为每个人物提取行为表示特征。 值得注意的是，此处的肢体局部特征指的是基于人物行为序列对应的视觉特征图中某个单元格（例如图 3.2 中橙色虚线单元格）的信息，而不是某个人物的明确肢体部位。 为了在实验中进行比较，本章方法还采用了不同的主干网络来提取人物行为特征。此外，本章还基于 CIB 提出了一个人物推理模块（Person Inference Module，PIM）以进一步探索个人行为特征间的时空依赖性（例如图 3.2 中的蓝色节点）。训练阶段，将每一帧中 PIM 输出的个体行为特征最大池化为单个向量并送入到一个分类层。对于推理阶段，来自每一帧的分类概率被平均池化为该视频片段的最终预测结果。

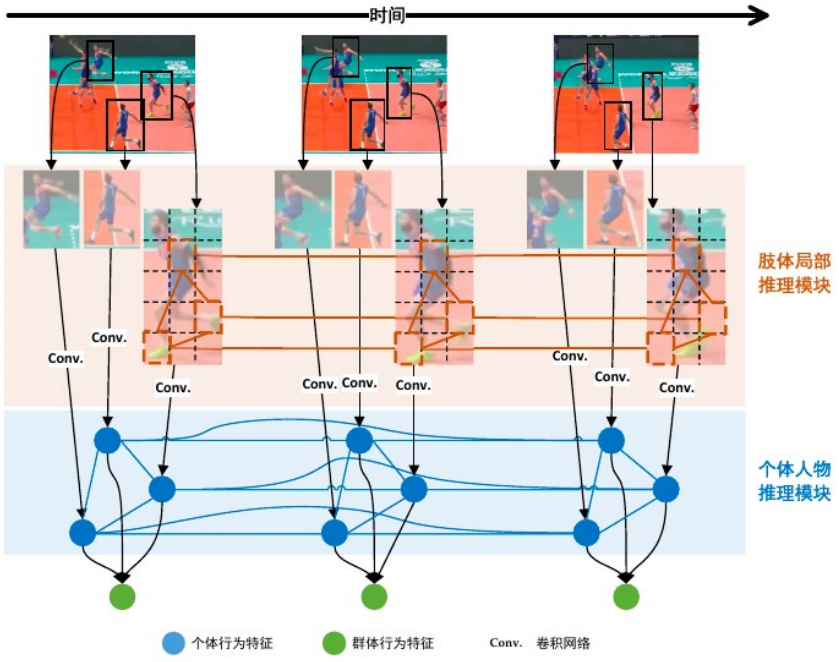


图 3.2 层级式交叉推理网络概述

成果 3: 基于交互自适应的弱标注群体行为识别

研究动机：现有方法严重依赖细粒度的人物监督信息（即每个人物的位置和个体行为的类别标签，甚至是两人间的交互行为标签），以辅助群体行为的感知与理解。通常情况下，这类传统的强标注方法根据场景中固定数量人物对应的边界框来提取个体行为特征，然后将这些个体行为特征通过交互建模并融合为帧级表示以分类。然而，这类强标注方法无法处理人物数量变化且无明确位置信息的场景，导致其难以落地到实际应用中。

方法简介：为此，本章提出一种弱标注群体行为识别任务，即仅为每一个视频提供一个粗粒度的群体行为标签（不标注人物具体位置及其相互关系等细粒度信息，也不保证群体行为与标签的严格时序对应）。此设置不仅更加符合实际应用需求，而且为采集更大规模的数据集提供了一种简单且低成本的思路。在弱标注设置下，本章采集到一个更大更具挑战性的基准数据集，NBA-NJUST。该数据集是从 181 场 NBA 篮球比赛视频中采集而得，共计 9172 个视频样本。它所定义的群体行为时序信息更丰富，人物移动速度更快。在弱标注设置下，可以利用现成的检测和跟踪算法从视频提取可能的人物框。但这带来了一个新的挑战，即不确定输入问题。例如图 4.1 所示，“Three shot：21 = 5 + 16”表示检测算法一共输出 21 个候选框，但其中只有 5 个是与群体行为相关的，其他 16 个检测框对理解该群体行为无帮助。在这种情况下，许多无关检测框将被输入到模型中，同时检测算法也会漏检一些行为相关的人物。此外，由于视频和标签之间的时序对应不严格，视频中也会出现大量不相关的帧。

图 4.1 弱标注设置下的不确定输入问题说明

为解决上述问题，本章进一步提出了一种简单有效的“交互自适应模块”（Adaptive Interaction Module，AIM），它可以从视频中自适应地选择具有判别性的个体行为和视频帧特征用于弱标注群体行为识别。AIM 基于“关键实例（人物 / 视频帧）间往往是彼此高度相关的”这一假设来协助弱标注下的模型训练。具体而言，如图 4.2 所示，本章方法首先在所有可能的输入特征之上构建一个密集的关系图来衡量它们彼此间的相关性，然后根据它们在关系图中的重要程度作出筛选。根据所选特征，构建一个稀疏关系图以进行推理。得益于 AIM 的有效性，本章方法在只有弱标注信息的情况下仍然能够在流行的 VD 数据集上获得了与当时方法相当的性能。

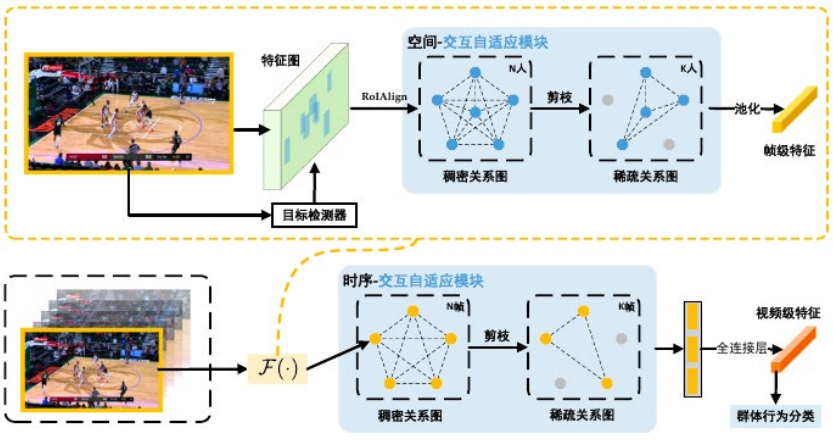


图 4.2 基于交互自适应的弱标注群体行为识别方法框架

成果 4: 基于渐进式实例感知的组合行为识别

研究动机：最近一些研究意识到现有视频表示算法仅适用于“简单”行为（比如一些通过单帧中的空间信息即可区分的行为），距离理解“复杂”行为（比如涉及一个或多个视觉实例的时序运动）还有很长的路要走。那么，为什么人类可以很容易地理解那些发生在不同环境或视觉实例之上的复杂行为呢？主要是因为人类具备对视觉实体进行组合推理的能力，使得其获取的知识不受限于实例的具体视觉内容。例如图 5.1（c）的场景，人类通常是先聚焦到场景中所有视觉实例（即两个盒子和两只手），然后通过观察实例间的相对位置变化来识别行为语义。这种组合推理能力帮助人类学习到一些可泛化到未知视觉内容上的知识。受此启发，本章工作也意在令机器在行为识别方面表现出类似能力，即组合行为识别。该任务要求训练集和测试集中的“行为 - 物体”组合不重叠。

根据上述定义，组合行为识别的主要挑战是测试集上出现的数据分布偏移问题。然而，当样本不足时，深度模型不可避免地会在训练集上对视觉输入与标签产生归纳偏差。例如，图 5.1（c）和（d）中的行为易混淆的原因之一是模型倾向于将外观信息作为归纳偏执。为了缓解这一问题，一个直观的解决方案就是引入额外模态信息，例如利用实例位置信息就能轻松区分图 5.1（c）和（d）的行为（"moving towards " 与 "moving away from"）。但是，位置信息对一些涉及物体属性的行为也并不起作用。例如图 5.1（a）和（b）所示，虽然勺子不像纸张一样能被撕破，但是准备撕“勺子”和撕一小部分“纸”时，勺子、纸、手的位置变化是很相似的。此时位置信息就不足以用来区分这两个动作。因此，整合多种信息已成为组合行为识别问题的一类有前景的解决方案，但也极具挑战性。

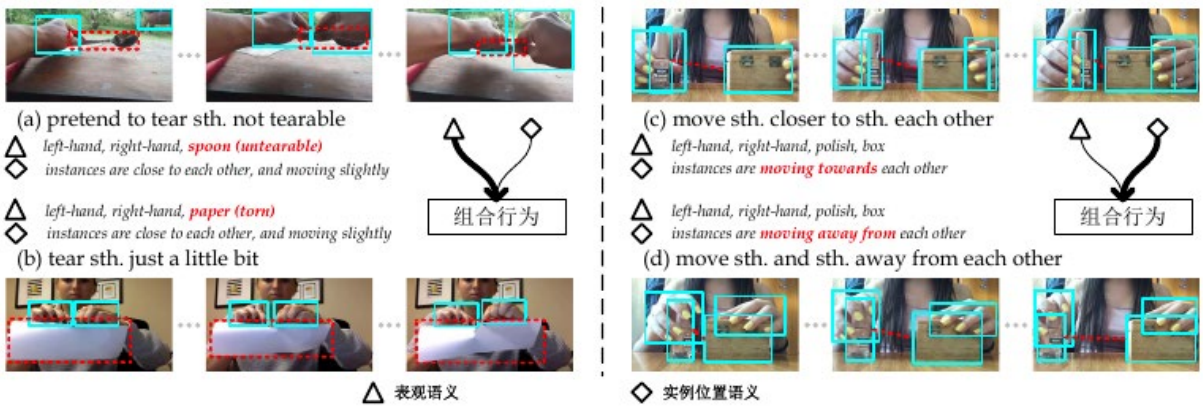


图 5.1 SSV2 数据集上的组合行为示例

过去的工作直接将实例信息（例如实例位置和身份）独立编码成特征后再进行交互，接着将它们与全局表观特征连接起来进行分类。这类方法可行但很粗糙，本章认为实例信息在行为特征提取的不同阶段都扮演着至关重要的角色。例如，当人类理解复杂的行为时，1）首先通常需要先关注到移动物体或区域；2）然后借助其身份来推理它们之间的潜在联系，3）接着甚至能够准确预测这些行为相关物体的运动轨迹。受此启发，本章方法旨在将实例信息（位置和身份）逐步注入到视频特征学习的过程中。

方法简介：为此，本章提出了一种渐进式实例感知特征学习（Progressively Instance-aware Feature Learning，PIFL）方法以理解组合行为。具体包括三步：1）位置感知的表观特征提取：根据视觉实例的运动轨迹从图像序列中构建出实例级表观特征，以增强局部动态线索抑制无关背景归纳偏差（并将它们与非表观特征结合起来，形成实例级混合特征）；2）身份感知的特征交互：在这些混合特征之间构建身份感知的关联，为每个实例生成语义关联特征；3）

语义感知的位置预测：从部分可观测的实例级语义特征中估计出其后续运动趋势，以促进模型感知实例运动的能力。本章实验在首个基于组合泛化划分的数据集 STH-ELSE 上对提出的方法进行了验证。实验结果表明，无论是使用视觉实例的（人工标注的）真实框还是（算法生成的）检测框，本章方法在组合行为识别任务上都显著优于当时最先进方法。此外，本章方法在少样本设置下也表现出了良好的泛化能力。

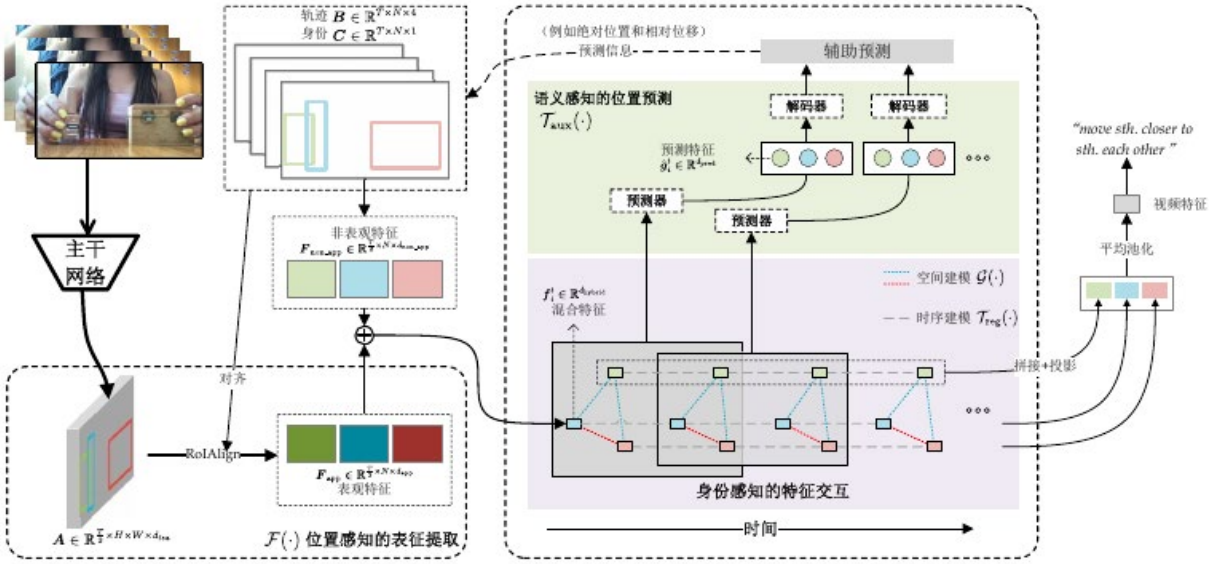


图 5.2 渐进式实例感知特征学习框架图

成果 5: 基于视觉 - 语言联合理解的组合行为识别

研究动机：组合泛化能力是使传统行为识别算法在复杂场景中正常运作的前提。但是，迄今为止，组合行为识别问题在定义形式和评估指标上都没有一个统一标准。过往的工作仅根据识别准确率指标来判断模型的组合泛化能力，显然是不够合理的。 因为这些方法所带来的增益也会适用于传统划分下的人体行为识别，而无法确定组合划分所引入的视觉偏差问题（即视觉输入和行为类别间的偏差关联）是否得到了缓解。例如，更强的主干或额外的信息在常规划分和组合划分下都有助于模型性能的提升。此外，直到目前为止只有一种（随机）组合划分策略用于组合行为识别的评估。因此，社区迫切需要规范该任务的问题定义并构建合理的评估协议。

另一方面，组合行为识别的主要挑战在于如何判别未见“行为 - 物体”组合下的人体行为（即分布偏移问题）。控制物体视觉外观和行为语义间的归纳偏差是缓解上述问题的直观方案。近期一些方法试图通过增强视频中物体运动特征并以各种策略将其与表征特征融合来实现这一目标，例如特征融合（特征拼接、多层级信息交互式融合、基于交叉注意力机制的融合） 和得分融合。然而，这些方法都忽略了物体与人体行为间存在的常识语义关系。例如图 6.1 所示，为什么人类可以撕“纸（paper）”或“树叶（leaves）”这两种视觉外观不同的物体呢？因为它们都具有一种“可撕裂”的共同属性。这些所谓的物体属性都是由人类在进行语言创作过程中，通过视觉、触觉等形式对自然界存在事物的总结归纳而得。受此启发，本章工作不仅控制物体视觉外观带来的归纳偏差，同时也探索物体与行为在语言上的常识性联系，以辅助机器对组合行为的理解。

方法简介：综上所述，1）目前组合行为识别问题的定义和评估都不够完备，并且 2）过去工作只专注于抑制物体视觉外观和行为语义之间的归纳偏差，而忽略了物体与行为标签之间的（语言）常识性关联。为此，本章重新梳理并定义了组合行为识别任务并提出一个更实际的组合划分策略和一个简单合理的评估指标 Drop Ratio（DR），以促进该任务更好地发展。除此之外，本章工作还提出了一个新颖的学习框架，Look Less Think More（LLTM）：1）在视觉表示空间，减少物体和行为语义间的归纳偏差（Look Less）；2）在语言表示空间，增强物体属性与行为标签间的常识性联系（Think More）。具体来说，本章方法提出了一种基于实例的视频突变技术来构建诸多反例，以打破视觉外观和行为之间潜在归纳偏差。然后进一步利用对比学习损失约束和挖掘视觉实例标签与行为标签文本表示间的联系。本章所提出框架（LLTM）适用于现有多数标准行为识别算法，以增强其组合泛化能力。

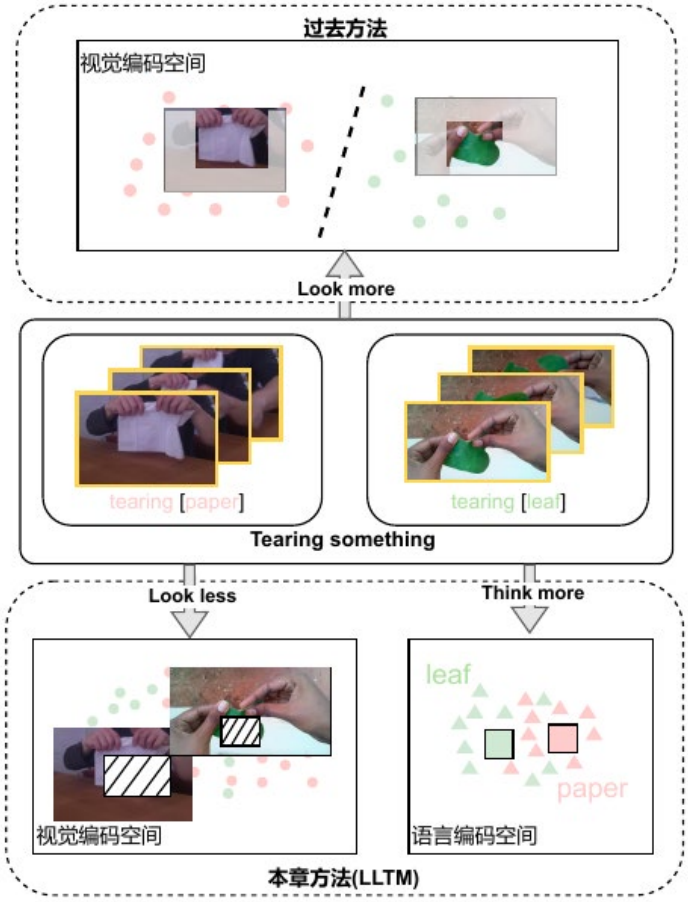


图 6.1 “少看多想”（Look Less Think More，LLTM）方法动机

具体而言，给定分辨率为 $H\times W$ 的 RGB 视频序列$V \in \mathbb{R}^{T\times 3\times H\times W}$，其中 T 表示视频帧数。传统视频分类方法旨在将输入视频 V 和目标类别 Y 直接关联为，$= \mathcal{M}(V)$。其中$\mathcal{M}(\bullet)$，通常由一个视觉编码器和一个简单的分类器组成。 然而，组合行为通常是被实例化在不同视觉实例（物体）上的。传统视频分类往往会在视觉实例外观与行为类别之间建立归纳偏差。基于以上考虑，本章提出了一种新颖的“少看多想（Look Less Think More）”框架（如图 6.2 所示）来减少对象的视觉外观和行为类别之间的归纳关联（“少看”），并在物体属性和行为语义间构建常识关联（“多想”）。给定视频序列，本章方法从中采样 T 帧并检测物体及其类别，作为本章方法的输入。“少看”：对视觉实例实施不同的突变以抑制物体视觉表观与行为类别之间的归纳偏差。“多想”：将不同的模态信息（即视频帧、物体和行为的文本标签）投影到统一的特征空间中，以对比学习机制挖掘它们之间的常识联系。该框架可以抽象为，$Y \Longleftrightarrow < \mathcal{T}(V), \mathcal{G}(O) >$。其中 O 表示物体类别的文本标签，$\mathcal{T}(\bullet)$和$\mathcal{G}(\bullet)$可以遵循以下要求以多种方式实现。$\mathcal{T}(\bullet)$用于在不干扰相关行为语义的情况下改变物体视觉内容；$\mathcal{G}(\bullet)$需要在物体类别和行为语义之间构建潜在联系。本章通过构造几个“干扰局部视觉输入但不改变行为语义的”视觉反例以实现函数$\mathcal{T}(\bullet)$, 通过将所有物体标签组合成一个完整的文本描述（句子）并且将其嵌入到一个向量中以实现函数$\mathcal{G}(\bullet)$。

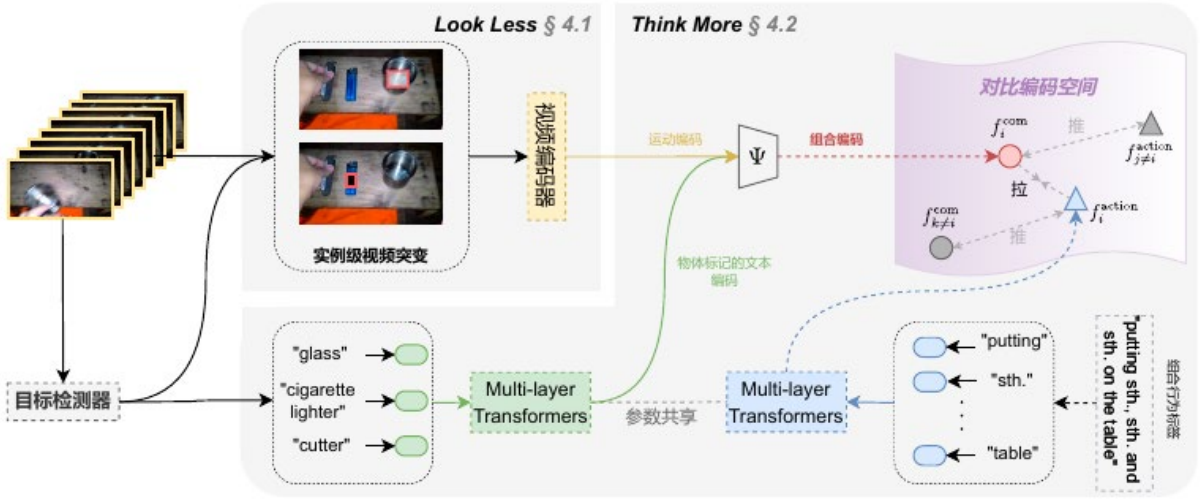


图 6.2 用于组合行为识别的“少看多想”框架图概述

作者介绍

严锐于 2022 年 11 月从南京理工大学计算机科学与工程学院获博士学位（导师为唐金辉教授），于 2023 年 3 月加入南京大学计算机科学与技术系从事博士后工作（合作导师为谭铁牛院士），于同年 10 月获聘为南京大学毓琇青年学者（助理研究员）。主要从事人体行为分析、视频内容理解方面的研究，发表 CCF A 类和 IEEE/ACM Trans. 论文 30 余篇，其中一作或通讯论文 11 篇，3 篇论文入选 ESI 高被引 / 热点论文。谷歌学术统计引用数逾 1400 次，引用者包括 120 余位 ACM/AAAI/IEEE Fellow 等国际权威专家。主持国家自然科学基金面上项目、青年项目、中国博士后科学基金“特别资助”和“面上资助”项目等，入选 2024 年江苏省科协青年人才托举工程、2024 年南京理工大学优秀博士学位论文、国家资助博士后、江苏省卓越博士后。此外，本人多次担任 CVPR、ICCV、ECCV、NeurIPS、AAAI、IJCAI、ACM MM 等 CCF-A/B 类会议的程序委员会委员，以及 TPAMI、TNNLS、TCSVT 等 CCF-A/B 类期刊的审稿人，担任中国图像图形学会多媒体专委会委员。

作者：严锐

导师：唐金辉教授

攻克低空智联网关键技术，服务低空经济国家战略

——2024 年江苏省计算机学会青年科技奖获得者屈毓锛副教授

个人简介

屈毓锛，南京航空航天大学电子信息工程学院副教授 / 硕士生导师、电磁频谱研究院（工信部唯一批复成立）认知网络创新中心主任，校企共建科研平台“低空智联网运营管理联合实验室”负责人，入选 2025 年度江苏省科技副总，中国通信学会第一届低空信息通信专业委员会委员，斯坦福全球前 2% 顶尖科学家（2025 年度），低空智联网南京市工程研究中心高级技术专家。曾入选国家博士后创新人才支持计划，获中国发明协会 2025 年度发明创业奖成果奖二等奖（排 1）、2025 年第 50 届日内瓦国际发明展金奖（排 1）、2024 年江苏省计算机学会青年科技奖、2022 年度军队科技进步二等奖、2021 年度 ACM China 新星奖（上海）。目前主要从事面向空天的边缘人工智能、低空智联网等方面的研究。作为项目负责人主持国家自然科学基金面上 / 青年 / 重点课题，以及中航工业企业委托课题等近 10 项。以第一作者或通信作者身份在 IEEE JSAC/TMC/INFOCOM/COMMAG/Network、IEEE/ACM ToN、计算机学报、通信学报等网络通信领域知名期刊和会议发表或录用论文 50 余篇，ESI 高被引论文 1 篇，申请 / 授权国家和国防发明专利 20 余项。担任中国计算机学会网络与数据通信专委会 / 分布式计算专委会执行委员，《电子与信息学报》编委、《西安交通大学学报》青年编委，CCF 推荐 A 类会议 IEEE INFOCOM、B 类会议 IEEE/ACM IWQoS 以及 IEEE ICC/ICPADS/ICCCN 等知名国际学术会议程序委员会委员，获评 IEEE INFOCOM 2023 杰出程序委员会委员。研究成果获中国科协第八届优秀科技论文、2024 CCF-IEEE 服务计算最佳论文奖，国际学术会议 GPC 2020、IEEE SAGC 2021、IEEE/CIC ICCC 2023 等国际学术会议最佳论文奖，2024 中国高校计算机教育大会最佳论文、第 15 届全国高校计算机网络教学暨网络工程专业建设研讨会优秀论文一等奖，2023 ACM SIGCOMM China Symposium 最佳海报奖，中国电子学会物联网专委会 2020-2021 年度十佳优秀论文奖，指导本科生获 2025 第十一届 3S 杯物联网大赛全国一等奖、2022 中国工程机器人大赛暨国际公开赛一等奖、2025 低空产业创新大赛专项攻关奖、2023 智能无人系统应用挑战赛协同跟踪赛道亚军、2025 金砖国家工业创新大赛优秀奖、2024 中国高校计算机大赛网络技术挑战赛华东赛区二等奖等奖励。

屈毓锛副教授

攻克低空智联网关键技术，服务低空经济国家战略

以低空无人机为主要载体的低空经济自 2021 年 2 月在中共中央、国务院印发的《国家综合立体交通网规划纲要》中提出后，在 2023 年 12 月被列入国家战略新兴产业之后，并于 2024 年 3 月首次写入政府工作报告，成为新质生产力的典型代表，预期具有万亿级市场规模。无人机通常需要搭载可见光、红外等多种传感器完成相应任务，而这些传感器可产生达 30Gb/s 量级感知数据，如何对这些机载感知数据进行处理是能否发挥其行业应用价值的关键。利用深度学习等主流人工智能技术可有效处理上述感知数据，但考虑到无人机网络通信链路带宽受限且动态变化，如将这些感知数据全部回传到地面云进行处理会导致时效性较差。为此，亟需研究如何在更靠近机载感知数据源的地方进行处理，即，在无人机网络边缘运行人工智能算法以提升机载感知数据处理的时效性，但面临无人机载设备资源受限导致 AI 模型精准部署难、无人机网络通信动态变化导致实时协同处理难、无人机网络通信不可靠导致机载模型在线更新难等挑战。针对上述挑战，聚焦作为低空经济关键信息基础设施的低空智联网，屈毓锛副教授团队开展了低空无人机网络边缘智能计算技术研究，取得如下代表性成果。

①代表性创新成果 1：机载资源受限下的 AI 模型轻量化与自适应压缩方法

（1）基于多尺度决策的深度神经网络轻量化。无人机载有限的计算能力、内存带宽、存储空间以及严格的能耗预算，使得直接在机载端部署高精度的复杂 DNN 模型极具挑战。传统模型轻量化方法通常只优化单一层面的模型参数，优化空间受限。因此，屈毓锛副教授团队将模型优化问题表达为多尺度马尔可夫决策过程，同时对块数量与通道数量进行协同优化，显著扩展了模型压缩的优化空间，进而提出了多尺度强化学习决策算法。基于典型机载嵌入式的实验结果表明，相比五种基准算法（含 MobileNet），在达成同样精度的情况下，可减少 98.6% 的浮点运算量和 95.7% 的模型大小。（2）通信链路感知的机载数据自适应智能压缩。现有压缩方法忽略了空地无线链路的动态性，采用固定的压缩策略导致机载感知数据回传效率较差。屈毓锛副教授团队充分考虑空地无线链路的动态受限性，在业界较早提出了通信链路感知的机载数据自适应智能压缩方法，在对空地通信链路轻量化感知的基础上，根据当前可用链路带宽和质量，能够将机载遥感图像等感知数据最大化自适应智能压缩。基于 1.4GHz、2.4GHz 以及 5G 等典型机载回传通信链路的外场实际实验结果表明，相比六种基准算法（含 JEPG、PNG），可减少约 30% 的回传通信开销。相关成果发表在 IEEE TMC’23、IEEE TMC’24、IEEE Network’21 等上，其中，ESI 高被引论文 1 篇，获 2025 年第五十届日内瓦国际发明展金奖，加拿大工程院院士 /IEEE 会士卡尔顿大学终身教授 F. Richard Yu 在其 IEEE IOT-J’25 论文指出“屈毓锛副教授团队论文所提多尺度轻量化方法通过利用神经网络层次化结构特点，在资源受限情况下实现了高效的网络轻量化”，支撑获得 2022 年中国工程机器人大赛暨国际公开赛全国一等奖、2023 年第三届智能无人系统应用挑战赛协同跟踪赛道亚军。

②代表性创新成果 2：轻量与复杂深度神经网络动态切换的无人机弹性协同推理方法

（1）复杂深度神经网络的弹性高效协同推理策略。单架无人机机载端资源受限仅能部署精度较低的轻量深度神经网络，处理实时性强但精度仍受限，利用模型分割等方式可将精度更高的复杂深度神经网络部署于多架无人机协同执行，但无人机机间无线通信链路易断链导致协同失败。因此，屈毓锛副教授团队提出基于 OODA 环（Observation 观察 -Orientation 判断 -Decision 决策 -Action 行动）的无人机弹性协同推理架构，有效应对断链

等突发情况。在多无人机协同任务调度方面，提出了基于数据并行与模型分割的弹性高效流水线推理任务调度方法，可在数百毫秒内响应重新生成协同调度策略。基于 24 个机载嵌入式节点和 5 架实物无人机的实验结果表明，相比 DeepSlicing、MoDNN 等业界基准算法，可减少约 98.5% 的平均推理时延，且可自主实时调整协同推理策略。

（2）轻量与复杂深度神经网络动态切换的自适应推理策略。不同于业界要么仅考虑本地推理轻量深度神经网络，要么仅考虑多节点协同推理复杂深度神经网络，屈毓锛副教授团队创新轻量与复杂深度神经网络动态切换执行新范式，即，根据当前无人机网络通信状态和任务需求，单节点本地计算（轻量深度神经网络的推理）与多节点协同计算（复杂深度神经网络的推理）动态切换，以实现较好的推理精度与推理延迟之间折衷，并提出基于多智能体深度强化学习的模型自适应选择与分割策略。基于典型机载嵌入式的原型验证系统测试结果表明，相比三种基准算法，推理精度平均提升 9.9%，推理延迟平均减少 46.3%，取得较好的推理精度与延迟折衷。相关成果发表在 IEEE JSAC’21、IEEE TWC’21、IEEE TMC’24、IEEE COMMAG’24、CJOA’24、计算机学报’22 等上，其中发表在中文 CCF A 类期刊《计算机学报》上的论文获第八届中国科协优秀科技论文、中科院 SCI 一区 /CCF A 类期刊 IEEE JSAC 上的论文获 2024 IEEE-CCF 服务计算最佳论文奖和 2020-2021 中国电子学会物联网专委会优秀论文奖，支撑获得 2024 年联合作战实验创客研练（智谋 -2024）二等奖、2023 年第四十八届日内瓦国际发明展银奖。

③代表性创新成果 3：不可靠通信条件下无人机在线鲁棒协同学习方法

（1）多无人机协同的鲁棒增量学习策略。离线训练样本与实际环境存在差异导致无人机载 AI 模型实测精度不足，如何利用多无人机实采数据样本进行有效的模型增量学习是可行思路但面临较大挑战。不同无人机采集的数据具有非独立同分布的特性，无人机个体的计算、通信和能量等资源各异，在开放链路环境下面临通信干扰发生丢包。为此，屈毓锛副教授团队设计了多无人机协同的鲁棒增量学习方法，利用联邦学习架构本身的容错性来减少重传次数，联合优化数据重传和客户端选择。基于典型无人机载嵌入式设备的性能评估结果表明，与三种基准算法相比，所提方法在不可靠通信场景（丢包率 10%-50%）下平均总训练时间减少约 45.8%，传输延迟减少约 67.9%，同时保持达成同样精度（约 90%）。（2）地面协同的在线自适应联邦学习策略。无人机采集的数据不断变化，需要学习新数据的知识，及时更新现有机载端 AI 模型。针对动态无人机网络中样本数据不断更新，同时考虑到低空经济应用场景中无人机跟地面往往有相对稳定的通信连接而无人机之间通信较少，屈毓锛副教授团队提出了一种地面协同的多无人机在线自适应联邦学习框架，并形式化了一个在线样本选择和客户端调度的联合优化问题。通过推导预期收敛率的闭式表达式，量化了在线学习和丢包错误对模型收敛性的影响，并提出了一种结合分支定界法和 Dinkelbach 算法的交替迭代优化算法 OFL-PR。大规模仿真和实物系统验证结果表明，OFL-PR 在精度、收敛性和鲁棒性方面均优于三种现有的联邦学习基准算法。相关成果发表在 IEEE TCCN’23&24、IEEE TMC’22、IEEE INFOCOM’23、IEEE/CIC ICCC’23、IEEE SAGC’21 等上，获得 IEEE 与中国通信学会联合主办旗舰会议 2023 年 IEEE/CIC 中国通信国际学术会议（ICCC’23）最佳论文奖、2021 年 IEEE 天空地一体化计算国际学术会议（SAGC’21）唯一最佳论文奖、2023 年 ACM SIGCOMM China 最佳海报奖等奖励。

未来，屈毓锛副教授将积极探索低空智联网关键技术赋能低空经济安全高质量发展，在南京航空航天大学“政、端、网、云、用、才”六位一体低空经济创新发展生态体系的指导下，重点聚焦低空智联网感传算融合关键技术的攻关，并充分利用学校低空全学科覆盖优势与高能级创新平台，同时依托与行业龙头企业的战略合作优势，加强与低空行业企业产学研合作，实现在低空智联网产学研用科研能力的全面提升。

以科技为盾，守护软件系统安全——在安全测评技术研究中砥砺奋进

——2025 年江苏省计算机学会优秀科技工作者陈锦富教授

个人简介

陈锦富，博士，教授，博士生导师，江苏大学计算机学院副院长，江苏省工业网络安全技术重点实验室主任，网络空间安全一级学科带头人，国家级一流专业建设点信息安全专业负责人。2009 年 6 月硕博连读毕业于华中科技大学计算机软件与理论专业，获工学博士学位。曾担任多个国际会议如 QRS、ICA3PP、NOPE、ICCIA 等程序委员会委员（主席），ACM、IEEE 会员，中国计算机学会杰出会员，中国计算机学会软件工程专业委员会执行委员、中国计算机学会容错计算专业委员会执行委员、中国计算机学会区块链专业委员会执行委员，江苏省计算机学会理事、江苏省网络空间安全学会理事，江苏省计算机学会信息安全专委会副主任委员。江苏省“333 工程”中青年科学技术带头人、江苏省“青蓝工程”中青年学术带头人、江苏省六大高峰人才。获批 2012 年国家公派访问学者资助项目，在澳大利亚斯文本科技大学 T. Y. Chen 教授课题组交流访问一年。主持国家某部委重点项目、国家重点研发计划子课题及国家自然科学基金面上项目等国家及省部级课题 20 余项，承担企业系统开发项目 4 项。在相关领域国内外权威期刊及会议发表高质量论文 100 余篇。此外，申请国家发明专利 20 余项，获批软件著作权 18 项，多项研究成果已有初步应用和转化。长期从事软件系统安全测评与软件漏洞挖掘相关研究工作，研发了一套基于漏洞特征和漏洞模型的软件漏洞综合检测系统，已应用于相关领域信息系统的安全性测试及保障。研究成果“基于数据挖掘和变异测试的构件漏洞检测技术”获 2019 年行业协会科学技术二等奖。

教学上，获江苏省教学成果奖二等奖 1 项，省级一流课程及案例 2 门，校级一流课程 2 门，主持教育部产学研协同育人项目 3 项，多次获评江苏大学优秀教师。指导学生获江苏省本科优秀毕业设计二等奖 1 项及中国大学生计算机设计大赛、全国大学生信息安全竞赛、全国大学生软件测试大赛等国家级赛事一等奖及二等奖 20 余项。

陈锦富教授

以科技为盾，守护软件安全——在安全测评技术研究中砥砺奋进

陈锦富教授一直从事软件安全测试、自适应随机测试、漏洞挖掘和区块链测评方面的研究工作，特别关注智能系统安全测评理论与技术。在自适应随机测试、漏洞挖掘技术和智能系统测评方面做了有益的探索，并取得了较好的研究成果。申请人及团队主要成员的主要相关研究成果已在 ICSE、ASE、ISSTA、ACM/IEEE Trans.、Journal of Systems and Software、Information and Software Technology、中国科学及计算机学报等重要学术期刊及学术会议上发表。

陈锦富教授对软件安全缺陷预测方法进行了深入的研究。提出了基于缺陷预测的自适应软件错误模型构建方法，探索了基于缺陷预测的测试用例生成方法，也对基于聚类分析的测试用例优先级排序方法进行了研究，并形成了一些有效的模型、方法和技术。 此外，对软件漏洞成因机理及检测方法进行了深入的研究和探索。提出了基于内因与外因的软件脆弱性成因分析方法，研究了基于程序数据控制流图等技术的软件漏洞检测方法，也对软件漏洞预测技术进行了研究，并形成了一些有效的模型、方法和技术。此外，团队研发过软件漏洞挖掘综合评价系统、物联网漏洞挖掘系统及第三方构件安全性测试系统，并相应地开发了状态变换的漏洞挖掘工具和基于程序控制流图的漏洞检测工具，积累了大量的漏洞测试案例和相关经验。

针对有源软件和无源软件，陈锦富教授团队分别提出了相关的软件安全测试框架及方法。主要有：（1）基于错误注入的构件安全测试模型及测试用例生成算法；（2）基于参数变异、条件变异及状态变异的软件安全性测试方法；（3）基于构件接口参数变异的软件测试用例生成算法；（4）基于数据挖掘技术的构件安全性测试模型及框架。在软件安全测试方面，申请人进行了持续多年的研究，提出了：（1）基于条件冲突和行为冲突序列的软件安全性测试用例生成算法；（2）基于状态转换的软件安全性测试用例生成算法。同时也实现了一个自动化的构件安全测试原型工具 CSTS，并具有较好的测试效果。相关研究成果已经发表在 ACM/IEEE International Conference on Software Engineering（ICSE）、IEEE/ACM International Conference on Automated Software Engineering（ASE）、ACM SIGSOFT International Symposium on Software Testing and Analysis（ISSTA）、IEEE International Symposium on Software Reliability Engineering（ISSRE）、Software: Practice and Experience（SPE）、Software Quality Journal（SQJ）等权威期刊和会议上，这些方法已经应用于软件脆弱性分析和漏洞检测中。

为了应对智能系统中的智能算法安全和隐私泄露等问题，陈锦富教授团队近年来结合攻防环境研究智能算法框架的检测防御以及安全测试等技术，以提高智能算法框架的安全可靠能力。主要研究内容有：一是基于蜕变测试技术的深度学习算法与智能系统安全测试方法；二是基于自适应变异算子的智能算法安全性测试方法；三是基于错误注入指导的智能算法框架攻击检测与安全防御方法；四是基于模糊理论的智能系统的安全等级评估体系与安全规范构建。研究内容关系如图 2 所示。

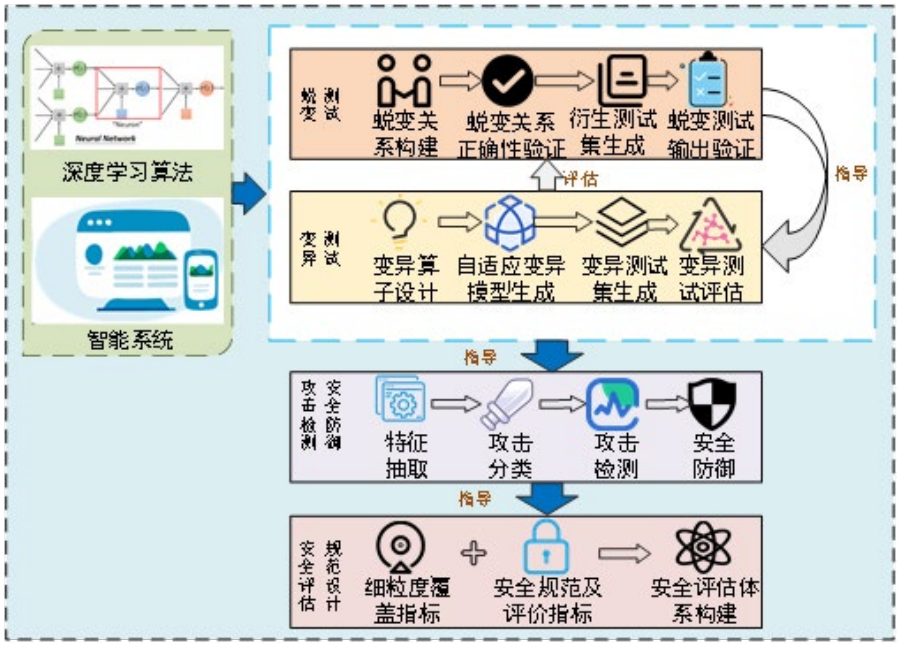


图 2 研究内容关系图

立德树人结硕果，育才征程初显成

在江苏大学的教育沃土上，陈锦富教授始终以“立德树人”为根本使命，深耕教学科研一线，用智慧与热忱浇灌出累累硕果。从博士生到本科生，他以严谨的治学态度、创新的育人理念，培养了一批批德才兼备的优秀人才，在学术探索与实践中书写着“育才征程初显成”的动人篇章。

深耕学术沃土，培育高层次科研人才

陈教授以“传道授业”为基，以“科研创新”为翼，在博士生培养中倾注心血。他坚持“因材施教”，根据学生特点定制个性化培养方案，带领团队攻坚前沿课题。近年来，他培养的 8 名博士研究生均以优异成绩毕业，其中 3 人获评校级优秀博士学位论文，2 人赴海外顶尖学府深造，1 人成为行业领军企业核心研发骨干。在硕士培养中，他累计指导 50 余名研究生完成学业，大部分学生以第一作者身份在国内外顶级期刊发表高水平论文，为学科发展注入新鲜血液。

创新实践育人，赋能学生全面发展

陈教授深知“实践出真知”，积极搭建“产学研用”一体化平台，推动学生将理论转化为创新成果。他指导本科生团队参与国家级 A 类学科竞赛，斩获二等奖以上奖项 30 余项，其中“基于信创环境的网络安全测试验证靶场平台”项目获第十八届“挑战杯”全国大学生课外学术科技作品竞赛三等奖，相关成果被企业采纳应用。此外，他注重以德立身、以德施教，多名学生在其指导下获评“国家奖学金”、“中国大学生自强之星”等国家级表彰和荣誉，彰显了德才兼备的育人成效。

未来，陈教授将继续以“育才报国”为己任，在人才培养的道路上砥砺前行，为教育事业贡献更多智慧与力量。

数据“中毒”会让 AI“自己学坏”

来源：科技日报

AI 系统在学习过程中，如果输入了错误或误导性数据，可能会逐渐形成错误认知，做出偏离预期的判断。

图片来源：英国《新科学家》网站

【今日视点】

◎本报记者 张佳欣

在一个繁忙的火车站，监控摄像头正全方位追踪站台的情况，乘客流量、轨道占用、卫生状况……所有信息实时传输给中央人工智能（AI）系统。这个系统的任务是帮助调度列车，让它们安全准点进站。然而，一旦有人恶意干扰，比如用一束红色激光模拟列车尾灯，那么摄像头可能会误以为轨道上已有列车。久而久之，AI 学会了把这种假象当作真实信号，并不断发出“轨道占用”的错误提示。最终，不仅列车调度被打乱，甚至还可能酿成安全事故。

澳大利亚《对话》杂志日前报道称，这是数据“中毒”的一个非常典型的例子。AI 系统在学习过程中，如果输入了错误或误导性数据，可能会逐渐形成错误认知，作出偏离预期的判断。与传统的黑客入侵不同，数据“中毒”不会直接破坏系统，而是让 AI“自己学坏”。随着 AI 在交通、医疗、媒体等领域的普及，这一问题正引起越来越多的关注。

AI“中毒”的现实风险

在火车站的例子中，假设一个技术娴熟的攻击者既想扰乱公共交通，又想收集情报，他连续 30 天用红色激光欺骗摄像头。如果未被发现，这类攻击会逐渐腐蚀系统，为后门植入、数据窃取甚至间谍行为埋下隐患。虽然物理基础设施中的数据投毒较为罕见，但线上系统，尤其是依赖社交媒体和网页内容训练的大语言模型中，它已是重大隐患。

一个著名的数据“投毒”案例发生在 2016 年，微软推出的聊天机器人 Tay 上线数小时后，就被恶意用户灌输不当言论，迅速模仿并发布到 X（当时的 Twitter）平台上，不到 24 小时就被迫下线并道歉。

据英国《新科学家》杂志报道，2024 年，互联网出现了一个标志性事件，即 AI 爬虫的流量首次超过人类用户，其中 OpenAI 的 ChatGPT-User 占据了全球 6% 的网页访问量，它本质上是 ChatGPT 的“上网代理”，在用户需要实时信息时替他们访问网站。而 Anthropic 的 ClaudeBot 更是长期大规模抓取网页内容，占到 13% 的流量。

互联网上的大量内容正被 AI 模型不断采集、吸收，用于持续训练。一旦有人故意投放有毒数据，比如篡改的版权材料、伪造的新闻信息，这些大规模采集的爬虫就可能把它们带进模型，造成版权侵权、虚假信息扩散，甚至在关键领域引发安全风险。

版权之争中的“投毒”反击

随着 AI 爬虫的大规模抓取，许多创作者担心作品被未经许可使用。为了保护版权，创作者采取了法律和技术手段。如《纽约时报》起诉 OpenAI，称其新闻报道被模型学习再利用，侵犯了版权。

面对旷日持久的版权拉锯战，一些创作者转向技术“自卫”。美国芝加哥大学团队研发了两款工具。名为 Glaze 的工具可在艺术作品中加入微小的像素级干扰，让 AI 模型误以为一幅水彩画是油画。另一款工具 Nightshade 更为激进，它能在看似正常的猫的图片中植入隐蔽特征，从而让模型学到“猫 = 狗”这样的错误对应。通过这种方式，艺术家们让自己的作品在训练数据中成为“毒药”，保护了原创风格不被复制。

这种反击方式一度在创作者群体中风靡。Nightshade 发布不到一年，下载量便超过一千万次。与此同时，基础设施公司 Cloudflare 也推出了“AI 迷宫”，通过制造海量无意义的虚假网页，将 AI 爬虫困在假数据的循环中，消耗其算力和时间。可以说，数据投毒在某些领域已经从一种反击手段，演变为版权与利益之争中的防御武器。

去中心化成为 AI 的防护盾

这种局面让人警觉。创作者的数据“投毒”是为了保护原创，但一旦同样的技术被用于大规模制造虚假信息，其后果可能比版权争议严重得多。

面对这种隐蔽的威胁，研究者正在探索新的防御手段。在美国佛罗里达国际大学的 Solid 实验室，研究人员正着力用去中心化技术来防御数据投毒攻击。其中一种方法叫联邦学习。与传统的集中式训练不同，联邦学习允许模型在分布式设备或机构本地学习，只汇总参数而非原始数据。这种方式降低了单点中毒的风险，因为某一个设备的“坏数据”不会立刻污染整个模型。

然而，如果在数据汇总环节遭遇攻击，损害依然可能发生。为此，另一种工具——区块链正被引入 AI 防御体系。区块链的时间戳和不可篡改特性，使得模型更新过程可被追溯。一旦发现异常数据，可追根溯源，定位投毒源头。同时，多个区块链网络还能互相“通报”，当一个系统识别出可疑模式时，可立刻警示其他系统。

任何依赖现实世界数据的 AI 系统都可能被操纵。利用联邦学习和区块链等防御工具，研究人员和开发者正在打造更具韧性、可追溯的 AI 系统，在遭遇欺骗时能发出警报，提醒系统管理员及时介入，降低潜在风险。

中国 AI 长卷（三）：算法生根

来源：脑极体 Unity

“中美 AI 差距究竟有几年？”这个问题困扰了不少人，也有很多声音尝试将中美 AI 实力进行比较。其中，算法，一定是评判的首要标准。

中美 AI 算法究竟是什么水平？我们可以用“第七个烧饼”来理解。

ChatGPT 就是 AI 的“第七个烧饼”。深度学习算法的热潮持续了十多年，终于在 LLM（大语言模型）智能涌现之后，看到了实现通用人工智能的曙光。就像一个饥饿的人，连续吃了六个烧饼都没吃饱，直到吃完了第七个烧饼，终于觉得饱了。

OpenAI 为代表的美国企业，在底层研发和核心算法上占据领先地位，率先吃到了 LLM 的“第七个烧饼”。随后，中国也极速跟进了这个领域，很快推出了对标 ChatGPT、GPT-4 水平的算法模型。

对此，有人欣慰：咱们虽然晚了一步，但也吃到了“第七块烧饼”（中国没有错过大模型的机会）。

有人愤怒：这一次技术突破又是美国公司主导，它们肚子里可比我们多好几块烧饼呢（美国领先我们至少十年）。

有人迷惑：早知道吃第七个烧饼就能饱，前面六个都不应该买（大模型之前的智能化探索全都白干了）。

还有人质疑：中国根本没有能力做烧饼，能吃上是因为别的摊主公开了做烧饼配方（谷歌 Transformer、OpenAI GPT-1/GPT-2 都是开源的）。

以上不同的情绪，有各自的道理，源于对算法的认知不同。

《终极算法》一书的作者写道：在农业中，人类进行播种，确保种子有足够的水分和营养，然后收割成熟的作物，而这也是机器学习的承诺。算法是种子，数据是土壤，程序是成熟的作物。

算法，就是将大规模数据转换成更合理、更智能决策的复杂程序，模型是它的软件形态。算法模型，是 AI 产学界最重要的“收成”。

从这个角度看，简单对比中美谁先拿下 ChatGPT，其实并没有太大意义。大众真正关心的，是中国有没有让算法这颗“种子”播种、生根、成长、结果的能力，能不能确保中国接下来吃到新算法的第八块、第九块……乃至第 N 块“烧饼”，持续满足各行各业享用 AI 的需求？

要搞清楚这个问题，我们得回到第三次 AI 浪潮的肇始，回到深度学习算法这颗“种子”刚刚萌芽的时候，看它是如何在中国落地生根的。

今天我们已经知道，深度学习是联结学派的主算法，主导了第三次 AI 浪潮。

可问题是，深度学习并不是在 2011 年才横空出世的概念。早在 20 世纪 40-60 年代，深度学习的雏形就出现在控制论中。训练多层神经网络的关键技术反向传播算法，是 1986 年提出的。联结学派，在 2006 年开始复兴。

那为什么，深度学习在 2011 年左右，才正式掀起了 AI 的新高潮呢？

背后有三个要素，构成了深度学习“种子萌芽”的土壤：

1. 越来越多的数据量。深度学习算法的中心思想，就是将大量计算单元连接在一起来实现智能行为，这个多层神经网络就类似于大脑的神经元，依靠大数据进行学习和训练，而互联网、智能手机提供了较好的数据基础，2011 年谷歌大脑成功识别了一只猫，2012 年苹果推出了 Siri，成为深度学习算法的先行者。

2. 越来越低的错误率，或者说越来越好的模型效果。2012 年，多层神经网络 Alex Net 在 ImageNet 大型视觉识别挑战（ILSVRC）中获得冠军，并大幅超越了使用传统机器学习算法的第二名，此后，深度学习每年都赢，证明了该算法的有效性。

3. 越来越多的成功应用，深度学习这逐步成为主导算法，被工业界用来解决很多实际问题，与上一代智能产品和应用相结合，让一度停滞不前的语音识别、图像识别、NLP 等任务都得到了提高。

大数据、技术能力、智能产品，当时在中国，具备让深度学习萌芽的条件吗？有两股力量可以。一是以 BAT 为代表的互联网公司，一是科大讯飞为代表的早期 AI 公司。

BAT 为代表的中国互联网公司，拥有海量数据以及国际化视野与人才团队，同时有搜索、语音、电商等数字化业务与应用，拥抱深度学习这一新算法是必然。

2010 年，百度成立自然语言处理部，由现任 CTO 王海峰带领，开始在语言与知识技术上布局，提出了“自然语言立足中国、面向世界一流水平”的定位。2012 年，百度积极关注并接触深度学习领域的领军人物 Geoffrey Hinton，并于 2013 年建立了 IDL 深度学习研究院，2014 年又成立了大数据实验室 BDL、硅谷人工智能实验室 SVAIL。除此之外，腾讯也在 2012 年成立了优图实验室，阿里巴巴成立了 iDST（数据科学与技术研究院）。

另一支探索路线，则是科大讯飞为代表的早期 AI 公司。

这些公司大多是中国在智能领域的早期探索者，比如科大讯飞成立于 1999 年，创始人团队主要来自中科大电子工程系人机语音通信实验室。

在 2011 年之前，科大讯飞就以智能语音技术为核心，进行了一系列技术、产品探索，比如科大讯飞联合高校开发的复杂语音合成、语音识别引擎，就打破了海外厂商的垄断，其语音软件在教育、电信、金融、学习机等领域都有商用。随着深度学习算法在国际上崭露锋芒，科大讯飞有意愿、有能力、有场景，将深度学习与原有的智能语音业务相融合。在 2011 年上线了中文语音识别 DNN 系统，2014 年启动了“讯飞超脑计划”，探索让“计算机能理解会思考”的感知智能和认知智能。

2023 年，面对“中国何时能有类 ChatGPT”“中美 AI 技术代差十年、三十年”的焦虑情绪， BAT、科大讯飞等企业作为中国大模型的第一梯队，很快带来了文心、混元、通义、星火等基础大模型。当然不是靠摘开源的“果子”，而是深度学习算法的“种子”，萌芽之初，就扎根在中国 AI 的土地上，并持续生长。

深度卷积神经网络（CNN）在图像识别和其他视觉任务中的突出表现，拉开了 AI 1.0 阶段的帷幕。

具体来说，此前传统的机器学习算法，虽然识别的精度和准确率也在提升，但始终无法同时保证准确率和识别效率，难以达到应用规模。而卷积神经网络 CNN 由于参数共享和稀疏连接，非常适合处理图像数据，在大规模图像数据上训练得到的深度卷积神经网络模型，可以不断从底层特征中提取更高层的特征（机器看得懂），最终更好地进行下游任务的处理（机器看得到）。

CNN 为核心技术，在图像识别、目标检测、图像分割、图像生成等算法方面，带来了极大的进步。2014 年，香港中文大学团队让机器在人脸识别任务上的表现第一次超越了人类，被认为 AI 1.0 阶段的里程碑事件。

叠加智慧城市、智能安防等概念的兴趣，CV 计算机视觉飞速发展，成为深度学习最成功的应用领域。

这一阶段，沐浴在新算法春风中茁壮成长的，自然就是 CV 企业。

2014-2017 三年间，旷视科技、商汤科技、依图科技、云从科技相继成立，依托于领先的计算机视觉技术，成为行业领导者和资本市场的宠儿，估值迅速上升，成为大家熟知的“CV 四小龙”。它们的算法模型，被广泛应用在城市、安防、医疗影像、工业质检等领域。

当然，除 CV 之外，我们也不能忽略深度学习算法在 NLP、语音、自动驾驶等多个领域中的进展，给许多行业带来了发展动力。

比如长短期记忆网络 LSTM 大幅提高了语音识别的准确性，智能助手在这一时期内得到了显著的性能提升，海外的苹果 Siri、谷歌 Google Assistant、亚马逊 Alexa、微软 Cortana 等，国内的百度小度、阿里天猫精灵等，被集成到多种智能终端软硬件当中，并开启了以语音交互为核心的智能家居元年。

自然语言处理方面，循环神经网络（RNN）和 LSTM 被应用于语言模型、情感分析、机器翻译等 NLP 任务。比如，

这一阶段的机器翻译，就从统计机器翻译（SMT）进入到NWT神经机器翻译时代，可以说是翻天覆地，中国的BAT（百度、阿里、腾讯）、科大讯飞、搜狗等公司，都在各自的产品中部署了 NWT，大幅提升了在线翻译的连贯性、准确性和语感。

同时，深度学习还可以在感知和决策方面，为自动驾驶汽车提供支持，吸引了很多投资基金的兴趣，进入了快速发展的黄金时期。百度在 2013 年启动了自动驾驶汽车项目，2017 年推出了 Apollo 平台，并出现了小马智行等一批面向 L4 自动驾驶技术的初创公司。

总的来看，AI 1.0 阶段，深度学习算法取代了传统机器学习算法，成为这一阶段的主算法，为很多领域的 AI 任务带来了跨越式发展。

但这一阶段的算法模型开发，仍是“手工作坊模式”，坊间戏称“有多少人工就有多少智能”。依靠对大量数据的依赖，需要组建庞大的标注团队，模型泛化性不足，专为某个特定任务而设计，需要投入开发人员进行大量重复开发和手工迭代优化等。

从“手工业作坊”到“工业化 AI 工厂”，算法仍需一场嬗变。

凯文凯利说过，技术带来的问题，只能靠技术进步来解决，算法也不例外。

从 AI 开发，从过去的手工作坊式向工业化升级，预训练模型就是一条可以规模化生产高性能 AI 模型的“工业生产线”。

2017 年，谷歌在论文《Attenlion is All You Needs》提出了 Transformer 架构。没有使用上一阶段流行的卷积神经网络

CNN、循环神经网络 RNN、长短期记忆网络 LSTM、GRU 等结构，仅使用了自注意（Self-attention）特性，引入了注意力机制和预训练模型（PTM）。在机器翻译、机器阅读、自动问答、情绪分析、自动摘要、语言建模等场景，显现出了前所未有的能力。2018 年，基于 Transformer 架构的预训练语言模型 BERT，刷新了 11 项 NLP 任务的最优性能纪录。同年，OpenAI 推出了 GPT-1。

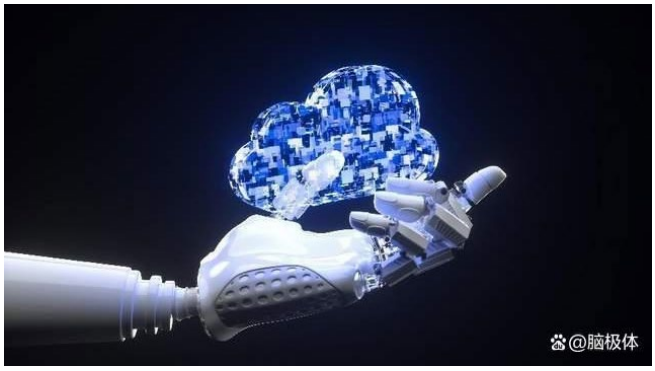
基于 Transformer 架构的预训练模型，可以通过模型的预先训练，带来效果更好、质量更高的算法模型，下游只需要任务微调就能应用。这种“预制菜”一样的“工业化模式”，一改小模型定制的积弊，让大规模、可复制的 AI 应用成为可能，成为 AI 去往下一个时代的必经之路。

迈向预训练模型的这条路上，中国几乎与世界一流水平同步，得益于一个关键变化：云智合流。

打造预训练模型，最困难的一项，就是专用算力不足，有的学校甚至买不起 GPU 卡，没有 AI 算力用。同时，这一阶段很多政企用户加速上云，也希望智能化升级，以更便捷的方式获取算法能力。

幸好，在这个算法更迭的关键窗口期，云 +AI 的融合基础设施，已经在建设中。

2017 年，将 AI 技术作为核心能力的华为云诞生。2018 年，百度云更名为百度智能云，阿里云升级为阿里云智能。将 AI 引入公有云的能力版图，成为主流。



云智合流，让 AI 开发从“手工业”迈入到“工业化”，将原本散落在算法全生命周期中的各类需求，进行了“融合”：

1. 算力融合。预训练模型不仅需要庞大规模的异构算力，而且需要高度的灵活性，从训练到推理的每个步骤，所需要的算力是差异巨大的。通过云厂商的基础设施，企业可以弹性、灵活、按需取用地接入多样、充沛的 AI 算力。获取算力的方式变得简单、高效、低门槛了，这就让更多人参与到 AI 算法模型的开发中来，进入大规模生产阶段。

2. 流程融合。借助云厂商提供完整、全栈的 AI 能力和开发工具，包括预制数据集、模型库、算子库等，让企业和开发者可以在云上完成从训练 开发 推理 部署的全部环节。比如百度智能云的 EasyDL\BML 平台、华为云的 AI 开发生产线 ModelArts 等。

3. 产品融合。时间来到 2018 年，智慧城市、智慧园区等都开始追求整体智能，希望构建一体化、解决方案式的“AI 大脑”，整合算法、芯片、云端算力、框架、网络、IoT 等软硬件，实现智慧决策能力的质变。这种情况下，云厂商和 AI 企业都要把自己变成一个“AI 超市”，集成并供应丰富的 AI 技术能力与应用，让行业用户和开发者可以体系化、轻松地，获取到所需要的 AI 能力。

比如百度智能云率先在业界提出了“云智一体，深入产业”的主张，发布了 200 多款产品和数十个解决方案，将百度 AI 技术释放到金融、物流、工业、农业等多个行业。华为云在 2021 年启动盘古大模型，并在 2022 年聚焦行业应用落地，基于盘古大模型的通用能力，打造了盘古气象大模型、盘古矿山大模型、盘古电力大模型、盘古药物分子大模型等。

可以说，云智合流，为中国 AI 跟上 ChatGPT 的大模型路线，奠定了基础。

2023 年以来，在海外算力形势愈发严峻的背景下，国产预训练大模型依然实现了“井喷”，在文本处理、图像生成、音视频生成、多模态等各个任务中，都完成了占位。放眼全球，唯有中美这两棵繁茂的 AI“榕树”。

让深度学习算法的这颗“种子”，在中国扎根、生长、成熟，这本身就是一种能力的自证。

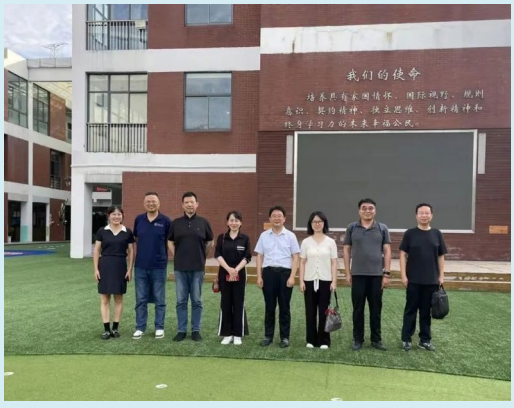
回顾深度学习的十多年历程，或许某一种具体的算法会被更新更好的算法所取代，但这个雨打风吹、反复更替的过程，也让中国 AI 在时光中变得愈发坚韧，积蓄了经验、汇聚了人才、释放了信心。

只要根深蒂固，任尔东西南北风，中国 AI 都能在每一次技术趋势中，生长出新的枝丫，结出产业期待的果实。

学会动态

江苏省计算机学会走进南京新书院悠谷学校——共探 AI 赋能基础教育新路径

2025 年 6 月 30 日，江苏省计算机学会秘书长金莹教授一行莅临南京新书院悠谷学校，进行了深入的参观与交流。此行旨在实地调研人工智能技术在基础教育阶段的创新应用与实践成果，探索“校企研”协同赋能未来教育的新模式。



面向中小制造企业的云边端协同关键技术及应用

——2024 年江苏省计算机学会科学技术奖一等奖

项目名称：面向中小制造企业的云边端协同关键技术及应用

完成单位：常州信息职业技术学院，南京信息职业技术学院，四川职业技术学院

项目简介：

制造业是立国之本、强国之基，也是科技创新的主战场。以工业互联网等为代表的新型基础设施，孕育着经济高质量发展的新动能，是推动制造业转型升级的重要动力。当前，中小制造企业面临着物质流、能量流、信息流等海量多源异构数据的流失，设备侧数据采集失效、边缘侧数据预处理缺失、云端侧运维管理效能低等诸多问题。本项目通过架构多云管理平台，设计多维工业大数据语义描述模型与方法，运用工业大数据采集统一框架，采取多源异构数据获取与融合技术，实现面向中小制造企业的云边端协同关键技术攻关与服务应用。

2019 年起，常州信息职业技术学院校长徐建俊教授牵头攻关中小制造业企业上云“最后一公里”难题，在工信部工业互联网创新发展项目和国家重点研发项目的支持下，实施“工业大数据应用技术与教学研究中心 - 中小制造企业设备数据采集项目”，该项目一举突破中小制造业企业多元异构数据融合技术瓶颈并取得预期效果。项目首创的工业互联网异构数据的边缘计算关键技术达国内领先水平。

1. 构建了面向工业互联网的多云管理平台，一体化协同公有云、私有云、边缘云。实现多云间数据协同、存储共享、容灾备份、安全管理，为中小企业便捷上云、协同资源、降本增效提供了可行方案。

2．研究了一种通用的工业生产数据统一采集框架，采用模块化设计方法将数据采集、运算、处理和信息传输等不同板块的自由配接，实现了多种数据接口、采集速率和传输方式的适配，以保证采集终端不受任何协议、接口、控制系统限制。本技术最终实现老旧设备数据接入，较传统单一接口数据接入率提高 70%，设备可接入率达 95% 以上。

3．提出了多源异构工业生产数据获取与融合技术。研发基于 GPRS/3G/4G/5G/ 北斗 /WIFI/RF 的远程数据采集终端，对设备生产数据的实时采集、数据打包、远程发送，消除信息孤岛，实现系统间数据联通共享，使得生产数据在生产过程中快速、平稳采集，从而实现 100% 的数据传输准确率。

4．设计了多维度工业大数据语义描述模型与方法。针对物联网大数据的时域特征、频域特征与时频特征组成的多维联合特征，搭建多维度数据语义描述模型，研究基于多维度语义描述方法。通过各类特征之间信息的相互补充，对多维联合特征进行降维，减少信息的冗余，实现工业数据 100% 准确解析。

本项目共申请专利 65 项，授权国内发明专利 17 项，实用新型专利 28 项，获得软件著作权 31 项，参与制定国家标准 7 项，主持制定团体标准 15 项。在本领域发表论文 34 篇。项目突破了中小制造业上云最后一公里技术瓶颈，

成果应用于 2,000 多家中小制造业企业，新增产值 28.2 亿余元，新增利润 2.5 亿余元。项目先后获得 2021 年中国轻工业联合会科技进步奖三等奖，2021 年江苏省轻工协会科技进步奖二等奖，2022 年江苏省轻工协会科技进步奖一等奖等科技奖项

主要科技创新

本项目在国家工信部项目资助基础上，与企业联合，自筹经费，攻关中小企业的云边端协同关键技术及装备，从新技术、新工艺到新装备，自主创新，突破了系列技术难题。创新研究了一种通用的工业生产数据统一采集框架，提出了多源异构工业生产数据获取与融合技术，设计了多维度工业生产大数据结构化描述与语义关联模型，开发了多云管理平台，完成数据信息粒化、同化处理，形成统一标准，实现工业生产现场设备状态监测、预测分析、预防性管理等远程的生产监控与运维。项目攻关了中小制造业企业数据采集“最后一公里”难题，建立了“工业大数据应用技术与教学研究中心”，一举突破中小制造业企业上云技术瓶颈，取得理想效果。项目首创的工业互联网异构数据的边缘计算关键技术达国内领先水平。

项目建设以满足中小制造业企业设备生产数据采集为目标，有力支撑中小制造业企业制造模式。多云平台主要可划分为边缘层，平台层以及应用层三方面。

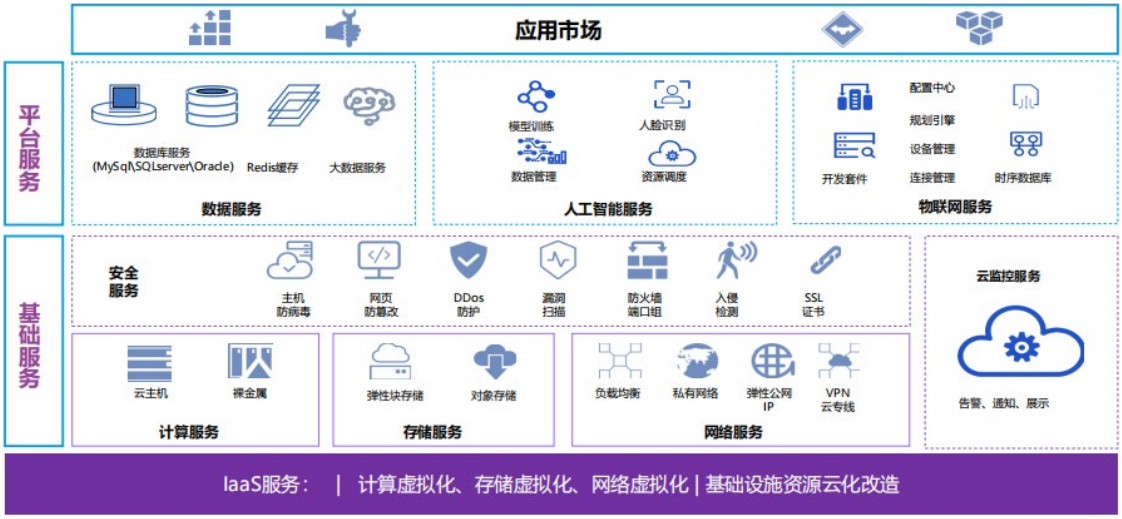


图 1 多云管理平台架构

图 1 为项目多云管理平台架构，开发了开源的多云管理平台帮助企业在不同的云平台之间进行集成与协同，提高资源利用效率和工作效率。通过多云管理平台，帮助企业动态地在不同云平台上部署和调配应用程序和工作负载，以实现资源的最优配置和负载均衡；通过多云架构的容灾方案，提供数据备份和容灾的解决方案，避免单点故障和数据丢失风险；为中小微企业提供了灵活的成本控制和优化方案，避免资源闲置或浪费，最大程度地降低云基础设施成本。

一、关键技术

1．工业装置嵌入式采集技术

目前工业装置几乎都含有电机，通过多种技术手段，将电机运行数据采集设备集成在电机接线盒内，可解决70% 以上工业设备数据采集。采用金属板将接内盒内的空间分为上下两个独立的空间，并对多传感器数据采集电路进行了特殊设计，从而采集电机相关数据，进而采集设备相关数据。基于当前工业设备，研发了工业级智能网关，结合常州信息职业技术学院工业大数据中心平台，内置设备通讯协议，实现远程采集数据。开发了通信“四码合一”系统，通过扫码进行安装，实现信息采集。

以工业电机数据采集为例（图 2），通过增加了电路板层和布局，提高信号路径的抗干扰能力以及电源回路的耦合滤波作用，合理安排强电回路和多传感器数据采集设备在空间上的分布和装配，消除机械振动对设备工作的可靠性带来的影响；为降低电机温度的升高对数据采集的影响，采集前端电路还增加了温度补偿功能。经过大量前期的基础性测试，测试结果显示了所设计的数据采集设备具有很好的测试性能和稳定的可靠性。

自主研发的工业级智能网关（图 3）为 RJ-45 网口、RS232 或 RS485 的 PLC、触摸屏等产品提供远程下载程序和远程数据采集功能。

开发通信“四码合一”系统（图 4），根据预置的策略定期生成与发布源设备凭证数据块，采集终端在对设备工作数据进行采集、上传的同时，该数据块所附着设备在平台的唯一编码、设备拥有者在平台的唯一编码、采集装置在平台的唯一编码及设备在生产商处的唯一编码，这四种编码关联程度极高，都将作为设备的身份数据。此外，结合数据采集时的地理位置与时间，并且考虑到数据的安全性，采用加密方法中的散列算法融合上述所有数据进行上传，将可以保证最终工业设备数据的真实性。

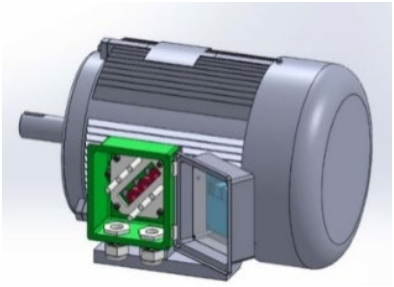


图 2 嵌入式数据采集装置

图 3 工业级智能网关

图 4 四码合一

2．异构数据获取融合技术

综合考虑多源异构数据的时域特征、频域特征与时频特征组成的多维联合特征，通过各类特征之间信息的相互补充，实现数据的准确解析。对特定数据进行时域、频域特征以及时频特征的提取，构建数据的多维联合特征。采用基于动态遗传算法的特征选择方法，实现多维联合特征的选择，基于主成分分析法（PCA）的特征融合方法对多维联合特征进行降维，减少信息的冗余。对数据特征值进行聚类分析，利用基于深度卷积神经网络的深度学习方法对数据特征进行分类处理，通过特征信号分类判断设备类型及加工类型，实现设备数据的正确识别，从而实现真正意义上的多维度数据采集。

异构数据转化解析过程（图 5），通过信号解析实现设备生产数据的实时采集（图 6）、数据打包、远程发送，自主完成故障预警、数据加密、身份验证等功能，信号指征分析实现了从设备信号到离散数据解析通道，把“数据采集”分割成了“前台信号采集、后台数据解析”两大模块，将大量工作移植到后台，实现了前台装机的极度简易化，数十倍提高了效率。

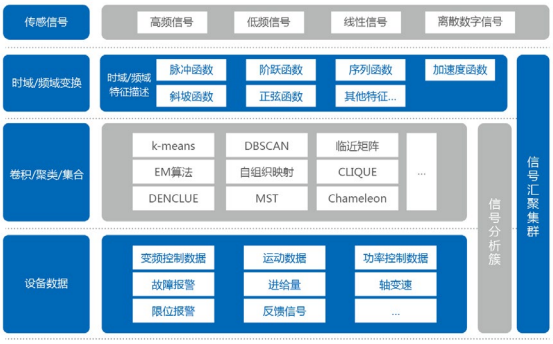


图 5 异构数据转化解析技术示意图

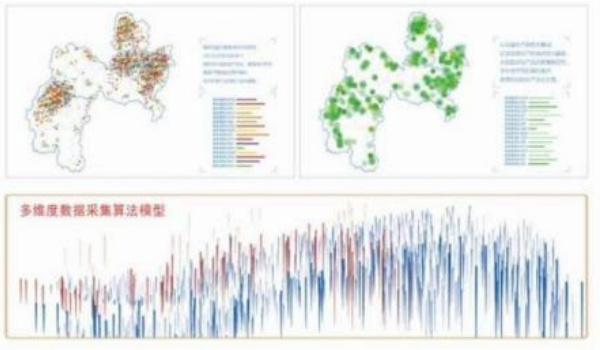


图 6 多维数据采集算法模型

3．数据结构化描述与语义关联技术

研究了多模态数据的语义描述模型和基于多类的语义描述方法（图 7），根据不同类型工业设备的差异性，以设备为中心区分不同类型的工业设备的数据；考虑同类型设备的数据除去相似点，其数据本身在语义关联的大小、频率、中心性等方面将存在差异，进一步以数据为中心区分同类型的工业设备数据，实现语义对齐与知识融合，为后面的数据存储、检索及应用提供支撑。

自主开发数据蜂巢技术（图 8），该技术依托开创性数据通信方式，进一步拓展的 3D 数据结构，专门容纳离散性异构数据；将 3D 数据压缩为三维空间模型；通过 GPU 服务器对空间图形对其进行三维解析，最终实现数据三维模型可视化。

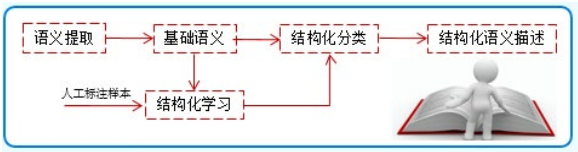


图 7 结构化描述与语义关联技术

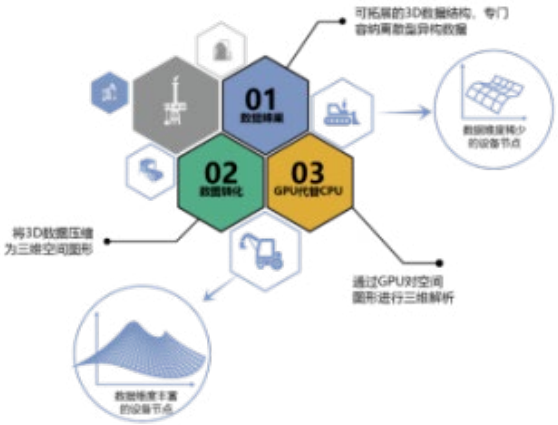


图 8 数据蜂巢技术

4．基于云边协同的产品缺陷检测技术

研发了基于边缘计算的产品缺陷检测系统（图 9），系统采用了一种复杂背景条件下缺陷智能检测技术，将对称注意力机制引入检测网络，并采用对称数据增强方法，解决了细微、遮挡、易混淆表面缺陷的漏检和误检难题，提升了整体检测准确性。同时，构建了一种图像小样本智能分类建模方法，基于多尺度特征构造多级标签传播网络，并基于信息扩散理论，解决训练样本不足情况下的模型构建难题，有效提升了不均衡样本的分类准确性。

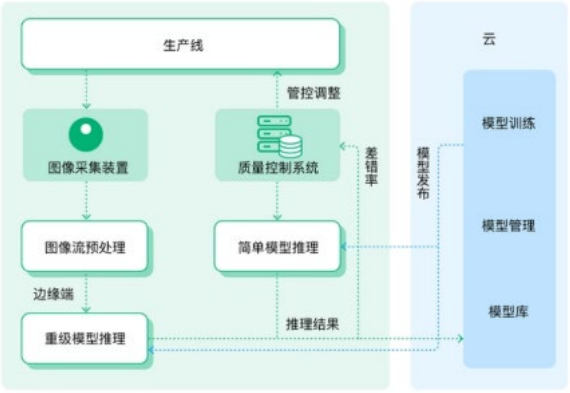


图 9 缺陷检测系统架构

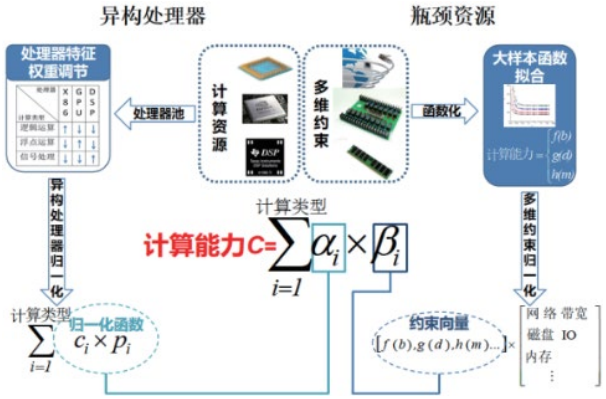


图 10 多维资源量化

5．多维资源算力度量

采用同构处理器集中式的规模化运算，计算负载时间开销与处理器数量关系，实现多维资源量化（图 10）。基于平台中计算资源结构复杂，边缘计算中异构的节点性能往往难以通过处理器主频等简单手段进行量化，相同的计算任务在不同处理器中执行的时间开销难以保障，由此可导致控制节拍下的配置参数错误等系统故障。平台中的任务执行时间受处理器结构、带宽、缓存等瓶颈资源的综合影响。平台在进行卸载和迁移操作前，需要根据各节点的实际负载和资源结构进行分析，以确保任务部署后的最坏执行时间满足其实时性需求，并通过现有虚拟化和实时演算技术提供资源的按需分配、动态配置、负载预测等技术支持。

创新点一：项目以工业设备电控信号 / 数据采集分析为核心，研究了一种通用的工业生产数据统一采集框架，采用模块化设计方法，将数据采集、运算、处理和信息传输等不同板块自由配接，构建精准、实时、高效的数据采集互联体系，实现了多种数据接口、采集速率和传输方式的适配，以保证采集终端不受任何协议、接口、控制系统限制；保证其适用于所有企业、任何设备。攻关中小制造业企业上云“最后一公里”难题，一举突破中小制造业企业上云技术瓶颈，关键技术达国内领先水平。

创新支持：

验收报告，检测报告，查新报告，专利，国家标准

专利：“耦合 Duffing 振子快速数字信号检测方法（ZL 2020 1 1172105.7）”

标准：国家标准 GB-20211126“数字可寻址照明接口 第 101 部分：一般要求系统组件”。

创新点二：项目提出了多源异构工业生产数据获取与融合技术。该技术采用信息熵与条件熵理论来度量不同数据采集渠道（如 GPRS/3G/4G/5G/ 北斗 /WIFI/RF 等）的稳定性；引入“时空散度”的概念来度量数据获取的空间均匀性，并设计支持实时更新的任务在线分配算法来保证多渠道采集过程的高效性。对设备进行边缘数据信号实时采集和预处理、数据打包、远程发送，自主完成故障预警、数据加密、身份验证等功能，消除信息孤岛，实现系统间数据联通共享。

创新支持：验收报告，检测报告，查新报告，专利，国家标准

“基于数字孪生的智能生产线触控系统及方法”（ZL 2021 1 0241258.0）。

标准：“国家标准 -20221014-LED 模块用直流或交流电子控制装置性能规范”。

创新点三：项目设计了多维度工业生产大数据结构化描述与语义关联模型。针对物联网大数据的时域特征、频

域特征与时频特征组成的多维联合特征，提出基于语义概念相似性网络的大规模结构化学习算法，以及基于无监督深度学习的多模态数据语义对齐方法。引入深度学习算法，挖掘适合大规模工业生产数据的高层次特征表示和自适应概念，实现基于深度学习的无监督语义模型提取。兼顾计算和网络资源以及数据传输的有效性，形成云端和边缘计算资源的合理和优化配置。通过各类特征之间信息的相互补充，对多维联合特征进行降维，减少信息的冗余，实现数据的准确解析。

创新支持：验收报告，检测报告，查新报告，专利

专利：“电子信息设备”（ZL 2018 1 0826064.5）；

“移动通讯终端”（ZL 2018 1 0485598.6）。

创新点四：项目基于工业互联网标准层次架构，以人工智能与边缘计算技术结合为基础，设计了产品瑕疵检测系统实现产品瑕疵自动化检测与分拣功能。针对工业制造过程中的产品质量问题，基于模板的瑕疵图像识别技术，收集产品多类正负样本模板；结合边缘检测与分割算法，精准定位检测细节；改进深度学习关键算法，自适应产品光照、角度、加工差异等细节差异；精准定位瑕疵类型与位置，实现产品自动化精确质检与分拣，在较短时间内完成大量产品的自动检测，极大提高了产品检测效率，减少检测环节人力资源需求。

创新支持：验收报告，检测报告，查新报告，专利

二、与当前主要国内外同类技术的主要参数、效益、市场竞争力的比较

项目创新的工业互联网异构数据的边缘计算等技术，成功突破了困扰中小制造业企业面临的上云瓶颈，项目数据采集许可表明，本项目 2,000 多家中小企业反馈采集的数据质量高，本项目技术对比情况见表 1。

表 1 典型系统对比

名称	指标点	龙头企业平台			本项目
		海尔	徐工信息	阿里云	常信院
基础情况	连接设备数	71w	70w	14w	4w
	数字模型数	1539	474	40+	100+
	工业 APP	2379	1542	450+	500+
	活跃用户	6.3w	13.5w	1000+	2000+
	活跃开发者	5336	3113	19000+	8000+
评价说明		世界级工业互联网平台	国家级工业互联网平台	行业级工业互联网平台	区域级工业互联网平台

说明：

1. 表一为几家企业工业互联网平台能力典型对比结果，数据来源 2019 年 7 月，中国工业新闻网《国家级工业互联网双跨平台（公示）能力分析》；

2. 近年来，项目成果逐渐转变为生产力，2021 年，2022 年新增产值近 20 亿，预计后两年新增产值可达 30 亿。

3. 本项目创新技术相比龙头企业技术，技术应用已延伸至长三角区域的建设，后期将辐射至全国，建立推广应用。包括制造、环保、消防等领域，在相关产业的升级和发展中将显现越来越大的市场竞争力。

郑州云海科技有限公司

单位介绍

郑州云海科技有限公司成立于 2015 年，作为北京航空航天大学计算机学院教学成果转化平台，是国家级高新技术企业、专精特新中小企业、科技型中小企业。也是机械工业出版社数字教材战略合作单位、华为生态伙伴、曙光教育政企合作伙伴、寒武纪高校实验体系合作伙伴、北京航空航天大学计算机学院优秀校友企业、中国软件行业协会高等教育产教融合分会委员会秘书处、全国青少年信息技术与计算思维（TCTY）能力评测与等级认证技术平台。全国大学生计算机系统能力大赛平台提供方。

公司面向教育用户的“希冀平台”系列产品，是人工智能赋能的全过程交互式在线教学平台，以大模型底座和知识图谱为核心，贯穿教学、考试、实验与实践、教学大数据自动分析整个教学全过程。可全面支撑计算机、大数据、人工智能、集成电路等信息类专业的教学实践。截至目前，“希冀平台”用户覆盖包括北京大学、中国科学技术大学等公立本科高校超过 437 所。平台建成了涵盖实验、质量指标及过程控制的完整在线实验体系，实现了“任何人、任何时间、任何地点均能开展实验学习”的目标。通过持续追踪和采集全过程学习数据，支撑教师开展个性化教学和教学方式创新研究。

产品体系：提供计算机系统能力实验平台、人工智能实验平台、大数据实验平台、大模型技术与应用实训平台、FPGA 在线实验平台、AI4S 智算平台、算力服务平台等产品，为高校信息类专业的实验、教学、科研提供一站式解决方案。

大赛支撑：支撑了全国大学生计算机系统能力大赛。基于在线化的硬件实验评测平台，可实现对参赛学生自主设计的 CPU、操作系统、编译系统、数据库系统、智能系统进行功能评测和性能评测，为培育我国高端芯片、关键基础软件的后备人才发挥了重要作用。

400+ 本科高校案例：用户已覆盖包含北航、武大、中科大、湖南大学、重庆大学、 西北农林科技大学、中国科学院大学、山东大学、东北大学、大连理工大学、北京大学、西北工业大学、四川大学、南开大学等在内的 400 余所本科高校。

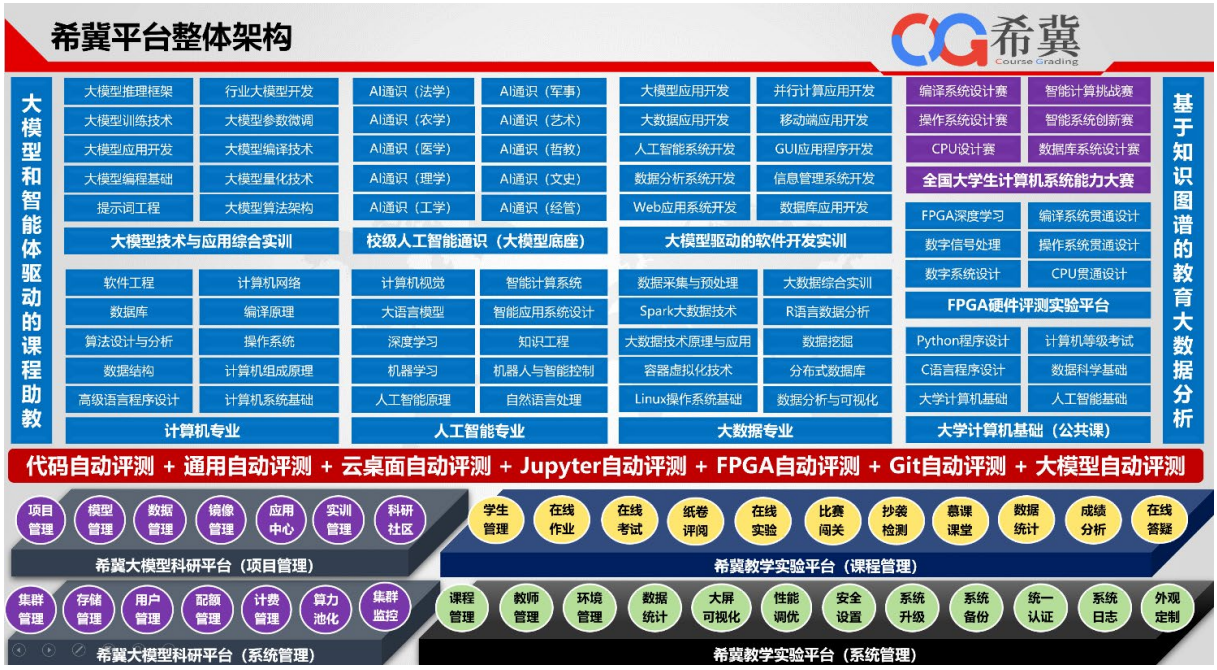
数十家企业案例：凭借领先的技术能力、可靠的产品质量、卓越的服务口碑，也被包括中国移动集团有限公司、中国建设银行总行、中国石油天然气集团有限公司、北京航天飞行控制中心、中国电子科技集团第二十二研究所等

在内的数十所企事业单位所采用。

希冀教学、实验、科研一站式解决方案

一、希冀信息类专业教学实验科研一体化平台

希冀信息类专业教学实验科研一体化平台 (简称希冀平台) 是融合课程管理、自动评判、代码评测、在线实验、代码查重、文档查重、作业考试、纸卷评阅、比赛闯关、在线答疑、MOOC 课堂、课堂工作台、课堂小程序、监考小程序、GitLab、毕业设计、算力平台、工程教育认证、教育大数据采集、教育大数据接口、教育大数据分析、教育大数据应用等功能为一体的大型综合教学实验科研平台。



二、人工智能通识课程实验平台

希冀人工智能通识课程实验平台提供多种智能化评测实验环境，包括代码自动评测、神经网络可视化自动评测、算法模型自动评测、Jupyter 自动评测、云桌面自动评测以及大模型自动评测等六种支持自动评测的在线实验环境。实验平台以大模型为底座，提供了数百个大语言模型和多模态大模型以支撑融合了各类学科领域知识的人工智能通识实验的开展。基于实验平台，建成了覆盖工、理、农、医、经管法、文哲史教、艺术、军事等 13 个学科门类的全学科人工智能通识实验体系。实验平台集成了大模型 AI 课程助教，教师可一键开启双师教学模式。实验平台支持本地化交付部署，已适配信创国产化硬件平台。

三、希冀大模型平台

希冀大模型平台为人工智能通识课程实验平台提供了大模型底座支撑。希冀大模型平台通过资源池化和 AI 加速卡虚拟化技术，实现高性能 AI 集群算力（由 25 台 8 卡国产服务器组成）的统一管理、调度与分配，提供了模型仓库管理、数据集管理、模型服务管理、模型应用管理等丰富功能。大模型平台通过自动感知不同模型服务的负载压

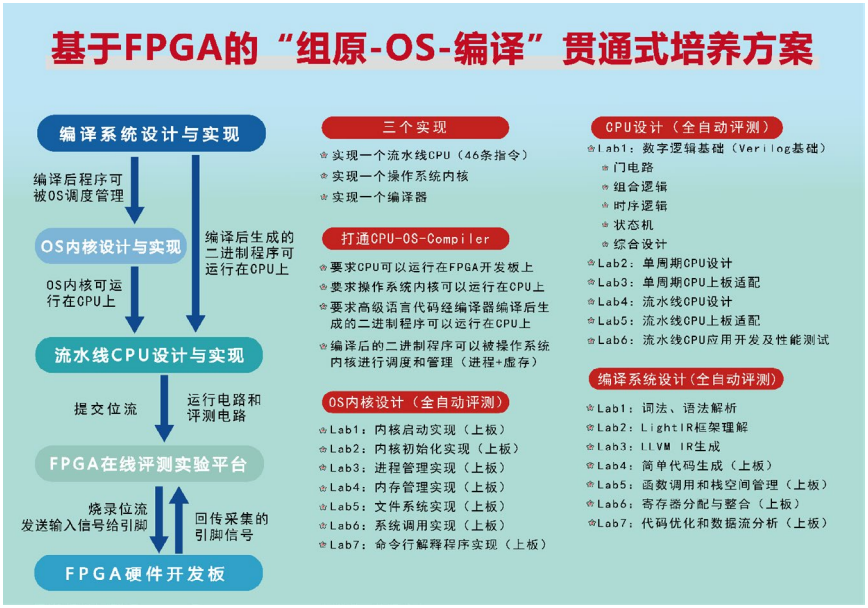
力变化，实现了模型实例并发数的自适应弹性伸缩。基于希冀大模型平台，提供了丰富的深度学习模型、计算机视觉模型、大语言模型、多模态模型、AI4S 科学智算模型，并保持定期更新。希冀大模型平台为通识课实验平台、AI 助教平台、知识图谱系统、大模型技术实训系统等提供稳定可靠的大模型基础服务。

四、FPGA 大规模在线评测实验平台

学生通过浏览器即可随时、随地打开 FPGA 在线实验环境，可随时下载比特流文件到远程 FPGA 硬件开发板上运行，彻底摆脱时间和空间限制。

通过将 FPGA 硬件开发板高密度封装于可 7*24 小时运行的 FPGA 服务器中，可有效避免传统 FPGA 开发板或者实验箱在使用过程中的损耗问题。

单台 FPGA 服务器可封装 28 块 FPGA 硬件开发板，每块开发板支持单独插拔替换，实现即插即用。



五、智能算力服务平台

平台针对传统算力使用场景中算力资源碎片化、用户需求多样化、运维管理工作量大等特点，提供灵活、易用、全面的算力服务一站式解决方案；

可整合零散、异构算力资源进行统一管理与调度，实现化零为整，提升算力资源整体利用率；

为算力租户提供一个可伸缩、可定制、相对隔离且开箱即用的在线计算环境，用户可在浏览器中通过多种接入方式使用平台算力资源；

有效支撑用户研发过程闭环，提供数据准备→运行环境→训练 / 计算→成果归档 / 复用的研发全流程的环境 / 工具支持，促进智能生态蓬勃发展。

希冀平台公众号

免费试用

单位信息

服务热线：037187772668

Email 地址：yunhaikj@aliyun.com

公司官网：www.educg.com

学会动态

面向高校数智素养发展暨人工智能通识课师资能力提升

7 月 3-5 日，面向高校数智素养发展暨人工智能通识课师资能力提升高级研修班在南京顺利召开，来自全国 14 个省市、100 余所高校、近 300 名专家学者齐聚南京航空航天大学。会议由江苏省高等教育学会、江苏省人工智能学会、江苏省计算机学会主办，南京航空航天大学、南京理工大学、南京信息职业技术学院、上海交通大学出版社有限公司承办，聚焦高校教师数智素养提升、人工智能通识课程建设、学科融合创新实践等核心议题开展深度交流。会议开幕式由江苏省高等教育学会秘书长邓志良主持。

学会动态

江苏省中小学人工智能与教育创新校长论坛暨首届优才计划·中小学教师 AI 跨学科教学能力提升营在南京召开

7 月 11 日，江苏省中小学人工智能与教育创新校长论坛暨首届优才计划·中小学教师 AI 跨学科教学能力提升营活动在南京拉开帷幕，来自全省 13 地市 50 余所高中的近 100 位专家、校长齐聚南京大学。会议由江苏省计算机学会主办，慧深学大中衔接交流中心承办，聚焦中小学人工智能与教育创新、教师数智素养提升、人工智能通识课程建设、学科融合创新实践等核心议题展开深度交流。

首届优才计划·中小学教师 AI 跨学科教学能力提升营在宁举办

2025 年 7 月 11 日，首届优才计划·中小学教师 AI 跨学科教学能力提升营于南京顺利召开，由江苏省计算机学会主办、慧深学大中衔接交流中心承办，江苏省计算机学会青少年信息与智能教育专委会副秘书长、优才计划副组长季海涛主持了本次活动。活动聚焦中小学教师人工智能核心素养提升与跨学科融合实践，2 位南京大学教授做了人工智能相关的专业培训，从全省 13 地市、100 多所学校中选拔出的 9 位优秀教师分享了示范课程。

学会动态

2025 年（第 18 届）中国大学生计算机设计大赛南京南决赛在南京大学落幕

7 月 22 日 -7 月 25 日，由南京大学 / 东北大学 / 江苏省计算机学会共同承办的 2025 年（第 16 届）中国大学生计算机设计大赛（Chinese Collegiate Computing Competition，简称“4C”）南京南决赛区决赛在南京大学举行。参加两大类别：“微课与 AI 辅助教学”“数媒静态设计”全国决赛的 896 件作品来到南京参加了这场为期3天全国决赛。来自全国500多所高校、2800多名参赛选手和领队老师、近 900 个参赛队伍顶着夏日炎炎带着灼灼热情在南京大学的赛场上，展现着青春与智慧。

智能制造产业交流 - 走进嘉盛中心

8 月 7 日下午，由江苏省计算机学会产业工委等五家单位联合主办的智能制造产业交流活动在苏州嘉盛中心成功举办。本次活动吸引了来自高校、企业、行业协会等 20 余位嘉宾参与，共同探讨智能建造与建筑产业数字化转型的前沿趋势。

鼓楼高新区管委会领导莅临我会调研交流

2025 年 8 月 8 日南京鼓楼高新技术产业开发区党工委副书记、管委会主任王媛一行莅临我会调研交流，学会秘书长金莹率秘书处全体成员热情接待，双方围绕人工智能技术创新、绿色经济产业融合及常态化合作机制建设展开深度交流。

简　介

江苏省计算机学会常务理事单位

南网数字运营软件科技（广东）有限公司
（南京分公司）

南网数字运营软件科技（广东）有限公司（简称“数字运营公司”）是南方电网数字电网研究院股份有限公司的全资子公司，通过南方电网数字平台（广东）有限公司更名成立，将原南方电网数字平台科技（广东）有限公司的数据平台、数据安全、网络安全业务等有关业务划出，并将原南方电网数字企业科技（广东）有限公司信息化系统建设有关业务划入，注册资本 13.21 亿元。公司成立于 1999 年 8 月，专注于“数字基础支撑平台 + 企业管理数字化智能化”建设运营。负责南网云、统一研发平台等基础平台建设，支撑电网管理平台、生产指挥系统优化升级和深化应用，做好综合办公、营销、财务等业务域管理系统能力提升，同时推动电网管理平台的轻量化改造，打造“四海 ERP”系列标准产品，大力向发电、交通等央国企跨域输出，公司已成为南方电网公司数字化转型和数字电网建设的战略支援部队和主力军。

数字运营公司内设 26 个机构，包括综合管理部（董事会办公室、党委办公室、总经理办公室）、战略运管部、人力资源部、计划与财务部、党建工作部、监督部（纪委办公室）等 6 个职能部门，技术管理部、市场客服部、基础平台研发部、业务研究与解决方案部、先进软件研究中心、交付中心、云南研发中心等 7 个运营支撑部门，人才发展中心、采购中心等 2 个共享服务部门，安全生产平台产品部、供应链平台产品部、规划平台产品部、云平台产品部、中台产品部、数字运营产品部、架构运营产品部、财务金融产品部、党群人资产品部、营销服务产品部、行政合规产品部等 11 个业务部门；下设广州分公司、云南分公司 2 家分公司。截至 2025 年 4 月 24 日，公司在职员工 1268 人，其中研究生学历 207 人；员工平均年龄 35 岁，研发人员占比 84.23%，共有专家 25 名。

公司通过 CMMI 开发和服务双五级评估认证，是国家规划布局内重点软件企业、国家级高新技术认证企业、深圳软件百强企业和重点软件企业，获广东省科学技术厅认定为“广东省电力大数据分析及应用工程技术研究中心”。截至 2025 年 4 月 24 日，共拥有专利 351 项、软件著作权 487 件、商标 50 件。