附件一：申报主题

1. 社会可持续发展 6
1.1 基于地图动态大数据的可持续社会价值创新研究 6
1.2 储能系统在超大规模数据中心领域的关键技术研究 6
2. 机器学习与深度学习 7
2.1 机器学习在新一代材料设计中的关键技术研究 7
2.2 农业中的机器学习算法探索 7
2.3 拟人 AI 研究 8
2.4 延时稀疏奖励环境下的多智能体协作与对抗 8
2.5 迁移学习在在线广告预估领域的技术研究 9
2.6 动态图网络的特征表示稳定性研究 9
2.7 基于机器学习的大数据平台自动调优技术研究 9
2.8 深度学习模型推理加速方法研究 10
2.9 给定模型和数据集下超大 BS 评估与收敛性研究 10
3. 数字图像处理与计算机视觉 10
3.1 针对移动端的 Transformer 小型化的探索 10
3.2 对抗机器学习 11
3.3 人脸活体检测 11
3.4 人体视觉信息的编辑、迁移、生成与建模 12
3.5 数字人驱动及渲染技术 12
3.6 三维人体形态恢复与重建 13
4. 知识图谱与自然语言处理 13
4.1 预训练语言模型研究 13
4.2 机器翻译 13
4.3 医疗机器学习与自然语言理解 14
4.4 常识知识理解与表达以及对话理解 14
5. 语音信号处理与语音合成 14
5.1 海量复杂短视频与直播场景的鲁棒声纹检测 14
5.2 基于非受控环境录音数据的语音合成方法 15
6. 多模态融合 15
6.1 基于深度学习的短视频背景音乐的时序定位 15
6.2 基于深度神经网络的多模态视频分类 16
6.3 医学内容理解与推荐技术研究 16
7. 智能化软件工程 16
7.1 深度学习在软件安全领域的应用研究 16
7.2 深度学习在大规模软件自动化漏洞挖掘中的应用研究 17
7.3 代码大数据和代码智能辅助技术研究 17
8. 密码学与区块链 18
8.1 国密算法的安全性与性能优化研究与实现 18
8.2 基于区块链的大规模实时广告归因技术研究 18
9. 边缘计算 19
9.1 智能边缘计算网络架构与关键技术研究 19
10. 数据库 19
10.1 高可用分布式数据库 19

申报主题介绍

（各主题均不限于给定的建议研究方向，申请人可自行拓展决定。）

1. 社会可持续发展

1.1 基于地图动态大数据的社会价值创新研究

本项目将通过时空大数据融合、分析、建模、评估与优化等技术和理论研究，开展可持续社会价值创新的前沿领域探索。关注领域包括但不限于：乡村振兴、能源、环境、水资源、粮食、碳排放、绿色出行、公众应急、社会公平、城市和区域发展等。提交的项目可以选取一个领域，基于创新的多源动态时空大数据感知、智能分析和数据驱动的专业领域理论模型设计，发现问题、诊断原因、预测趋势和优化决策，形成可理解可落地的理论方法和技术体系。

建议研究方向：

1) 乡村振兴：基于国家统计和社会多源大数据感知技术，精细分析和量化评估全国乡村经济活动、人口结构和资源配置的动态变化，建立乡村振兴战略要素的动态感知、模式分析、决策优化的基础信息理论与技术；
2) 绿色出行：在“碳达峰、碳中和”国家战略的背景下，通过对城市交通设施、路网结构、出行需求、交通方式选择、资源空间布局、可达性等综合分析，探索城市交通的高质量发展和运营方式，优化空间布局，引导绿色出行，服务惠及全民，推动城市交通规划、管理、运营和生活方式的绿色转变、高质量发展和公平服务；
3) 公众应急信息服务：探索基于物联网、互联网和政务的时空大数据的应急识别预警、决策支持和公众服务技术体系；探索不同应急场景的相关技术和服务模式，比如地震、滑坡、洪水、火灾、交通事故、医疗急救，设计和实现可行的落地方案等；
4) 能源和资源：通过时空关联融合自然、人文和社会经济数据，量化和洞察能源经济和资源消耗的时空规律和深层问题，比如水、粮食、碳排放、PM2.5 等；基于基础地图数据和时空动态大数据建立专业模型、分析数据、评估现状、预测趋势和优化决策；设计和实现示范性落地技术和方案。

返回目录

1.2 储能系统在超大规模数据中心领域的关键技术研究

在中国 3060 的能源结构转型与新基建数字化推进的大背景下，低碳数据中心成为关注的热点。传统的数据中心储能系统正在经历变革与挑战。传统的冗余备份系统例如非间断电源（UPS）和铅酸蓄电池，柴油发电机等应用场景正在受到新能源接入后的源网荷储综合能源体系，整机柜锂电池，氢燃料电池等技术的挑战。如何利用数据中心现有的电池和备份资源，构建新型的更加高效，更加清洁，更加安全，更加稳定的数据中心储能系统，并且配合未来可能的大规模新能源接入，会成为一个前沿的课题。如何结合机器学习的能力，对这个领域进行分析也是关注的重点。我们会提供相应的超大规模数据中心样本资源，包括但不限于相关运营数据，技术参数等。

建议研究方向：

1) 锂电池在数据中心中应用安全性的深度研究；
2) 氢燃料电池取代柴油发电机技术研究；
3) 新型储能系统在数据中心领域学科综述发展研究；
4) 储能系统在数据中心新能源增量配电网场景下的技术研究；
5) 基于机器学习的数据中心智慧用能调节技术研究。

返回目录

2. 机器学习与深度学习

2.1 机器学习在新一代材料设计中的关键技术研究

随着人工智能技术的快速发展，数据驱动科学发现继“实验范式”、“理论范式”和“仿真范式”之后正成为“第四研究范式”。当前，可编程材料设计与自动化实验、人工智能、量子化学模拟的交叉融合是材料科学研究的前沿和热点。该技术的发展有助于推动材料研发由“科学直觉与试错”的传统模式迈向“数字化和智能化”的新模式。

建议研究方向：

1) 开发机器学习模型赋能可编程材料设计；
2) 结合机器学习与量子化学模拟，对材料在微观尺度建模，进而提升材料性质预测的准确度；
3) 设计与实践“量子化学计算-可编程材料设计-自动化材料制备与表征-机器学习再设计”的新一代材料设计范式。

返回目录

2.2 农业中的机器学习算法探索

现代农业研究把作物仿真模型和真实自动化温室结合到统一的开发平台，充分利用高效的计算机运算能力，从而加快农业技术迭代速度，突破人类种植经验局限。虽然农作物生长周期长且数据获取成本高，对算法（尤其是强化学习算法）的性能也提出了很高的要求，但此类研究为计算机科学及控制科学提供了一套标准的应用实验平台，推动了相应的理论及算法研究，从而创立了跨学科研究的理论基础。本课题将为研究者提供一个优秀的农业应用场景，以测试新算法的样本效率、鲁棒性、可迁移性等核心能力。

建议研究方向：

1) 能降低物理鸿沟（Reality Gap）的算法工具：在真实的农业环境交互中进行策略学习的成本高昂（例如一次交互就长达几个月，实验成本几十万），因此我们必须寻找一些高精度的仿真工具（如温室模拟器），或者开发一些新的学习算法降低对仿真工具的依赖程度，确保在此基础上学习到的算法能在真实农业场景中应用并获得良好的性能；
2) 能降低新作物开发成本的算法:各类农作物的生长特点各异，需要针对不同作物开发不同的控制算法。由于新作物的仿真器和数据积累都极其昂贵，全国各地的温室大棚配

置也不一，因此需要开发有物种迁移和温室迁移能力的算法，以降低新作物的开发成本，扩大算法的适用范围；

3) 能增加鲁棒性的控制算法：由于气候变化，传感器和控制老化，控制维度高等问题，只有鲁棒性达到一定标准的算法才有可能进行实际部署。在硬件成本有限的前提下，需要通过算法（例如对控制器做多智能体建模）来提高控制的鲁棒性。

返回目录

2.3 拟人 AI 研究

近年来，以 Deepmind 的 Alphastar 及 OpenAI 的 OpenAI Five 为代表，基于强化学习的 AI 技术在游戏领域广泛应用并产生了很大价值。这其中 AI 的拟人化行为是重要的研究课题，其分为两个研究层面：1）基础行为的拟人：AI 的基础行为要符合人类的习惯，比如行走的时候要朝前走，而不能倒着走，也不能走一步退两步；2）宏观策略上的拟人：不同能力的人类对于相同情况的应对方法会有不同，比如开车过弯时，新手一般会减速通过，而高手则可能选择漂移通过。

本课题期望在 AI 拟人化方面开展研究，使得不同能力的 AI 都能表现的像同等能力的人类或者不同能力的 AI 在行为模式上具有不同的表现。合作团队将提供真实游戏中的人类数据（可以从实际玩家的数据中获取人类的经验）以及大规模分布式强化学习平台（10w 核 cpu，1000 块 gpu 的训练资源）对研究予以支持。

建议研究方向：

1) 模仿学习：直接从人类的数据中学习策略；
2) 离线强化学习：基于强化学习的建模方式，从人类的数据中学习策略；
3) 逆强化学习：从人类数据中学习对奖赏的建模。

返回目录

2.4 延时稀疏奖励环境下的多智能体协作与对抗

多智能体协作、对抗、以及人机交互，作为人工智能领域的核心热点问题，广泛应用于现实生活和虚拟游戏环境中的分布式集群控制，无人驾驶，人机交互等领域。本命题旨在研究智能体如何在延时稀疏奖励的复杂环境下自主学习和进化，在下一个或多个行为方面展现出一定程度的智能 与其他智能体的协作与对抗，与环境的交互，与人的协作、对抗和交互。合作过程中，腾讯合作团队将提供相应的实验环境和计算资源。

建议研究方向：

1) 延时稀疏奖励场景下的多智能体协作与对抗；
2) 大规模 3D 复杂游戏环境下的表征学习；
3) 多智能体的超长时间配合建模；
4) 同一游戏不同任务的 AI 能力迁移和泛化。

返回目录

2.5 迁移学习在在线广告预估领域的技术研究

计算广告是当前工业界算法应用最为成熟的领域之一。游戏展示广告是各大广告平台重要的业务组成部分，涉及到游戏广告的定向、点击、转化、付费等链路的模型预估。该领域存在着诸多技术挑战，如多目标建模、延迟反馈、样本稀疏、跨领域跨媒体等。此命题旨在利用腾讯游戏相关数据，来提升游戏展示广告的效率，尤其是利用跨领域（CROSS-DOMAIN），迁移学习（TRANSFER-LEARNING）等前沿算法框架深度挖掘腾讯游戏的数据价值，并迁移应用到游戏展示的广告场景中。

建议研究方向：

1) 设计高效且实用的跨领域、领域自适应、迁移学习等算法与框架；
2) 利用迁移学习框架结合前沿深度学习技术改进在线广告点击率、转化率、付费率等模型精度；
3) 小样本学习，解决数据稀疏与冷启动的问题。

返回目录

2.6 动态图网络的特征表示稳定性研究

社交支付行为受到人与人之间动态变化的关系网络的影响，随着人群行为变化，会有新的用户结点加入、结点与结点之间边的关系也不断调整，整个网络是一个随着时间变化而不断动态演进的过程。金融场景中的很多需求本质上是对用户投资风险策略、投资知识经验、可投资产等潜在特征的把握，如何通过一个动态网络去推理这些潜在的本质特征，是金融行业亟需解决的问题。

建议研究方向：

1) 动态网络的构建及更新技术；
2) 动态网络的特征表示形式及可解释性研究；
3) 不变性特征的提取及度量；
4) 效果验证方案设计及评估。

返回目录

2.7 基于机器学习的大数据平台自动调优技术研究

随着数据规模和用户场景的不断增加，传统基于启发式的调优技术已经很难满足大数据平台在性能和可靠性上的需求，大数据平台实现自动化调优已成为技术发展的主要趋势。这其中也面临着诸多研发挑战：1）智能化地采集关键性能指标并利用采集的指标实时对模型进行更新；2）通过机器学习方法深入分析历史数据和用户行为、自动优化复杂查询任务；3）设计应用特征感知的视图选择和索引技术；4）准确实时地预测工作负载，进行作业故障的自动诊断等。本课题期待通过对这些关键技术的合作探索，推动对大数据平台研究工作的进一步发展。

建议研究方向：

1) 基于机器学习技术的查询优化技术，包括查询代价评估、查询计划选择和分布式执行计划生成等；
2) 应用特征感知的视图选择和索引生成技术，支持从数据接入到数据查询的全流程优化；
3) 基于负载预测的作业自动化配置和智能调度；
4) 作业故障自动诊断。

返回目录

2.8 深度学习模型推理加速方法研究

近年来，深度学习技术在服务器端的应用越发广泛。但随着深度学习模型的愈发复杂，参数越来越庞大，导致推理计算延时很高，单机不能承载等问题出现。本命题专注于深度学习的推理加速，期望在模型服务器端部署方面带来新的研究进展，推动在业务场景的实际落地。

建议研究方向：

1) 推理加速研究，如基于 CPU/GPU 高效支持大规模参数的推理系统或基于模型压缩相关技术的推理加速工具的研究；
2) 业界框架增强研究，如基于 Tensorflow 进行改造，使其能够轻松支持相比于 TFserving 更加高效且支持大规模参数的推理服务。

返回目录

2.9 给定模型和数据集下超大 BS 评估与收敛性研究

在机器学习训练场景中，经常通过使用多机多卡来加速训练从而提升迭代效率，但这随之产生了 BS（BatchSize）收敛的问题，导致收敛精度下降或不收敛。本课题将研究在给定数据集和模型的情况下，如何科学评估 BatchSize 的合理范围，以及评估后，如何在单卡到多卡的扩展过程中，有效保持线性收敛。腾讯将为合作者提供加速机器学习的平台来验证实验效果，并有机会在现场环境中落地。

建议研究方向：

在常见的主流开源模型上，实现一套完整的大 BS 收敛性量化评估手段，通过可以适用于业务实践的科学评估手段，评估最为合理的 BatchSize 值，并在多卡扩展中保持线性收敛。

返回目录

3. 数字图像处理与计算机视觉

3.1 针对移动端的 Transformer 小型化的探索

Visual Transformer 技术相比与 CNN 网络技术，在计算机视觉领域有更好的实现效果以及更合理的结构设计。但目前 Transformer 的模型都是针对 GPU 设计的大型模型，主要原因是 Transformer 整体的复杂度很高，参数量大，同时需要比较强的算力来支撑，所以很难

在移动端实时运行。因此，在移动端支持实时模型计算的探索，对于 Transformer 在移动端 AI（发布器）场景下的落地具有非常重要的意义和价值，可以显著的提升移动端 AI 算法的整体效果。

合作团队将提供相应的场景，模型训练平台（基于腾讯机智与 Venus 做过上层的训练加速和多机多卡的适配），以及 TNN Inference 层面的 OP 加速支持。

建议研究方向：

1) Self-Attention 的小型化；
2) 针对计算机视觉任务的 Transformer 跟 CNN 结构的科学结合；
3) 基于底层 Inference 框架，实现 Transformer 的运算加速。

返回目录

3.2 对抗机器学习

在对抗样本攻击对深度神经网络及其相关应用带来了很大的安全隐患的情况下，对抗机器学习方向研究具有的学术与应用价值与日增加。近期虽然不同的攻击和防御方法相继被提出并取得了一定的攻击/防守效果，但对抗样本的理论机制还非常不明确，并且目前最为有效的基于对抗训练的防御方法存在泛化性不足、训练时间开销大等缺点，无法直接应用到实际的业务中。此外，目前黑盒/物理场景下的攻击效果相比于白盒攻击还比较弱，无法有效的衡量实际系统的对抗脆弱性。建议聚焦对抗性原理探究以及实际场景下的对抗攻击/防御需求，如轻量级防御方法和高效的黑盒/物理攻击方法等。

建议研究方向：

1) 深度神经网络对抗性原理探究；
2) 高效的黑盒攻击、物理对抗攻击算法研究；
3) 高效的对抗防御方法研究，包括轻量级对抗防御和对抗训练泛化性问题等。

返回目录

3.3 人脸活体检测

人脸识别技术的应用越来越普及，如何保证人脸应用的安全变得越发重要。活体检测就是判断人脸是否来自真实的用户，而非照片、面具等其它介质的攻击，保证人脸识别系统安全的关键技术。但很多攻击与真人在视觉上差异非常小，特别是一些高逼真的 3d 面具攻击，这给活体检测算法提出了很高的要求。本课题聚焦活体检测中的难点问题，从 rPPG、域泛化、域迁移、异常检测等方向进行研究，提升活体模型的鲁棒性和准确度。

建议研究方向：

1) 从 rPPG 心率检测着手解决活体问题，重点关注如何消除人脸运动、光照、肤色等带来的噪声及影响；
2) 从图像细节分析、网络结构设计等着手，提升模型精度和效率；
3) 从视频序列分析技术着手，分析真人与介质攻击在时序运动过程中的不同，提升模型稳定性；

4) 从域泛化、域迁移等方法着手，提升人脸活体检测模型对光照、场景、采集设备的鲁棒性；
5) 从异常检测、可解释性分析等方法着手，研究如何提升模型对未见过攻击样式的有效防御。

返回目录

3.4 人体视觉信息的编辑、迁移、生成与建模

随着云游戏技术与产品的发展，面向大屏及客厅场景的云游戏应用成为重要的发展趋势。这些场景中玩家所面对的选择将不再局限于狭义的电子游戏，而是包括体感游戏、健身、舞蹈、视频创作与分享、换装试衣、会议交流等丰富的娱乐场景。

这些应用中，人体视觉信息的迁移、生成、或建模及渲染能力成为关键技术。近年来，虽然相关课题吸引了学术界越来越多的关注，但当前大部分方案在输出稳定性、质量、效率等方面仍然有不足，离商用水平有一定差距。

因此，在这个命题中，我们希望合作方可以通过视觉或图形学的算法研发，实现对人体姿态、服饰、动作、风格等视觉信息中的一项或几项的解耦与编辑能力。无论是基于生成网络、或是 3D 建模与渲染的技术方向，我们均希望以最终呈现效果优先，实现对人体相关图像高品质、高拟真度算法方案的攻关及技术储备。

建议研究方向：

1) 基于 RGB/单目摄像头的人体姿态、服饰、动作的编辑、迁移与生成；
2) 基于 RGB 信息的高品质人体 3D 建模。

返回目录

3.5 数字人驱动及渲染技术

近年来，数字人在虚拟主播、AI 助手、虚拟偶像等领域的应用迅速增加。虚拟卡通形象主播、支持不同形象不同语言的虚拟 AI 主持人、直播带货主播的应用，体现了数字人具有广泛的应用场景以及高确定性的相关市场。

数字人涉及的技术中，驱动和渲染技术是目前业界关注的重点，既有方案通常因高成本、高耗时、难迁移等原因难以应用。探索能够在服务器（CPU/GPU）或移动端等目标平台实时处理，同时生成逼真自然的动作、表情、模型效果的轻量级、高质量的数字人驱动/渲染技术，同时产出高质量的学术成果，是本次研究关注的重点。相关研究成果也有机会在腾讯相关数字人技术中得以应用落地。

建议研究方向：

1) 高精度动作实时识别技术；
2) 高精度人脸表情实时识别技术；
3) 高自然度文本/语音转嘴型技术；
4) 基于多模态的人物动作/表情渲染技术；
5) 高逼真度真人三维采集技术。

返回目录

3.6 三维人体形态恢复与重建

随着 VR/AR 的发展，给人体重建技术带来了许多的发展应用的机遇，例如人体换装，虚拟人等等。然而，3D 数据的缺失，场景与动作的多样性，对算法研发和应用带来了许多的挑战。本课题旨在研究基于 SMPL 一类的参数化模型的三维人体网格恢复与重建，希望在提升算法鲁棒性、建模精细度等方面有所突破。

建议研究方向：

1) 基于 SMPL/SMPL-X 的三维人体形态恢复与重建，提升全身/半身/运动等多种场景和动作的鲁棒性和精度；
2) 着重于脸部和手部的预测，并将精细的局部建模融入整个人体模型当中；
3) 提升模型在不同形体的人物上的表现，特别在边缘贴合度上有所提升；
4) 借助视频多帧或者多视角图片进行重建，获取更富连续性的的精细建模；
5) 探索对于人体衣物的 3D 表现，将不同的衣物建模同时融入人体建模当中。

返回目录

4. 知识图谱与自然语言处理

4.1 预训练语言模型研究

预训练语言模型是近些年自然语言处理领域最重要的创新工作之一。预训练语言模型是采用自监督学习从大规模无监督文本中学习建模文本的有效方式，能够极大地提升模型在下游任务（如文本分类、序列标注、自动问答、对话系统等）的文本理解能力。然而，预训练语言模型的深度文本理解能力相比于人类仍然有较大差距。一方面，语音、图像、视频等多模态信息对于理解文本，尤其是文本中的常识信息具有重要意义；另一方面，可控性、可解释性对于文本理解应用于实际场景十分重要，现有预训练语言模型对这两方面的研究仍处于初步探索阶段。

建议研究方向：

1) 预训练语言模型的多模态训练；
2) 预训练语言模型的可控性；
3) 预训练语言模型的可解释性。

返回目录

4.2 机器翻译

本课题旨在开展基础及应用研究，提升商用机器翻译系统的效果。本命题的主要研究方向是如何缓解真实系统中常见的错翻、漏翻等核心的忠实度问题，同时探索如何更充分地利用当前海量的双语（数亿句对）和单语（百亿句子）数据。

建议研究方向：

1) 基于大规模（含噪声、多领域）语料上的模型学习；
2) 探索针对机器翻译的预训练，以更好利用单语数据；

3) 探索新型网络结构和训练框架；
4) 改善实体翻译及低频词翻译问题。

返回目录

4.3 医疗机器学习与自然语言理解

医疗自然语言处理面临患者口述口语化、标注难度大、临床电子病历结构化等难题，我们希望通过医疗医保领域的机器学习与自然语言理解技术，来提升机器学习模型在智慧医疗及医保领域产品中的表现。

建议研究方向：

1) 医疗医保智能问答：包括文本匹配、答案生成、问题生成、对话系统、阅读理解、摘要生成、标签树扩展与构建等；
2) 医疗医保 NLP 基础能力：包括医疗实体识别、链接、医疗语言模型、知识蒸馏、文本分类、序列标注、同义词挖掘等。

返回目录

4.4 常识知识理解与表达以及对话理解

本命题的主要研究方向是如何结合符号和向量进行对话的精确表达，同时探索如何更充分地利用当前海量数据进行对话领域的预训练，从而提升对话理解和建模的效果。

建议研究方向：

1) 常识知识的提取表达：常识作为一种特殊的知识，跟已有的知识图谱中实体知识有很大不同，因为常识在句子中的理解和使用往往是隐含的。常识知识应该如何提取表达，如何让模型更好的具备常识理解推理的能力，以及如何评估模型常识理解推理能力的准确率和召回率是本方向期待研究的内容；
2) 结合符号化和向量化的对话表示：防止对话中出现答非所问的问题，并且提高对话模型的可解释性；
3) 结合符号化理解的成果进行对话领域的预训练模型：如何充分考虑对话领域的语言特点（省略、指代），结合符号化理解的成果进行对话领域的预训练模型，提升对话建模的整体质量。

返回目录

5. 语音信号处理与语音合成

5.1 海量复杂短视频与直播场景的鲁棒声纹检测

探索如何从海量 UGC，PGC 音视频数据中检测出指定的已注册说话人，实现基于声纹的稀疏查找和时间戳定位。短视频与直播场景复杂，目标语音会受到背景音乐、各类噪声、混响和编解码的影响，加之目标语音片段时长可能很短，如何准确检测声纹是一个极具挑战的问题。另外，短视频和直播数据中也可能存在主动对抗，如变速，变声、伪造等，进一步增加了声纹检测的难度和挑战。

建议(但不限于)研究方向：

1) 基于 Vocoder 的音频前处理方法，降低信道失配、噪声、对抗对检测性能的影响；
2) 端到端声纹检测与识别方法，提升系统的检测性能；
3) 训练数据的仿真与生成，扩充声纹检测与识别系统的训练数据，提高系统的性能与泛化能力。

返回目录

5.2 基于非受控环境录音数据的语音合成方法

目前大多数成功的语音合成系其训练采用的是由专业人员在录音棚录制的语音数据，这种专业录音的数据量一般有限，从而限制了合成语音的风格，韵律和音色的多样性。如何利用非受控环境的录音数据来训练或改进语音合成系统是一个值得探索的研究方向。

建议研究方向：

1) (基于数据驱动、对抗学习等的)音质、韵律解耦方法；
2) 基于非受控环境录音数据的韵律迁移方法；
3) 基于非受控环境录音数据的高音质语音合成方法。

返回目录

6. 多模态融合

6.1 基于深度学习的短视频背景音乐的时序定位

短视频配以适合的背景音乐片段可以增强其情感氛围及表现力，影响观众的行为和情感反应。然而，从海量的音乐库中为短视频定位合适的背景音乐片段需要熟练的视频制作经验，这提高了短视频制作的壁垒以及成本。因此，一种能够从音乐库中为短视频搜索并时序定位合适的音乐段落的算法变得十分有意义，不仅可以降低一般用户的短视频创作门槛，还能够为专业视频创作者提供有效的背景音乐建议，降低制作成本。

学者们对例如图像-文本的多模态信号匹配技术的研究已经持续多年，而作为新兴领域的视频-音乐片段匹配尚未得到足够深入的研究。本命题旨在通过研究基于深度学习的多模态内容理解技术，探索为短视频在音乐库中时序定位出合适的背景音乐片段的可能性。

根据研究的需要，我们可以提供带有背景音乐的短视频数据集，具有版权的音乐数据集和一系列所需的计算资源。

建议研究方向：

1) 视频-音频内嵌表征生成：将输入的视频和候选背景音乐转换至共享低维空间的内嵌模型，并使用度量函数进行匹配；
2) 音频片段时序定位：时序定位背景音乐的片段，从而生成与输入视频产生最高置信度的音频片段；
3) 多模态信号对齐：由于通常完整的背景音乐会比短视频更长，因此对齐两个长度不同的视频-音频多模态信号对于匹配和时序定位非常重要。

返回目录

6.2 基于深度神经网络的多模态视频分类

视频是一种融合视觉、文本、听觉等多种模态的多媒体数据。随着短视频业务的增长，对海量的视频数据进行内容理解显得十分重要，在视频推荐、视频检索等领域有着广泛的应用。其中视频分类是视频内容理解中最为基础的任务，目前在业务场景中对于视频的理解，主要还是通过对于视频中的视觉、文本和听觉等信息独立建模，然后对独立模型所得结果进行融合。随着业务的发展，基于独立模型基础上的融合已经不能满足精度的需求，如何在学习过程中融合音频、文本、图像等多个模态的信息，通过不同模态间进行协同学习，实现不同模态间的信息互补，具有非常重要的研究、实践意义。

建议研究方向：

1) 多模态联合建模：单个模态信息可以提取出多种语义信息，该方向研究如何利用不同模态的结构化信息进行建模，提升视频内容理解效果；
2) 多模态协同学习：不同模态包含的信息量不同，对结果的贡献度也不同，该方向研究如何协同学习不同模态特征，综合判断得到全局最优解。

返回目录

6.3 医学内容理解与推荐技术研究

医学数据的信息化产生了大量的多模态数据，包括文本数据，图片数据，影像数据，时序数据等等。这些数据中蕴含着大量的知识，而目前没有被很好的挖掘利用。我们部门积累了大量的医学数据，包括医学知识图谱，医学文献，医学视频，患者行为数据，电子病历，影像数据等等，如何深入理解这些数据，挖掘出可用的知识，更好的服务于患者和医生，就成了非常有价值的研究课题。

建议研究方向：

1) 基于无结构文本的医学知识抽取、表示和推理；
2) 结合医学知识图谱，融合本文、图像和视频数据的医学预训练模型；
3) 多模态医学内容（视频、直播和文章）的个性化推荐技术研究；
4) 基于知识图谱和多轮问答的疾病初筛系统；
5) 患者诊疗周期中的预测服务研究，疾病阶段预测，恶化预测，复发预测等。

返回目录

7. 智能化软件工程

7.1 深度学习在软件安全领域的应用研究

随着软件复杂度的不断提升，大规模源代码和二进制软件的漏洞挖掘工作面临新的机遇和挑战。本命题希望把深度学习相关技术（例如自然语言处理、图神经网络、深度强化学习等）应用于软件安全研究中，其成果可以对传统的逆向工程、模糊测试、漏洞挖掘等有较大促进。

建议研究方向：

1) 计算机语言的表征和分类研究，例如识别二进制软件对应的编译器、编译优化选项、第三方库、开发作者等信息；
2) 计算机语言的自动生成和翻译技术研究，例如自动生成用于编译器(解释器)模糊测试的符合语法结构的程序代码；利用机器翻译技术实现二进制和源代码之间的相互翻译工作；
3) 基于程序语义表征的安全属性分析研究，例如代码相似性分析、API 误用分析、已知/未知漏洞检索等；
4) 二进制可执行文件的软件成分分析，如第三方库及其版本号等的分析与识别。

返回目录

7.2 深度学习在大规模软件自动化漏洞挖掘中的应用研究

随着企业对软件安全要求的提升，模糊测试被认为是行之有效的从内部提升产品安全程度的测试方法。企业与开源项目的大量软件都有自动化安全测试的需求，这也为安全测试提出了新的机遇和挑战。

本命题希望把深度学习的相关技术，如自然语言处理、图神经网络、深度强化学习等应用于软件安全研究中。其成果可以对软件自动化测试、大规模软件测试、模糊测试外壳生成、安全分析、漏洞挖掘等领域的技术发展有较大的促进作用。

建议研究方向：

1) 计算机语言的分析及自动生成技术研究，例如：自动分析给定软件源代码，然后自动生成符合语法结构、可编译的 Fuzz 外壳代码；
2) 闭源软件的自动分析以及自动生成技术研究，例如：将其他工具（如 IDA）生成的闭源软件的反汇编代码，进行自动处理，生成符合语法结构、可编译的 Fuzz 外壳代码；
3) 大规模分布式 Fuzz 效率提升的研究，例如：对 Fuzzer 的样本生成或变异策略等进行优化，以提升 Fuzz 效率；或优化开源的大规模分布式框架（如 OSS-Fuzz）以提高框架自身的效率等。

返回目录

7.3 代码大数据和代码智能辅助技术研究

在大型企业的软件开发过程中，每天会产生海量的代码和行为数据，对这些数据进行规范化存储后加以分析利用，以生成具有一定价值的关联画像和数据索引，可用于内部开源和协作行为分析、效能度量、全局搜索、风险监控和异常发现等目的。进一步，在企业级海量代码库等大尺度数据规模条件下，自动代码补全、智能提示可以提高软件研发效率，文档、注释生成和风险预估可以帮助改善代码评审体验，克隆检测、代码水印、行为风险预测可以用来保障代码的合法合规的高效复用。此外，一些特定场景下（如电商小程序、游戏运营活动等），编程行为具有高重复性，自动编程可将开发工作量降低而加速产品迭代和试错能力。以上各种辅助程序员代码开发工作的研究探索，具有非常重要的产业实践意义。

建议研究方向：

1) 代码大数据分析、代码搜索等研究；
2) 基于机器学习、知识推理及 NLP 方法的软件研发辅助研究，如代码自动补全、智能提示、注释和文档自动生成；
3) 软件产权保护和可追溯性研究，如代码克隆检测和传播跟踪；

4) 特定场景的自动编程。

返回目录

8. 密码学与区块链

8.1 国密算法的安全性与性能优化研究与实现

随着《中华人民共和国密码法》的颁布与实施，密码合规成为了工业界的一大课题。而国密算法软件实现的安全高效应用成为密码合规的重要一环，具有重要的研究意义。

与此同时，软件密码模块也面临很多业界难点需要攻关。首先，在安全性方面面临很大的挑战，如密钥的安全管理、在不可信环境下的内存安全风险、终端设备的侧信道攻击风险、随机数安全等；其次，在性能上也有某些算法与国际算法存在差距的问题，如 AES 有成熟的 CPU 扩展指令集支持、比特切片等各种加速算法，而国密 SM4 在性能加速上仍有很大的提升空间。

本课题希望结合国密算法体系，在软件密码模块的安全性和性能上进行探索，攻克业界难题，进而联合推动软件密码模块相关技术领域标准的制定。

建议研究方向：

1) 研究可增强 SM2/SM3/SM4 算法安全性的方法，如抗侧信道攻击、协同签名/加解密等；
2) 研究扩展 SM4 算法或者密钥安全强度的方法，使其达到 AES256 的安全强度；
3) 研究基于国密的可应用于软件密码模块的高强度密钥管理机制；
4) 研究 SM2/SM3/SM4 算法的性能优化手段，包括但不限于算法优化、工程优化等；
5) 研究基于国密的密码学安全的随机数发生器。

返回目录

8.2 基于区块链的大规模实时广告归因技术研究

广告业界中常说的广告转化归因，本质上是将流量方的曝光和点击数据与广告主的转化数据从用户维度进行求交。但是流量方与广告主双方存在信任和数据隐私的问题，不管是广告主归因还是流量方归因，都需要将所有数据给到对方进行归因，对方不仅可以伪造归因，还会利用数据进行牟利。

对于这种信任和数据隐私的问题，其中一种解决方向就是基于区块链可信计算进行广告归因。基于区块链技术，双方把数据实时存证到区块链网络，并在链上进行求交，保证归因的可信以及数据的私密性。如何基于区块链技术，设计互信隐私的归因机制，提高归因的实时性以及吞吐量，并降低计算资源，是区块链广告归因技术需要重点研究解决的问题。

建议研究方向：

1) 通过区块链去中心化特性，解决第三方监控的信任问题；
2) 通过区块链匿名性特性，解决广告归因的隐私问题。

返回目录

9. 边缘计算

9.1 智能边缘计算网络架构与关键技术研究

随着 5G、人工智能、虚拟现实/增强现实（VR/AR）、自动驾驶、云游戏等技术与业务的发展，中心式云计算正在向“云-边”协同式计算转变。计算任务可能分布在云、边的多个节点上，节点的互联协议异构，终端接入方式多样。如何面向此新型架构构建一张边边/边云互联的网络，提供多量纲的网络服务，以实现更优业务体验、更低网络成本的目标，将是一个值得研究的课题。

建议研究方向：

1) 在大流量计算密集型业务场景下，多种边缘节点资源可以被综合利用以及时响应业务请求，如算力、网络资源等，探索优化算力分配、提升业务质量等多维目标的跨层网络优化技术及算法；
2) 可以在云边、边边之间存在公网/内网等多条链路的场景下，考虑如何设计基于确定性质量、成本等多量纲的网络/传输技术及流量调度算法。

返回目录

10. 数据库

10.1 高可用分布式数据库

数据库需要具备高可用性，这项要求对于单机数据库和分布式数据库系统都适用。如何让分布式数据库系统具备高可用性，而此背景下的高可用性与单机数据库系统的高可用性的相同与不同之处在哪里？如何体系化地建立分布式背景下数据库的高可用性？特别是一些极限情况下如多数据中心被损毁时如何确保数据库依旧满足高可用性？这些基本问题对于构建分布式数据库有很高价值。

建议研究方向：

1) 理论（CAP 的 A 和 ACID 之间的关系）与体系结构层面，建立分布式数据库的可用性的可量化评价体系（如可涵盖用户体验、资源利用、事务执行效率等）；
2) 极限情况下，分布式数据库的可用性如何保障。如分区发生、物理机器较多受损、部分数据中心受损、数据副本被较多破坏等；
3) 双向研究：在以效率为主题目标的情况下，高可用性对数据库的影响；反之，在以高可用性为目标的情况下，事务处理的吞吐量如何兼顾；
4) 面向行业的高可用性分布式数据库：在不同的行业，如金融保险、工业制造等，分布式数据库的高可用性如何建立。

返回目录