一年来目标检测前沿论文最新进展

2018.11.03 方建勇

提示：采用手机 safari 微软翻译技术

1. 建议: 1810.13049[pdf,其他] Cs。简历

   协同整体场景理解: 统一 3d 对象、布局和相机姿态估计

   作者:黄思远,齐思元,肖银雪,朱义新, 吴英年,朱宗春

   摘要: 整体 3d 室内场景理解是指联合恢复 i) 对象边界盒, ii) 房间布局, 和 iii) 相机姿势, 所有在 3d。现有的方法要么无效, 要么只是部分解决这一问题。在本文中, 我们提出了一个端到端模型, 同时解决所有三个任务的实时给定一个单一的 rgb 图像。该方法的实质是改进 (i) 对**目标**(-g, 3d 框) 进行参数化的预测, 而不是直接估计**目标**, 以及 (ii) 跨不同模块进行合作训练, 而不是对这些模块进行训练模块。具体来说, 我们通过来自多个模块 (ie、3d 相机姿势和对象属性) 的预测对 3d 对象边界框进行参数化。该方法提供了两个主要优点: i) 参数化有助于保持 2d 图像和 3d 世界之间的一致性, 从而在很大程度上减少 3d 坐标中的预测方差。(二) 可以对参数化施加限制, 以便同时训练不同的模块。我们将这些制约因素称为 "合作损失", 因为它们能够进行联合培训和推断。我们对 3d 边界框、2d 投影和物理约束采用三个协同损耗来估计几何上一致且物理上可信的 3d 场景。在 sun rgb-d 数据集上的实验表明, 该方法在三维目标检测、三维布局估计、三维摄像机姿态估计和整体场景理解等方面明显优于以往的方法。少

   2018 年 10 月 30 日提交;最初宣布 2018 年 10 月。

   评论:2018 年 NIPS 接受

2. 第 1810.11920[pdf,其他] 反渗透委员会

   一种适用于受保护种植环境的甜辣椒收获机器人

   作者:chris lehnert, chris mccool, inkyu sa, tristan perez

   摘要: 尽管研究界几十年来做出了相当大的努力, 但在受保护的种植环境中使用机器人收获甜椒仍未得到解决。在本文中, 我们提出了机器人收割机, 哈维, 设计的甜椒在受保护的种植环境中, 达到了 76.5 的成功率 (在修改后的情况下), 这提高了我们以前的工作, 达到了 58% 和相关的甜椒收获工作达到 33%。这一改进主要是通过引入一种新的花梗分割系统, 结合三维后滤波检测关键切割位置来**实现**的。我们根据现有技术对 pe 足叔叔分割进行了基准测试, 证明了性能有了相当大的提高, F_1 分数为 0.564, 而不是 0.302。机器人收割机使用感知管道来**检测目标**甜椒和适当的把握和切割姿势, 用于确定多模式收获工具的轨迹, 以掌握甜椒并将其从植物中切割。一种新的解耦机制使抓取和切割操作能够独立执行。我们对整个机器人采集系统进行深入分析, 以突出未来工作可以解决的瓶颈和故障点。少

   2018 年 10 月 28 日提交;最初宣布 2018 年 10 月。

3. 第 1810.1215[pdf,其他] Cs。简历

   胶囊取证: 使用胶囊网络检测伪造的图像和视频

   作者:huy h. nguyen, junichi yamagishe, isao echizen

   摘要: .. 。最先进的方法使从社交网络获得的单个视频能够实时创建伪造版本。虽然已经开发了许多方法来**检测**伪造的图像和视频, 他们一般是.. 。更多

2018 年 10 月 26 日提交;最初宣布 2018 年 10 月。

4. **第: 1810.09012[pdf,其他] Cs。简历**

多伊10.1109/VAST.2016.7883508

c2a: 用于虚拟结肠镜检查的人群共识分析

作者:ji hwan park, saad nadeem, seyedkoosha mirhosseini, arie k 索特 k 海湾

抽象: 我们推出了一个医学众包可视化分析平台，称为 c {2} 用于可视化、分类和筛选众包临床数据。更具体地说, c2a 用于通过可视化人群反应和过滤掉异常活动来建立对临床诊断的共识。众包医疗应用最近显示出了希望，非专家用户 (人群) 能够达到与医学专家相似的准确性。这样做有可能减少解释/阅读时间，并可能通过事先就调查结果达成共识并让医学专家做出最终诊断来提高准确性。在本文中，我们重点介绍了一个虚拟结肠镜 (vc) 应用，临床技术人员作为我们的**目标**用户，放射科医生充当顾问，并将细分为良性或恶性。特别是, c2a 用于分析和探索视频段上的人群响应，这些视频段是由虚拟冒号中的飞行通道创建的。C2a 提供了几个交互式可视化组件，用于在视频段上建立人群共识,**检测**人群数据和 vc 视频段中的异常，最后，由 a/b 提高非专家用户的工作质量和性能测试最佳众包平台和特定应用的参数。案例研究和领域专家的反馈证明了我们的框架在提高工人产出质量方面的有效性、减少放射科医生解释时间的潜力，从而证明了改进传统临床工作流程的潜力根据人群共识，将大部分视频段标记为良性。少

2018 年 10 月 21 日提交;最初宣布 2018 年 10 月。

评论:ieee 可视化分析科学与技术会议 (vast)，第 21-30 页, 2016 年 (10 页, 11 个数字)

日记本参考:ieee 可视化分析科学与技术会议 (vast)，第 21-30 页, 2016 年

5. **建议: 181009003[pdf,其他] cs. it**

适用于非正交多址的鲁棒接收机设计

作者:王坤

摘要: 提出了非正交多址访问 (noma)，用于未来几代无线通信中的大规模连接。一个主要的 noma 方案是基于功率优化的，在这种方案中,**目标**用户的解码被认为是完美的。在这项工作中，我们的目标不是在电源域上进行优化，而是提出一个强大的接收机，可以通过 fec 代码的多样性**来检测和解码目标**用户的数据流。与现有的 noma 接收器相比，我们的新型接收器大大提高了误码率 (ber) 性能，甚至可以通过为不同的用户分配适当的交错模式来消除误码率 (ber)。少

2018 年 10 月 21 日提交;最初宣布 2018 年 10 月。

评论:13 页，文章

6. **第 1810.08726[pdf,其他] Cs。Lg**

Sl2mf: 通过逻辑矩阵分解预测人类癌症的合成杀伤力

作者:刘勇,吴敏,刘成浩,李晓丽,郑杰

文摘:合成杀伤力 (sl) 是一种很有前途的抗癌药物**靶**点新发现的概念。然而,**用于检测** sl 的湿实验室实验面临着各种挑战，例如成本高、跨平台或细胞系的低一致性。因此，需要计算预测的方法来解决这些问题。更多

2018 年 10 月 19 日提交;最初宣布 2018 年 10 月。

7. **第 1810.0425[pdf,其他] Cs。简历**

划痕: 训练单次射击对象探测器的探索

作者:朱瑞, 张世峰, 王晓波,文龙音,石海林, 李峰波,陶梅

摘要: 目前最先进的对象反对者从预先培训的大规模分类数据集 (如 imagenet) 的现成网络中进行微调, 这会产生一些附件问题: 1) 源数据集和**目标**数据集之间的域差距;2) 分类与**检测**之间的学习客观偏差;3) 用于**检测**的分类网络的体系结构限制。本文结合基于 resnet 和 vggnet 的 ssd 模型的体系结构, 设计了一种新的单镜头无抓物检测器, 称为 scratchdet, 以缓解上述问题。具体而言, 我们从零开始研究 batchnorm 对训练探测器的影响, 并发现在主干和**检测**头子网络上使用 batchnorm 可使探测器从零开始很好地收敛。在此基础上, 通过对 resnet 和 vggnet 检测性能的**分析**, 探讨了网络体系结构, 并引入了一种新的 rot-restnet 主干网, 进一步提高了网络体系结构的准确性。在 pascal voc 2007、2012 和 ms coco 数据集上进行的大量实验表明, scratchdet 在所有列车从零开始的探测器中实现了最先进的性能, 甚至优于现有的单级预培训方法, 无需响铃即可。口哨。守则将于 https://github.com/KimSoybean/ScratchDet 公布。少

2018 年 10 月 19 日提交;最初宣布 2018 年 10 月。

评论:14 页, 9 个数字, 提交给 aaai2019

8. **第 1810.08415[pdf,其他] Cs。铬**

   物联网: 确保边缘网络中的物联网通信

   作者:ibbad hafeez, markku antikainen, aaron yiding, sasu tarkoma

   摘要: 物联网设备的日益普及使其成为攻击者的利润目标。由于不安全的产品开发实践, 这些设备通常容易受到非常小的攻击, 并且很容易受到损害。由于物联网设备的数量众多且异质性, 因此无法使用传统的端点和网络安全解决方案来保护物联网生态系统的安全。为了解决边缘网络中保护物联网设备的挑战和要求, 我们提供了 iot-保管器, 这是一个能够实时保护网络免受任何恶意活动攻击的新型系统。该系统使用轻量级异常**检测**技术, 在使用网关上可用的有限资源的同时, 保护设备到设备和设备对基础结构的通信。它使用未标记的网络数据来区分在网络中观察到的良性和恶意流量模式。通过真实世界测试台进行的详细评估显示, iot-coureper **检测**到任何设备以高精度 (0.982) 和低假阳性率 (0.01) 生成恶意流量。结果表明, iot-保管器重量轻、响应迅速, 能够有效地处理复杂的 d2d 交互, 而无需显式攻击签名或复杂的硬件。少

   2018 年 10 月 19 日提交;最初宣布 2018 年 10 月。

   评论:20 页, 9 个数字, 4 个表

9. **决议: 1810.08126[pdf,其他] Cs。Lg**

   ktan: 知识转让对抗网络

   作者:刘培业,刘武,马华东, 陶梅, 明古肖克

   摘要: 为了降低深卷神经网络的大量计算和存储成本, 基于知识蒸馏的方法率先将大型 (教师) 深部网络的泛化能力转移到轻量级 (学生) 网络中。然而, 这些方法主要集中在教师网络中软最大层的概率分布上, 从而忽略了中间表示。在本文中, 我们提出了一个知识转移对抗网络, 以更好地培训学生网络。我们的技术从整体上考虑教师网络的中间表示和概率分布。为了传授中间表示的知识, 我们将高级教师地形图设置为**目标**, 并对学生地物图进行训练。具体而言, 我们安排了一个教师对学生层, 使我们的框架适合各种学生结构。与概率分布相比, 中间表示有助于学生网络更好地理解转移的泛化。此外, 我们还通过使用鉴别器网络注入了一个对抗性学习过程, 该网络可以在训练学生网络时充分利用地形图的空间相关性。实验结果表明, 该方法能显著提高学生网络在图像分类和目标**检测**任务中的性能。少

   2018 年 10 月 18 日提交;最初宣布 2018 年 10 月。

   评论:8 页, 2 个数字

10. **建议: 1810.07063[pdf,其他] Cs。马**

电动汽车集料机分布式优化中的战略操作检测

作者:alvaro perez-diaz, enrico gerding, frank mmcroarty

摘要: 鉴于全球电动车的迅速崛起，以及为近期制定的雄心勃勃的**目标**，大型电动车车队的管理必须被视为优先事项。具体而言，我们研究的方案是通过利己主义的电动汽车聚合器进行电动汽车充电管理，这些聚电动汽车聚集器在未来的市场上竞争，以购买满足客户需求所需的电力。为了降低电力成本和对电力市场的影响，文献中提出了一个集中的投标协调框架，雇用了一名协调员。为了提高隐私和限制对协调员的需求，我们建议重新拟订协调框架，作为一种分散的算法，采用乘法器的交替方向方法 (admm)。然而，考虑到聚合器的利己性质，它们可以偏离算法，以提高其个人效用。因此，我们研究了 admm 算法的战略操作，并在此过程中描述和分析了不同的攻击向量，并提出了一个数学框架来量化和**检测**操作。此外，此**检测**框架不限于考虑的 ev 方案，可应用于一般的 admm 算法。最后，我们使用来自西班牙的真实市场和驱动程序数据，在现实场景中测试了所提出的分散协调和操作**检测**算法。我们的经验结果表明了协调算法的收敛性,**并表明该检测**算法在多达 96% 的情况下准确**地检测**偏离行为。少

2018 年 10 月 12 日提交;最初宣布 2018 年 10 月。

类:I.2.0;I.2.11

11. **建议: 1810.06917[pdf,其他] Cs。Lg**

tne: 一种潜在的网络表示学习模型

作者:abdulkadir celikkanat, fragkiskos d. malliaros

摘要: 网络表示学习 (nrl) 方法旨在通过保留给定网络的本地和全局结构，将每个顶点映射到低维空间中，近年来，由于它们在几个方面取得的成功，它们受到了极大的关注具有挑战性的问题。尽管提出了各种计算节点嵌入的方法，但许多成功的方法都受益于随机游走，以便将给定的网络转换为节点序列的集合，然后**以**学习表示为目标通过预测序列中每个顶点的上下文来控制节点。本文介绍了一个通用的框架，以增强通过随机步行方法获得的节点的嵌入。与 nlp 中的主题单词嵌入概念类似，该方法将每个顶点分配给一个主题，并得到各种统计模型和社区**检测**方法的青睐，然后生成增强的社区表示。我们对我们的方法进行了两个下游任务的评估: 节点分类和链路预测。实验结果表明，顶点和主题嵌入的结合优于众所周知的基线 nrl 方法。少

2018 年 10 月 16 日提交;最初宣布 2018 年 10 月。

评论:9 页

12. **修订: 1810.06809[pdf,其他] Cs。Ds**

关于二部图中求密集子图的研究: 线性算法

作者:潘一坤

摘要: 从大图**中检测**密集子图是许多应用中的核心组成部分，包括社交网络挖掘、生物信息学。本文主要研究了用二部图挖掘密集子图的问题。这项工作的动机是**检测同步**行为的任务，这些行为通常可以被表述为挖掘由源节点 (关注者、客户) 和**目标**节点 (关注者、产品等) 为恶意而形成的二部图模式。我们引入了一个新的受限双脂问题，最大半隔离双色 (mhi biclique)，并表明该问题在欺诈**检测中**的直接应用。我们证明，不像许多其他双脂问题，如最大边缘二重度问题，已知是 np 完成, mhi 双性问题承认一个线性时间解。我们提供了一种新的算法 s-tree，它的扩展是 s 林算法，有效地解决了这一问题。我们还证明了该算

法是鲁棒性的故意伪装和其他扰动。此外，我们的方法可以自动组合多个功能并确定其优先级，从而减少对功能工程的需求，同时保持对看不见的攻击的安全性。在多个公共和专有数据集上进行的大量实验表明，s-trees-林在所有配置中的性能优于强大的竞争对手，成为欺诈**检测领域**的新领域。少

2018 年 10 月 16 日提交;v1 于 2018 年 10 月 16 日提交;最初宣布 2018 年 10 月。

评论:2018 年 10 月提交给 icde 2019 年

13. **建议: 1810.05989[pdf,其他] Cs。简历**

多伊10.1007/978-3-030-0096-5 _ 16

通过 ct cn 培训加强胸部 x 线照片的肺结构

作者:opir gozes, hayit greenspan

文摘: 胸部 x 线片中出现的大量重叠解剖结构，可以降低自动算法 (cad) 和人类阅读器检测肺病理**学的**性能。本文提出了一种基于深度学习的图像处理技术，利用完全对流神经网络 (fcnn) 增强胸片软性肺结构的对比度。两个 2d fcnn 架构被训练来完成任务: 第一个执行 2d 肺分割，用于肺区域的正常化。第二个 fnnn 被训练提取肺结构。为了创建训练图像，我们使用了模拟 x 射线或数字重建射线 (drr)，这些 x 光片 (drr) 来自 516 属于 ldc-idri 数据集的 516 扫描。通过首先对 ct 域中的肺进行分割，我们能够创建一个 2d 肺掩码数据集，用于训练分割 fncn。为了训练提取 fcnn，我们创建了只属于三维肺分割的体素的 drr 图像，我们称之为 "肺 x 线"，并将其用作**目标**图像。一旦提取肺结构，可以通过融合原始输入 x 射线和合成的 "肺 x 射线" 来增强原始图像。我们表明，我们的增强技术适用于真实的 x 射线数据，并显示我们的结果在最近发布的 nih 胸部 x-ray-14 数据集。当我们训练基于 densenet-121 的体系结构直接处理肺增强 x 射线图像时，我们看到了很有希望的结果。少

2018 年 10 月 14 日提交;最初宣布 2018 年 10 月。

14. **第: 1810.05939[pdf] Cs。Sy**

错误数据注入网络攻击检测

作者:李兴鹏,霍里·海德曼

文摘: 状态估计实时估计系统状态，为其他能源管理系统 (ems) 应用提供了一个基本案例，包括实时应急分析和安全约束经济调度。最近的文献中的研究表明，恶意网络攻击可能会注入错误的测量，绕过传统的错误数据**检测**并导致实际超载。因此,**检测**这种网络攻击非常重要。本文提出了多种指标来监测异常负荷偏差和可疑的支路流量变化。提出了一种系统的两阶段方法**来检测**虚假数据注入 (fdi) 网络攻击。第一阶段确定系统是否受到攻击，而第二阶段确定**目标**分支。数值模拟证实了 fdi 是否会导致严重的系统违规，并证明了拟议的两阶段 fdi **检测**(fdid) 方法的有效性。结果表明，所提出的 fdid 方法能够有效地**检测** fdi 网络攻击并识别**目标**分支;此外，相关的虚警率和虚警率也很低。少

2018 年 10 月 13 日提交;最初宣布 2018 年 10 月。

评论:8 页, 9 个数字

15. **第: 1810.04989[pdf,其他] Cs。Sd**

警民的倾听: 城市场景中声学警报的定位与分类

作者:letizia marchegiani, paul newman

文摘: 本文是关于在城市场景中发出警报的声学**事件检测**和声源定位。具体而言，我们有兴趣发现急救车的喇叭和警笛的存在。为了获得一个可靠的系统，即使存在交通噪声，也能运

行可靠，而交通噪声可能是丰富的、非结构化的和不可预测的，我们建议将传入立体声信号的光谱作为图像进行处理，并应用语义分割,基于 unet 体系结构，从背景噪声中提取**目标**声音。在多任务学习方案中，结合信号去噪，我们执行声学事件分类，以识别警报声音的性质。最后，我们使用去噪信号定位的声源在地平线平面上，通过反演的方向的声音到达通过 cnn 架构。我们的实验评估显示，平均分类率为 94%，在 0.5 的音频帧上运行时，本地化的绝对误差为 0.5s，在 2.5 秒帧上工作时的本地化误差为 2.5s。该系统在噪音水平非常高的特别具有挑战性的情况下提供出色的性能。少

2018 年 10 月 11 日提交;最初宣布 2018 年 10 月。

评论:6 页, 9 个数字

16. **第 xiv: 1810.04301[pdf, ps,其他] Cs。Sy**

分布式估计网络偏置攻击的检测与缓解

作者:mohammad deghat, valery ugrinovskii, imman shames , cedric langbort

文摘: 本文研究了**针对**协同状态估计算法的状态观测器网络的**偏置**攻击检测和缓解问题。这个问题是在最近开发的分布式估计框架内利用向量离散度的方法提出来的。本文表明，分布式观测器网络可以被赋予一个额外的攻击**检测**层，能够**检测**偏置攻击并纠正其对网络产生的估计的影响。通过实例说明了所提出的分布式攻击检测器的性能。少

2018 年 10 月 9 日提交;最初宣布 2018 年 10 月。

评论:在 "自动" 中接受发布

17. **建议: 1810.03851[pdf,其他] Cs。简历**

通过对等学习进行深度注意跟踪

作者:史普,宋一宾,马超,张洪刚,杨明轩

摘要: 视觉注意，来自认知神经科学，促进人类对感官数据最相关的子集的感知。最近，为利用关注计划推进计算机视觉系统作出了重大努力。对于可视化跟踪，跟踪正在进行较大外观更改的**目标**对象通常具有挑战性。注意图通过有选择地注意时间鲁棒性特征，方便了视觉跟踪。现有的逐检**检测**方法主要使用额外的注意模块来生成特征权重，因为分类器不具备此类机制。本文提出了一种往复式学习算法，以利用视觉注意力训练深度分类器。该算法由前馈和后向操作组成，用于生成注意图，这些运算与训练中的原始分类损失函数相结合，作为正则化项。深层分类器学习关注目标对象对外观变化具有鲁棒性的**区域**。对大型基准数据集的大量实验表明，所提出的注意跟踪方法与最先进的方法相比具有较好的效果。少

2018 年 10 月 15 日提交;v1 于 2018 年 10 月 9 日提交;最初宣布 2018 年 10 月。

评论:2018 年 NIPS

18. **建议: 1810.03783[pdf,其他] Cs。简历**

无监督的在线视频对象分割与运动性能的理解

作者:陶卓,程志勇,张鹏, 黄永康,莫汉干甘哈利

摘要: 无监督的在线视频对象分割 (vos) 旨在自动分割移动对象在不受约束的视频上，而无需任何先前有关对象或摄像机运动的信息。因此，对于高级视频分析来说，这是一个非常具有挑战性的问题。到目前为止，文献中报道的此类方法数量有限，其中大多数仍有距离，无法取得令人满意的业绩。**针对**这一具有挑战性的问题，本文提出了一个新的无监督的在线 vos 框架，将运动属性理解为与分段区域的 "一致" 对象 "的运动属性。通过将以下位置的显著运动**检测**} 和 "对象" 方案} 结合起来，提出了一种像素化融合策略，以有效去除

背景运动和静止物体等**检测**噪声。此外，利用从前面的帧中获得的分割，提出了一种正向传播算法来处理不可靠的运动**检测**和目标建议。在 datve-2016 和 segearack-v2 基准数据集上的实验结果表明，该方法的性能优于其他最先进的无监督在线细分，至少实现了 5.6% 的绝对改进，此外甚至实现了比 dovs-2016 数据集上最好的无监督离线方法具有更好的性能。另一个重要的优势还需要解决的另一个方面，即在所有实验中，只有一个现有的对象建议训练模型 (coco 数据集上的掩语 rcnn) 在没有任何微调的情况下使用，这就是鲁棒性的演示。这项工作的最大贡献可能会揭示潜力，并激励更多基于特征运动特性的 vos 框架研究。少

2018 年 10 月 8 日提交;最初宣布 2018 年 10 月。

19. **建议: 1810.03303[pdf,其他] 反渗透委员会**

使用 rgb-d 相机的自主机器人进行精确浇注

作者:周道, wolfram burburard

摘要: 家庭环境中的机器人助手应为其用户执行各种复杂的任务。一个特别具有挑战性的任务是将饮料倒进杯子中，为了顺利完成，需要**在倒入**过程中检测和跟踪液位，以确定何时停止。本文提出了一种新的自动浇注方法，利用 rgb-d 摄像机跟踪液位，并根据液位反馈调整浇注速度。我们在不同类型的液体和不同条件下对我们的系统进行全面评估，使用 pr2 机器人进行超过 250 的浇注。结果表明，我们的方法能够将液体倒入目标高度，精度为几毫米。少

2018 年 10 月 8 日提交;最初宣布 2018 年 10 月。

评论:12 页

20. **建议: 1810.0373[pdf, ps,其他] Cs。简历**

基于绝对方向均值差分算法的小红外目标检测

作者:saed moradi, payman moallem, mohamad farzan sabahi

文摘: 红外搜索和跟踪 (irst) 系统中的红外**小目标检测**是一项具有挑战性的任务。当高灰强度结构背景出现在红外导引头的视场 (fov) 时，这种情况就变得更加复杂。在大多数红外**小目标检测**算法忽视方向信息的情况下，本文提出了一种抑制结构背景、开发更有效检测的定向方法. 算法。为此，采用与平均绝对灰度差 (aagd) 相似的概念，构造了一种称为绝对方向均值差 (admd) 的定向**小目标检测**算法。并对该算法提出了有效的实现程序。该算法有效地增强**了目标**区域，消除了背景杂波。对真实红外图像的仿真结果证明了该算法的有效性。少

2018 年 10 月 7 日提交;最初宣布 2018 年 10 月。

评论:提交给 ieee 地球科学和遥感交易

21. **建议: 1810.0148[pdf,其他] Cs。Cl**

机器翻译中跨语语语篇关系的评估

作者:karin sim smith, lucia 特点

摘要: 为了提高整体翻译质量，人们越来越重视将更多的语言元素集成到机器翻译 (mt) 中。虽然已经取得了重大进展，特别是最近在神经模型方面，但自动评估此类系统的输出仍然是一个悬而未决的问题。目前 mt 评价的实践依赖于单一的参考翻译，尽管有很多翻译特定文本的方法，而且往往忽视更高层次的信息，如话语。我们提出了一种新的方法，根据原文而不是参考翻译来评估翻译的产出，并衡量源文本中话语元素 (特别是语篇关系) 的语义在多大程度上保存在 mt 输出中。面临的挑战是**检测**源文本中的语篇关系，并确定这

些关系是否正确地交叉转移到**目标**语言---而不进行参考翻译。这种方法可以独立用于语篇一级的评价，也可以作为其他指标的一个组成部分，而此时大量的 mt 是在线的，在源文本作为基准的情况下，评估将从中受益。少

2018 年 10 月 7 日提交;最初宣布 2018 年 10 月。

22. **建议: 1810.00345[pdf,其他] Cs。简历**

基于像素和特征级的自动驾驶中目标检测的域调整

作者:玉虎山,文峰路,志蒙周

摘要: 对大型数据集进行注释以训练现代卷积神经网络对于许多实际任务来说，成本高、费很长。一种替代方法是在标记的合成数据集上对模型进行训练，并将其应用于真实场景。然而，这种简单的方法往往无法很好地概括，主要原因是合成数据集和真实数据集之间的域偏差。为了解决这个问题，引入了许多无监督域适应 (uda) 方法，但大多数方法只关注简单的分类任务。本文提出了一种新的 uda 模型，以解决在自主驾驶环境下更复杂的目标**检测**问题。我们的模型集成了像素级和基于特征级别的转换，以完成跨域**检测任务,**并可在端到端进行进一步培训，以追求更好的性能。我们采用生成对抗网络的目标和周期一致性损失的图像转换在像素空间。为了解决潜在的语义不一致问题，我们建议基于区域建议的特征对抗训练，以保留**目标**对象的语义，并进一步减少域的变化。对几种不同的数据集进行了广泛的实验，结果证明了该方法的鲁棒性和优越性。少

2018 年 9 月 30 日提交;最初宣布 2018 年 10 月。

23. **第 1810.00119[pdf,其他] Cs。简历**

基于自适应暹罗和运动估计网络的视觉对象跟踪

作者:hossein kasiani, shahriar b. shokouhi

摘要: 近年来，卷积神经网络 (cnn) 以其强大的抽象特征表示方式，在计算机视觉的不同领域引起了广泛的关注。视觉目标跟踪是近年来计算机视觉中具有显著意义和重要意义的领域之一，取得了显著的进步。在这项工作中，我们的目标是利用 cnn 的表示能力，改进视觉目标跟踪中的运动和观测模型。为此，利用运动估计网络 (名为 men) 寻找**目标**最可能的位置，并在以前的**目标**位置之外准备进一步的线索。因此，运动估计将通过在两个可信的职位附近产生少数候选人来加强。然后将生成的候选人输入训练有素的暹罗网络，以**检测**最可能的候选人。将每个候选项与可调整缓冲区进行比较，该缓冲区在预定义条件下进行更新。考虑到**目标**外观的变化，一个加权 cnn (称为 wcnn) 自适应分配权重的最后相似度分数的暹罗网络使用特定于序列的信息。对知名基准数据集 (otb100、otb50 和 otb2013) 的评价结果证明，拟议的跟踪器优于最先进的竞争对手。少

2018 年 9 月 28 日提交;最初宣布 2018 年 10 月。

评论:28 页, 1 个算法, 7 个数字, 2 个表，提交给 elsevier，图像和视觉计算

24. **第 1809. 10417[pdf,其他] Cs。简历**

基于配值融合的可变形目标跟踪

作者:刘文喜,宋一兵,陈登生, 于元龙,何胜峰,刘瑞森 w.h. 刘先生

文摘: 通过与卷积神经网络 (cnn) 的集成，检测跟踪框架受到越来越多的关注。但是，现有方法无法跟踪外观变化严重的对象。这是因为传统的卷积操作是在固定网格上进行的，因此在物体改变姿态或在不同的环境条件下可能无法找到正确的响应。本文提出了一个可变形卷积层，以丰富目标外观的表示在跟踪的检测框架.我们的目标是捕捉**目标**的外观变化，通过变形卷积和补充其原始外观通过剩余学习。同时，我们提出了一个门控融合方案，以控

制变形卷积捕获的变化如何影响原始外观。通过变形卷积丰富的特征表示，有利于对 cnn 分类器在**目标**对象和背景上的判别。对标准基准的大量实验表明，所提出的跟踪器在最先进的方法下表现良好。少

2018 年 9 月 27 日提交;最初宣布 2018 年 9 月。

25. 决议: 1809.10242[pdf, ps,其他] Cs。简历

通过自动图像注释解决训练偏差

作者:肖竹军,朱延子,陈玉欣,赵文英,姜俊晨,郑海涛

摘要: 构建准确的 dnn 模型需要对大型标记的上下文特定数据集进行培训，尤其是那些与**目标**方案匹配的数据集。我们相信，无线本地化的进步与摄像机一致，可以在野外拍摄的图像和视频上对**目标**进行自动注释。以行人和车辆**检测**为例，论证了自动图像标注系统的可行性、优点和挑战。我们的工作要求在被动本地化、移动数据分析和具有错误弹性的 ml 模型方面进行新的技术开发，以及用户隐私策略中的设计问题。少

2018 年 10 月 10 日提交;v1 于 2018 年 9 月 22 日提交;最初宣布 2018 年 9 月。

26. 第 1809. 100447[pdf,其他] Cs。Sd

用于开放式声场分析的可扩展群集图分类

作者:helen l bear, emmanouil benetos

摘要: 我们提出了一种新的可扩展和可分可分的分类，用于开放式声场分析。这种新模型允许使用有形描述符和感知标签进行复杂的场景分析。它的新结构是一个聚类图，这样每个集群 (或子集) 都可以单独进行**有针对性**的分析，如办公室声音**事件检测**，同时保持标签整个图 (超集) 的完整性。关键的设计优势在于它的可扩展性，因为在新的数据捕获过程中需要新的标签。此外，使用相同分类的数据集可以轻松地进行扩充，从而节省了未来的数据收集工作。我们在复杂场景分析所需的细节与避免 "一切分类" 与我们的框架之间取得平衡，以确保标签的超集中没有重复性，并通过 dcase 挑战分类来证明这一点。少

2018 年 9 月 26 日提交;最初宣布 2018 年 9 月。

评论:将在 2018 年 11 月音频场景和事件的检测和分类 (dcase) 研讨会上展出

27. 第 1809. 09502[pdf] Cs。Ce

地震活化前兆探测的区域地震信息熵

作者:奥泽幸雄

文摘: 本文提出了一种**从目标**区域地震时间序列数据中**检测**地震前兆的方法。介绍了地震信息的区域熵，它是**指目标**区域地震对地震分布的星团多样性的平均影响。根据地壳动力学的粗略定性模型，假设地震信息区域熵增加后的饱和度先于地震的激活。在开放式地震目录上，验证了这一假设。与比较的基线方法相比，这一时间变化与日本地区地震的激活有更多的相关性，优先级为一至两年。少

2018 年 9 月 25 日提交;最初宣布 2018 年 9 月。

评论:30 (主要:19 页，补充:11 页)，15 页 (主要: 6 页，补充: 9 页) 数字，1 页。在任何地方进行同行评审之前进行预打印

28. 第 1809. 08793[pdf,其他] 反渗透委员会

一种使用主动目标搜索的人员跟踪体系结构

作者:minkyu kim, miguel arduengo, nick walker, yu 前 jiang yuk 荒·art, justin w. hart, peter stone, luis sentis

摘要: 本文研究了一种新的基于主动搜索的人跟踪机器人的体系结构。该系统可实时应用于一般移动机器人，用于学习人的特征,**进行检测**和跟踪，并最终导航到该人。要想在人的跟踪方面取得成功，就需要正确地整合感知、规划和机器人行为。为此，提出了一种主动**目标**搜索能力，包括预测和导航到寻找人类**目标**的有利位置。拟议的能力旨在提高在拥挤环境等动态条件下跟踪和跟踪人员的鲁棒性和效率。采用融合 rgb-d 传感器和激光扫描仪等多模态传感器信息方法，对人体**目标**进行了有力的跟踪和识别。研究了用于跟踪人的贝叶斯滤波和预测人的轨迹的回归算法。为了使机器人自主，提出的框架依赖于行为树结构。利用丰田人力支持机器人 (hsr)，实时实验证明，该体系结构能够产生快速、高效的人跟踪行为。少

2018 年 9 月 24 日提交;最初宣布 2018 年 9 月。

评论:7 页, 6 个数字

29. **第 1809. 08613[pdf, ps,其他] 反渗透委员会**

使用深度学习检测机器人中的工具、对象和操作的特征

作者:namiko saito, kitae kim, shingo murata , Tetsuya ogata, shigeki sugano

文摘: 我们提出了一个工具使用模型，它可以从对象操作提供的效果中**检测**工具、**目标**对象和操作的特征。我们构建了一个模型，使机器人能够使用工具操作对象，并将婴儿学习作为一个概念。为了实现这一点，我们训练在机器人进行深度学习的工具使用任务期间记录的传感器-运动数据。实验包括四个因素: (1) 工具、(2) 对象、(3) 动作和 (4) 模型同时考虑的效果。为了进行评估，机器人在获得使用未知工具和物体效果的信息时，会产生预测的图像和运动。我们确认机器人能够通过学习效果和执行任务来**检测**工具、对象和动作的特征。少

2018 年 9 月 23 日提交;最初宣布 2018 年 9 月。

评论:7 页, 9 个数字

30. **第 1809. 08136[pdf, ps,其他] cs. it**

用震级测量恢复圆锥可检测联合信号的两步 pr 方案

作者:李友发,韩德广

抽象: 本文在研究子空间联合采样问题的基础上，研究了存在于 (有限生成的) 锥 (简称 uoc) 联合中的信号的相位检索问题。R^n.我们建议采取两步性的 pr-pc--计划:公使 = 检测 + 恢复功能 .我们首先为 uoc 的**可探测性**建立一个充分和必要的条件，然后设计一个**检测**算法，使我们能够确定**目标**信号所在的锥。然后，相位检索将在**检测到的**圆锥内执行，这可以通过最多使用按-测量次数和非常低的复杂度，其中按 ($\leq n$) 是 uoc 发电机等级的最大值。通过数值实验证明了该方法的有效性，并与现有的几种相位检索方法进行了比较。少

2018 年 9 月 29 日提交;v1 于 2018 年 9 月 21 日提交;最初宣布 2018 年 9 月。

31. **第: 189.07896[pdf,其他] 反渗透委员会**

3d 移动到查看: 多视角可视化伺服，通过语义分割改进对象视图

作者:chris lehnert, dorian tsai, anders eriksson, chris mccool

摘要: 在本文中，我们提出了一种新的方法，视觉伺服机器人，称为 3d 移动到查看 (3dmts) 的原则，找到下一个最佳视图使用 3d 相机阵列和机器人机械手，以获得多个样本的场景从不同的透视。该方法使用语义视觉和应用于每个透视的目标函数来采样代表下一个最佳视图方向的渐变。该方法在模拟和包含自定义 3d 摄像机阵列的真实机器人平台上进行了演示，以应对在高度封闭和非结构化环境中进行机器人采集的具有挑战性的场景。在一个真正的机器人平台上显示，通过使用目标函数的梯度移动末端执行器，可以对感兴趣的对象进行局部最优的查看，即使在遮挡中也是如此。与使用单 rgb-d 相机的基线方法相比，3dmts 方法的总体性能平均增加了 29.3%. 结果从质量和数量上证明，3dmts 方法在大多数情况下表现更好，与基线方法相比，得到的结果是**目标**大小的三倍。最终视图中目标大小的增加将改进对感兴趣对象的关键特征的**检测**，以便进一步操作，例如抓取和收获。少

2018 年 9 月 20 日提交;最初宣布 2018 年 9 月。

32. **第 xiv:1809.07091[pdf,其他] Cs。简历**

计数数不数：来自空间的深层语义密度估计

作者:andres c. rodriguez, jan d. wegner

摘要: 我们提出了一种新的方法来计算比卫星图像的地面采样距离明显小的特定类别的物体。由于出现不同对象类别的场景的杂乱性质，此任务非常艰巨。**目标**对象可以部分被遮挡，在同一个类中的外观会有所不同，并且在不同的类别中看起来也很相似。由于传统的对象**检测**由于对象的大小相对于像素大小较小而不可行，因此我们将对象计数转换为密度估计问题。为了区分不同类的对象，我们的方法将密度估计与语义分割结合在一个端到端学习卷积神经网络 (learnable) 中。实验表明，在杂乱的场景中，深语义密度估计可以有力地计算不同类的对象。实验还表明，我们需要特定的美国有线电视新闻网遥感架构，而不是盲目地应用计算机视觉中的现有架构。少

2018 年 9 月 20 日提交;v1 于 2018 年 9 月 19 日提交;最初宣布 2018 年 9 月。

评论:2018 年 gcr 中接受

33. **第 xiv:180 099.07081[pdf,其他] 反渗透委员会**

rprg：利用一个多任务卷积神经网络实现实时机器人感知、推理和抓取

作者:张汉波,阮秀光,黎鹏湾，杨晨杰,周新文，郑南宁

摘要: 自主机器人抓取在智能机器人中发挥着重要作用。然而，由于以下原因，机器人抓取具有挑战性，这是一项涉及感知、规划和控制的综合性任务;(2) 复杂场景中的自主机器人抓取需要推理能力。本文提出了一种多任务卷积神经网络，用于机器人感知、推理和抓取 (rprg)，该网络可以帮助机器人找到**目标**，制定抓取的计划，并最终逐步把握**目标**。堆叠场景。将基于视觉的机器人抓取检测和视觉操作关系推理集成到一个单一的深部网络中，构建了自主机器人抓取**系统**。拟议的网络在这两项任务中都具有最先进的性能。实验表明，在目标杂乱场景、熟悉的堆叠场景和复杂的堆叠场景中，巴克斯特机器人可以自主把握**目标**，成功率分别为 94.2、77.1% 和 62.5，速度为 6.5 fps。对于每个**检测**.少

2018 年 9 月 19 日提交;最初宣布 2018 年 9 月。

评论:提交给 icra2019

34. **第 xiv:180 099.07039[pdf] Cs。铬**

智能假数据注入对电网状态估计的攻击

作者:muneer mohammad

摘要: 本文考虑了电网状态估计的一类新的网络攻击。这类攻击被称为虚假数据注入攻击。我们表明，在了解系统配置的情况下，攻击者可以成功地将错误数据注入某些状态变量，同时绕过现有的错误数据**检测技术.**在初步部分，我们考虑了这种攻击的可行性和成功避免**被发现的**必要条件。之后，我们表明，有了系统配置的知识，某些线路流量测量可以纵，从而导致有利可图的不当行为。通过控制区域传输组织 (rto) 对系统电源流和拥塞的看法，攻击者可以根据事先的投标来操纵**目标**总线的 lmp。此外，本文还展示了虚假数据注入攻击的实现。将所考虑的数值例子应用于在微控制器上设计的恶意数据**检测**算法。结果表明，在电网状态估计中注入虚假数据测量是有效的。少

2018 年 9 月 19 日提交;最初宣布 2018 年 9 月。

35. **建议: 1809.06663[pdf,其他] Cs。简历**

适用于陷阱图像中单个和触摸飞蛾计数的支持向量机 (svm) 识别方法

作者:mohamed chafik bakkay, silvie chambon, hatem a.rashwan, christian lubat, sébastien barsotti

文摘: 本文旨在开发一种在实际条件下从陷阱图像中识别飞蛾的自动算法。此方法使用我们以前的工作进行**检测**[1]，并介绍了一个合适的分类步骤。更准确地说，Curviness 分类器是用多尺度描述符--曲率直方图 (hcs) 进行训练的。该描述符对光照变化具有鲁棒性，能够在多尺度上**检测**和描述**目标**昆虫的外部和内部轮廓。所提出的分类方法可以用一小套图像进行训练。定量评价表明，该方法能够比最先进的方法对昆虫进行更高的分类，准确率 (9.5.8%)。少

2018 年 9 月 18 日提交;最初宣布 2018 年 9 月。

36. **第: 1809. 06147[pdf,其他] Cs。简历**

特征 2 质量: 现实标记大规模生成的潜在空间中的视觉特征处理

作者:jae-hyeoklee, seong tae kim, hakminlee, yong man 罗

摘要: 本文讨论了一种生成逼真标记质量的方法。近年来，人们多次尝试将深度学习应用于各种生物图像计算领域，包括计算机辅助**检测**和诊断。为了在生物图像计算领域学习深入的网络模型，需要大量的标记数据。然而，在许多生物成像领域，标记数据集的大尺寸是几乎不可用的。虽然已经有一些研究致力于通过生成模型来解决这个问题，但也存在以下问题: 1) 生成的生物图像似乎不现实;2) 生成的生物图像的变化是有限的;3) 需要额外的标签注释任务。在本研究中，我们提出了一种现实的标记生物图像生成方法，通过视觉特征处理在潜在空间。实验结果表明，该方法产生的质量图像是真实的，具有**广泛的目标**质量特征表达范围。少

2018 年 9 月 17 日提交;最初宣布 2018 年 9 月。

评论:本文在 eccv 2018 研讨会上发表

37. **第 xiv:1809. 05966[pdf,其他] Cs。简历**

通过背景上的感知补丁攻击对象探测器

作者:李月尊,仙边,四维柳子

摘要: 深度神经网络已被证明是脆弱的对抗摄动。最近的作品成功地在整个图像或对损坏的物体探测器的**利益**目标产生了对抗性扰动。本文从一个新的角度研究了目标检测器的脆弱性--在**目标**之外的小背景补丁上添加最小扰动，使**检测**结果失败。我们的工作重点是攻击最先进的探测器 (如更快的 r-cnn)、区域建议网络 (rpn) 中的公用组件。

由于 rpn 产生的接受场往往大于建议本身，我们提出了一种新的方法来生成背景摄动补丁，并表明仅在**目标**之外的扰动会严重损害通过同时降低真阳性和增加误报，提高了多种类型检测器的性能。我们展示了我们的方法在 ms coco 2014 数据集上的 5 个不同的最先进的对象探测器上的有效性。少

2018 年 9 月 16 日提交;最初宣布 2018 年 9 月。

38. 第 xiv:1809.05820[pdf,其他] Cs。Cl

跨域文本分类的跨域标记 lda

作者:景宝玉,陆晨伟, 王德清, 富镇庄,程牛

摘要: 跨域文本分类旨在为**目标**域构建一个分类器，该分类器利用来自源域和**目标**域的数据。一个有希望的想法是最大限度地减少这两个域的特征分布差异。大多数现有的研究通过精确的对齐机制 (通过一对一特征对齐、投影矩阵等对齐要素) 显式地最大限度地减少了这种差异。然而，这种精确的对齐将限制模型的学习能力，并在不同域的语义分布非常不同的情况下进一步影响模型在分类任务上的性能。为了解决这个问题，我们提出了一种新的群对齐方法，它在群级别对齐语义。此外，为了帮助模型更好地学习这些群中的语义群和语义，我们还提出了对源域中模型学习的部分监督。为此，我们将组对齐和部分监控嵌入到跨域主题模型中，并提出了跨域标记 lda (cdl-lda)。在标准的 20 新闻组和路透社数据集上，进行了广泛的定量 (分类、困惑等) 和定性 (主题**检测**) 实验，以显示所建议的组对齐和部分的有效性。监督。少

2018 年 9 月 16 日提交;最初宣布 2018 年 9 月。

评论:icdm 2018

39. 第 1809. 05258[pdf,其他] Cs。Lg

智能电网中的网络攻击在线检测: 一种强化学习方法

作者:mehmet necip, oyetunji ogundijo, chong li , jodong wang

文摘: 早期**发现**网络攻击对于智能电网的安全可靠运行至关重要。在文献中，提出了进行样本决策的异常检测方案和需要完善攻击模型的在线**检测**方案。本文将在线攻击异常**检测**问题作为部分可观察的马尔可夫决策过程 (pomdp) 问题，提出了一种基于无模型框架的通用鲁棒在线**检测**算法。增强学习 (rl)。数值研究表明，该算法在及时、准确**地检测针对**智能电网的网络攻击方面是有效的。少

2018 年 9 月 14 日提交;最初宣布 2018 年 9 月。

40. 第 xiv:180 9.04758[pdf,其他] Cs。Lg

多元时间序列的生成对抗性网络异常检测

作者:dan li, dacheng chen, jonathan goh, See-kiong ng

摘要: 今天的网络物理系统 (cps) 是庞大、复杂的，并贴有网络传感器和执行器，这些传感器和执行器是网络攻击**的目标**。传统**的检测**技术无法处理 cps 日益动态和复杂的性质。另一方面，网络传感器和执行器会生成大量数据流，这些数据流可以持续监控入侵事件。无监督机器学习技术可用于对系统行为进行建模，并将异常行为分类为可能的攻击。在这项工作中，我们提出了一种新的生成对抗性网络的异常**检测**(gan-ad) 方法，用于此类复杂的网络化 cps。我们在 gan 中使用 lstm-rnn 来捕获传感器和执行器在 cps 正常工作条件下的多变量时间序列的分布。我们没有独立处理每个传感器和执行器的时间序列，而是同时对 cps 中多个传感器和执行器的时间序列进行建模，以考虑它们之间潜在的相互作用。为了利用发电机和鉴别器，我们部署了甘训练鉴别器以及发

电机重建数据和实际样本之间的残差，以**检测**复杂的 cps 中可能存在的异常。我们使用 gan-ad 来区分异常攻击情况和正常工作条件的复杂的六阶段安全水处理 (swat) 系统。实验结果表明，与现有方法相比，该策略能有效识别各种攻击引起的异常,**检测**率高，假阳性率低。少

2018 年 10 月 9 日提交;v1 于 2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

评论:本文在 2018 年 8 月在伦敦举行的第七届大数据、流和异构源挖掘国际研讨会上发表：算法、系统、编程模型和应用。美国

41. **第 xiv:1800.7041 [pdf] Cs。简历**

用于高效视觉跟踪的对抗性特征采样学习

作者:尹英杰,张磊,徐德辉,王新刚

文摘: 检测跟踪框架通常由两个阶段组成：在第一阶段围绕**目标**对象绘制样本，并在第二阶段将每个样本分类为**目标**对象或背景。目前流行的基于**跟踪检测**框架的跟踪器通常在原始图像中提取样本作为深卷积网络的输入，这通常会导致较高的计算量和较低的运行速度。本文提出了一种利用深度卷积特征采样的视觉跟踪方法来解决这一问题。**在目标**对象周围只输入一个裁剪图像到设计的深卷积网络中，并通过空间双线性重采样在网络要素图上采样样本。此外，生成对抗网络被集成到我们的网络框架中，以增加阳性样本并提高跟踪性能。在基准数据集上进行的大量实验表明，该方法实现了与最先进的跟踪器相当的性能，并有效地加速了基于原始图像样本的**逐检跟踪**跟踪。少

2018 年 9 月 15 日提交;v1 于 2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

42. **第 xiv:1809.04570 [pdf,其他] 中心**

finn-r：用于快速探索量化神经网络的端到端深度学习框架

作者:michaela blott, thomas preusser, nicolas fraser, giulio gambardella, kenneth o ' brien , yaman umuroglu

摘要: 卷积神经网络已迅速成为最成功的机器学习算法，即使是嵌入式计算系统也能实现无处不在的机器视觉和智能决策。虽然底层算法在结构上很简单，但计算和内存需求具有挑战性。其中一个有希望的机会是利用较低的精度表示输入、激活和模型参数。由此产生的性能、能效和存储占用空间的可扩展性提供了有趣的设计妥协，以换取精度的小幅降低。fpga 是利用低精度推理引擎利用自定义精度来实现给定应用所需的数值精度的理想选择。在本文中，我们描述了 finn 框架的第二代，这是一个端到端工具，它支持设计空间探索，并自动在 fpga 上创建完全自定义的推理引擎。给定神经网络描述，该工具可针对给定的平台、设计**目标**和特定精度进行优化。介绍了资源成本函数的形式化和性能预测，并对优化算法进行了阐述。最后，我们在包括 pynq 和 aws-f1 在内的一系列平台上评估了一系列降低精度神经网络，从 cifaar-10 分类器到基于 yob 的对象**检测**，并展示了在 50top 时前所未有的测量吞吐量。在嵌入式设备上的 aws-f1 和 5topp。少

2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

评论:将发表在《深度学习》特别版上

43. **第 xiv:1809. 04444 [pdf, ps,其他] Cs。CI**

来自白人至上论坛的仇恨演讲数据集

作者:ona de gibert, naiara perez, aitor garcía-pablos , monse cuadros

摘要: 仇恨言论通常被定义为基于种族、肤色、族裔、性别、性取向、国籍、宗教或其他特征等某种特征而诋毁**目标**群体的任何交流。由于社交媒体上用户生成的网页内容大量增加，仇恨言论的数量也在稳步增加。在过去几年里，人们对在线仇恨言论**检测，**特别是这一任务的自动化程度不断提高，同时也产生了这一现象的社会影响。本文描述了一个仇恨言论数据集，该数据集由数千句构成，手动标记为是否包含仇恨言论。这些句子是从一个白人至上主义者论坛 "风暴面前" 中提取的。开发了一个自定义注释工具来执行人工标记任务，除其他外，该工具允许注释者在给句子贴标签之前选择是否阅读句子的上下文。本文还对结果数据集进行了深思熟虑的定性和定量研究，并利用不同的分类模型进行了几次基线实验。数据集是公开的。少

2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

评论:在第二次滥用语言在线研讨会上接受

44. 第 xiv:1809.04320[pdf,其他] Cs。简历

用于长期视觉跟踪的学习回归和验证网络

作者:张云华,王东,王立军,齐金清,陆湖川

摘要: 在长期的单个对象跟踪任务中,**目标**频繁移出视野。很难确定**目标**的存在并在整个图像中重新搜索**目标**。本文通过引入协作框架来规避这一问题，该框架利用匹配机制和判别特征来考虑目标识别和全图像重新**检测**。在建议的协作框架内，我们开发了一个基于匹配的回归模块和一个基于分类的长期视觉跟踪验证模块。在回归模块中，我们提出了一个回归器，用于进行匹配的学习，并应对急剧的外观变化。在验证模块中，我们提出了一个有效过滤干扰的分类器。与以前的长期跟踪器相比，拟议的跟踪器能够在长期序列中更有力地跟踪**目标**对象。大量实验表明，该算法在多个数据集上获得了最先进的结果。少

2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

评论:6 页

45. 第 1809. 04280[pdf,其他] 反渗透委员会

复杂场景中的人的指令安全导航

作者:哲胡,潘佳,范廷祥,杨瑞刚 ， 迪内什·马诺查

摘要: 在本文中，我们提出了一个机器人导航算法与自然语言接口，使机器人通过遵循人类的指示，如 "去餐馆，远离人，安全地走在不断变化的环境中".我们首先将人工指令分为三种类型: 目标、约束和不提供信息的短语。接下来，我们在导航过程中，以动态的方式为提取的目标和约束项提供接地，以处理距离太远的**目标**对象，而这些目标对象对于传感器的观察和像人类这样移动的障碍物的出现。特别是，对于目标短语 (例如, "去餐厅")，我们将其接地到预定义语义地图中的某个位置，并将其视为全局运动规划师的目标，该规划师在工作区中规划一个无冲突路径，供机器人遵循。对于约束短语 (例如, "远离人员")，我们通过根据对象**检测**模块返回的结果调整本地成本映射的值，动态地将相应的约束添加到本地规划师中。然后使用更新的成本图计算用于计算机器人安全导航的局部避碰控制。通过将自然语言处理、运动规划和计算机视觉相结合，我们开发的系统被证明能够成功地遵循自然语言导航指令，在模拟和现实世界中完成导航任务场景。视频可在 https://sites.google.com/view/snhi 少

2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

46. 第 1809. 04274[pdf,其他] Cs。Sd

改变声学特性，欺骗扬声器验证系统的播放欺骗对策

作者:fuming fang, junichi yamagishi, isao echizen, md sahidullah, tomi kinnunen

摘要: 自动扬声器验证 (asv) 系统使用播放检测器来过滤播放攻击并确保验证可靠性。由于当前的回放**检测**模型几乎总是使用正真语音和回放语音进行训练，因此可能会通过将回放语音的声学特性转换为接近真诚的讲话。这样做的一种方法是在播放之前增强**目标**扬声器的语音 "被盗"。我们使用此方法测试了播放攻击的有效性，方法是使用语音增强生成对抗网络来转换声学特性。实验结果表明，使用这种 "强化窃取语音" 方法可显著提高 asvspoof 2017 年挑战中使用的基线和基于光卷积神经网络的方法的等误码率。结果表明，该系统的使用降低了基于高斯混合模型通用背景模型的 asv 系统的性能。因此，这种攻击是一个亟待解决的问题。少

2018 年 9 月 13 日提交;v1 于 2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

评论:接受 wifi 2018

日记本参考:ieee 信息取证和安全国际研讨会 (wirs), 2018 年

47. **第 xiv:1809.04127[pdf,其他] Cs。红外**

多伊 10.114/327469.327477006

基于图形的推荐系统的中毒攻击

作者:方明红,杨国雷，龚振强,刘佳

摘要: 推荐系统是许多 web 服务的重要组成部分，可帮助用户找到符合其兴趣的项目。几项研究表明，推荐系统容易受到中毒攻击，攻击者将假数据注入给定的系统，以便系统根据攻击者的需要提出建议。然而，这些中毒攻击要么与推荐算法无关，要么经过优化，推荐不基于图形的系统。与基于关联的规则和基于矩阵因素的推荐系统一样，基于图形的推荐系统也在实践中部署，例如 ebay、华为应用商店。然而，如何为基于图形的推荐系统设计优化中毒攻击仍是一个悬而未决的问题。在这项工作中，我们对基于图形的推荐系统的中毒攻击进行了系统的研究。由于资源有限，为了避免**检测**，我们假设可以注入系统的假用户数量是有限制的。关键的挑战是如何将评分分数分配给假用户，以便向尽可能多的普通用户推荐目标项目。为了应对这一挑战，我们将中毒攻击作为一个优化问题来解决，它决定了假用户的评分分数。我们还提出了解决优化问题的技术。我们评估我们的攻击，并将它们与白盒 (建议算法及其参数已知)、灰盒 (推荐算法是已知的，但其参数未知的) 和黑盒 (推荐算法是已知的) 下的现有攻击进行比较未知) 使用两个实际数据集的设置。我们的结果表明，我们的攻击是有效的，并且优于现有的基于图形的推荐系统的攻击。例如，当 1% 的假用户被注入，我们的攻击可以使**目标**项目推荐到 580 倍以上的正常用户在某些情况下。少

2018 年 9 月 11 日提交;最初宣布 2018 年 9 月。

评论:第 34 届计算机安全应用年会 (acsac), 2018 年;由于 "抽象字段不能超过 1, 920 个字符" 的限制，此处出现的抽象比 pdf 文件中出现的抽象略短

类:D.4.6;e.3;I.2。6

48. **第 xiv:1809. 03994[pdf] Cs。简历**

基于深度学习的高效道路车道标记检测

作者:陈炳荣,罗少元,洪秀明, 陈胜伟, 林景杰

文摘: 车道**标记检测**是高级驾驶员辅助系统 (adas) 道路场景分析中的一个重要元素。由于受机载计算能力的限制，降低系统复杂性并同时保持高精度仍是一项挑战。本文提

出了一种利用深卷积神经网络提取鲁棒车道标记特征的车道标记检测器 (lmd)。为了提高其性能，降低了复杂度的目标，采用了膨胀卷积。设计了一种较浅、较薄的结构，以降低计算成本。此外，我们还设计了后处理算法来构造三阶多项式模型，以适应曲线车道。我们的系统在拍摄的道路场景上显示出很有希望的结果。少

2018 年 9 月 11 日提交;最初宣布 2018 年 9 月。

评论:2018 年国际数字信号处理会议 (dsp) 接受

49. 第 xiv:1809.03981[pdf,其他] cs.PL

vandal: 一种可扩展的智能合同安全分析框架

作者:lexi brent, anton jurisevic, michael kong, ericliu, francois gauthier, vincent gramoli, ralph holz, bernhard scholz

摘要: 现代区块链的兴起促进了智能合同的出现: 在区块链上生存和运行的自主项目。智能合同迅速攀升至突出位置，预测了法律、商业、商业和治理领域的应用。智能合同通常用高级语言 (如 ethereum 的 "稳定性") 编写，并转换为紧凑的低级字节码，以便在区块链上部署。部署后，字节码将自动执行，通常由% turing-d 雅式虚拟机执行。与所有程序一样，智能合同由于缺乏编程方法、语言和工具链 (包括错误编译器) 而极易受到恶意攻击。同时，智能合同也是高价值**的目标,**通常占用大量的加密货币。因此，开发人员和审核员需要能够分析低级字节码的安全框架，以**检测**潜在的安全漏洞。在本文中，我们提出了一个安全分析框架的以太智能合同。vandal 由一个分析管道组成，该管道将低级以太虚拟机 (evm) 字节码转换为语义逻辑关系。框架的用户可以以声明性的方式表示安全分析: 安全分析以用 \souffle 语言编写的逻辑规范表示。针对一组常见的智能合同安全漏洞，进行了大规模的实证研究，并展示了 vandal 的有效性和效率。vandal 速度快、鲁棒性强，成功分析了所有 141k 唯一合约的 95% 以上，平均运行时间为 4.15;在同等条件下，表现优于最先进的工具----奥恩特、ethir、mythril 和 rattle。少

2018 年 9 月 11 日提交;最初宣布 2018 年 9 月。

评论:28 页, 11 位数字

50. 第 xiv:1809.03653[pdf, ps,其他] cs. it

无线传感器网络分布式检测的节能决策融合

作者:n. sriranga, k.g. nagananda, r.s. blum, a. saucan, p. k. varshney

抽象: 本文提出了一种在无线传感器网络中对传感器传输进行排序的分布式**检测**节能计数规则。在计算基于规则的**检测中**,n--传感器网络，本地传感器将二元决策传输到融合中心，在融合中心，所有 n 对本地传感器**检测**进行计数，并将其与阈值进行比较。在排序方案中，传感器以顺序的方式将其未量化的统计信息传输到融合中心;信息丰富的传感器享有更高的传输优先级。当在融合中心收集足够的证据进行决策时，传感器的传输就会停止。排序方案实现了与最佳无约束能量方法相同的误差概率 (这需要从所有 n 传感器传输量少得多。本文提出的方案通过订购传感器传输来提高计数规则检测器的能效: 每个传感器的传输时间与其观测函数成反比。由此产生的方案结合了计数规则提供的优势 (有效利用网络的通信带宽，因为本地决策以二进制形式传输到融合中心) 和排序传感器传输 (带宽效率，因为融合中心不需要等待所有的 n 传感器，以传输其本地决策)，从而显著节省能源。作为一个具体的例子，考虑了大规模无线传感器网络中的**目标检测**问题。在一定条件下，基于订单的计数规则方案实现了与原始计数规则检

测器相同的**检测**性能，小于 n/2 传感器传输;在某些情况下，传输的节省方法 (n--1). 少

2018 年 9 月 10 日提交;最初宣布 2018 年 9 月。

评论:7 页, 3 个数字。《2018 年融合论文集》，英国剑桥

51. 第 xiv:1809.002861[pdf,其他] Cs。Lg

论反正化、输入梯度与发射中毒攻击的有趣联系

作者:ambra demottis, marco melis, ma 莫拉平托, matthew jagielski, battista biggio , alinaoprea, cristina nita-rotaru, fabio roti

摘要: 可转换性捕获对机器学习模型的攻击对不同的、可能未知的模型有效的能力。由于部署了基于机器学习的网络攻击检测服务，研究攻击的可转移性在过去几年中引起了人们的兴趣。对于机器学习的这些应用，服务提供商避免披露有关其机器学习算法的信息。因此，试图绕过**检测的**攻击者被迫对代理模型进行攻击，而不是对服务使用的实际**目标**模型进行攻击。虽然先前的工作表明，找到测试时间可转移的攻击样本是可能的，但人们并不十分了解攻击者如何构建可能针对不同模型转移的对抗示例，特别是在训练时间中毒发作。本文首次进行了实证分析，旨在研究测试时间规避和训练时间中毒攻击的可转移性。我们对此类攻击的可转移性提供了统一、正式的定义，并说明了它与**代理和目标**分类模型的输入梯度之间的关系。我们评估一些最知名的机器学习系统在多大程度上容易受到传输攻击，并解释为什么此类攻击在不同模型中成功 (或不成功)。为此，我们利用了本工作中强调的机器学习模型的对抗脆弱性、它们的正则化多参数和输入梯度之间的一些有趣的联系。少

2018 年 9 月 8 日提交;最初宣布 2018 年 9 月。

msc 类: 68t10;68t45

52. 第 xiv:1809.02319[pdf] Cs。Sy

入侵者拦截多机器人团队的无碰撞导航

作者:阿里·马尔佐吉

文摘: 在本报告中，我们提出了一个分散的运动控制算法，为移动机器人拦截入侵者进入 (k 拦截) 或逃逸 (电子拦截) 受保护区域。在继续，我们提出了一个分散的导航策略 (动态拦截) 的多机器人团队被称为捕食者拦截入侵者，换句话说，猎物，从逃脱一个围攻环，这是由捕食者创造的。得到了解决这一问题的必要条件和充分条件。此外，我们还提出了一种基于智能游戏的移动机器人群的基于 igd 的决策算法，以最大限度地提高在有界区域**的检测**概率。证明了所提出的分散协作和非合作博弈决策算法使每个机器人能够做出最佳决策，以最小的局部信息选择最短路径。然后，我们提出了一个基于领先的无碰撞导航控制方法，为一群移动**机器人穿越未知**的杂乱环境，其中被多个障碍占领的目标。我们证明，每个团队成员都能够在该区域安全地遍历，该区域被许多带有任何形状的障碍物所杂乱，可以在某些不确定的开关点上使用传感器而不是连续地捕获**目标**，从而导致从而节省能耗，延长机器人的电池寿命。最后，提出了一种基于虚拟场力算法的独轮车移动机器人在具有运动障碍的杂乱区域的导航策略。通过对导航规律和计算机仿真的数学证明，验证了所提出的方法的有效性、鲁棒性和可靠性。少

2018 年 9 月 7 日提交;最初宣布 2018 年 9 月。

53. 第 09iv:1809.02152[pdf,其他] Cs。铬

浏览器内加密顶升的端到端分析

作者:muhammad saad , aminollah khormali, aziz mohaisen

摘要: 浏览器内的加密劫持包括劫持网站访问者的 cpu 能力，以执行 cpu 密集型加密货币挖掘，并且一直在上升，2017 年增长了 8500%。虽然一些网站主张将加密作为在线广告的替代品，但网络攻击者通过在排名靠前的网站中嵌入恶意加密代码来利用加密来创收。在密码劫持兴起和以往缺乏系统工作的推动下，我们对恶意密码顶字进行了静态、动态的分析，并考察了作为广告替代的加密劫持的经济基础。对于静态分析，我们执行基于内容、货币和代码的分析。通过基于内容的分析，我们揭示了加密劫持是针对各种网站类型的广泛威胁 。通过基于货币的分析，我们突出了采矿平台和货币之间的亲和力：大多数加密网站使用硬币对 monero 进行开采。通过基于代码的分析，我们突出了加密劫持脚本的独特代码复杂性功能，并使用它们检测良性和其他恶意 javascript 代码之间的加密劫持代码，准确率为 96.4%。通过动态分析，我们强调了加密劫持对系统资源的影响，如 cpu 和电池消耗 (在电池供电设备中);我们用后者建立一个分析模型，研究加密劫持作为在线广告替代方案的可行性，并显示出巨大的负利润/损失差距，表明该模型是不切实际的。通过对现有对策及其局限性的调查，运用分析的见解，得出长期对策的结论。少

2018 年 9 月 6 日提交;最初宣布 2018 年 9 月。

54. **第: 1809. 009 2013[pdf,其他] Cs。燃气轮机**

用于对抗和防御性网络欺骗的动态贝叶斯游戏

作者:黄林安,朱全燕

摘要: 安全方面的挑战伴随着效率。信息和通信技术 (信通技术) 的普遍整合使网络物理系统容易受到**具有**欺骗性、持续性、适应性和战略性的攻击。stuxnet、dyn 和 wannacry 勒索软件等攻击实例表明，包括防火墙和入侵**检测**系统在内的现成防御方法是不足的。因此，必须设计最新的安全机制，以减轻风险，尽管成功渗透和复杂的攻击者的战略反应。在本章中，我们使用博弈论来模拟防御者和攻击者之间的竞争互动。首先，我们使用静态贝叶斯游戏来捕捉攻击者的隐身和欺骗特征。一个名为 "具有" "" 的随机变量描述了用户的本质和目标，例如合法用户或攻击者。用户类型的实现是由于网络欺骗而产生的私人信息。然后，我们将单次同时交互扩展到具有非对称信息结构的单次交互中，即信令游戏。最后，我们在高级持久性威胁 (apt) 和田纳西州 eastman (te) 过程的案例研究下研究了多阶段过渡。引入双面不完全信息的原因是，后卫可以采用防御欺骗技术，如蜂蜜文件和蜜罐，为攻击者创建足够数量的不确定性。在本章中，通过对纳什平衡 (ne)、贝叶斯纳什平衡 (bne) 和完美贝叶斯纳什平衡 (pbne) 的分析，可以对对手进行政策预测，并设计主动和战略性防御来震慑攻击者并减轻损失。少

2018 年 9 月 8 日提交;v1 于 2018 年 9 月 6 日提交;最初宣布 2018 年 9 月。

55. **第十四条: 1809. 01444[pdf,其他] Cs。简历**

重剩余注意力的条件传递: 从街景图像中合成交通标志

作者:clclt sebastian, ris uittenbogaard, julen vijverberg, bas boom, peter h. n. de

文摘: 街景图像中交通标志的对象**检测**和分类是资产管理、地图制作和自主驾驶的重要组成部分。然而，一些交通标志很少发生，因此，很难自动识别。为了提高**检测**和分类率，我们建议生成交通标志图像，然后用于训练检测器/分类器。在这项研究中，我们提出了一个端到端框架，从一个给定的交通标志图像和**目标**类的象形图生成一个交通标志的真实图像。我们提出了一种密集串联的剩余注意机制，称为密集剩余注意，在传输对象信息的同时保留背景信息。我们还建议使用多尺度鉴别器，使较小的输出尺度指导

更高的分辨率输出。我们通过使用真实数据和生成数据的组合对检测器进行培训，在大量交通标志类中进行了**检测**和分类测试。在**检测**测试中，新训练的模型将误报数量减少了 1.2-1.5%，在检测测试中召回率为 99%，在分类测试中绝对提高了 4.65 (前 1 名精度)。少

2018 年 9 月 5 日提交;最初宣布 2018 年 9 月。

评论:前两位作者的贡献是平等的。2018 年模式识别国际会议 (icpr) 接受

56. 第: 1809.07[pdf,其他] cse

多伊 10.11145/288916. 2889182

如何在课堂软件工程项目中帮助调查、导师和软件来评估 scrum 采用情况

作者:christoph matthies, thomas kwark, keven richly, Matthies uflacker, husso plattner

摘要: 敏捷方法最好在现实的项目中以动手的方式教授。这样做的主要挑战是评估学生是否正确地应用了这些方法，而不需要在整个项目中进行全面监督。本文介绍了一个课堂项目的经验，在这个项目中，38 名学生使用一个缩放版本的 scrum 开发了一个单一的系统。调查帮助我们确定 scrum 的哪些元素与学生满意度最相关或构成了最大的挑战。这些见解得到了一个导师小组的补充，该小组在整个项目期间陪同主要会议，向团队提供反馈，并记录了对实践中方法应用的印象。最后，我们对协作工件进行了事后、工具支持的分析，以**检测** scrum 采用过程中反模式的具体指标。通过这些技术的结合，我们能够了解学生如何在本课程中实现 scrum，以及哪些元素需要在未来的迭代中进行进一步的授课和辅导。对协作工件的自动化分析被证明是对开发过程的一个有希望的补充，有可能减少未来课程中的手动工作，并允许更具体和**更有针对性**的反馈，以及更客观评估。少

2018 年 9 月 3 日提交;最初宣布 2018 年 9 月。

日记本参考:第三十八届软件工程陪同会议 (icsea16) 论文集。2016 年,, 纽约，纽约，美国, 313-322

57. 第: 1809.00289[pdf,其他] si

多伊 10.114/3274386

意见冲突: 微博中检测无信性的有效途径

作者:suan kalyan maity, aishik chakraborty , pawan goyal , animesh mukherjee

摘要: 在微博上，虐待行为呈上升趋势，往往导致不文明。这一趋势在心理上影响着用户，因此他们往往离开推特和其他此类社交网站，从而耗尽了活跃的用户基础。在本文中，我们研究了与不文明相关的因素。我们观察到，不礼貌的行为与账户持有人 (即编写不文明推特的用户) 和**目标**(即不文明推特所针对或**针对的用户**) 之间的意见差异高度相关,向一个命名实体。我们引入了一个字符级 cnn 模型，并结合实体特定的情绪信息进行有效的不文明**检测**，显著优于多个基线方法，实现了高达 93.3% (4.9%) 的精度在最佳基线上的改进)。在事后分析中，我们还研究了**目标**和账户持有人的行为方面，并试图了解不文明事件背后的原因。有趣的是，我们观察到，有强烈的信号重复在不文明的行为。特别是，我们发现，有相当一部分账户持有人充当累犯----袭击**目标**的次数甚至超过 10 倍。同样，也有一些**目标**多次成为**目标**。一般来说,**这些目标**的声誉得分高于账户持有人。少

2018 年 9 月 2 日提交;最初宣布 2018 年 9 月。

评论:27 页, 14 个数字, 4 个表格, cscw 2018

58. 第 09iv:18009.00223[pdf,其他] Cs。镍

多伊10.100/0.2044

评估具有海量数据的自动流量报告生成中的性能挑战

作者:carlos vega moreno, eduardo miravalls sierra, guillermo julián moreno，豪尔赫 e. lópez de vergara,eduardo magaña, javier aracil

摘要: 本文分析了为大型 it 基础架构生成自动匹配的流量报告所涉及的性能问题。这样的报告使 it 经理能够主动**发现**可能出现的异常情况，并推出相应的相关操作。随着当前网络带宽的不断增加，自动流量报告生成系统的设计具有很大的挑战性。第一步，收集到的大量流量被转化为从不同的收藏者和部门获得的丰富的流量记录。然后，进一步处理此类流记录以及从原始流量中获得的时间序列，以生成可用的报告。如图所示，流记录中的数据量也非常大，需要仔细选择要包括在报告中的关键绩效指标。在这方面，我们讨论了高级语言与低级语言在速度和多功能性方面的使用。此外，我们的设计方法**针对**的是商品硬件的快速开发，这对于经济高效地应对苛刻的流量分析方案至关重要。少

2018 年 9 月 1 日提交;最初宣布 2018 年 9 月。

评论:预打印。预同行评审版本。15 页。7 个数字。1 桌

59. 第 1808. 10313[pdf,其他] 反渗透委员会

基于 roid 的基于罗氏机器人抓取的基于卷积神经网络的目标重叠场景检测

作者:张汉波,阮旭光,周新文,郑南宁

摘要: 掌握**检测**是机器人广泛使用的一项基本技能。最近的研究证明了卷积神经网络 (cnn) 在机器人抓取**检测方面**的先进性。然而，现有**抓取检测**算法的一个重要缺点是它们都忽略了抓取与**目标**之间的联系。本文提出了一种基于感兴趣区域 (roi) 的机器人抓取检测算法，用于在目标重叠场景中同时**检测目标**及其抓取.我们提出的算法在**对目标**进行分类和定位回归时，使用感兴趣的区域 (rois)**来检测**把握。为了训练网络，我们贡献了一个比康奈尔大学掌握数据集更大的多对象抓取数据集，后者是基于可视操作关系数据集。实验结果表明，该算法在 1fppi 下的误码率达到 24.9%，掌握了数据集，达到了 682% 的 map。机器人实验表明，该算法可以帮助机器人以 84% 的成功率在多目标场景中把握指定**的目标.**少

2018 年 9 月 18 日提交;v1 于 2018 年 8 月 30 日提交;最初宣布 2018 年 8 月。

评论:提交给 2019 年 icra

60. 第 1808. 09211[pdf,其他] Cs。简历

深度 gum: 基于高斯均匀混合模型的学习深度鲁棒回归

作者:stphane lathuilière, pablo mesejo, xavier alameda-pineda, radu horaud

摘要: 在本文中，我们讨论了如何有力地训练一个凸网进行回归，或深度鲁棒回归的问题。传统上，深度回归使用 l2 损失函数，已知它对异常值敏感，即样本要么与大多数训练样本存在异常距离，要么对应于错误注释的**目标**。这意味着，在反向传播过程中，异常值可能会由于其梯度的高度而使训练过程产生偏差。在本文中，我们提出了一个深入回归模型，是鲁棒性的异常值由于使用高斯均匀混合模型。我们提出了一种优化算法，该算法在使用期望最大化的异常**值的**无监督检测和使用随机梯度下降的清洁样本的监督训练之间交替使用。deepgum 能够适应不断变化的异常值分布，避免手动对训练集中异常值的比例设置任何阈值。对四种不同任务 (面部和时尚地标**检测**、年龄和头部姿

势估计) 进行了广泛的实验评估，使我们得出结论，我们新颖的稳健技术在各种噪声和噪声的情况下提供了可靠性。防止高比例的异常值。少

2018 年 8 月 28 日提交;最初宣布 2018 年 8 月。

评论:在 2018 年 eccv 会议上接受

61. 第 1808. 08517[pdf, ps,其他] Cs。艾

非平稳数据流可持续学习深神经模糊系统的增量构建

作者:mahardhika pratama, witold Pedrycz, geoffrey i. webb

摘要: 现有的模糊神经网络 (fnn) 大多是在浅层网络结构下发展起来的，其泛化功率低于深部结构。提出了一种新的自组织深度模糊神经网络，即深度演化模糊神经网络 (devfnn)。模糊规则可以自动从数据流中提取，或者如果它们在其生命周期中作用不大，则可以将其删除。通过采用漂移检测方法堆叠**附加**层，不仅可以**检测**协变漂移、输入空间变化，还可以准确地识别实际漂移，从而加深网络的结构,特征空间和**目标**空间的动态变化。devfnn 是在堆叠泛化原理下通过功能增强概念开发的，在该概念中，最近开发的算法，即泛型分类器 (gclass) 驱动隐藏层。它由一种自动特征选择方法组成，该方法控制输入属性的激活和停用，以诱导输入特征的不同子集。针对构建深层网络结构中特征增强方法的性质，提出了一种基于隐藏层合并概念的深层网络简化程序，以防止输入空间维数的不可控制的增长。devfnn 以采样方式工作，并与数据流应用程序兼容。利用 6 个具有非平稳特性的数据集，在当时的预测试训练协议下，对 devfnn 的有效性进行了全面评估。将其与四种最先进的数据流方法及其浅相方法进行了比较，其中 devfnn 在分类精度上有提高。少

2018 年 8 月 26 日提交;最初宣布 2018 年 8 月。

评论:本论文目前正在 ieee 的出版物中进行审查

62. 第 1808. 08296[pdf,其他] Cs。简历

深部学习和 fmri 在 asd 中的脑生物标志物解释

作者:李晓晓, nicha c. dvornek, juntang 壮号, pamela ventola, james s. duncan

摘要: 自闭症谱系障碍 (asd) 是一种复杂的神经发育障碍。找到与 asd 相关的生物标志物对于了解这种疾病的潜在根源非常有帮助，并能导致更早的诊断和更**有针对性**的治疗。尽管深神经网络 (dnn) 已应用于功能磁共振成像 (fmri) 来识别 asd，但以前还没有探讨过数据驱动的计算决策过程。因此，在这项工作中，我们解决了解释与识别 asd 相关的可靠生物标志物的问题;具体而言，我们提出了一种两阶段的方法，使用 fmri 图像对 asd 和控制对象进行分类，并解释分类器激活的显著性特征。首先，我们训练了一个精确的 dnn 分类器。然后，利用脑 fmri 的**解剖**结构，提出了一种频率归一化的图像破坏方法，用于检测不同于计算机视觉中 dnn 可视化工作的生物标志物。此外，在 asd 与对照组的分类场景中，我们提供了一种新的方法来**检测**和表征重要的大脑特征分为三类。我们通过该方法发现的生物标志物是稳健的，与以前在文献中的发现一致。我们还通过神经功能解码和与 dnn 激活图的比较来验证**检测到的**生物标志物。少

2018 年 8 月 23 日提交;最初宣布 2018 年 8 月。

评论:8 张传呼机，被 miccai 2018 年接受

63. 第 1808. 08114[pdf,其他] Cs。简历

注意分型网络: 学习利用医学图像中的显著区域

作者:jo schlemper, ozan oktay, michiel scaap, mattias heinrich, bernhard kainz, benglocker, daniel rueckert

文摘: 我们提出了一种新的医学图像分析注意门 (ag) 模型，该模型可以自动学习到关注不同形状和大小的**目标**结构。使用 ag 训练的模型隐式学习抑制输入图像中不相关的区域，同时突出显示对特定任务有用的突出特征。这使我们能够消除在使用卷积神经网络 (cnn) 时使用显式外部组织器官定位模块的必要性。ag 可以很容易地集成到标准的 cnn 模型，如 vgg 或 u-net 架构，同时将计算开销降至最低，同时提高模型的灵敏度和预测精度。对所提出的 ag 模型进行了多种任务的评估，包括医学图像的分类和分割。对于分类，我们演示了在胎儿超声筛查的扫描平面**检测**中使用 ag 的例子。我们表明，所提出的注意机制可以提供有效的对象定位，同时通过减少误报来提高整体预测性能。为了分割，在两个大型三维 ct 腹部数据集上对所提出的体系结构进行了评估，并对多个器官进行了手动注释。实验结果表明，ag 模型在保持计算效率的同时，一致地提高了基础体系结构在不同数据集和训练规模上的预测性能。此外，ag 还指导模型激活以突出区域为中心，从而更好地洞察模型预测是如何进行的。拟议的 ag 模型的源代码是公开的。少

2018 年 8 月 22 日提交;最初宣布 2018 年 8 月。

评论:提交给医学图像分析 (关于医学成像深度学习的特刊). arxiv 管理说明: 实质性文本重叠与 arxiv:804.03999, arxiv:18004.05 338

64. **第 1808.07371 [pdf,其他] Cs。Gr**

大家现在跳舞

作者:陈嘉玲, shiry ginosar, tinghui zhou,阿列克谢 a. efros

摘要: 本文提出了一个简单的方法 "做我做" 的动作转移: 给定一个人跳舞的源视频，我们可以转移到一个小说 (业余) 目标只有几分钟的**目标**执行标准动作后。我们将此问题描述为具有时空平滑的每帧图像到图像的转换。利用姿势**检测**作为源和**目标**之间的中间表示形式，我们学习了从姿势图像到**目标**主体外观的映射。我们调整这种设置的时间连贯的视频生成，包括现实的人脸合成。我们的视频演示可以在 https://youtu.be/PCBTZh41Ris 找到。少

2018 年 8 月 22 日提交;最初宣布 2018 年 8 月。

65. **特别报告: 1808. 07330[pdf,其他] Cs。简历**

使用少量射击对象检测理解多域文档布局

作者:pranaydeep singh, srikrid 什 na varadarajan, ankit narayan singh, muktabh mayrik srivastava

摘要: 我们试图使用一种简单的算法来解决文档布局理解的问题，该算法在跨多个域的过程中进行概括，而对每个域的例子进行培训。我们通过监督对象**检测**方法来解决这个问题，并提出了一种克服大型数据集需求的方法。我们使用转移学习的概念，在一个简单的人工 (源) 数据集上对对象检测器进行预训练，并在一个微小的域特定 (**目标**) 数据集上对其进行微调。我们证明了这种方法适用于多个领域，训练样本只有 10 个文档。我们在最终结果中证明了该方法的各个组成部分的效果，并证明了这种方法相对于简单对象检测器的优越性。少

2018 年 8 月 22 日提交;最初宣布 2018 年 8 月。

66. **第: 188.07276[pdf, ps,其他] Cs。毫米**

利用颜色成分中的差度检测深部网络生成图像

作者:李浩东,李斌,谭顺泉,黄继武

摘要: 借助强大的深层网络架构 (如生成对抗网络和变分自动编码器), 可以生成大量的逼真图像。生成的图像已经成功地愚弄了人的眼睛, 最初并不是欺骗图像认证系统的**目标**。然而, 研究界和公共媒体对这些图像是否会导致严重的安全问题表示严重关切。本文通过分析真实场景图像与 dng 图像之间颜色分量的差异, 解决了检测深网络生成 (dng) 图像的**问题**。现有的深网络在 rgb 色彩空间中生成图像, 对颜色相关性没有显式约束;因此, dng 图像与其他颜色空间 (如 hsv 和 ycbcr) 中的真实图像有更明显的差异, 尤其是在色度成分中。此外, dng 图像在考虑红色、绿色和蓝色组件时与实际图像不同。基于这些观察, 我们提出了一个特征集, 以捕获彩色图像统计, 以**检测** dng 图像。此外, 在实际考虑的情况下, 还考虑了三种不同的**检测**方案, 并设计了相应的**检测**策略。为了评价该方法的有效性, 对人脸图像数据集进行了大量实验。实验结果表明, 该方法能够区分 dng 图像和真实图像, 具有较高的精度。少

2018 年 8 月 22 日提交;最初宣布 2018 年 8 月。

评论:提交给 ieee 控制论交易

67. **第: 1808. 06991[pdf,其他] Cs。铬**

mlpdf: 一种有效的基于机器学习的 pdf 恶意软件检测方法

作者:张先生

摘要: 由于便携式文档格式 (pdf) 的普及和主要 pdf 查看器应用程序中的漏洞数量不断增加, 恶意软件编写者继续使用它通过 web 下载、电子邮件附件和目标中的其他方法来传递恶意软件和非目标攻击。关于如何有效阻止恶意 pdf 文档的话题在网络安全行业和学术界都获得了巨大的研究兴趣, 没有放缓的迹象。本文提出了一种基于多层感知器 (mlp) 神经网络模型 (mlpdf) 的基于 pdf 的恶意软件检测新方法. 更具体地说, mlpdf 模型使用反向传播算法与随机梯度体面搜索模型更新。从两个真实世界的数据集中提取一组高质量的功能, 其中包含大约 105000 良性和恶意 pdf 文档。评价结果表明, 所提出的 mlpdf 方法性能优异, 明显优于所有评价良好的 8 台商业防病毒扫描仪, 实际阳性率要高得多, 达到 95.12, 而维持一个非常低的假阳性率 0.08%。少

2018 年 8 月 21 日提交;最初宣布 2018 年 8 月。

评论:在 2018 年美国黑帽展会上展出

68. **建议: 1808. 06463[pdf] cs. cy**

多伊 10.1109/MITS.2017.2743201

一种协同车辆对行人安全应用的实现与评价

作者:amin tahmathi-sarvestani, hossein nourkhiz mahjoub, yaser p.fallah, ehsan moradi-pari, oubada abuchaar

摘要: 虽然基于专用短途通信 (dsrc) 的车辆对车辆 (v2v) 安全应用程序的开发已经广泛地进行了十多年的标准化, 但对于脆弱道路来说, 这种应用极为缺失用户 (vru)。vru 和车辆之间不存在协作系统是缺乏关注的主要原因。wi-fi director 和支持 dsrc 功能的智能手机的最新发展正在改变这一观点。利用现有的 v2v 平台, 我们建议使用支持 dsrc 的智能手机建立一个新框架, 以便将安全优势扩展到 vru。通过 sae j2735 个人安全消息 (psm) 实现了车辆和便携式 dsrc 支持的设备之间的应用程序互操作性。但是, 考虑到 vru 的运动动态、响应时间和崩溃场景与车辆有着根本的不同, 因此应为 vru 安全应用程序设计一个特定的框架来研究其性能。在本文中, 我们首先提出了一个

端到端车辆到行人 (v2p) 框架，以提供基于最常见和最容易发生伤害的崩溃场景的态势感知和危险**检测**。下面将详细介绍我们的 vru 安全模块，包括**目标**分类和碰撞**检测**算法。此外，我们还针对此类系统中的拥塞和功耗问题提出并评估了缓解方案。最后，针对现实的崩溃场景，对整个系统进行了实现和分析。少

2018 年 8 月 1 日提交;最初宣布 2018 年 8 月。

日记本参考:ieee 智能交通系统杂志，第 9 卷，第 4 号，62-75 页，2017 年冬季

69. **第: 1808. 06 216[pdf,其他] cse**

二值代码克隆分析的基于语义的混合方法

作者:胡一坤,张元元,李娟如, 王辉, 李伯东,顾大武

文摘: 二进制代码克隆分析是一项重要的技术，在软件工程中有着广泛的应用 (如剽窃检测、错误**检测**)。该主题的主要挑战在于语义等效代码转换 (例如，优化、混淆)，它将极大地改变二进制代码的表示形式。另一个挑战是**检测**精度和覆盖范围之间的权衡。遗憾的是，现有的技术仍然依赖于容易受到代码转换影响的无语义代码功能。此外，它们仅采用静态或动态方法来**检测**二进制代码克隆，而不能同时实现较高的精度和覆盖率。本文提出了一种基于语义的混合方法来**检测**二进制克隆函数。我们执行模板二进制函数及其测试用例，并模拟每个**目标**函数的执行，以便与从该模板函数迁移的运行时信息进行克隆比较。语义签名是在模板函数的执行和**目标**函数的仿真过程中提取的。最后，从他们的签名中计算出相似度分数，以测量他们的相似度。我们在一个原型系统中实现了该方法，该系统被指定为 binmatch，分析 linux 平台上的 ia-32 二进制代码。我们使用不同的编译配置和常用的模糊处理方法编译的八个实际项目评估 binmatch，总共执行超过 1 亿对函数比较。实验结果表明, binmatch 对语义等效代码变换具有鲁棒性。此外，它不仅涵盖了克隆分析的所有**目标**函数，而且与最先进的解决方案相比，提高**了检测**精度。少

2018 年 8 月 19 日提交;最初宣布 2018 年 8 月。

70. **第 xiv: 1808. 05998[pdf] Cs。哦**

利用 synopsys 工具创建和修复光刻热点

作者:曾一伦, valerio perez, yongfuli, zhao chuan lee, vikas tripathi, jonathan yoong seang ong

文摘: 在先进的工艺节点中，模式匹配技术已被应用于光刻热点的**检测**中，这可能会影响集成电路的产量。尽管已经开发了商业模式匹配和设计中的热点修复工具，但工程师们仍然需要验证路由设计中的特定热点模式确实可以通过软件工具**检测到**甚至修复。因此，需要创建测试用例，通过使用 apr (自动放置和路由) 工具，可以在路由布局中生成**目标**热点模式。本文提出了一种利用 synopsys 工具在路由空间中创建热点模式的方法。并提出了在物理设计阶段修复热点的方法。利用所提出的热点创建方法，可以生成包含**目标**热点模式的路由设计。因此，可以验证热点**检测**规则、热点固定制导规则和相关软件工具功能的有效性。少

2018 年 8 月 16 日提交;最初宣布 2018 年 8 月。

71. **第 1808. 08705[pdf,其他] Cs。铬**

通过嵌入式特征选择缓解对抗性攻击

作者:ziyi bao, luis muñoz-zález, emil c. lupu

摘要: 机器学习已成为许多应用领域任务自动化的主要组成部分之一。尽管机器学习取得了进步和令人印象深刻的成就，但事实表明，学习算法在训练和测试时都可能受到攻击者的攻击。机器学习系统特别容易受到对抗示例的影响，在这些示例中，添加到原始数据点的小扰动可能会在测试时在学习算法中产生不正确或意外的输出。减轻这些攻击是很困难的，因为很难**发现**敌对的例子。现有的相关工作表明，在应用特征选择以降低系统复杂性时，机器学习系统相对于对抗实例的安全性可能会受到削弱。本文对这一观点进行了实证分析，表明**当目标**使用一组较小的功能时，攻击者在攻击中成功所带来的相对失真更大。我们还表明，最小的对抗性例子在统计上与特征数量较少的真实示例的差异更大。但是，减少功能计数可能会对系统的性能产生负面影响。我们用具体的例子说明了安全性和准确性之间的权衡。我们提出了一种设计方法，以评估机器学习分类器的安全性与嵌入式特征选择的对手的例子使用不同的攻击策略。少

2018 年 8 月 16 日提交;最初宣布 2018 年 8 月。

72. **第 xiv: 1808. 05560[pdf,其他] Cs。简历**

R3 个-网络: 航空图像和视频中的多定向车辆检测的深层网络

作者:李庆鹏,莫立超,徐启志，张云,朱晓香

文摘: 车辆**探测**是航空遥感应用中一项具有重大挑战性的任务。现有的大多数方法**都检测**出有常规矩形箱的车辆，未能提供车辆的方向。然而，方向信息对于车辆的轨迹和运动估计等几个实际应用至关重要。本文提出了一种新的深部网络，称为可旋转区域的剩余网络 (r) 。3 个-网络)，以检测空中图像和视频**中的**多方向车辆。更特别的是, r3 个-利用网络在半坐标系中生成可旋转矩形**目标**盒。首先，我们使用可旋转区域建议网络 (r-rpn) 从深卷积神经网络生成的地形图中生成可旋转的感兴趣区域 (r-rois)。在这里，提出了一个批量平均可旋转锚点 (bar 锚点) 策略，以初始化车辆候选的形状。接下来，我们提出了一个可旋转**的检测**网络 (r-dn)，用于 r-rois 的最终分类和回归。在 r-dn 中，设计了一种新的可旋转位置敏感池 (r-ps 池)，在对 r-rois 特征图进行下采样时，同时保持位置和方向信息。在我们的模型中, r-rpn 和 r-dn 可以联合训练。我们在两个开放的车辆**检测**图像数据集 (即 dlr 3k 慕尼黑数据集和 vegai 数据集) 上测试我们的网络，证明了我们的方法的高精度和鲁棒性。此外，对航空视频的进一步实验表明，该方法具有良好的泛化能力，具有在航空视频中跟踪车辆的潜力。演示视频可在 https://youtu.be/xCYD-tYudN0 上找到。少

2018 年 8 月 16 日提交;最初宣布 2018 年 8 月。

73. **第 1808. 04234[pdf,其他] Cs。简历**

基于深层结构模型的快速视频拍摄转换本地化

作者:唐世涛,冯立东，张奎光,陈一民，张伟

摘要: 视频镜头转换检测是视频分析中的一个关键预处理步骤。以往的研究仅限于通过相似度测量来**检测**帧之间的突然内容变化，而多尺度运算被广泛用于处理不同长度的过渡。然而，由于相邻帧之间的视觉相似性较高，渐进转换的本土化仍未得到充分的探索。剪切射弹转换是突然的语义中断，而渐进的拍摄转换包含由视频效果引起的低级时空模式，以及逐步语义中断，例如溶解。为了解决这个问题，我们提出了一个结构化网络，能够分别使用 **目标**模型检测这两个镜头转换。考虑到速度性能的权衡，我们设计了一个智能框架。使用一个 titan gpu，该方法可以实现 30X 实时速度。在公共 trecvid07 和 rai 数据库上的实验表明，我们的方法优于最先进的方法。为了训练高性能的镜头转换探测器，我们提供了一个新的数据库剪贴画，其中包含 128636 切割过渡

和 38120 逐步过渡从 4039 在线视频。剪贴画有意收集短视频，用于由手持相机振动、大物体运动和遮挡引起的更困难的情况。少

2018 年 8 月 13 日提交;最初宣布 2018 年 8 月。

评论:向 accv 提交 16 页, 3 个数字

74. 第 xiv:1808. 03712[pdf,其他] Cs。CI

基于异常检测的无监督关键字提取

作者:eirini papagiannopoulou, grigorios tsoumakas

文摘: 提出了一种新的基于异常**点检测**的无监督关键字提取方法。我们的方法从**在目标**文档上训练单词嵌入开始，以捕获单词之间的语义规律性。然后，它使用最小协方差行列式估计来建模非关键字向量的分布，假设这些向量来自相同的分布，这表明它们与由学习的向量表示的维数。候选关键字短语基于的单词是此主要分布的异常值。经验结果表明，我们的方法优于最先进的无监督关键字短语提取方法。少

2018 年 8 月 10 日提交;最初宣布 2018 年 8 月。

评论:作者预打印版本

75. 建议: 1808. 03515[pdf,其他] Cs。铬

基于 gps/ins 的道路定位跟踪系统的安全性

作者:sashank narain, aanjhan ranganathan, guevara noubir

摘要: 位置信息对于各种导航和跟踪应用程序至关重要。如今, gps 是事实上的户外定位系统，但已被证明容易受到信号欺骗攻击。惯性导航系统 (ins) 正在成为一种流行的补充系统，特别是在道路运输系统中，因为它们能够改进导航和跟踪，并提供对无线信号欺骗和干扰攻击的恢复能力。本文对道路运输系统中由 ins 辅助 gps 跟踪和导航的安全保障进行了评估。我们认为需要对手从源位置前往目的地，并由 ins 辅助 gps 系统进行监控。对手的目标是在不被**发现**的情况下前往其他地点。我们开发和评估了实现此类目标的算法，为对手提供了很大的自由度。我们的算法为给定的路网构建了一个图形模型，并使我们能够在不发出警报的情况下，即使使用 ins 辅助的 gps 跟踪和导航系统，也能得出攻击者可以到达的潜在目的地。这些算法使陀螺仪和加速度计传感器变得无用，因为它们产生的道路轨迹与合理的路径无法区分 (在转弯角度和道路曲率方面) 都无法区分。我们还设计、建造并演示了磁力计可以使用精心控制的线圈组合进行主动欺骗。我们在世界各地的 10 多个城市使用真实世界和模拟驾驶痕迹实施和评估了袭击的影响。我们的评估显示，攻击者有可能在不被**发现**的情况下到达距离真实目的地 30 公里的目的地。我们还表明，在一些城市，对手有可能达到**目标**区域内近 6 0%-8 0% 的可能点。少

2018 年 8 月 10 日提交;最初宣布 2018 年 8 月。

76. 第 188.03513[pdf,其他] Cs。简历

高阶多变量累积带的波段选择，用于高光谱图像中的小目标检测

作者:przemyslaw gvomb, krzysztof domino, michal romaszewski, michal cholewa

摘要: 在小**目标检测**问题中，要定位的模式的数量级小于数据集中存在的其他模式。这既适用于监督**检测**的情况，即已知模板预计仅在几个区域匹配，而非监督异常**检测**则是罕见的，因为异常根据定义是罕见的。此问题通常与成像应用有关，即摄像机在场景中进行**检测**。为了最大限度地利用有关场景的现有数据，使用了高光谱摄像机;在每个像素，他们记录在数百个狭窄的波段的光谱数据。高光谱成像的典型特征是目标材料的

特征特性在少量波段中可见，在这些波段中，特定波长的光与特征分子相互作用。基于统计原理的目标独立波段选择方法是在不同实际应用中解决这一问题的通用工具。规则背景和罕见的站立异常的结合会在高光谱像素的联合分布中产生畸变。高阶累积量是这个分布的一个自然的 "窗口"，可以测量属性，并建议候选波段删除。虽然有人试图产生基于第 3 个累积量的张量，即关节偏斜的波段选择算法，但文献中缺乏对累积张量使用顺序如何影响波段选择有效性的系统分析。**检测**应用。本文分析了一种基于高阶累积量的带选择通用算法。我们讨论了它与性能中观察到的断点有关的可用性，这取决于方法顺序和所需的波段数量。最后，我们进行了实验，并在高光谱**检测场景中**对这些方法进行了评估。少

2018 年 8 月 10 日提交;最初宣布 2018 年 8 月。

77. **xiv:1808.3350[pdf,其他] cs. cy**

发现查加斯病在阿根廷和墨西哥的传播

作者:juan de 修道院, alejo salles, carolina lang, diego weinberg, martin minuni, matias travizano, carlos sarraute

摘要: 恰加斯病是一种被忽视的疾病，其地理传播信息非常可怕。我们在这里分析流动性和通话模式，以便通过使用公共卫生信息和手机记录，确定这种疾病的潜在风险区。地理定位通话记录具有丰富的社会和流动性信息，可用于推断个人是否生活在流行地区。我们介绍了拉丁美洲国家的两个案例研究。我们的目标是制作风险图，供公共卫生运动管理人员使用，以确定**检测**活动的优先次序并**针对**特定领域。最后，分析了手机数据对推断长期迁移的价值，长期迁移在查加斯病的地域传播中发挥着至关重要的作用。少

2018 年 8 月 9 日提交;最初宣布 2018 年 8 月。

评论:发表于 netmob 2017 (第五次移动电话数据集科学分析会议)，意大利米兰。4 月 5, 2017

类:j.4;H.2。8

78. **建议: 1808.03 114[pdf,其他] Cs。简历**

培训设计设计: 一种用于解决图像分类培训数据错误的交互式、网络支持的可视化分析系统

作者:alex bäuerle, heiko neumann, timo ropinski

摘要: 卷积神经网络在图像分类任务中的应用越来越受到人们的欢迎，因为它们甚至能够超越人类分类器。虽然很多研究都是针对网络架构优化的，但标记训练数据的优化还没有明确**针对**。由于培训数据的标签很耗时，因此通常由经验不足的领域专家执行，甚至外包给在线服务。遗憾的是，这会导致标记错误，从而直接影响训练网络的分类性能。为了克服这个问题，我们提出了一个交互式可视化分析系统，帮助发现和纠正训练数据集中的错误。为此，我们确定了实例解释错误、类解释错误和相似性错误，将其确定为频繁发生的错误，这些错误应解决，以提高分类性能。**在我们检测到**这些错误后，将通过两步可视化分析过程引导用户向他们走去，在该过程中，他们可以直接重新分配标签以解决**检测到的**错误。因此，使用所提出的可视化分析系统，用户必须检查较少的项目，以解决训练数据集中的标记错误，从而更快地获得满意的训练结果。少

2018 年 8 月 9 日提交;最初宣布 2018 年 8 月。

79. **第 xiv:1808. 02996[pdf,其他] Cs。简历**

基于两步卷积神经网络的卫星图像目标检测

作者:hiroki miyamoto, kazuki uehara, masahiro murakawa, hidenori sakanashi, hirokazunosato, toru kukoyama, ryosuke nakamura

文摘: 本文提出了一种有效的卫星图像**目标检测**方法。在多项机器学习算法中，我们提出了两个卷积神经网络 (cnn) 的组合，分别针对高精度和高召回。我们使用高尔夫球场作为**目标**对象验证了我们的模型。所提出的深度学习方法比以往的目标识别方法具有更高的精度。少

2018 年 8 月 8 日提交;最初宣布 2018 年 8 月。

评论:4 页 5 个数字

80. **第 xiv:1808.02741[pdf, ps,其他] Cs。铬**

偷看：我看到你的智能家居活动，甚至加密了!

作者:abbasacar , hossein fereidooni, tigist ab 板, amit kumar sikder, markus miettinen, hidayetaksu, mauro conti, ahad-reza sadeghi , a. selcuk Uluagac

摘要: 智能家居环境中的各种物联网设备 (如灯泡、开关、扬声器) 使用户能够轻松控制周围的物理世界，并促进他们的生活方式。但是，智能家居环境内或附近的攻击者可能会利用这些设备使用的固有无线媒体来泄露有关用户及其活动的敏感信息，从而侵犯用户隐私。考虑到这一点，在这项工作中，我们介绍了一个新的多阶段隐私攻击的用户隐私在智能环境中。它是利用最先进的机器学习方法，通过被动地观察无线技术，以级联方式检测和识别特定类型的物联网设备、它们的行为、状态和正在进行的用户活动来**实现**的来自智能家居设备的流量。攻击有效地适用于加密和未加密的通信。我们利用一系列不同的网络协议 (如 wifi、zigbee 和 ble)，从一系列流行的现成智能家居物联网设备中进行实际测量，从而评估攻击的效率。我们的研究结果表明，对手被动嗅到网络流量可以在识别**目标**智能家居设备及其用户的状态和行为方面达到非常高的精度 (超过 90%)。与早期的简单方法不同，我们的多级隐私攻击可以在没有大量背景知识或分析协议规范的情况下自动执行活动**检测**和识别。这使得对手能够有效地聚合目标用户的广泛行为配置文件。为了防止这种隐私泄漏，我们还提出了一种基于生成欺骗网络流量的对策，以隐藏设备的真实活动。我们还证明，所提供的解决方案比现有解决方案提供了更好的保护。少

2018 年 8 月 8 日提交;最初宣布 2018 年 8 月。

评论:14 页, 6 个数字

81. **第 1808.02134[pdf,其他] Cs。直流**

克尔曼：一种混合轻量级跟踪算法，使智能监控成为边缘服务

作者:seyed yahya nikouei, yu chen, sejun song, timothy r. faughnan

摘要: 边缘计算通过利用接近数据源和**目标的**计算过程，将云计算边界推向不确定的网络资源之外。时间敏感和数据密集型视频监控应用程序受益于现场或现场数据挖掘。近年来，利用人工智能 (ai) 和机器学习 (ml) 算法提出了许多用于目标**检测**和跟踪的智能视频监控方法。但是，由于计算要求较高，仍很难将这些计算和数据密集型任务从云迁移到边缘。本文设想通过提出一种名为 kerman (kerman 滤波器) 的混合轻量级跟踪算法，实现智能监控作为一种边缘服务。克尔曼是一种基于决策树的混合神经化相关滤波器 (kcf) 算法，该算法是为人体目标跟踪而提出的，它与轻量级的卷积神经网络 (l-cnn) 相结合，具有较高的性能。拟议的克尔曼算法已在几台单板计算机 (sbc) 上作为边缘设备实现，并使用现实世界的监控视频流进行了验证。实验结果有望使克尔曼

算法能够在边缘设备负担得起的资源消耗条件下，以相当的准确性跟踪感兴趣的对象。少

2018 年 8 月 6 日提交;最初宣布 2018 年 8 月。

评论:提交给 ieee ccnc 2019 年

82. 第 xiv:1808. 02066[pdf,其他] Cs。Db

数据计算器的内部结构

作者:stratos idreos, kostas zoumpatianos, brian hentschel, michael s.kester , demi guo

摘要: 在任何数据驱动的方案中，数据结构都是至关重要的，但众所周知，由于设计空间巨大，性能依赖于不断发展的工作负载和硬件，因此很难进行设计。我们提出了一个设计引擎，数据计算器，它支持数据结构的交互式和半自动设计。它带来了两个创新。首先，它提供了一组细粒度设计原语，用于捕获数据布局设计的首要原则：数据结构节点如何布局数据，以及它们之间的相对定位。这样就可以对可能的数据结构设计的宇宙进行结构化描述，这些设计可以作为这些基元的组合进行合成。第二个创新是使用学习成本模型计算性能。这些模型在不同的硬件和数据配置文件上进行了培训，并捕获了基本数据访问原语 (例如随机访问) 的成本属性。通过这些模型，我们综合了任意数据结构设计上复杂操作的性能成本，而无需: 1) 实现数据结构, 2) 运行工作负载，甚至 3) 访问**目标**硬件。我们证明，数据计算器可以通过精确地回答大约几秒钟或几分钟的丰富假设设计问题，即计算给定数据结构的性能 (响应时间) 如何，来帮助数据结构设计人员和研究人员设计受到以下方面变化的影响: 1) 设计、2) 硬件、3) 数据和 4) 查询工作负载。在开始漫长的实施、部署和硬件获取步骤之前，可以轻松地测试大量的设计和想法。我们还演示了数据计算器可以合成全新的设计、自动完成的部分设计以及**检测**次优设计选择。少

2018 年 8 月 6 日提交;最初宣布 2018 年 8 月。

83. 新建: 1808. 1957[pdf,其他] Cs。铬

多伊 10.1109/TETC.2017.2756908

认识异常，发现邪恶：频繁的模式挖掘勒索软件的威胁狩猎和情报

作者:sajad homayoun, ali dehghantanha, marzieh ahadadeh, sattar hashemi, raouf khayami

摘要: 密码勒索软件的出现极大地改变了网络威胁格局。加密勒索软件通过加密受害者计算机上的宝贵数据来消除数据托管人访问，并要求通过解密数据向重新建立的托管人访问支付赎金。及时**检测**勒索软件在很大程度上取决于如何快速和准确的系统日志可以开采，以寻找异常和阻止邪恶。在本文中，我们首先建立了一个环境，以收集活动日志 517 locky 勒索样本, 517 cerber 勒索软件样本和 572 个样本的 teslacrypt 勒索软件。我们利用序列模式挖掘来查找不同勒索软件家族中活动的最大频率模式 (mfp)，作为使用 j48、随机林、套袋和 mlp 算法进行分类的候选特征。从恶意软件样品中**检测**勒索软件实例的精度达到 99%，在**检测**给定勒索样品的族数方面达到 96.5 的准确性。我们的研究结果表明，应用模式挖掘技术检测勒索软件狩猎的良好功能是有用和实用的。此外，我们还展示了在不同勒索软件家族中存在独特的频繁模式，可用于识别勒索样本系列，以建立有关威胁行为者的情报和特定**目标**的威胁配置文件.少

2018 年 8 月 6 日提交;最初宣布 2018 年 8 月。

评论:11 页不: 要获得论文的最后一个版本，请转到
https://doi.org/10.1109/TETC.2017.2756908

84. 第 188.01155[pdf,其他] Cs。铬

多伊10.107/978-3-319-7391-9 _ 10

用于暗网威胁情报的自适应流量指纹识别

作者:hamish haughey, gregory epifaniou, haider al-khateeb, ali dehghantanha

摘要: tor 等暗网技术已被各种威胁行为体用于组织非法活动和数据泄露。因此，各组织有理由阻止这类交通，或试图确定何时使用和用于何种目的。然而，网络空间的匿名一直是利益冲突的领域。虽然它赋予邪恶的行为者足够的权力来伪装他们的非法活动，但它也是促进言论自由和隐私的基石。我们提出了一个新的算法的概念证明，可以形成一个能够黑暗的网络威胁情报平台的基本支柱。该解决方案可以降低 tor 用户的匿名性，并在启动**有针对性**或广泛的 bgp 拦截之前考虑网络流量的现有可见性。结合服务器 http 响应操作，该算法尝试减少候选数据集，以消除最不可能负责感兴趣的服务器端连接的客户端通信。我们的测试结果显示, mitm 操作的服务器响应会导致 tor 客户端收到预期的更改。利用阴影生成的仿真数据，证明了该**检测**方案是有效的，假阳性率为 0.001，灵敏度**检测**非**目标**为 0.016 +-0.001 。我们的算法可以帮助愿意在调查期间分享威胁情报或合作的合作组织。少

2018 年 8 月 3 日提交;最初宣布 2018 年 8 月。

评论:26 页

85. 第 xiv:1808. 00588[pdf,其他] Cs。简历

天气分类: 一种新的多级数据集、数据增强方法及对流神经网络的综合评价

作者:jose carlos villarreal guerra, zeba khanam, shoaib ehsan, rustam stolkin, klaus mcdonald-maier

摘要: 天气状况往往扰乱运输系统的正常运行。当前系统可以部署一系列传感器，也可以使用车载摄像头来预测天气状况。这些解决方案导致了成本的增加和范围的限制。为确保所有运输服务在全天候条件下顺利运作，需要一个可靠的**检测**系统对野外天气进行分类。解决这一问题所涉及的挑战是，天气条件多种多样，各种天气条件之间没有歧视特征。现有的解决这一问题的工作是针对现场的，并**有针对性**地对两类天气进行分类。在本文中，我们创建了一个新的开源数据集，其中包含描述三类天气 (即雨、雪和雾) 的图像，称为 rfs 数据集。提出了一种新的算法，该算法利用超级像素划分掩码作为数据增强的一种形式，对十个卷积神经网络架构产生了合理的效果。少

2018 年 8 月 1 日提交;最初宣布 2018 年 8 月。

86. 第 xiv:1808. 00529[pdf,其他] Cs。Lg

使用 pac 保证进行开放类别检测

作者:siliu, risheek Garrepalli: thomas g. dietterich, alan fern, dan hendrycks

文摘 开放类别**检测**是**检测**属于训练数据中不存在的类别或类的 "外来" 测试实例的问题。在许多应用中，可靠**地检测**此类外星人对于确保测试集预测的安全性和准确性至关重要。不幸的是，没有任何算法为他们在一般假设下**检测外星人的**能力提供理论保证。此外，虽然有开放类别**检测**的算法，但直接报告外星**检测**率的经验结果很少。因此，在我们对开放类别**检测**的理解上存在着显著的理论和经验差距。在本文中，我们通过研究一种简单但与实践相关的开放类**检测变体,**朝着解决这一差距迈出了一步。在我们的环

境中，我们会得到一个 "干净" 的培训集，其中只包含感兴趣的**目标**类别，以及一个未标记的 "受污染" 培训集，其中包含一小部分αα外星人的例子。在假设，我们知道一个上限αα，我们开发了一个算法与 pac 风格保证外星**检**出率，同时旨在最大限度地减少误报。综合和标准基准数据集的经验结果表明了该算法能够有效的制度，并为进一步的改进提供了基线。少

2018 年 8 月 1 日提交;最初宣布 2018 年 8 月。

87. 第 xiv:1808.00163[pdf,其他] Cs。毫米

下一代宣传的广告创作体系

作者:atul nautiyal , killian mccabe, murhaf hossari, soumyabratadev, matthew nicolson, clare conran, declan mckibben, jian tang, xu wei, 弗朗索瓦·皮蒂

摘要: 随着互联网多媒体数据的迅速普及，为观众制作的视频也在迅速上升。这使得观众可以跳过视频中的广告中断，使用广告拦截器和 "跳过广告" 按钮-将在线营销和宣传带到摊位。本文演示了一个能够有效地将新广告集成到视频序列中的系统。我们使用最先进的技术，从深度学习和计算摄影测量，有效**地检测**现有的广告，并无缝地将新广告集成到视频序列。这对**有针对性**的广告很有帮助，为下一代的宣传铺平了道路。少

2018 年 8 月 1 日提交;最初宣布 2018 年 8 月。

评论:2018 年欧洲机器学习与数据库知识发现原理与实践会议 (ecml-pkdd)出版

88. 第 1808.00157[pdf,其他] Cs。简历

通过部件分组网络进行实例级人工分析

作者:kegong, xi 晓丹 liang, y 童 li, yimin chen, ming yang, lilin

摘要: 由于缺乏足够的数据资源和在一次传递中分析多个实例的技术困难，对真实世界的人工分析场景进行实例级人工分析的研究仍然不足。一些相关的作品都遵循 "逐检" 管道,该管道在很大程度上依赖于单独训练的**检测**模型来本地化实例，然后按顺序对每个实例执行人工分析。尽管如此,**检测**和解析的两个不一致**优化目标**导致了最终结果的不理想表示学习和误差积累。在本工作中，我们首次尝试探索无**检测**部件分组网络(pgn)，以便在一次传递中有效地分析图像中的多个人。我们的 pgn 将实例级人工解析重新表述为两个可通过统一网络共同学习和相互细化的分段任务: 1) 语义部分分割，用于将每个像素指定为人工部分 (例如，人脸、手臂);2) 实例感知边缘**检测**，将语义部分分组到不同的人员实例中。因此，共享中间表示法将被赋予对细粒度部分进行定性和推断每个部件的实例财产的能力。最后，采用一个简单的实例划分过程，在推理过程中得到最终结果。我们在 pascal-人的零件数据集上进行了实验，我们的 pgn 优于所有最先进的方法。此外，我们还展示了它在新收集的多人分析数据集 (cihp) 上的优势，其中包括 38, 280 种不同的图像，这是迄今为止最大的数据集，可以促进更高级的人体分析。cihp 基准和我们的源代码可在 http://sysu-hcp.net/lip/。少

2018 年 7 月 31 日提交;最初宣布 2018 年 8 月。

评论:被 eccv 2018 款 (口头) 接受

89. 第 1807.11110[pdf,其他] Cs。铬

基于深神经网络的 ropnn 有效载荷检测

作者:李旭生,胡志生,傅义伟, 陈平,朱明辉,刘鹏

摘要: 面向返回的编程 (rop) 是一种代码重用攻击，它将现有代码 (称为小工具) 的短片段链接到**目标**计算机上执行任意操作。现有的针对 rop 的**检测**机制通常依赖于某些启发式规则，或者需要对程序或编译器进行检测。因此，它们表现出较低的**检测**效率和/或具有较高的运行时开销。本文介绍了将地址空间布局引导拆卸和深度神经网络创新地结合起来的 romnn，以**检测** http 请求、pdf 文件和图像等中的 rop 有效负载。拆装器将应用程序输入数据视为指向潜在小工具的代码指针，旨在查找任何潜在的小工具链。然后，被深层神经网络归类为良性或恶意的已识别的潜在小工具链。提出了分别生成两个训练数据集并处理大量原始输入数据以获得足够训练数据的新方法。实验表明, romnn 具有较高的**检**出率 (98.3%)，同时保持了极低的假阳性率 (0.01%)。为了显示 ropnn 在实际情况下是可用的，我们还针对在野外收集、手动创建或 rop 利用生成工具 roper 和 ropc 创建的 rop 漏洞对其进行测试。romnn 成功**地检测到**所有的 80 漏洞。同时, rpnn 是完全非侵入性的，不会给受保护的程序带来任何运行时开销。少

2018 年 7 月 29 日提交;最初宣布 2018 年 7 月。

90. 第: 1807. 11024[pdf] Cs。红外

基于本体特征的网上评论的意见垃圾邮件识别方法

作者:l. h. nguyen, n.t . h. pham, v. m. ngo

摘要: 如今，有很多人利用社交媒体的意见来决定购买产品或服务。意见垃圾邮件**检测**是一个难题，因为假评论可以由组织以及个人为不同的目的。他们写虚假的评论误导读者或自动**检测**系统，通过推广或降级目标产品，以促进他们或损害他们的声誉。本文提出了一种利用基于知识的本体论检测高精度 (高于 75%) 的语音垃圾邮件**的**新方法。关键词: 意见垃圾邮件，虚假审查，电子商务，本体论。少

2018 年 7 月 29 日提交;最初宣布 2018 年 7 月。

评论:15 页，《科学杂志，特刊: 自然科学与技术》，胡志明市教育大学

91. 第 xiv: 1807. 10819[pdf,其他] Cs。简历

多伊 10.1007/978-3-319-66179-7 _ 73

cased: 针对极端数据不平衡的课程自适应采样

作者:andrew jason, nicolas guizard, sina hamidi Ghalehjegh, damiengoblot, florian soudan, nicolas chapados

文摘: 我们介绍了一种新的课程采样算法--caed，该算法便于优化具有极优的类不平衡的数据集的深度学习分割或**检测**模型。我们评估了 cfed 学习框架的任务肺**结节检测**胸部 ct。与两阶段解决方案不同的是，在这种解决方案中，结核候选项首先由分割模型提出，并由第二个**检测**阶段细化，与此不同, cfed 将深结核分割模型 (如 unet) 的训练改进到了艺术成果是只使用一个微不足道的**检测**阶段来实现的。cased 通过让它们首先了解如何区分结核和周围环境，同时不断增加更大比例的难以分类的全局环境，直到均匀，从而改进了深度分割模型的优化从经验数据分布的抽样。在训练中使用 caed 可以对肺结节**检测**问题提出最低限度的建议，该问题超过了 lua16 结节**检测**基准，平均敏感性评分为 8835%。此外，我们发现，使用 cased 训练的模型对结核注释质量具有鲁棒性，因为它表明，如果在训练期间只提供每个地面真相结核的点和半径，就可以取得可比的结果。最后, cased 学习框架没有对成像模式或分割**目标**做出任何假设，应推广到其他医学成像问题，其中班级失衡是一个持续存在的问题。少

2018 年 7 月 27 日提交;最初宣布 2018 年 7 月。

评论:2017 年第 20 届医学图像计算与计算机辅助干预国际会议

92. **新建: 1807. 10501[pdf, ps,其他] Cs。Sd**

国内环境下的大型弱标记半监管声事件检测

作者:romain serizel, nicolas turpault, hamid eghbal-zadeh, ankit parag shah

文摘: 本文介绍了 dcase 2018 年任务 4。该任务评估使用弱标记数据 (没有时间边界) 大规模**检测**声音事件的系统。系统的**目标**不仅是提供事件类，还提供事件时间边界，因为音频录制中可能存在多个事件。这项任务的另一个挑战是探索利用大量不平衡和未标记的培训数据以及一个小的弱标记训练集来提高系统性能的可能性。这些数据是来自国内背景的优酷视频节选，有许多应用，如环境辅助生活。之所以选择该领域是由于科学挑战 (各种声音、时间局部事件.) 和潜在的工业应用。少

2018 年 7 月 27 日提交;最初宣布 2018 年 7 月。

93. **第 xiv:1807. 10443[pdf] Cs。铬**

多伊 1011186/1363-016-0623-3

基于熵的云计算 ddos 检测多滤波器特征选择方法

作者:opeyemi Osanaiye, k2-kwang raymond choo2, ali dehghantanha, 郑旭, mqhele dlodlo

摘要: 人们 人们对采用云计算的兴趣越来越大，使其面临网络攻击。其中之一是分布式拒绝服务 (ddos) 攻击,**其目标是**云带宽、服务和资源，使云提供商和用户都无法使用。由于需要处理的流量非常大，提出了数据挖掘和机器学习分类算法来对异常中的正常数据包进行分类。要素选择也被确定为云 ddos 攻击防御中的预处理阶段，它可以通过识别原始数据集中的重要要素，从而提高分类精度并降低计算复杂性。有监督的学习。在本文中，我们提出了一种基于镜头的多滤波器特征选择方法，该方法结合了四种滤波器方法的输出，以实现最佳选择。利用入侵**检测**基准数据集、nsl-kdd 和决策树分类器对该方法进行了广泛的实验评价。结果表明，与其他分类技术相比，该方法有效地将特征数量从 41 种减少到 13 种，具有较高的**检测**率和分类精度。少

2018 年 7 月 27 日提交;最初宣布 2018 年 7 月。

评论:20 页

94. **第 xiv:1807. 10438[pdf] Cs。铬**

多伊 10.1016/j.future.2017.07.060

物联网安全与取证: 挑战与机遇

作者:mauro conti, ali dehghantanha, k 不安 in franke,steve watson

摘要: 物联网 (iot) 设想普及、互联和智能节点自主交互，同时提供各种服务。物联网对象分布广泛、开放性强，处理能力相对较高，使其成为网络攻击的理想**目标**。此外，由于许多物联网节点正在收集和处理私人信息，它们正在成为恶意行为者的数据宝库。因此，在成功部署物联网网络时，安全性，特别是检测受损节点的能力，以及收集和保存攻击或恶意活动的证据，将成为优先事项。在本文中，我们首先介绍了物联网领域中现有的主要安全和取证挑战，然后简要讨论**了在**这一特殊问题中发表的针对已确定挑战的论文。少

2018 年 7 月 27 日提交;最初宣布 2018 年 7 月。

95. **第 xiv:1807. 10436[pdf] Cs。铬**

多伊 10.107/978-3-319-7391-9 _ 16

来自云的启示：云取证研究的文献计量分析

作者:james baldwin, omar m. k.alhawi, simone shaughnessy, alex akinbi, ali dehghantanha

摘要: 云计算技术的出现改变了我们存储、检索和归档数据的方式。由于承诺存储无限、可靠和始终可用，现在大量的私有和机密数据存储在不同的云平台上。云平台是如此的数据金矿，是攻击者最有价值的**目标**之一。因此，许多法医调查人员试图开发工具、战术和程序，以收集、保存、分析和报告不同云平台上袭击者活动的证据。尽管发表的文章数量众多，但没有一个文献计量研究来呈现云取证研究的趋势。本文件旨在通过对 2009 年至 2016 年期间的云取证研究趋势进行全面评估来解决这一问题。此外，我们还提供云取证过程的分类，以**检测**最深入的研究领域，并突出剩余的挑战。少

2018 年 7 月 27 日提交;最初宣布 2018 年 7 月。

评论:22 页

96. 第 1807. 09884[pdf,其他] Cs。简历

领域程式化：合成到真实图像域适应的一个强大、简单的基线

作者:aysegul dundar, m-yuliu, ting-chunwang, john zedlewski, jan kautz

摘要: 由于协变移位问题，深度神经网络在实际图像中应用时，在很大程度上未能有效地利用合成数据。本文表明，通过对现有的真实风格转换算法进行直接修改，我们获得了最先进的同步到真实的域适应结果。我们对四个用于语义分割和对象**检测**的综合到实际任务进行了广泛的实验验证，并表明我们的方法超过了当前任何最先进的基于 gan 的图像转换的性能通过分割和对象**检测**指标来衡量的方法。此外，我们还提供了基于距离的分析，该方法显示源域和**目标**域之间的 frechet 初始距离显著减小，并提供了一个定量指标，以演示我们的算法在弥合同步到真实的差距。少

2018 年 7 月 24 日提交;最初宣布 2018 年 7 月。

97. 第 1807. 08275[pdf,其他] 反渗透委员会

快速：用于辅助机器人抓取中的腕部控制的轻量级计算机视觉

作者:mireia ruiz maymo, ali shafti, a. aldo faisal

文摘: 可穿戴和辅助机器人为人掌握支持是广泛地或者是远程操作的机器人手臂或通过对瘫痪者的手的矫形控制的行为。这样的装置需要正确的定位，才能成功、高效地抓取。在许多人机辅助设置中，最终用户需要明确控制许多自由度，从而使有效或高效的控制成为问题。在这里，我们展示了通过自动终端效应定向控制的辅助机器人和主动矫形器的低级控制的卸载，用于抓取。本文介绍了一种实现快速计算机视觉技术的紧凑算法，通过对定位在机器人末端执行器上的摄像机获取的图像进行分割，获得要掌握的**目标**物体的方向。装置。优化抓取所需的旋转直接从对象的方向计算。该算法在 6 个不同的场景背景下进行了评估，并对 26 个不同的对象采用了末端效应方法。在所有背景下**检测到** 99.8% 的对象。在 91.1 的情况下，对目标进行了抓取，并用机器人模拟器进行了评估，确认了算法的性能。少

2018 年 7 月 22 日提交;最初宣布 2018 年 7 月。

评论:6 页。接受在 ieee birob 2018 出版

98. 第: 1807. 06 180[pdf,其他] Cs。Lg

一种预测配电系统中与植被有关的断电的数据驱动方法

作者:milad doostan, reza sohrabi, badrul chowdhury

摘要: 本文提出了一种新的数据驱动方法，用于预测配电系统中每月发生的与植被相关的停机次数。为了制定能够成功实现这一目标的办法，应当应对两个主要挑战。第一个挑战是确定**目标**区域的范围。为克服这一难题，提出了一种无监督的机器学习方法。第二个挑战是正确识别与蔬菜有关的停机的主要原因，并彻底调查其性质。本文将这些中断分为两大类：与增长相关的故障和与天气相关的中断，并提出了两种类型的模型，即时间序列模型和非线性机器学习回归模型来执行预测任务,分别。此外，设计和使用各种功能，可以解释与植物相关的停机的可变性。除了不同类型的天气和地理数据外，还利用从美国一家主要公用事业公司获得的实际停机数据来构建拟议的方法。最后，进行了全面的案例研究，以说明如何利用拟议的方法成功地预测与蔬菜有关的停机次数，并帮助决策者发现其系统中**的**脆弱区域。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

99. 第 1807. 05812[pdf,其他] Cs。Sd

通过深度学习自动检测鸟类的声学：鸟类音频检测的第一挑战

作者:dan stowell, yannis stylianou, mike wood, hanna pamuva, hervéglotin

摘要: 评估鸟类的存在和数量对于监测特定物种以及整个生态系统健康十分重要。许多鸟类最容易被**它们的声音检测到**，因此被动声学监测是非常合适的。然而，声学监测往往受到实际限制的阻碍，如需要手动配置、依赖示例声音库、精度低、鲁棒性低以及对新的声学条件进行泛化的能力有限。在这里，我们报告了一个协作数据挑战的结果，表明通过现代机器学习，包括深度学习，通用声鸟**检测**可以在远程监测数据中实现非常高的检索率--无需手动重新校准，并且没有对**目标**物种或**目标**环境中的声学条件的探测器进行预训练。多种方法的性能约为 88% 的 auc (roc 曲线下的面积)，比以前的通用方法要高得多。我们提出了新的声学监测数据集，总结了挑战团队提出的机器学习技术，进行了详细的性能评估，并讨论了如何将这些**检测**方法集成到远程监控中项目。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

100. 第: 1807. 05519[pdf,其他] Cs。Cl

基于概念的自然语言处理嵌入

作者:ma yunun, erik cambria

摘要: 在这项工作中，我们专注于通过将概念和单词投影到一个较低的维空间中，有效地利用和整合概念级和词类的信息，同时保留最关键的语义。在广泛的意见理解系统中，我们研究了融合嵌入在几个核心 nlp 任务中的应用：命名实体**检测**和分类、自动语音识别重新记录和**有针对性**的情绪分析。少

2018 年 7 月 15 日提交;最初宣布 2018 年 7 月。

101. 第 xiv:1807. 084856[pdf, ps,其他] Cs。简历

caddy 水下立体视觉数据集在潜水员活动中的人机交互 (hri)

作者:arturo gomez chavez, andrea ranieri, davandde chiarella, enrica zereik, anja babić, andreas birk

摘要: 在本文中，我们提出了一个新的水下数据集收集从几个实地试验内的欧盟 fp7 项目 "认知自主潜水伙伴 (caddy)"，其中一个自主水下航行车 (auv) 用于与潜水员互动和监测他们的活动。据我们所知，这是在水下环境中收集针对对象分类、分割和人体姿势估计任务的大型数据集的第一批努力之一。数据集的第一部分包含在不同环境条件下执行手势与 auv 进行通信和交互的潜水员的立体摄像机记录 (约 10k)。这些手势

样本用于测试针对水下图像失真 (即颜色衰减和光反向散射) 的目标**检测**和分类算法的鲁棒性。第二部分包括潜水员在 auv 前自由游泳的立体声镜头 (~ 12.7k), 以及位于潜水员西服 (divernet) 中的同步 imu 测量, 这些测量是人类姿势和跟踪方法的地面特征。在这两种情况下, 这些校正图像允许调查三维表示和推理管道从低纹理**目标通常**存在于水下场景。本文介绍了我们的记录平台、传感器校准过程以及数据格式和使用数据集的实用程序。少

2018 年 7 月 12 日提交;最初宣布 2018 年 7 月。

评论:提交给 ijrr

102. 特别报告: 1807. 04807[pdf,其他] Cs。简历

基于学习的领域适应能力心脏应变分析的正则化

作者:allen lu, nripesh parajuli, maria zontak, john stendahl, kevinminhta , zhao liu, nabil boutagy, geng-shi jeng, imran alkhalil, lawrence h 。staib, matthew o ' donnell, albert j. sinusas, james s. duncan

文摘: 利用 3D+time 超声心动图 (4de) 进行可靠的运动估计和应变分析, 对心肌损伤的定位和表征具有重要价值, 有助于早期**发现**和**有针对性**的干预。然而, 由于 4de 固有的图像特性导致的低信噪比, 运动估计是困难的, 而智能正则化对于产生可靠的运动估计至关重要。在这项工作中, 我们将域适应的概念整合到一个受监督的神经网络正则化框架中。我们首先提出了一个无监督的自动编码器网络, 它具有生物力学约束, 用于学习一种潜在的表示形式, 该表示被证明具有更多的生理上合理的位移。我们扩展了这一框架, 将合成数据的监督损失项包括在内, 并显示了生物力学约束对网络域适应能力的影响。我们用植入的肿瘤学计对体内数据进行了自编码器和半监督正则化方法的验证。最后, 我们展示了我们的半监督学习正则化方法的能力, 以识别梗死区域使用估计的区域应变图与人工追踪的梗死区域从死后切除心脏。少

2018 年 7 月 12 日提交;最初宣布 2018 年 7 月。

103. 第 1807. 03833[pdf, ps,其他] Cs。铬

坏: 区块链异常检测

作者:matteo sinorini, matteo pontecorvi, wael kanoun, roberto di pietro

摘要: 异常**检测**工具在保护网络和系统免受不可预见的攻击方面发挥着至关重要的作用, 通常是通过自动识别和过滤异常活动。多年来, 设计了不同的方法, 都注重降低假阳性率。然而, 没有任何提案涉及**针对**基于区块链的系统的攻击。本文提出了一种 bad: 第一个区块链异常**检测**解决方案。bad 利用名为分叉的区块链元数据来收集网络/系统中的潜在恶意活动。bad 具有以下特点: (i) 它是分布式的 (从而避免任何中心故障点), (ii) 它是防篡改的 (使恶意软件不可能删除或更改其自身的痕迹), (iii) 它是受信任的 (任何行为数据都是被收集和由大多数网络验证) 和 (iv) 它是私有的 (避免任何第三方收集敏感信息)。我们的建议通过实验结果和理论复杂性分析得到验证, 突出了我们区块链异常**检测**解决方案的质量和可行性。少

2018 年 7 月 12 日提交;v1 于 2018 年 7 月 10 日提交;最初宣布 2018 年 7 月。

104. 特别报告: 1807. 03760[pdf] Cs。艾

模拟拱形: 建筑设计中人类路径仿真的多智能体系统

作者:许延嘉

摘要: 人的运动路径是建筑设计中的一个重要特征。通过研究路径，建筑师知道在哪里安排空间中的基本元素 (如结构、眼镜、家具等)。本文介绍了用于人体运动路径仿真的多智能体系统 simarch。它涉及使用马尔可夫决策过程建立的行为模型。该模型模拟了人类的精神状态、**目标**范围**检测**和碰撞预测，当代理者在地板上，在一个特定的小画廊，看展览，或离开地板。它还通过分配不同的过渡概率来模拟不同类型的人类特征。改进的加权 a * 搜索算法快速规划代理的次优路径。在实验中, simarch 将一系列预处理平面图作为输入，模拟移动路径，并输出用于评估的密度映射。密度映射提供了一个人在某个位置发生的可能性的预测。下面的讨论说明了架构师如何使用密度图来改进其平面图设计。少

2018 年 7 月 10 日提交;最初宣布 2018 年 7 月。

105. **第: 1807. 03713[pdf,其他] Cs。Hc**

辩证法: 利用线性回归加强对平滑追求眼动的检测

作者:heiko drewes, Khamis khamis, florian alt

文摘: 我们引入并评估了一种检测平滑追眼运动的新方法，该方法可增加可区分目标的数量，并增强对误报的鲁棒性。追求是自然和无校准，在过去的几年中越来越受欢迎。同时，当使用 8 个以上**屏幕上的目标**时，当前的实现显示出较差的性能，从而限制了其适用性。我们的方法 (1) 利用回归线的斜率, (2) 引入最小的信号持续时间，改进了新的和传统的**检测**方法。在介绍了该方法和实现方法后，将其与传统的基于相关的追求检测方法进行了比较。我们测试了多达 24 个**目标**的方法，并表明，如果接受类似的错误率，可以区分的目标几乎是最先进的**两倍**。对于较少的**目标**，精度显著提高。我们相信我们的方法将实现更强大的基于追求的用户界面，从而使其对研究人员和从业者都有价值。少

2018 年 7 月 10 日提交;最初宣布 2018 年 7 月。

106. **第 xiv: 1807. 03675[pdf,其他] si**

社交媒体上的事件检测与检索

作者:manos schinas, symeon Papadopoulos, yiannis kumpatsiaris, permits mitkas

摘要: 近年来，我们目睹了推特、脸书和 youtube 等社交媒体平台的迅速采用，以及这些平台被用作全世界数十亿人日常生活的一部分。考虑到人们习惯利用这些平台分享想法、日常活动和经验，用户生成的内容数量达到了前所未有的水平，其中很大一部分与现实世界有关，这并不奇怪事件，即在特定时间和地点发生的行动或事件。鉴于事件在我们生活中的关键作用，对周围社交媒体内容进行注释和组织的任务对于确保实时和未来访问有关感兴趣事件的多媒体内容至关重要。在本章中，我们介绍了近年来的一些研究工作，这些工作解决了两个主要问题: a) 事件检测和 (b) 基于事件的媒体检索和总结。给定社交媒体项目的存档集合或实时流，事件**检测**方法的目的是以描述以前未知的事件集的形式标识这些事件。一般来说，这些事件可以是任何类型的，但也有一些针对特定类型事件的方法。给定目标事件，事件摘要的目标首先是识别相关内容，然后以简洁的方式表示，选择最吸引人和最具代表性的内容。少

2018 年 7 月 10 日提交;最初宣布 2018 年 7 月。

107. **建议: 1807.03135[pdf,其他] Cs。简历**

用于核检测的具有形状优先级的深部网络

作者:mohammad Tofighi, tiantong guo, jairam k. p.vanamala, vishal monja

摘要: 在显微图像中**检测**细胞核是一个具有挑战性的研究课题，因为细胞图像质量有限，核形态的多样性，即不同的细胞核形状、大小和多个细胞核之间的重叠。这是一个长期感兴趣的话题，最近有希望的成功表现在深入的学习方法上。例如，这些方法训练卷积神经网络 (cnn)，训练一组输入图像和已知的、标记的原子核位置。其中许多方法得到了空间或形态处理的补充。我们开发了一种新的方法，我们称之为形状优先与卷积神经网络 (sp-cnn)，以执行显著增强的核检测。在领域专家的帮助下，准备了一组规范形状。随后，我们提出了一个新的网络结构，它可以通过两个组件包含原子核形状的 "预期行为": {\ em 可学习} 层,用于执行原子核检测，以及一个 {\ em 固定} 处理部分，用于指导学习事先的信息。从分析上看，我们制定了一个新的正则化项，旨在惩罚假阳性，同时鼓励细胞核边界内**的检测**。在具有挑战性的数据集上的实验结果表明, sp-nnn 具有与几种最先进的方法的竞争优势或优于最先进的方法。少

2018 年 6 月 29 日提交;最初宣布 2018 年 7 月。

评论:2018 年 ieee 图像处理国际会议 (icip 2018) 的接受文件

108. 建议: 18007. 03124[pdf,其他] Cs。简历

园艺机器人感知方法综述: 从授粉到收获

作者:ho seok ahn, feras dayoub, marija popovic, bruce macdonald , ro 兰齐格瓦特, inkyu sa

摘要: 随着其**目标**作物范围的扩大，园艺企业变得越来越复杂。提高效率和生产力的要求推动了现场操作自动化的需求。然而，各种问题仍有待解决，因为它们在现实场景中进行了可靠、安全的部署。本文探讨了园艺机器人的主要研究趋势和当前的挑战。具体而言，我们的工作重点是三个主要园艺过程中的感知和感知: 授粉、产量估计和收获。对于每个任务，我们都会揭示现场环境中非结构化、杂乱和坚固耐用的主要问题，包括可变的照明条件和特定于水果的**检测**困难，并突出有希望的当代研究。少

2018 年 6 月 26 日提交;最初宣布 2018 年 7 月。

评论:6 页, 5 个数字, 2 个表

109. 第 1807. 02851[pdf,其他] 反渗透委员会

使用基于事件的传感器进行实时聚类分析和多目标跟踪

作者:francisco barranco, cornelia fermuller, eduardo ros

摘要: 聚类分析对于许多计算机视觉应用 (如鲁棒跟踪、目标**检测**和分割) 至关重要。本工作提出了一种利用基于事件的视觉传感器的独特特性的实时聚类技术。由于基于事件的传感器仅在强度变化时触发事件，因此数据稀疏，冗余率较低。因此，我们的方法使用异步事件而不是传统帧重新定义了众所周知的均值移位聚类方法。我们的方法的潜力在多目标跟踪应用程序中得到了证明，该应用程序使用卡尔曼滤波器来平滑轨迹。我们评估了具有不同形状和速度模式的现有数据集的方法，以及收集的新数据集。该传感器连接到 baxter 机器人的眼睛设置监测现实世界的物体在一个动作操作任务。聚类分析精度达到了 0.95 的 f 测量值，与基于框架的方法相比，计算成本降低了 88%。跟踪的平均误差为 2.5 像素，聚类分析实现了随时所需的一致的聚类数。少

2018 年 7 月 8 日提交;最初宣布 2018 年 7 月。

评论:会议文件。2018 年离子被接受

110. 第 xiv:1807. 02340[pdf,其他] Cs。CI

测试不可测试的神经机器翻译: 一个工业案例

作者:郑武杰,王文宇,刘迪安,张昌荣,曾钦松, 邓月腾,杨伟,何平佳,谢涛

摘要: 神经机器翻译 (nmt) 由于与传统的统计机器翻译 (smt) 相比的优势, 近年来得到了广泛的应用。然而, 由于自然语言的复杂性和神经网络设计的复杂性, nmt 系统仍然经常产生翻译失败。虽然基于参考翻译 (即有效翻译示例) 的内部黑盒系统测试一直是 nmt 质量保证的常见做法, 这是一种日益关键的行业实践, 即称为体内测试、暴露的类型或当实际用户使用已部署的工业 nmt 系统时, 会出现翻译失败的情况。为了填补 nmt 系统体内测试缺乏测试的空白, 本文提出了一种自动识别翻译失败的新方法, 而不需要翻译任务的参考翻译;我们的方法可以直接作为体内测试的测试甲骨文。我们的方法侧重于可系统检查的自然语言翻译的属性, 并使用 nmt 系统的测试输入 (即要翻译的文本) 和测试输出 (即正在检查的翻译) 中的信息。我们对实际数据集进行的评估表明, 我们的方法可以有效地**检测**到**翻译**失败的目标属性冲突。我们在微信 (每月有超过 10 亿活跃用户的信使应用程序) 的生产和开发环境中部署我们的方法的经验证明了我们的方法的有效性以及对行业的高度影响。少

2018 年 10 月 3 日提交;v1 于 2018 年 7 月 6 日提交;最初宣布 2018 年 7 月。

评论:10 页

111. 第 xiv:180. 002143[pdf] Cs。简历

用于在线多目标跟踪的时空 ksvd 词典学习

作者:huynh manh, gita alaghband

文摘: 本文提出了一种新的空间判别 ksvd 字典算法 (stksvd), 用于在线多目标跟踪中**的目标**外观学习.与其他分类识别任务 (如人脸、图像识别) 不同, 学习目标在在线多**目标**跟踪中**的**出现受到诸如位置/发音变化、部分遮挡等因素的影响。背景场景或其他**目标**、背景变化 (人体**探测**边界框涵盖人体部分和场景的一部分) 等。然而, 我们观察到, 这些变化发生的空间和时间动态逐渐发生。我们通过一种新的 stksvd 外观学习算法来描述**目标**样本之间的时空信息, 以更好地区分稀疏代码、线性分类器参数, 并最大限度地减少单个帧的重建误差优化系统。我们的外观学习算法和跟踪框架在两阶段关联的每个阶段采用两种不同的计算外观相似性分数的方法: 第一阶段的线性分类器和第二阶段的最小残差。使用 2dmot2015 数据集及其公共聚合通道特征 (acf) 进行所有比较的测试结果表明, 我们的方法优于现有的相关学习方法。少

2018 年 7 月 5 日提交;最初宣布 2018 年 7 月。

评论:将出现在《2018 年计算机与机器人视觉十届会议论文集》 (口头)

112. 建议: 1807. 074[pdf,其他] Cs。简历

多伊 10.1109/TIP.2018.2808770

基于密集亚像素视差图估计的路面三维重建

作者:瑞凡,晓爱,奈姆·大农

摘要: 各种 3d 重建方法使土木工程师能够**检测**到路面上的损坏。为了达到路况评估所需的毫米精度, 需要使用具有亚像素分辨率的视差图。然而, 现有的立体匹配算法都不特别适合于路面的重建。因此, 本文提出了一种新的具有较高计算效率和鲁棒性的密集亚像素视差估计算法。这首先是通过将**目标**框架的透视视图转换为参考视图来实现的, 这不仅提高了路面块匹配的精度, 而且提高了处理速度。然后使用我们以前发布的算法迭代估计差异, 其中搜索范围从三个估计的邻近差异传播。由于搜索范围是从上一次迭代获得的, 因此当传播的搜索范围不够时, 可能会发生错误。因此, 执行相关最大值验证以纠正此问题, 并通过执行抛物线插值增强来实现子像素分辨率。此外, 还引入了一

种新的基于马尔可夫随机场和快速双边立体声的差异全局细化方法，以进一步提高估计差异图的准确性，其中差异通过最大限度地减少与它们的插值相关多项式相关的能量函数。该算法采用 c 语言实现，具有接近实时性的特点。实验结果表明，重建的绝对误差从 0.1 毫米到 3 毫米不等.

2018 年 7 月 5 日提交;最初宣布 2018 年 7 月。

评论:11 页, 16 个数字, ieee 图像处理事务

日记本参考:基于密集亚像素视差图估计的范仁 r、艾比、大农北路三维重建 [j]。ieee 图像处理交易, 2018, 27 (6): 3025-3035

113. 第 xiv:1807. 01864[pdf,其他] Cs。简历

在卫星视频中检测微小的移动车辆

作者:魏奥,傅艳伟,徐峰

摘要: 近年来，卫星视频被移动的卫星平台捕捉到。与消费者、电影和普通监控视频不同，卫星视频可以记录城市规模场景的快照。在卫星视频的广阔视野中，每个移动**的目标**都非常小，通常由框架中的多个像素组成。更糟糕的是，视频帧中也存在噪声信号，因为由于卫星的运动，视频帧的背景具有亚像素级和不均匀的运动。我们认为，这是一种新型的计算机视觉任务，因为以前的技术无法有效地**检测**到这种微小的车辆。本文提出了一种新的识别卫星视频中小型移动车辆的框架。特别是，我们提供了一种新的基于局部噪声建模的**检测**算法。我们通过指数概率分布来区分潜在的车辆**目标**和噪声模式。随后，设计了一种基于多形态线索的识别策略，以进一步区分正确的车辆**目标**和一些现有的噪声。另一个重要的贡献是引入了一系列的评估方案，以系统地测量微小运动车辆**检测**的性能。我们手动对卫星视频进行注释，并使用它在不同的评估标准下测试我们的算法。并将该算法与最先进的基线进行了比较，并展示了我们的框架相对于基准的优点。少

2018 年 7 月 5 日提交;最初宣布 2018 年 7 月。

114. 第 1807. 01838[pdf,其他] Cs。铬

多伊 10.1007/978-3-319-30840-1 _ 16

利用软件复杂性指标改进模糊

作者:maksim shudrak, vyacheslav zolotarev

摘要: 易受攻击的软件对现代信息系统构成巨大威胁。广泛应用程序中的漏洞可能被用来传播恶意软件、盗取资金和进行**目标**攻击。为了解决这个问题，开发人员和研究人员使用不同的动态和静态软件分析方法;其中一种方法被称为模糊。fuzzing 是通过生成和向被测试的应用程序发送可能格式错误的数据来执行的。自 1988 年首次出现以来，模糊化已经有了很大的发展，但涉及有效性评估的问题到现在还没有得到充分的调查。在我们的研究中，我们提出了一种新的模糊有效性评估方法，同时考虑到已执行代码的语义以及定量评估。为此，我们使用特定的源代码复杂性评估指标，以执行机器代码的分析。我们对 104 个已知漏洞的广泛应用进行了有效性评估。作为这些实验的结果，我们能够确定一组更适合查找 bug 的指标。此外，我们还使用一组指标，在 7 个应用程序上进行了单独的实验，但没有已知的漏洞。实验结果表明，该方法可用于提高模糊效果。此外，这些工具还有助于**检测**广泛应用中的两个关键的零日 (以前未知) 漏洞。少

2018 年 7 月 5 日提交;最初宣布 2018 年 7 月。

日记本参考:icisc 2015: 信息安全与密码学-icisc 2015 页 246-261

115. 建议: 1807. 01136[pdf,其他] Cs。简历

噪声训练数据中利用有机组织进行视觉检测的半监督异常检测

作者:木村正成,柳木原隆志

文摘: 图像数据异常的**检测**和量化是工业场景中的关键任务，如检测产品上**的微**划痕。近年来，由于异常识别的难度和对其标签的修正限制，利用生成模型进行无监督异常检测的研究引起了人们的关注。一般来说，在这些研究中，只有普通图像被用来进行训练，以模拟正态图像的分布。该模型通过复制最相似的图像和打分显示**其适合学习分布**的图像补丁来测量目标图像中的异常。这种做法是建立在强有力的推定基础上的;训练后的模型不应该能够生成异常图像。然而，在现实中，该模型主要由于噪声的正常数据包括小异常像素而产生异常图像，这种噪声严重影响模型的精度。因此，我们提出了一种新的半监督方法，用现有的异常图像来扭曲模型的分布。该方法从实际用于工业场景的 1024x1024 高分辨率图像中，以高精度检测像素级**微**异常。在本文中，由于数据的保密性，我们分享了开放数据集的实验结果。少

2018 年 7 月 3 日提交;最初宣布 2018 年 7 月。

116. 第 1807. 00182[pdf,其他] cse

合奏: 从合奏学习到合奏融合

作者:陈元良,姜宇,梁杰,王明哲,迅娇

文摘: 模糊技术广泛应用于软件漏洞**检测**。有各种不同的模糊策略，而且大多数在**目标**上表现良好。然而，在行业实践和实证研究中，这些设计良好的模糊策略的性能和泛化能力受到现实应用复杂性和多样性的挑战。本文在整体学习思想的启发下，首先提出了一种集成模糊方法 entfuzz，该方法集成了多个模糊策略，以获得比任何组成模糊器更好的性能和泛化能力。首先，我们定义了基本模糊器的多样性，并选择那些最新的和设计良好的模糊器作为基本模糊器。然后, enfuzz 将这些基本模糊器与种子同步和结果集成机制组合在一起。为了进行评估，我们实现了 enfuzz，这是一个基于四个强大的开源模糊器 (afl、aflfast、aflgo、fairfuzz) 的原型，并在 google 的模糊测试套件上进行测试，该套件由广泛使用的实际应用组成。24 小时实验表明，在相同的资源使用情况下，这四个基本模糊器在不同的应用程序上执行不同的操作，而 enfuzz 则表现出更好的泛化能力，在路径覆盖率、分支覆盖率方面始终优于其他模糊器和崩溃的发现。即使与最好的武警部队病例相比, afris、aflgo 和 fairfuzz、enfuzz 发现 26.8%、117%、38.8% 和 39.5% 以上的独特崩溃，执行 9.16、39.2%、19.9% 和 20.0 以上的路径，分别覆盖 5.96、12.0、21.4% 和 11.1 的分支机构。少

2018 年 6 月 30 日提交;最初宣布 2018 年 7 月。

评论:10 页, 11 位数字

117. 第 1807. 00072[pdf,其他] Cs。CI

基于动态类加权的领域分类和领域外检测的联合学习，以满足虚假接受率

作者:jo-kyung kim, young-bum kim

摘要: 在语音对话系统的域分类中，正确**检测**领域外 (ood) 话语至关重要，因为它减少了用户和系统之间的混淆和不必要的交互成本。以前的工作通常使用与域 (ind) 分类器分开训练的 ood 检测器，以及给定**目标**评价分数的 ood **检测**的置信度阈值。本文介绍了一种用于域分类和 ood **检测**的神经联合学习模型，在模型训练中采用动态类加权来满足给定的 ood 错误接受率 (far)，同时最大限度地提高域分类精度。通过对大

型口语对话系统话语的两个域分类任务的评价，表明我们的方法显著提高了域分类性能，满足了给定**的目标**场。少

2018 年 6 月 29 日提交;最初宣布 2018 年 7 月。

评论:2018 年互动

118. **第 xiv:1806. 10741[pdf,其他] Cs。艾**

仿真序列学习的鲁棒神经恶意检测模型

作者:rakshit agrawal, jack w.stokes, mady marinescu, karthik selvaraj

摘要: 恶意软件 (即恶意软件) 在计算机安全方面带来了不断变化的挑战。这些嵌入的代码片段以恶意文件的形式或隐藏在合法文件中，会给能够运行恶意命令序列的系统带来重大风险。恶意软件作者甚至使用多态性来重新排序这些命令，并创建几个恶意变体。但是，如果在安全环境中执行，则可以对模拟的命令序列执行早期恶意软件**检测**。本文提出的模型利用通过仿真获得的序列数据进行神经恶意检测. 这些模型通过从这些序列中了解恶意事件操作的存在和共存模式，以恶意操作的核心为**目标**。我们的模型可以捕获整个事件序列，并使用已知的**目标**标签直接进行培训。这些端到端学习模型由两个常用结构提供动力--长期短期内存 (lstm) 网络和卷积神经网络 (cnn)。以前建议的顺序恶意软件分类模型处理的事件不超过 200 个。攻击者可以通过将任何恶意活动延迟到文件的开头之外来逃避**检测**。我们提供专门的模型，可以处理极长的序列，同时成功地执行恶意软件**检测**的有效方式。我们提出了一个实现的卷积划分长序列方法，以解决此漏洞，并在长序列上操作。我们在一个由 664, 249 个文件序列组成的大型数据集上显示我们的结果，该数据集具有非常长的文件序列。少

2018 年 6 月 27 日提交;最初宣布 2018 年 6 月。

119. **第 xiv:1806. 09301[pdf,其他] Cs。Sd**

用于无监督语音活动检测的鲁棒特征聚类

作者:harishchandra dubey, abhijeet sandwan, john h. l. hosen

摘要: 在某些应用中，如零资源语音处理或极低资源语音语言系统，收集语音活动**检测** (sad) 注释可能不可行。然而，基于神经网络或其他机器学习方法的最先进的监督 sad 技术需要与**目标**域匹配的注释训练数据。本文为完全无监督的 sad 建立了一种聚类方法，该方法适用于 sad 注释不可用的情况。该方法利用 hartigan 浸渍测试的递归策略，将功能空间分割为突出的模式。统计倾角对失真是不变的，这使得该方法具有鲁棒性。我们评估 nist opensad 2015 和 nist opopsat 2017 公共安全通信数据的方法。结果表明，该方法优于双组分 gmm 基线。索引术语: 聚类分析、哈提根浸渍测试、nist opensad、nist opensat、语音活动**检测**、零资源语音处理、无监督学习。少

2018 年 6 月 25 日提交;最初宣布 2018 年 6 月。

评论:5 页, 4 个表, 1 图

120. **第 1806.08970[pdf] Cs。简历**

基于 mcs 2018 对白盒脸识别系统对抗攻击的动量多元输入快速梯度符号法 (m-d2-fgsm) 攻击方法的评价

作者:md ashraful alam milton

摘要: 卷积神经网络是近年来在分类、分割和**检测**等各种计算机视觉任务上成功的关键工具。卷积神经网络在这些任务中实现了最先进的性能，每天都在推动计算机视觉和人工智能的极限。然而，对计算机视觉系统的对抗攻击正在威胁其在现实生活和安全关键

应用中的应用。在必要的情况下，找到敌对性的例子对于**发现**容易受到攻击的模型和采取保障措施以克服对抗攻击是很重要的。在这方面，mcs 2018 对白装人脸识别挑战的攻击旨在促进寻找新的对抗性攻击技术及其生成对抗实例的有效性的研究。在这一挑战中，攻击的性质是对黑盒神经网络的**有针对性**的攻击，我们对黑块的内部结构一无所知。攻击者必须修改一组由一个人的五个图像组成的图像，以便神经网络错误地将它们归类为**目标**图像，而目标图像是另一个人的一组五个图像。在本次比赛中，我们采用动量等输入迭代快速梯度签名方法 (m-d2-fgsm) 对黑匣子人脸识别系统进行了对抗攻击。我们在 mcs 2018 对黑盒面部识别挑战的反攻击中测试了我们的方法，并发现了竞争结果。我们的解决方案得到了 1.404 的验证分数，比基线分数 1.407 要好，在领导板 132 支球队中排名第 14 位。通过从源图像中找到改进的特征提取、精心选择的超参数、找到改进的黑匣子替代模型和更好的优化方法，可以进一步改进。少

2018 年 6 月 23 日提交;最初宣布 2018 年 6 月。

评论:该代码可在以下 github 链接下载:
https://github.com/miltonbd/mcs_2018_adversarial_attack

121. **第 xiv:1806.08893[pdf,其他] Cs。铬**

安卓恶意软件网络基础设施的自动调查框架

作者:elmouatez billah karbab, mouarad debbabi

摘要: android 系统的普及，不仅在手机设备中如此，在物联网设备中也是如此，这使得它成为恶意软件非常有吸引力的目的地。事实上，恶意软件正在以类似的速度扩展，**这些**设备的目标在大多数情况下依赖于互联网才能正常工作。最先进的恶意软件缓解解决方案主要侧重于检测实际的恶意 android 应用，使用动态和静态分析功能来**区分**恶意应用和良性应用。但是，android 恶意应用程序的 internet®网络维度的覆盖率很小。在本文中，我们提出 to 聚集，一个自动调查框架，将 android 恶意软件样本作为输入，并产生有关这些样本家族的恶意网络基础结构的情况感知。tog 表扬利用最先进的图论技术生成可操作的细粒度智能，以减轻 android 恶意软件应用程序的恶意 internet 活动所带来的威胁。我们实验 to 绝大多数从各种 android 家族的真正的恶意软件样本，并获得的结果是有趣的，很有希望少

2018 年 6 月 22 日提交;最初宣布 2018 年 6 月。

评论:12 页

122. **第 1806.08503[pdf,其他] Cs。简历**

零射击学习的全局语义一致性

作者:范武,启田,关继宏,周水庚

摘要: 在图像识别中，在许多情况下，训练样本不能覆盖所有**目标**类。零拍摄学习 (zsl) 利用类语义信息对训练集中没有相应样本的看不见的类别的样本进行分类。在本文中，我们提出了一个端到端框架，称为全球语义一致性网络 (简称 gsc-net)，它完全利用有已看到类和看不见类的语义信息，以支持有效的零镜头学习。我们还采用了软标签嵌入丢失，以进一步利用类之间的语义关系。为了使 gsc-net 适应更实用的环境，通用零镜头学习 (gzsl) 引入了一种参数化**的新颖性检测**机制。我们的方法通过三个可视化属性数据集在 zsl 和 gzsl 任务上实现了最先进的性能，从而验证了所建议框架的有效性和优势。少

2018 年 6 月 22 日提交;最初宣布 2018 年 6 月。

123. **第 1806.07944[pdf, ps,其他] si**

在图形中搜索单个社区

作者:avik ray, sujay sanghavi, Sujay shakottai

摘要: 在标准图形聚类/社区**检测**中，人们有兴趣将图形划分为连接更紧密的节点子集。相反，本文的 "搜索" 问题旨在从可能存在的许多社区中找到 "单一" 这样的社区中的节点,**即目标**。为此，我们获得了有关**目标**的适当的侧面信息;例如,**目标**中极少数节点被标记为此类节点。我们考虑了一个一般但简单的侧信息概念：假定所有节点都有随机权重,**目标**中的节点平均权重较高。考虑到这些权重和图形，我们开发了一种矩方法的变体，该方法比不使用侧面信息和方法的通用社区**检测**方法更可靠、计算更低的时刻方法进行了分析。对整个图形进行分区。我们的经验结果表明，与其他图聚类算法相比，我们在运行时获得了显著的提高，而且准确性也有所提高。少

2018 年 5 月 24 日提交;最初宣布 2018 年 6 月。

评论:计算系统 (tomecs) 建模和性能评价杂志 [将出现]

124. 第 xiv:1806.07844[pdf,其他] Cs。简历

隐藏和查找跟踪器：从目标丢失中实时恢复

作者:alessandro bay, panagiotis sidiropoulos,edward vazquez, mic 其米歇尔·sasdelli

摘要: 在本文中，我们使用从原始跟踪器中已经提供的信息，在没有大量计算开销的情况下，检查视频跟踪器从**目标**丢失中的实时恢复。更具体地说，在使用跟踪器输出更新**目标**位置之前，我们估计检测的**置信**度。在置信度较低的情况下，位置更新将被拒绝，跟踪器将传递到单帧故障模式，在此期间，修补程序低级可视内容用于快速更新对象位置，然后从下一帧。在进行这一改进的基础上，进一步增强了用于创建具有相似性的查询模型的运行平均方法。通过对标准跟踪数据集 (otb-50、otb-100 和 otb-2013) 的评估提供的实验证据验证了在不影响**目标**位置实时更新的情况下成功实现**目标**恢复的能力.少

2018 年 6 月 20 日提交;最初宣布 2018 年 6 月。

125. 第 xiv:1806.07755[pdf,其他] Cs。Lg

生成性对抗网络评价指标的实证研究

作者:徐钱通,高黄,杨元, 川国,孙宇, 吴费利克斯,基莲温伯格

摘要: 评估生成性敌对网络 (gans) 本身就具有挑战性。本文对几个具有代表性的有机遗传组织的基于样本的评价指标进行了重新审视，并探讨了如何评价评价指标的问题。我们从一些生成有意义分数的度量条件开始，例如区分真实样本和生成的样本、识别模式下降和模式崩溃，以及**检测**过度拟合。通过一系列精心设计的实验，我们全面研究了现有的基于样本的度量，并确定了它们在实际环境中的优势和局限性。在此基础上，我们观察到，只要在合适的特征空间内计算样本之间的距离，内核最大平均方差 (mmd) 和 1-nerest-nestor (1-nn) 双样本测试似乎满足了大多数理想的特性。我们的实验还揭示了一些流行的 gan 模型的行为的有趣属性，例如它们是否在记忆训练样本，以及它们距离了解**目标**分布还有多远。少

2018 年 8 月 16 日提交;v1 于 2018 年 6 月 19 日提交;最初宣布 2018 年 6 月。

评论:arxiv 管理说明：文本重叠与 arxiv:1802.0 3446 由其他作者

126. 第 1806.07245[pdf, ps,其他] Cs。Ce

camirada：癌症微 rna 协会发现算法，乳腺癌的案例研究

作者:sesedeh shamsizadeha, sama goliaea , zahra razaghi moghadamb

摘要: 在最近的研究中，非编码蛋白 rna 已被确定为微 rna，可作为癌症早期诊断和治疗的生物标志物，从而降低癌症死亡率。微 rna 可能**针对**数百或数千个基因，而基因可能调节多个微 rna，因此确定哪些微 rna 与哪些癌症是一个很大的挑战。已经采用了许多计算方法来**检测** microrna 与癌症的关联，但还需要更多的努力和更高的准确性。越来越多的研究表明，微 rna 与 tf 之间的关系在癌症诊断中发挥着重要作用。因此，我们开发了一个新的计算框架 (camirada)，根据蛋白质网络中微 rna 与疾病基因 (dg) 之间的关系、微 rna 与转录之间的功能关系来识别与癌症有关的微 rna。共同表达网络上的因子 (tf)，以及微 rna 与共表达网络上差异表达基因 (deg) 的关系。camirada 被用于评估两个 hmdd 和 mir2 疾病数据库中的乳腺癌数据。在这项研究中，auc 的 65 微 rna 的顶部是 0.95，这是更准确的比类似的方法用于**检测**微 rna 与癌症动脉。少

2018 年 6 月 16 日提交;最初宣布 2018 年 6 月。

127. 第 xiv:1806.06519[pdf,其他] Cs。简历

hitnet：一种嵌入在命中或错过层中的胶囊的神经网络，通过混合数据增强和幽灵胶囊进行扩展

作者:adien deliège, anthony cioppa, marc van droogenbroeck

摘要: 近年来，为分类任务而设计的神经网络已成为一种商品。许多作品**的目标是**开发更好的网络，这导致其架构与更多的层，多个子网络，甚至多个分类器的组合的复杂。在本文中，我们展示了如何重新设计一个简单的网络，以达到优异的性能，这是比 capsnet 在多个数据集中复制的结果更好，通过替换一个图层的命中或错过层。这一层包含激活的载体，称为胶囊，我们训练击中或错过一个中央胶囊通过量身定制一个特定的向心损失函数。我们还展示了我们的网络，名为 hitnet，是如何通过包括重建网络来合成特定类的具有代表性的图像样本的。这种可能性允许开发一个数据增强步骤，结合来自数据空间和要素空间的信息，从而实现混合数据扩充过程。此外，我们还介绍了 hitnet 的可能性，即在需要时使用新概念的幽灵胶囊 (此处用于**检测**训练数据中可能错误标记的图像)，从而采用真正目标的替代方案。少

2018 年 6 月 18 日提交;最初宣布 2018 年 6 月。

128. 第 1806.06198[pdf,其他] Cs。简历

利用弱监督的零件检测网络对局部感知细粒度目标分类

作者:张亚斌,奎佳,王志新

摘要: 细粒度对象分类旨在区分属于同一入门级对象类别的从属类别的对象。这项任务具有挑战性，因为事实是: (1) 训练图像与地面真相标签是很难获得，和 (2) 不同的下属类别之间的差异是微妙的。众所周知，不同从属类别的特征位于对象实例的本地部分。事实上，在许多细粒度分类数据集中都有仔细的零件批注。但是，手动注释对象部件需要专业知识，这也很难推广到新的细粒度分类任务。在这项工作中，我们提出了一个弱监管的部件**检测**网络 (partnet)，它能够**检测**到判别局部部件，以使用细粒度分类。香草 partnet 建立在一个基本子网的基础上，两个并行的上层网络层的流，分别计算分类概率的分数 (超过从属类别) 和**检测**概率 (超过指定的数字有区别的零件探测器) 为地方地方利益 (rois)。图像级预测是通过聚合这些区域级概率的元素级乘积来获得的。为了生成一组不同的 rois 作为 partnet 的输入，我们提出了一个简单的离散部分建议模块 (dpp)，直接**针对**提出有歧视的地方部分的候选人，没有通过对象级的建议进行沟

通。在基准的 cub-200-2011 和牛津花 102 数据集上的实验表明，我们提出的判别零件**检测**和细粒度分类方法的有效性。特别是，在没有地面真相部分注释的情况下，我们在 cub-200-2011 数据集上实现了新的最先进的性能。少

2018 年 6 月 16 日提交;最初宣布 2018 年 6 月。

129. 第 6.6: 1806. 06 195[pdf,其他] Cs。简历

显示、出席和翻译: 无监督的图像翻译与自我规范和关注

作者:朝阳,金泰万，王瑞哲，郝鹏，郭杰杰

摘要: 两个域之间的图像转换是一类问题，旨在学习从源域中的输入图像到**目标**域中的输出图像的映射。它已应用于许多领域，如数据扩充、域适应和无监督培训。当配对训练数据无法访问时，图像转换将成为一个不恰当的问题。我们在假设翻译后的图像需要在感知上与原始图像相似，并且似乎也从新的领域中提取的假设下对问题进行了约束，并提出了一个由单个生成器组成的简单而有效的图像转换模型培训与自我正规化的术语和敌对的术语。我们进一步注意到，现有的图像翻译技术与感兴趣的主体无关，并且经常会对输入引入不需要的更改或工件。因此，我们建议增加一个注意模块来预测注意图，以指导图像的翻译过程。该模块学习关注图像的关键部分，同时保持其他所有内容不变，实质上是避免不需要的工件或更改。预测的注意力图也为无监督分割和显著性**检测**等应用打开了大门。大量的实验和评价表明，我们的模型虽然简单，但比现有的图像翻译方法具有明显的性能。少

2018 年 6 月 16 日提交;最初宣布 2018 年 6 月。

130. 第 xiv: 1806. 05620[pdf,其他] Cs。简历

多伊 10.1109/LRA.2018.2860039

dynaslam: 动态场景中的跟踪、映射和绘制

作者:berta bescos, josém. fácil, javier civera, joséneira

摘要: 场景刚度的假设是 slam 算法中的典型。这种强有力的假设限制了大多数可视化 slam 系统在居住在现实世界中的使用，而这些环境是服务机器人或自主车辆等多个相关应用的**目标**。本文介绍了 dynaslam，它是一种可视化的 slam 系统，它在 orb-sam2 [1] 上构建，增加了动态对象**检测**和背景绘制的能力。dynasam 在单目、立体声和 rgb-d 配置的动态场景中是强大的。我们能够通过多视图几何、深度学习或两者兼而有之来**检测**运动物体。拥有场景的静态地图，可以绘制被此类动态对象遮挡的框架背景。我们在公共单目、立体声和 rgb-d 数据集中评估我们的系统。我们研究了几种精确的速度权衡的影响，以评估拟议方法的局限性。dynaslam 在高度动态的情况下优于标准视觉 slam 基线的准确性。它还估计了场景静态部分的地图，这对于现实环境中的长期应用是必须的。少

2018 年 8 月 15 日提交;v1 于 2018 年 6 月 14 日提交;最初宣布 2018 年 6 月。

评论:这项工作已被 ieee 机器人和自动化信函所接受，并将在 2018 年 ieee 智能机器人和系统会议上展出

日记本参考:ieee 机器人与自动化信函 (第 3 卷，第 4 期, 2018 年 10 月)

131. 第 xiv: 1806. 05530[pdf] Cs。简历

通过稳健的区域建议进行相关跟踪

作者:韩玉琪,南景洪，张增硕,王晶晶，赵宝军

文摘: 近年来，基于相关滤波器的跟踪器由于其简单性和优越的速度而受到广泛关注。但是，当**目标由于预定**义的采样策略而受到遮挡、视点更改或其他具有挑战性的属性时，此类跟踪器的性能较差。为了解决这些问题，本文提出了一个自适应区域建议方案，以方便视觉跟踪。更具体地说，提出了一种新的跟踪监测指标来预测跟踪失败。然后，我们分别结合**检测**和规模建议，从模型漂移和处理长宽比变化中恢复。我们在几个具有挑战性的序列上测试了该算法，这表明所提出的跟踪器与最先进的跟踪器相比具有良好的性能。少

2018 年 6 月 14 日提交;最初宣布 2018 年 6 月。

评论:4 页, 3 个数字, iet2018

132. **第 xiv:1806. 05130[pdf,其他] cse**

在开发人员问题中检测语音行为类型--在错误修复过程中回答对话

作者:andrew wood, paige rodeghero, amerarmayy , collin mcmillan

文摘: 本文**针对**有关错误修复的对话中的语音行为**检测**问题。我们与 30 名专业程序员进行了 "绿野仙踪" 实验，其中程序员修复错误两个小时，并使用模拟虚拟助手寻求帮助。然后，我们使用开放的编码手动注释过程来识别对话中的语音行为类型。最后，我们训练和评估一个监督学习算法，以自动检测对话中的语音行为类型。在 30 个两小时的对话中，我们做了 2459 注解，并发现了 26 个语音行为类型。我们的自动检测实现了 69% 的精度和 50% 的召回。这项工作的关键应用是提高软件工程虚拟助理的最新水平。虚拟辅助技术正在迅速发展，尽管软件工程的应用落后于其他领域，主要原因是缺乏相关数据和实验。本文**针对**开发人员 q\ a 关于错误修复的对话中的这一问题。少

2018 年 7 月 3 日提交;v1 于 2018 年 6 月 13 日提交;最初宣布 2018 年 6 月。

评论:12 页 (10 页用于内容, 2 页用于参考)，被纳入 fse (软件工程基金会) 2018

133. **特别报告: 1806. 04808[pdf,其他] Cs。Lg**

多伊 10.11145/3219819832200042

基于随机距离异常点检测的超高维数据的学习表示

作者:庞冠松,曹龙兵，陈玲,刘欢

摘要: 学习超高维数据的表达性低维表示，例如，具有千百万个特征的数据，一直是使学习方法能够解决维度诅咒的主要方法。然而，现有的无监督表示学习方法主要侧重于保存数据规律性信息，独立于后续异常**值**检测方法的方法进行检测，从而导致次优和**不**稳定的性能检测不正常 (即异常值)。本文介绍了一种基于排名模型的框架，称为 ramodo，以解决此问题。ramodo 将表示学习和异常**值检测**结合起来，学习为最先进的异常点**检测**方法 (基于随机距离的方法) 量身定制的低维表示。这种自定义的学习为**目标**异常值检测器提供了更优化、更稳定的表示形式。此外, ramodo 还可以利用标记较少的数据作为先验知识，以学习更具表现力和与应用程序相关的表示。我们将 ramodo 实例化为一种名为 repen 的有效方法，以演示 ramdo 的性能。对 8 个真实世界超高维数据集的大量经验结果表明, repen (i) 使基于随机距离的检测器能够获得明显更好的 auc 性能和两个数量级的加速;(ii) 与四种最先进的表示学习方法相比，表现大大好，更稳定;和 (iii) 利用不到 1% 的标记数据来实现高达 32% 的 auc 改进。少

2018 年 6 月 12 日提交;最初宣布 2018 年 6 月。

评论:10 页, 4 个数字, 3 个表。出现在 kdd18 的诉讼程序中，长介绍 (口头)

134. 第 xiv:1806.0765[pdf,其他] Cs。简历

用于黑色素瘤诊断的全卷网络

作者:abdon phillips, iris teo, jochen lang

摘要: 这项工作旨在确定如何现代机器学习技术可以应用到以前未探索的主题黑色素瘤诊断使用数字病理。我们用数字病理方法为 50 例皮肤黑色素瘤患者提供了一个新的数据集。我们为三种组织类型 (肿瘤、表皮和真皮) 提供金标准注释，这对于称为布雷斯洛厚度和克拉克水平的预后测量非常重要。然后，我们设计了一个新的多步完全卷积网络 (fcn) 架构，其性能优于其他网络，根据标准指标使用相同的数据进行了训练和评估。最后，我们训练了一个模型来**检测和定位目标**组织类型。在处理以前看不见的情况时，我们模型的输出在质量上与金本位非常相似。除了作为我们的方法的基准计算的标准指标外，我们还要求另外三位病理学家测量网络输出上的布雷斯洛厚度。他们的反应是诊断相当于地面真相测量，当删除不合适的测量情况下，四个病理学家之间的距离内的可靠性 (irr) 为 75.0%。考虑到定性和定量的结果，有可能克服皮肤和肿瘤解剖的歧视性挑战，使用现代机器学习技术进行分割，但还需要做更多的工作来提高网络的性能在真皮分割。此外，我们还表明，可以达到手动执行布雷斯洛厚度测量所需的精度水平。少

2018 年 6 月 12 日提交;最初宣布 2018 年 6 月。

135. 第 xiv:1806.04599[pdf,其他] Cs。简历

自适应 gpr 目标分类的词典学习

作者:fabio giovanneschi, kumar vijay mishra, maria antonio gonzalez-huici, yonina c . eldar, joachim h. g. ender

文摘: 探地雷达 (gpr)**目标的探测**和分类是一项具有挑战性的任务。在这里，我们考虑了各种在线字典学习 (dl) 方法来获得 gpr 数据的稀疏表示 (sr)，以增强通过支持向量机进行**目标**分类的特征提取。由于传统的批量 dl 如 k-svd 等方法不能扩展到高维训练组，且不可行，因此无法实时操作，因此首选在线方法。我们还开发了下拉式小批量在线词典学习 (dominodl)，它利用了许多培训数据可能是相关的这一事实。dominodl 算法以迭代方式考虑训练集的元素，并将相关性降低的样本掉掉。对于废弃杀伤人员地雷的分类，我们将 k-svd 的性能与三种在线算法进行了比较: 经典在线词典学习、基于相关的变体和 dominodl。我们对 l 波段 gpr 真实数据的实验表明，在线 dl 方法比 k-svd 减少了 36-93 的学习时间，并使地雷**探测**量增加了 4-28。我们的 dominodl 是最快的，并保持类似于其他两种在线 dl 方法的分类性能。我们使用 kolmoorov-smirnoff 测试距离和德沃雷茨基-基弗-沃尔福威茨不等式来选择 dl 输入参数，从而提高分类结果。为了与最先进的分类方法进行进一步的比较，我们对卷积神经网络 (cnn) 分类器进行了评价，该分类器的性能比提出的方法差。此外，当获得的样本随机减少 25%, 50% 和 75%，稀疏分解的分类与 dl 保持鲁棒性，而 cnn 的准确性受到极大的损害。少

2018 年 5 月 24 日提交;最初宣布 2018 年 6 月。

评论:15 页, 10 个数字, 8 个表

136. 特别报告: 1806.03753[pdf] Cs。简历

强大的对象跟踪与乌鸦搜索优化多线索粒子过滤器

作者:kapil sharma, gurjit singh walia, ashish kumar , Astitwa saxena, kuldeep singh

文摘: 粒子滤波器 (pf) 被广泛用于**估计目标**非线性和非高斯状态。然而，由于样本退化和贫困的内在问题，其性能受到影响。为了解决这一问题，我们提出了一种新的基于乌鸦搜索优化的重采样方法，以克服检测到的表现不佳的粒子异常。提出的具有传感器可靠性的离群检测机制实现了所提出的 pf 跟踪框架的更快收敛。此外，我们提出了一个自适应模糊融合模型，以集成提取的多个线索的每个被评估的粒子。利用所提出的融合模型自动提升和抑制粒子，不仅提高了重采样方法的性能，而且实现了最优状态估计。通过 12 个基准视频序列对所建议的跟踪器的性能进行评估，并与最先进的解决方案进行比较。定性和定量结果表明，所提出的跟踪器不仅优于现有的解决方案，而且还有效地处理了各种跟踪挑战。平均结果，我们达到 cle 7.98 和 f 措施 0.734。少

2018 年 6 月 10 日提交;最初宣布 2018 年 6 月。

评论:25 页, 8 个数字, 3 个表

137. **第 xiv:1806. 03581[pdf] 反渗透委员会**

基于前沿的自主机器人探索

作者:anirudh topiwala, pranav inani, abhishek kthpal

摘要: 探索是在最初未知的环境中选择对特定增益函数贡献最大的目标点的过程。基于前沿的探索是最常见的探索方法，其中前沿是开放空间和未探索空间之间边界上的区域。通过移动到一个新的前沿，我们可以不断地绘制环境地图，直到没有新的边界可以**探测.**本文描述并实现了一种基于前端的自主勘探策略，即波前前沿检测器 (wfd)，该策略在 Wavefront 仿真环境以及硬件平台上进行了描述和实现，即利用机器人操作系统 (ros) 的 kobuki turtlebot。该算法的优点是机器人可以探索大的开放空间以及小杂乱的空间。此外，该技术生成的地图与使用 turtbot _ teleop ros 包生成的地图进行了比较和验证。少

2018 年 6 月 10 日提交;最初宣布 2018 年 6 月。

138. **第 xiv:1806. 03516[pdf,其他] Cs。铬**

入侵检测系统的恶意流量分类

作者:hanan hindy, e 型 hodo, ethan bayne, amar seeam, robert atkinson, xavier bellekens

摘要:随着网络威胁数量的不断增加，为了设计出更好的入侵**检测**系统，了解现有的和新的网络威胁是非常必要的。在本文中，我们提出了一个分类分类，以一个一致的方式对网络攻击进行分类，使安全研究人员能够将精力集中在创建准确的入侵.

2018 年 6 月 9 日提交;最初宣布 2018 年 6 月。

评论:4 页, 2 个数字，接受 ieee cybersa 2018 诉讼

139. **第 xiv:1806. 03378[pdf,其他] si**

多伊10.98/rss. 170413

文化投资与城市社会经济发展: 一种地理社会网络方法

作者:xiaozhou, desislava hristova, anastasios noulas, cecilia mascolo, max sklar

摘要: 能够评估政府主导的投资对城市社会经济指标的影响长期以来一直是城市规划的一个重要**目标**。然而，由于缺乏具有良好时空分辨率的大规模数据，规划人员如何跟踪文化投资对小城市地区的影响和衡量其有效性存在局限性。利用伦敦近 400 万张基于广受欢迎的基于位置的社交网络服务 foursquare 的 3 年过渡记录，研究如何**检测**政府文化支出的社会经济影响,预测。我们的分析表明，可以利用平均聚类系数或中心

度等网络指标来估计当地增长的可能性，以应对文化投资。随后，我们将这些特征整合到监督学习模式中，以推断伦敦街区的社会经济贫困变化。这项研究介绍了如何利用地理社会和移动服务作为代理，跟踪和预测社会经济贫困的变化，因为政府的财政努力被投入到城市地区的发展中，从而为进一步提供证据和建议决策和投资优化。少

2018 年 6 月 8 日提交;最初宣布 2018 年 6 月。

日记本参考:英国皇家学会开放科学 2017 4 (9), 170413

140. 第 xiv:1806. 03369[pdf,其他] Cs。CI

#SarcasmDetection 太一般了!一种独立于领域的方法来检测讽刺

作者:natalie parde , rodney d. nielsen

摘要: 自动讽刺**检测**方法传统上是为在特定域上实现最大性能而设计的。这对那些希望将这些方法转移到其他现有或新领域的人来说是一个挑战，这些领域可能以截然不同的语言特点为典型。我们开发了一组通用的功能，并利用域内和域外的培训数据在不同的培训场景下对其进行评估。效果最好的方案，在使用域适应步骤的同时进行这两方面的培训，实现了 0.780 的 f1，远远高于 0.780 和 0.780 的基准 f1 措施。我们还表明，该方法优于以前在同一**目标**域上的工作所产生的最佳结果。少

2018 年 6 月 8 日提交;最初宣布 2018 年 6 月。

评论:第 30 届佛罗里达国际人工智能研究会论文集

141. 第 1806.0228[pdf,其他] Cs。简历

具有多尺度深度强化学习代理的自动视图规划

作者:amir alansary, loic le folgoc, ghislain vaillant, ozan oktay, giwweili, wengia bai, jonathan paserat-palmbach, ricardo guerrero, konstantinoskamnitsas, benjaminhou, steven mcdonagh, ben glocker, bernhard kainz, daniel rueckert

摘要: 我们提出了一种在三维图像采集中寻找标准化视图平面的全自动方法。标准视图图像在临床实践中很重要，因为它们提供了一种从类似解剖区域进行生物识别测量的手段。这些视图通常受限于 3d 图像采集的本机方向。在**目标**解剖中导航以查找所需的视图平面是繁琐和运营商依赖的。对于这项任务，我们采用了多尺度增强学习 (rl) 代理框架，并对几种基于深 q 网络 (dqn) 的策略进行了广泛的评估。rl 通过与环境的互动实现了自然的学习范式，可用于模仿有经验的运算符。我们使用解剖地标和**检测**平面之间的距离以及它们的法线向量和**目标**之间的角度来评估我们的结果。该算法在脑 mri 的中矢状面和前后部平面上进行了评估，并对心脏 mri 常用的 4 室长轴平面进行了评估，分别达到 1.53 mm、1.53mm 和 4.84 毫米的精度。少

2018 年 6 月 8 日提交;最初宣布 2018 年 6 月。

评论:适用于 miccai2018

142. 特别报告: 1806. 03002[pdf,其他] Cs。简历

基于模拟和无监督学习的卫星图像领域自适应生成

作者:seo junghoon, seunghyun jeon, taegyun jeon

文摘: 飞机目标**的检测**和分类是卫星图像分析中最重要的任务。现代**检测**和分类方法的成功是建立在机器学习和深度学习的基础上的。这些学习过程的关键要求之一是需要培训的海量数据。然而，飞机的比例不足，因为**目标**是军事行动和行动。考虑到卫星图像的特点，本文试图在没有任何额外的视觉或物理假设的情况下，提供一个模拟和无

监督方法的框架。最后，定性和定量分析显示，有可能为卫星图像分析的机器学习平台补充不足的数据。少

2018 年 6 月 8 日提交;最初宣布 2018 年 6 月。

评论:在 2017 年亚洲机器学习会议 (mlaip @ acml) 举行的人工智能平台机器学习国际研讨会上发表

143. 第 xiv:1806. 01633[pdf,其他] Cs。镍

扩展中的群集: 理解和取消 ipv6 hitist

作者:oliver gasser, quirin Scheitle , pawel foremski, qasim lone, maciej korczynski, stephen d.strowes, luuk hendriks, georg carle

摘要: 网络测量是理解互联网的重要工具。由于 ipv6 地址空间的广阔, ipv6 无法进行 ipv4 中的详尽扫描。近年来，有几项研究建议使用 ipv6 地址的**目标**列表，称为 ipv6 命中列表。在本文中，我们证明 ipv6 命中列表中的地址是大量聚集的。我们介绍了一些新技术，允许将 ipv6 命中列表从数量推送到质量。我们在 6 个月内进行纵向主动测量研究,**针对**超过 50m 的地址。我们开发了一种严格**的方法来检测**别名前缀，该方法将 1.5% 的前缀标识为别名，大约一半的**目标**地址。利用熵聚类，我们将整个命中列表分组为仅 6 个不同的寻址方案。此外，我们还利用众包来执行客户测量。为了鼓励网络测量研究的重现性，并作为未来 ipv6 研究的起点，我们发布源代码、分析工具和数据。少

2018 年 9 月 28 日提交;v1 于 2018 年 6 月 5 日提交;最初宣布 2018 年 6 月。

评论:有关每日 ipv6 命中列表、历史数据和其他分析，请参阅 https://ipv6hitlist.github.io

日记本参考:2018 年互联网测量会议论文集 (imc ' 18)

144. 第 xiv:006: 727[pdf,其他] 反渗透委员会

用于协作人自主目标搜索的闭环贝叶斯语义数据融合

作者:luke burks, ian loefgren, luke barbier, jeremy muesing, jamison mckinley, sousheel vunnam , nisar ahmed

摘要: 在搜索应用中，自主无人飞行器必须能够有效地重新获取移动**目标**并将其本地化，这些目标可以在大空间中长时间不在视野中。因此，必须积极利用所有可用的信息来源----包括人类提供的不准确但随时可用的语义观察。为此，本工作开发并验证了一种用于动态**目标**搜索的新型协作人机传感解决方案。我们的方法使用连续的部分可观察马尔可夫决策过程 (cpomdp) 规划来生成车辆轨迹，以最佳方式利用机载传感器中不完美的**检测**数据，以及语义自然语言观察可以从人类传感器中特别要求的。关键的创新是一个可扩展的分层高斯混合模型公式，以有效地解决 comdp 与语义观测在连续动态空间。该方法通过一个真正的人机团队在自定义测试台上进行动态室内**目标**搜索和捕获场景的演示和验证。少

2018 年 6 月 2 日提交;最初宣布 2018 年 6 月。

评论:最终版本被接受并提交给 2018 年融合大会 (2018 年 7 月，英国剑桥)

145. 第 1805 5.12511[pdf] Cs。铬

基于变分推理的深层生成模型的网络攻击检测

作者:salin e. chandy, amin rasekh, zachary a.barker, m. ehsan shafiee

摘要: 近年来，**针对**关键基础设施系统的网络攻击的频率和强度有所上升。本研究为基础设施系统网络安全设计了一个多功能、数据驱动的网络攻击检测平台，并在水部门进行了专门演示。具有变分推理的深层生成模型自主学习正常的系统行为，并在攻击发生时**进行检测**。该模型可以处理原始形式的自然数据，并自动发现和学习其表示形式，从而增强系统知识发现，减少对费力的人机工程和领域专业知识的需求。将该模型应用于一个模拟的网络攻击检测问题，该系统涉及可编程逻辑控制器黑客攻击、恶意执行器激活和欺骗攻击的饮用水**分配**系统。该模型只提供了对系统的观测，如水泵压力和水箱水位读数，对配水系统的内部结构和运行情况视而不见。模拟攻击体现在模型生成的复制概率图中，表明其识别攻击的能力。然而，在减少假警报方面需要改进，特别是通过优化**检测**阈值。总之，研究结果表明，该模型能够区分输水系统中的攻击及其对正常系统运行的影响，并为其他领域的网络攻击检测带来了希望。少

2018 年 5 月 31 日提交;最初宣布 2018 年 5 月。

日记本参考:2018 年水资源规划与管理杂志

146. **第 1805 5.12277[pdf,其他] Cs。简历**

开放式领域适应的学习表象

作者:mahsa baktashmotlagh, masoud faraki, tom drummond, mathieu salzmann

摘要: 近年来，视觉识别领域适应取得了很大进展。然而，大多数现有方法在所谓的闭集方案中工作，假设**目标**图像所描述的类与源域所描述的类完全相同。在本文中，我们讨论了更具挑战性但更现实的开放式域适应案例，其中目标数据中可能存在新的未知类. 虽然在无人监督的情况下，我们不能期望能够识别每个特定的新类，但我们的目标是自动检测哪些样本属于这些新类，并将它们从识别过程中丢弃。为此，我们依赖于一种直觉，即描述已知类的源和**目标**样本可以由共享子空间生成，而来自未知类的**目标**样本来自不同的私有子空间。因此，我们引入了一个框架，将数据分解为共享部分和私有部分，同时鼓励共享表示是歧视性的。我们在标准基准上的实验证明，我们的方法明显优于开放式域适应领域的最先进方法。少

2018 年 5 月 30 日提交;最初宣布 2018 年 5 月。

147. **第 1805 5.11902[pdf,其他] Cs。镍**

联合雷达通信网络的性能权衡

作者:ren pingren, andrea munari , marina petrova

摘要: 这封信考虑了一个网络，在这个网络中，节点共享一个无线通道，作为**用于目标检测**的脉冲雷达和作为数据交换的发射机而工作。利用随机几何工具研究了雷达**探测**范围和网络吞吐量。我们推导出闭形式表达式，确定雷达和通信业务之间的关键权衡。结果揭示了有趣的设计提示，并强调了雷达**检测**对通信干扰的显著敏感性。少

2018 年 5 月 30 日提交;最初宣布 2018 年 5 月。

148. **第 1805 5.11714[pdf,其他] Cs。简历**

深层视频肖像

作者:hyeongwookim, pablo garrido, ayush tewari, weipeng xu, justus thies, matthias niesner, patrick pérez, christian richardt, michael zollhöfer, 克里斯蒂安·特奥巴尔特

摘要: 我们提出了一种新的方法，使照片逼真的动画视频只使用输入视频。与现有的仅限于操作面部表情的方法不同，我们首先将整个三维头部位置、头部旋转、面部表情、

眼睛注视和眼睛闪烁从源演员转移到一个肖像视频. **目标**演员。我们的方法的核心是具有新的时空结构的生成神经网络。该网络将参数面模型作为输入合成渲染，在此基础上预测给定**目标**参与者的照片逼真视频帧。这种渲染到视频传输中的真实感是通过仔细的对抗训练来实现的，因此，我们可以创建修改后的**目标**视频，以模拟合成输入的行为。为了启用源到**目标**视频重新动画，我们使用源视频中重建的头部动画参数渲染合成**目标**视频，并将其输入训练有素的网络，从而完全控制**目标**。凭借自由重组源和**目标**参数的能力，我们能够演示各种视频重写应用程序，而无需显式建模头发、身体或背景。例如，我们可以使用交互式用户控制编辑重现满头，实现高保真视觉配音。为了证明我们的高质量输出，我们进行了一系列广泛的实验和评估，例如，用户研究表明，我们的视频编辑很难**被发现**。少

2018 年 5 月 29 日提交;最初宣布 2018 年 5 月。

评论:2018 年信号，视频: https://www.youtube.com/watch? v=qc5P2bvfl44

149. 第 1805 5.11514[pdf,其他] cs. it

大型多用户 mimo 检测: 算法和体系结构

作者:hadi sarieddeen

文摘: 本文研究了大型 mimo 和高阶 mu-mimo 系统中的高效数据**检测**问题。首先，针对常规 mimo 系统，提出了近乎最优的低复杂度**检测**算法。在此基础上，提出了一种基于信道矩阵刺穿目标的大型 mimo 系统低复杂硬输出和软输出**检测**方案。对这些方案的性能进行了数学表征和分析，推导了容量、分集增益和位误差概率的边界。之后，在关节调制分类和子空间**检测**的基础上，提出了高效的高阶 mu-mimo 探测器，其中估计了干扰器的调制类型，同时分别存在**多个解耦流检测到**。针对所提出的算法设计了硬件体系结构，并通过仿真验证了所得到的增益。最后，将所研究的基于搜索的**检测**方案映射到大体积 mimo 中发射机侧的低分辨率预编码，并报告了性能复杂度的权衡。少

2018 年 5 月 29 日提交;最初宣布 2018 年 5 月。

评论:博士论文-hadi sarieddeen

150. 第 1805 5.11482[pdf,其他] cs. it

通过机器学习实现 lte rach 碰撞多重检测

作者:davedmagrin, chiara pielli, cedomir stefanovic, miche zorzi

摘要: 在机器类型的流量情况下，已知长期演化 (lte) 标准的随机访问通道 (rach) 过程中的碰撞解析机制是一个严重的瓶颈。它的主要缺点是，基站 (eNBs) 通常无法推断碰撞用户设备 (ue) 的数量，而碰撞的 ue 由于缺乏在 rach 后期阶段的反馈，才含蓄地了解碰撞程序。然后，碰撞的 ue 重新启动过程，从而增加 rach 负载，使系统更容易发生碰撞。在本文中，我们利用机器学习技术设计了一个系统，该系统在 lte rach 过程的前导**检测**方面优于最先进的方案。最重要的是，我们的方案还可以估计碰撞多样性，从而收集有关有多少设备选择相同的序言的信息。此数据可由 enb 用于解决冲突、增加支持的系统负载并减少传输延迟。该方法适用于针对大规模物联网 (如 lte-m 和 nb-iot) 的新型 3gpp 标准. 少

2018 年 5 月 29 日提交;最初宣布 2018 年 5 月。

评论:提交给 ieee globeicom 2018

151. 第 1805 5.848[pdf] Cs。铬

入侵检测系统签名设计中缺陷的识别

作者:nancy Agarwal, syed zeeshan hussain

文摘: 基于签名**的入侵检测**系统 (sids) 为 web 应用程序安全问题提供了一个很有前途的解决方案。但是，系统的性能在很大程度上取决于旨在**检测**攻击的签名的质量。弱签名集可能会显著导致虚警率的增加，使系统的部署不切实际。本文的目的是找出签名结构中的缺陷，这些缺陷是为了降低**检测**系统的效率。本文特别**针对** sql 注入签名。最初，已经讨论了开发人员在设计签名之前应该重点关注的攻击领域的一些基本概念。随后，我们对众所周知的 phpids 工具进行了案例研究，以分析其 sql 签名的质量。在分析的基础上，我们发现了设计实践中产生低效签名的各种缺陷。我们将弱签名分为六类，即不完整、不相关、半相关、易受影响、多余和不一致的签名。此外，我们量化这些弱点，并根据集合论对其进行数学定义。据我们所知，我们已经确定了一些新的签名设计问题。该文件将基本上有助于签名开发者了解设计一套质量签字集需要何种程度的专门知识，以及一点无知如何可能导致小岛屿发展中国家业绩恶化。此外，安全专家可通过对探测器的签名集进行结构分析，对照已查明的缺陷对探测器进行评估。少

2018 年 5 月 28 日提交;最初宣布 2018 年 5 月。

152. **第 1805 5.815[pdf,其他] Cs。铬**

netra: 利用基于 nfv 的边缘流量分析增强物联网安全

作者:rishi sairam, suan sankar bhunia, vijayanand thangavelu, mohan gurusamy

摘要: 这是一个智能设备或东西的时代，它们正在推动物联网 (iot) 的发展。它正在影响我们周围的每一个领域，使我们的生活依赖于这一技术壮举。令人高度关切的是，这些智能事物正成为网络犯罪分子利用这些设备内的异质性、微小的安全功能和漏洞的目标。传统的集中式 it 安全措施在可扩展性和成本方面存在局限性。因此，需要对这些智能设备进行更靠近其位置的监控，理想情况下，要在物联网网络的边缘进行监控。在本文中，我们探讨了如何在网络边缘实现一些安全功能，以保护这些智能设备。为了在网络边缘部署安全功能，我们解释了网络功能虚拟化 (nfv) 的重要性。为了实现这一目标，我们引入了 netra-一种基于鸽子的新型轻量级体系结构，用于虚拟化网络功能，以提供物联网安全性。此外，我们还强调了与标准化 nfv 体系结构相比，所建议的体系结构在存储、内存使用、延迟、吞吐量、负载平均值、可扩展性方面的优势，并解释了标准化体系结构不适合物联网的原因。我们研究了基于 nfv 的物联网安全边缘分析的性能，表明在不到一秒的时间内**可以检测到**精度超过 95% 的攻击。少

2018 年 5 月 28 日提交;最初宣布 2018 年 5 月。

153. **建议: 1805 5.3364[pdf,其他] Cs。铬**

利用生成性对抗网络检测欺骗性评论

作者:hojjat aghakhani, aravind machiry, shirin nilizadeh, christopher kruegel , giovanni vigna

摘要: 在过去的几年里，消费者评论网站已经成为骗人意见垃圾邮件的主要**目标**，在这些网站上，虚构的意见或评论被故意写得听起来真实。现有的检测欺骗性评论的工作大多集中在基于观点的句法和词汇模式的监督分类器的构建上。随着神经网络在各种分类应用中的成功应用，本文提出了一个首次增强并采用生成对抗性网络 (gans) 进行文本分类任务的系统，特别是**:检测**欺骗性评论。与具有单个生成器和判别模型的标准 gan 模型不同, fakegan 使用两种鉴别模型和一个生成模型。将生成器建模为增强学习 (rl) 中的随机策略代理，鉴别器利用蒙特卡罗搜索算法对中间动作值进行估计并将其

作为 rl 奖励。通过从两个真实和欺骗性的评论中学习，为生成器模型提供两个鉴别器模型，避免了 mod 崩溃问题。事实上，我们的实验表明，使用两个鉴别器提供了 fakegan 的高稳定性，这是 gan 架构中已知的问题。虽然 fakegan 是建立在半监督分类器的基础上的，以精度较低著称，但我们对 tripadvisor 酒店评论数据集的评估结果在准确性方面显示了与应用监督机器的最先进方法相同的性能学习。这些结果表明，gans 可以有效地进行文本分类任务。具体而言，fakegan 可以有效**地检测**欺骗性评论。少

2018 年 5 月 25 日提交;最初宣布 2018 年 5 月。

评论:与第 39 届 ieee 安全与隐私研讨会同时举办的第一次深度学习和安全研讨会上被接受

154. 第 1805 5.09749[pdf,其他] Cs。简历

移动人脸跟踪：一个调查和基准

作者:林一明,沈洁,程石阳,马雅·潘蒂奇

摘要: 随着智能手机的快速发展，面部分析在众多移动应用中发挥着越来越重要的作用。在大多数情况下，人脸跟踪是关键的第一步，因为移动应用程序通常只需要专注于在复杂的环境中分析特定的人脸。尽管在一般视觉跟踪问题中继承了许多公共特征，但移动场景中的人脸跟踪具有一系列独特的挑战。在这项工作中，我们提出了 ibug mobisface 基准，这是第一个移动人脸跟踪基准，由智能手机用户在不受约束的环境中捕获的 50 个序列组成。这些序列总共包含 50，736 帧，具有 46 个不同的标识来跟踪。选择每个序列中的跟踪**目标**时，移动方案中存在不同的困难。除了逐帧边界框外，还提供了 9 个序列属性 (例如多个面) 的批注。我们进一步对 23 个最先进的视觉跟踪器进行了调查，并对这些方法进行了对拟议基准的全面定量评估。特别是，研究了两个最流行的框架的跟踪器，即基于相关筛选器的跟踪和基于深度学习的跟踪。我们的实验表明: (a) 所有现有通用对象跟踪器在移动人脸跟踪场景中的性能显著下降，这表明需要对移动人脸跟踪进行更多的研究; (b) 深度跟踪的有效组合学习跟踪和与面部相关的算法 (例如人**脸检测**) 为该领域的未来发展提供了最有希望的基础。数据库、注释和评估协议代码将在 ibug 网站上公开提供。少

2018 年 5 月 24 日提交;最初宣布 2018 年 5 月。

评论:13 页，6 个数字

155. 第 1805 5.09738[pdf,其他] Cs。铬

用暹罗神经网络检测语符号攻击

作者:jonathan woodbridge, hyrum s.anderson, anjum ahuja, daniel grant

摘要: 同字符号 (名称欺骗) 攻击是对手用来混淆文件和域名的常用技术。此技术创建的进程或域名在视觉上类似于合法和可识别的名称。例如，攻击者可能会创建名为 svch0ste. exe 的恶意软件，以便在对正在运行的进程或目录列表进行可视检查时，进程或文件名可能会被误认为是 windows 系统进程 svchost. exe。关于**检测**同音图攻击的研究数量有限。目前的方法依赖于字符串比较算法 (如 levenshtein 距离)，这些算法会产生计算量大、误报数量较高的解决方案。此外，可用于可重现研究的公开数据集数量不足，大多数数据集侧重于网络钓鱼攻击，其中并不总是使用同甘油酯。本文利用暹罗卷积神经网络 (cnn) 提出了解决这一问题的根本不同的方法。而不是利用基于字符交换和删除的相似性，这种技术使用一个经验说过的指标作为图像呈现的字符串: 美国有线电视新闻网学习的功能，经过优化，以**检测**渲染的字符串的视觉相似性。训练

后的模型用于将数千个潜在**的目标**进程或域名转换为特征向量。这些特征向量使用随机 kd-交税，以使相似性搜索速度极快，计算处理最少。该技术在接收机操作特性曲线(roc auc) 下的面积方面比基线技术有了 13% 至 45% 的改进。此外，我们还提供代码和数据，以进一步进行未来的研究。少

2018 年 5 月 24 日提交;最初宣布 2018 年 5 月。

156. 建议: 1805 5.09563[pdf,其他] Cs。铬

r-packdroid: 安卓勒索软件的实用设备检测

作者:mic 其 lee sc 社会科学, davde Maiorca, francescomercaldo, corrado aaron visaggio, fabio martinelli, giorgio giacinto

摘要: 勒索软件对 android 操作系统构成重大威胁。它可以锁定或加密**目标**设备，受害者可能被迫支付赎金以恢复其数据。尽管以前的工作在恶意软件**检测**，很少做，以具体识别 android 恶意软件作为勒索软件。这一点至关重要，因为勒索软件需要立即采取对策，以避免数据被完全泄露。在本文中，我们提出 r-packdroid，一个基于机器学习的应用程序 (直接在 android 手机上运行) 检测 android 勒索软件。r-pacdroid 是一种轻量级方法，它利用了基于从系统 api 包中提取信息的方法。我们通过在大量合法、恶意和基于勒索的应用程序上对其进行测试来证明其有效性。我们的分析指出了三个主要结果: 第一, r-packdroid 可以非常高的准确性区分勒索软件和恶意软件以及合法的应用程序;其次, r-packdroid 保证了抵御重混淆尝试 (如类加密) 的恢复能力;第三, r-packdroid 可以有效地预测和**检测**新的勒索样本，这些样品是在用于训练系统后释放的。r-packroidid 可在 google play 商店上使用，它是首款面向勒索的面向 android 的学术探测器。少

2018 年 6 月 27 日提交;v1 于 2018 年 5 月 24 日提交;最初宣布 2018 年 5 月。

157. 第 xiv: 180 5.09061[pdf,其他] 反渗透委员会

基于 uav 的辐射检测的可视化惯性目标跟踪与运动规划

作者:Indrajeet yadav, kevin eckenhoff, gugul huang guguan, herbert g. tanner

文摘: 本文讨论了使用最小传感能力的无人机探测运输中**的**放射性物质的问题，目的是在车辆规划其路径时对**目标的**放射性进行分类。同时跟踪**目标**的时间间隔很短。为此，我们提出了一个运动规划框架，该框架集成了紧密耦合的视惯性定位和**目标**跟踪。在这个框架中, 3d 工作空间是已知的，这个信息与无人机动力学一起，被用来构建一个导航函数，产生动态可行的安全路径，避免障碍，并可以证明收敛到移动**的目标**.通过在 gazebo 中的逼真仿真验证了该方法的有效性。少

2018 年 5 月 23 日提交;最初宣布 2018 年 5 月。

158. 第 1805.08168[pdf,其他] cs. cy

"你知道该怎么做": 主动检测 youtube 视频的目标协调仇恨攻击

作者:enrico mariconti, guillermo suarez-tengil, jeremy blackburn, emiliano de cristofaro, nicolaskourtellis, ilias leontiadis, jordi luque serrano, gizanluca 斯特林吉尼

摘要: 多年来，网络缩小了世界，允许个人与更多的人分享观点，而不是他们在现实生活中的能力。然而，与此同时，它也使反社会和有毒行为以前所未有的规模发生。像 youtube 这样的视频共享平台接收来自数百万用户的上传，涵盖了各种各样的主题，并允许其他人进行评论和互动。不幸的是，这些社区经常受到侵略和仇恨袭击的困扰。特别是，最近的工作表明，这些袭击往往是 "袭击" 的结果，即由第三方社区的临时暴

民协调的有组织的努力。尽管这一现象的相关性越来越大，但在线服务往往缺乏有效的对策来减轻这一现象。与垃圾邮件和网络钓鱼等经过充分研究的问题不同，协调的攻击性行为既是目标，也是人类所为,这使得寻找自动化活动的防御机制不合适。因此，事实上的解决办法是重新依赖用户报告和人的评论。在本文中，我们提出了一个自动化的解决方案，以确定可能成为协调骚扰者目标的视频。首先，我们根据突袭受害者的地面真相数据集，沿多个轴（元数据、音频记录、缩略图）对 youtube 视频进行描述和建模。然后，我们使用分类器的组合来确定视频被高精度突袭的可能性（auc 高达 94%）。总体而言，我们的工作为为 youtube 等视频平台提供主动系统以**检测**和减轻协同仇恨攻击铺平了道路。少

2018 年 5 月 21 日提交;最初宣布 2018 年 5 月。

159. 第 1805.08105[pdf,其他] Cs。简历

水平-天空线检测语义分割方法的比较

作者:touqeer ahmad, pavel campr, martin Čadík, george bebis

摘要: 地平线或天际线**检测**对山地视觉地理定位起着至关重要的作用，但最近提出的大多数视觉地理定位方法都依赖于 \ textbf{用户在环中的天际线**检测**方法。完全自主**地检测**这样的分割边界，对于这些本地化方法来说，肯定是向前迈出的一步。本文对广泛数据集上的四种自主水平**线检测**方法进行了定量比较。具体而言，我们提供了最近提出的四种分割方法的比较;一个明确**针对**地平线**探测**问题 \ cemenedn.15}，第二个重点是视觉地理定位，但依靠准确检测天际线 \ cite\ saurer16} 和其他两个建议的一般**语义**分割--完全卷积网络（fcn）\ citeeinlong15} 和 segnet-citetex\ citexen {badrinarayanan15}。前两种方法都是在由大约 200 张图像组成的通用训练集 \ cecebaatz12} 上进行训练的，而第三和第四种方法的模型则通过使用相同的数据集进行传输学习，针对天空分段问题进行微调。每种方法都在广泛的测试集（约 3k 图像）上进行测试，涵盖各种具有挑战性的地理、天气、照明和季节性条件。我们报告每个公式的平均精度和平均绝对像素误差。少

2018 年 5 月 21 日提交;最初宣布 2018 年 5 月。

评论:神经网络国际联席会议论文集（口头介绍），ieee 计算情报学会，2017 年

160. 第 09iv:1805 5.0767[pdf,其他] Cs。简历

无推力节体目标检测的 f-度量优化

作者:赵凯,高尚华,侯启斌,李丹丹，程明明

文摘: 目前基于 cnn 的显著目标检测（sod）解决方案主要依靠交叉熵损失（celoss）的优化。然后,**检测到的**显著性映射的质量往往是根据 f 测量的方法进行评估的。在本文中，我们研究了一个有趣的问题：我们能否在 sod 的训练和评估中始终使用 f-测量公式？通过重新设计标准的 f 量，我们提出了一种可微分的放松的 f 措施，后部可轻松附加到 cnn 的背面作为损失函数。与饱和区梯度显著减小的传统交叉熵损失相比，即使激活接近**目标**，我们的损耗函数，称为 floss，也具有相当大的梯度。因此，fl 失会不断地迫使网络产生极化的激活。几个流行数据集上的综合基准显示，floss 的表现优于艺术的地位，并有相当大的优势。更具体地说，由于偏振预测，我们的方法能够获得高质量的显著性映射，而无需仔细调整最佳阈值，显示出在实际应用中的显著优势。少

2018 年 5 月 19 日提交;最初宣布 2018 年 5 月。

161. 第 1805 5.0157[pdf,其他] Cs。简历

混合区域嵌入的零射击目标检测

作者:berkan demirel, ramazan gokberk cinbis, nazli ikizler-cinbis

摘要: 目标**检测**被认为是计算机视觉中最具挑战性的问题之一，因为它需要正确预测图像中对象的类和位置。在本研究中，我们定义了一个更困难的场景，即零拍摄对象检测 (zsd)，其中没有针对某些**目标**对象类的可视化训练数据。我们提出了一种新的方法来解决 zsd 问题，即嵌入的凸组合与**检测**框架结合使用。对于 zsd 方法的评估，我们建议使用医学博士-mnist 图像构建一个简单的数据集，并针对 pascal voc **检测**挑战提供自定义零拍摄拆分。实验结果表明，该方法为 zsd 取得了很有希望的效果。少

2018 年 5 月 17 日提交;v1 于 2018 年 5 月 16 日提交;最初宣布 2018 年 5 月。

162. 第 1805.06070[pdf, ps,其他] Cs。铬

利用主机数据的入侵检测系统研究综述

作者:tarrah r. Glass-Vanderlan, michael d. iannacone, maria s.vincent, qian, chen, robert a.bridge

摘要: 本调查的重点是利用基于主机的数据源检测企业网络攻击的入侵**检测**系统 (ids). 基于主机的 ids (hids) 文献由输入数据源组织，利用系统日志、审计数据、windows 注册表、文件系统和程序分析，对 hids 研究进行**有针对性**的子调查。虽然系统调用通常包含在审计数据中，但一些公开的系统调用数据集已经生成了一系列 ids 关于此主题的研究，值得单独进行单独的部分。同样，还包括一个适用于 hids 但在网络数据集上进行测试的章节测量算法发展，因为这是一个越来越大的适用文献领域。为了适应当前的研究人员，我们增加了一个补充部分，介绍公开的数据集，概述了它们在用于 ids 评估时的特点和缺点。组织和描述相关调查。所有部分都附有简要整理文献和数据集的表格。最后，挑战、趋势和更广泛的观察贯穿于整个调查过程和结论以及 ids 研究的未来方向。少

2018 年 5 月 16 日提交;v1 于 2018 年 5 月 15 日提交;最初宣布 2018 年 5 月。

163. 第 09iv:1805.06066[pdf,其他] Cs。简历

语义目标驱动导航的可视化表示

作者:arsalan mousavian,亚历山大 toshev, marek fiser, jara kosecka, james davidson

摘要: 什么是自主代理的良好视觉表示？我们在语义视觉导航的上下文中解决了这个问题，这是机器人通过复杂的环境找到目标对象的问题，例如去冰箱。我们的方法不是获取环境的度量语义映射并使用导航规划，而是在捕获空间布局和语义上下文线索的表示的基础上学习导航策略。我们建议使用高级语义和上下文功能，包括通过现成的最先进的视觉获得的分割和**检测**掩码作为观察，并使用深层网络来学习导航策略。这种选择允许使用来自正交源的其他数据来更好地训练模型的不同部分，表示提取是在大型标准视觉数据集上训练的，而导航组件则利用大型合成环境来实现培训。这种实际和综合的组合是可能的，因为公平的特征表示在这两种方面都有可用 (例如，分割和**检测**掩码)，从而减少了对域适应的需求。如活动视觉数据集 [1] 所示，表示和导航策略都可以很容易地应用于实际的非合成环境。在未开发的环境中，我们的方法成功地达到了 54% 的病例的目标，而非基于学习的方法的这一比例为 46%，基于学习的基线的这一比例为 28%。少

2018 年 5 月 15 日提交;最初宣布 2018 年 5 月。

164. 第 1805. 05132[pdf,其他] Cs。简历

利用中心-暗通道的值进行显著的目标检测

作者:朱春标,张文豪,李嘉思,葛丽

文摘: 显著性**检测**旨在**检测**图像中最吸引人的物体，并被广泛用作各种应用的基础。本文提出了一种新的利用中心-暗通道原点对 rgb-d 图像**进行**突出目标检测的算法。首先，我们基于给定 rgb-d 图像的颜色显著性映射和深度显著性映射生成初始显著性映射。然后，我们生成一个基于中心显著性和暗通道原点的中心-暗通道图。最后，我们将初始显著性映射与中心暗通道映射融合在一起，生成最终的显著性映射。对四个基准数据集的广泛评估表明，我们提出的方法与大多数最先进的方法相比具有良好的效果。此外，我们还进一步讨论了该算法在小**目标检测**中的应用，并论证了中心-暗通道前置在目标**检测**领域的普遍价值。少

2018 年 5 月 14 日提交;最初宣布 2018 年 5 月。

评论:项目网站: https://chunbiaozhu.github.io/ACVR2017/

165. 第 1805.05098[pdf,其他] Cs。铬

胡福: 基于神经网络的硬件和软件协同攻击框架

作者:李文硕,于金成,宁雪飞,王鹏军,齐伟，王玉华, 杨华忠

摘要: 近年来，深度学习 (dl)，特别是卷积神经网络 (cnn) 发展迅速，应用于图像分类、人脸识别、图像分割和人**的检测**等许多任务。基于 dl 的型号由于其卓越的性能，在许多领域具有广泛的应用，其中一些领域对安全至关重要，例如智能监控和自动驾驶。由于云计算的延迟和隐私问题，嵌入式加速器在这些安全关键领域很受欢迎。但是，嵌入式 dl 系统的鲁棒性可能会因为将硬件软件 trojans 插入加速器和神经网络模型而受到损害，因为加速器和部署工具 (或神经网络模型) 通常由第三方提供公司。幸运的是，插入硬件特洛伊木马只能实现不灵活的攻击，这意味着硬件特洛伊木马程序可以很容易地打破整个系统或交换两个输出，但不能使美国有线电视新闻网识别未知图片为**目标**。尽管插入软件特洛伊木马程序具有更多的攻击自由，但它通常需要篡改输入图像，这对攻击者来说并不容易。因此，在本文中，我们提出了一个硬件-软件协作攻击框架，以注入隐藏的神经网络特洛伊木马程序，它作为后门，无需操纵输入图像，并且对不同的场景是灵活的。我们测试了图像分类和人脸识别任务的攻击框架，并分别在 cifar10 和 youtube 面上获得了 92.6 和 100% 的攻击成功率，同时在正常模式下保持了与未攻击模型几乎相同的精度。此外，我们还展示了一个特定的攻击场景，在这种情况下，人脸识别系统受到攻击，并给出了一个具体的错误答案。少

2018 年 5 月 14 日提交;最初宣布 2018 年 5 月。

评论:6 页, 8 个数字, 5 个表格，接受 isvlsi 2018

166. 第 1805 5.04262[pdf,其他] Cs。简历

利用条件生成模型生成的增强训练图像检测航空图像的毒刺

作者:周一民,陈建红,刘建浩，陈楚松

文摘: 本文提出了一种基于航拍图像**的**目标**检测**方法。在这个问题上，图像是通过使用无人飞行器 (uav) 在海面上进行空中拍摄的，在海面下 (但靠近) 的黄鼠狼是我们要**探测**和定位的目标. 为此，我们使用了一种深度的物体**检测**方法，更快的 rcnn，基于有限的训练图像集训练一个黄鼠狼探测器。为了提高性能，我们开发了一种新的生成方法，条件 glo，以增加黄原的训练样本，这是生成潜在优化 (glo) 方法的扩展。与传统的仅为图像分类生成新数据的数据扩充方法不同，我们提出的将前景和背景混合在一起的方法可以为对象**检测任务生成**新数据，从而提高训练水平美国有线电视新闻网探

测器的功效。实验结果表明，采用我们的航空图像黄原检测方法可以获得满意的性能。少

2018 年 6 月 25 日提交;v1 于 2018 年 5 月 11 日提交;最初宣布 2018 年 5 月。

评论:将出现在 cvpr 2018 研讨会 (cvpr 2018 研讨会和挑战: 用于环境监测的海洋视频自动分析)

167. 第 xiv:180 5.03647[pdf,其他] Cs。Sd

利用具有经验器的时频表示输入的卷积递归神经网络进行端对端复音声音事件检测

作者:emre cakr, tuomas Virtanen

摘要: 声音事件检测系统通常包括两个阶段: 从原始音频波形中提取手工制作的要素，以及使用分类器学习这些特征与目标声音事件之间的映射。近年来，声音事件检测研究的重点大多转移到了后期，使用的标准特征，如 mel 光谱图作为输入的分类器，如深神经网络。在这项工作中，我们利用端到端的方法，并建议将这两个阶段结合在一个单一的深度神经网络分类器中。通过前馈层块对原始波形进行特征提取，并对其参数进行初始化，提取时频表示。在训练期间会更新特征提取参数，从而为特定任务优化表示形式。在这个特征提取块之后，还有一个卷积的经常性网络 (并与之共同训练)，该网络最近在许多声音识别任务中获得了最先进的结果。拟议的系统的性能并不优于具有固定手工制作特征的卷积经常性网络。特征提取块参数的最终幅度谱特征表明，给定任务最相关的信息包含在 0-3 khz 频率范围内, sed 的经验结果也支持了这一点性能。少

2018 年 5 月 9 日提交;最初宣布 2018 年 5 月。

评论:接受 ijcnn 2018 年

168. 第 1805.03532[pdf, ps,其他] si

信息源查找中的必要和充足预算: 适应性差距

作者:蔡永英,容毅

文摘: 在本文中，我们研究了通过查询个体来检测扩散信息来源的问题，给出了信息扩散图的样本快照，其中询问了两个查询: {\ em (i)} 是否为答复者是源，以及 {{如果没有，哪个邻居将信息传播给应答者。我们考虑的情况是，答复者可能并不总是真实的，每个查询都要承担一定的费用。我们的目标是量化必要的和足够的预算，以实现检测概率 1-- 对于任何给定的 0& lt; & lt;(一)为此，我们研究了两种类型的算法: 自适应算法和非自适应算法，每一种算法都对应于我们是否根据以前的答复自适应地选择下一个受访者。我们首先为这两种算法类型的必要预算提供了信息理论下限。在预算充足的基础上，我们提出了两种实用的估计算法，每种算法都是非自适应型和自适应型，并对每种算法的预算进行了定量分析，保证了预算的存在。1-- 检测精度。这种理论分析不仅量化了实际估计算法所需的预算，在寻找扩散源时实现了给定的目标检测精度，而且使我们能够定量地描述在非自适应类型的估计中所需的额外预算量，称为 {\ em 自适应缺口}。我们通过合成和现实世界的社交网络拓扑来验证我们的理论发现。少

2018 年 5 月 8 日提交;最初宣布 2018 年 5 月。

评论:这是 isit 2018 的技术文件. arxiv 管理说明: 文本与 arxiv:1711.545496 重叠

169. 建议: 1805.03296[pdf,其他] cse

中间测试器的鲁棒性测试

作者:陈玉婷,卡洛 a. furia

摘要: 程序验证程序不能幸免于影响几乎每一个软件的错误。此外，它们通常表现出脆弱的行为：它们的性能会发生很大的变化，因为输入程序是如何表达的细节，这些细节应该是不相关的，例如独立声明的顺序。这种缺乏鲁棒性的情况使用户感到沮丧，他们必须花费大量时间来找出工具的特性，然后才能有效地使用它。本文介绍了一种**检测**程序验证器鲁棒性不足的技术;该技术是轻量级和全自动的，因为它是基于测试方法(如突变测试和变质测试)。关键的想法是生成最初通过验证的程序的许多简单变体。所有的变种，从结构上说，都相当于原来的程序;因此，任何失败验证的变体都表明验证程序缺乏鲁棒性。我们在一个名为 "mugie" 的工具中实现了我们的技术，该工具在使用流行的 boogie 语言编写的程序上进行操作，用于验证，作为许多程序验证的中间表示形式。**针对** 135 个 boogie 程序的实验表明，脆性行为发生的频率相当高 (16 个程序)，不难触发。在此基础上，讨论了脆性行为的主要来源，并提出了提高鲁棒性的方法。少

2018 年 5 月 8 日提交;最初宣布 2018 年 5 月。

170. **第 xiv:180 5.02861[pdf, ps,其他] Cs。艾**

互联网环境下巡型问题的综合高效解决方案

作者:tomášbrázdil, antonín kučera , Vojtěch 苦苦提克

文摘: 我们提出了一种在互联网环境中构建高效巡逻策略的算法，在这种环境中，受保护**的目标**是连接到网络的节点，而专利者是能够**检测**到/防止节点上的不受欢迎的活动。该算法基于针对一类特殊策略设计的新的组合原理，即使**目标**数达到数亿，也能快速构造 (次) 最优解。少

2018 年 5 月 10 日提交;v1 于 2018 年 5 月 8 日提交;最初宣布 2018 年 5 月。

171. **第 09iv:1805 5.02834[pdf,其他] Cs。简历**

通过损失加权和对象交互从文本中进行弱监控的视频对象接地

作者:周罗伟, nathan louis, jason j. corso

摘要: 我们研究弱监督视频对象接地：给定视频段和相应的描述性句子，我们的目标是本地化从视频中的句子中提到的对象。在训练期间，没有可用的对象边界框，但可能要接地的对象集事先知道。图像域中的现有方法通过强制执行可视特征和语义特征之间的匹配来使用多实例学习 (mil) 来接地对象。这种方法在视频领域的一个简单的扩展是将整个段视为一袋空间对象建议。但是，在多个帧中稀疏存在的对象可能无法完全**检测到**，因为成功地从一个帧中发现该对象将触发令人满意的匹配。为此，我们将微弱的监控信号从段级别传播到可能包含**目标**对象的帧。对于不可能包含**目标**对象的帧，我们使用另一种惩罚损失。我们还利用对象之间的交互作为接地的文本指南。我们在新收集的基准 youcook2 边界框上评估我们的模型，并显示对竞争基线的改进。少

2018 年 7 月 20 日提交;v1 于 2018 年 5 月 8 日提交;最初宣布 2018 年 5 月。

评论:16 页，包括附录

172. **第 1805 5.02730[pdf,其他] Cs。简历**

多伊 10.10077/978-3-319-66179-7 _ 54

具有非常少量阳性样本的建筑疾病检测算法

作者:ken c. l. wong ， 亚历山大·卡拉吉里斯, tanveer Syeda-Mahmood, mehdi moradi

文摘: 尽管深度学习可以为医学图像分析提供有希望的结果，但由于缺乏非常大的注释数据集，其潜力已被限制。此外，有限的阳性样本还会创建不平衡的数据集，从而限制所训练模型的真实正率。由于不平衡的数据集大多是不可避免的，如果我们能从负样本中提取有用的知识，以提高有限阳性样本的分类精度，那将是非常有益的。为此，我们提出了**建立以疾病检测为目标的**医学图像分析管道的新策略。我们只在正常图像上训练鉴别分割模型，为疾病**检测**分类器提供知识来源。我们表明，使用训练分割网络的特征图，可以通过一个极不平衡的训练数据集上的两级分类网络来了解与正常解剖的偏差，对 17 个负样本的检测结果只有一个正。我们证明，即使分割网络只训练正常的心脏计算机断层扫描图像，由此产生的特征图可以用来**检测**心包积液和心脏间隔缺损与二类卷积分类网络。少

2018 年 5 月 7 日提交;最初宣布 2018 年 5 月。

173. **建议: 1805 5.02628[pdf,其他] Cs。铬**

prada: 防止 dnn 模型窃取攻击

作者:mika juuti, sebastian szyller,亚历克西·德米德雷科, samuel marchal, n. aso kan

摘要: 随着机器学习 (ml) 应用程序变得越来越普遍，保护 ml 模型的机密性变得至关重要，原因有二: (a) 模型可能对其所有者构成商业优势, (b) 对手可能使用被盗模型来查找可转让的对抗实例，可用于逃避原始模型的分类。保护模型机密性的一种方法是仅通过定义良好的预测 api 限制对模型的访问。这不仅在模型处于远程状态的机器学习即服务 (mlaas) 设置中很常见，而且在自驾车等情况下也很常见，例如，模型是本地的，但对其的直接访问受到硬件安全机制的保护。但是，预测 api 仍然会泄漏信息，因此可以由通过预测 api 反复查询模型的对手发起模型提取攻击。本文将生成综合查询的新方法与训练深度神经网络的最新进展结合起来，描述了一种新的模型提取攻击。这种攻击在使用提取的模型 (+ 15-30 个百分点, pp) 生成的**目标**对抗实例的可转移性和两个模型提取的预测准确性 (+ 15-30 页) 方面优于最先进的模型提取技术数据。然后，我们提出了第一个有效**检测**模型提取攻击的通用方法: prada。它分析了连续查询到模型的分布如何随着时间的推移而演变，并在出现突然偏差时发出警报。我们表明，prada 可以**检测**到所有已知的模型提取攻击与 100% 的成功率和没有误报。prada 特别适用于**检测**针对本地模型的提取攻击。少

2018 年 6 月 13 日提交;v1 于 2018 年 5 月 7 日提交;最初宣布 2018 年 5 月。

评论:16 页, 8 个数字, 4 个表

174. **第 1805.02400[pdf,其他] Cs。铬**

主题: 生成特定于上下文的假餐厅评论

作者:mika juuti, bo sun, tatsuya mori, n. as 藤 an

摘要: 自动生成的假餐厅评论是对在线评论系统的威胁。最近的研究表明，用户很难**检测**到机器产生的假评论隐藏在真正的餐厅评论。这项工作中使用的方法 (char-lstm) 有一个缺点: 它难以停留在上下文中，即当它为特定**目标**实体生成审阅时，所产生的评审可能包含与**目标**无关的短语，从而提高其**可探测性**。在这项工作中，我们提出并评估了一种基于神经机器翻译 (nmt) 的更复杂的技术，我们可以用它来生成停留在主题上的评论。我们使用亚马逊机械土耳其人的母语为英语的人测试我们的技术的多种变体。我们证明，最好的变种产生的评论几乎具有最佳的不可探测性 (类平均 f-分数 47%)。我们对持怀疑态度的用户进行了用户研究，并表明，与具有统计意义的最先进 (平均规避 3.2/4 对 1.5/4) 的最先进 (平均规避 3.2/4 对 1.5/4) 相比，我们的方法更频繁地

避免**检测**,其水平是α= 1% (第 4.3 节)。我们开发了非常有效的**检测**工具，并在对这些工具进行分类时达到了 97% 的平均 f 分。虽然假评论是非常有效的愚弄人，有效的自动检测仍然是可行的。少

2018 年 6 月 28 日提交;v1 于 2018 年 5 月 7 日提交;最初宣布 2018 年 5 月。

评论:21 页, 5 个数字, 6 个表。接受在 2018 年欧洲计算机安全研究专题讨论会上发表

175. 第 1805.01514[pdf, ps,其他] cs et

分子通信的高级目标检测

作者:reza mosayebi, wayan wicke, vahid jamali, arman ahadzadeh, robert schober , masoumeh nasiriri-kenari

文摘: 本文考虑了通过扩散分子通信 (mc) 对可疑组织进行目标检测的**问题** .如果**目标**存在，它就会不断地以恒定的速率将特定类型的分子，即所谓的生物标志物，分泌到介质中，这些分子是**目标**存在的症状。**这些**生物标志物的检测具有挑战性，因为由于扩散和降解，这些生物标志物只能在目标附近**检测到** .此外,**目标**在组织内的确切位置尚不清楚。在本文中，我们建议在组织中分布几种反应性纳米传感器 (ns)，以便至少其中一些能与生物标志物接触，从而使它们被激活。激活后, ns 将一定数量的二级分子释放到介质中，以提醒融合中心 (fc)，在那里做出有关**目标**存在的最终决定。特别是，我们考虑一个复合假设测试框架，假设**目标**的位置和生物标志物的分泌率是未知的，而 ns 的位置是已知的。我们推导出在 ns 上检测的**一致**最强大 (ump) 测试。对于 fc 的最终决定，我们表明 ump 测试并不存在。因此，我们推导出一个基因辅助探测器作为性能的上限。然后，我们提出两个次优检测器，并通过模拟评估其性能少

2018 年 5 月 3 日提交;最初宣布 2018 年 5 月。

176. 第 09iv:18005.011184[pdf] Cs。Sy

公园场景的视觉路径跟踪控制

作者:朱林强,王文福,杨伟杰,潘志杰, 陈安晨

文摘: 自动驾驶应用正在向特定场景发展。公园场景具有低速、固定路线、连接短、交通不复杂等特点，适合将自主驾驶技术落到实处。本文**针对**公园场景，提出了一种仅使用一个网络摄像头的视觉路径跟踪横向控制方法。首先，我们计算了相机图像中的距离误差和角度误差，然后利用模糊逻辑将其模糊到一个组合误差程度。pid 控制算法以它为输入，输出方向盘角度控制命令。模糊化可以容忍图像变换和车道**检测**带来的误差，使 pid 控制更加稳定。我们在虚拟和真实场景中的实验表明，即使在夜间，我们的方法也能准确、有力地沿着路径进行。与纯粹的追求相比，我们的方法可以使 5 米的转动。少

2018 年 5 月 12 日提交;v1 于 2018 年 5 月 3 日提交;最初宣布 2018 年 5 月。

评论:第三届机器人与机器视觉国际会议 (icrmv 2018), 2018 年 8 月 11-13 日成都，中国

报告编号:mv007

177. 第 09iv:1805. 00969[pdf,其他] Cs。铬

物联网中一切事物的认证: 学习与环境影响

作者:yan sharaf dabbagh, walid saad

摘要: 要从物联网 (iot) 系统中获益，就必须开发特定于物联网的安全解决方案。由于物联网对象的计算有限和可移植性，传统的安全和身份验证解决方案通常无法满足物联网安全要求。本文提出了一种物联网对象认证框架。该框架使用特定于设备的信息

(称为指纹) 以及传输学习工具来对物联网中的对象进行身份验证。该框架跟踪物理环境变化对指纹的影响，并使用独特的物联网环境效应功能来**检测**网络和网络物理仿真攻击。提出的环境影响估计框架在不增加误报率的情况下提高了攻击者的**检**出率。该框架还证明能够检测到能够**复制**传统方法无法**检测**到的**目标**物体指纹的网络物理攻击者。提出了一种转移学习方法，允许在环境影响估计过程中使用具有不同类型和功能的对象，以提高框架的性能，同时捕获具有不同对象类型的实际物联网部署。利用实际物联网设备数据进行的仿真结果表明，该方法可以使网络仿真**攻击检测提高** 40%，并能够**检测**出传统方法无法**检测到的网络物理仿真攻击。检测**。结果表明，该框架提高了认证精度，而转移学习方法可获得高达 70% 的额外性能提升。少

2018 年 4 月 24 日提交;最初宣布 2018 年 5 月。

178. 第 1805.00385[pdf,其他] Cs。简历

通过知识转移促进自我监督学习

作者:mehdi noroozi, ananth vinjimoor, paolo favaro, hamed pirsiavash

摘要: 在自我监督的学习中，你训练一个模型来解决数据集上所谓的借口任务，而不需要人为的注释。然而，主要目标是将此模型转移到**目标**域和任务。目前，最有效的转移策略是微调，限制一个人在借口和**目标**任务中使用相同的模式或部分。本文提出了一个新的自我监督学习框架，克服了设计和比较不同任务、模型和数据域的局限性。特别是，我们的框架将自我监督模型的结构与最终的特定任务微调模型分离。这使我们能够: 1) 定量评估以前不兼容的模型，包括手工制作的特征;2) 表明更深入的神经网络模型可以从同一借口任务中更好地学习表现;3) 将用深层模型学到的知识传递给更浅的知识，从而促进其学习。我们使用此框架设计了一个新颖的自我监督任务，在 pascal voc 2007、ilsvrc12 和地点的通用基准上实现了最先进的性能。我们学到的功能将通过自我监督学习和监督学习训练的模型之间的 map 差距从 5.9% 缩小到 2.6% 。少

2018 年 5 月 1 日提交;最初宣布 2018 年 5 月。

179. 第 1805 5.00342[pdf,其他] cs. ne

一种用于杂波背景下小目标运动检测的反馈神经网络

作者:王宏新,彭继根,岳世刚

摘要: 小**目标**运动**检测**对于昆虫来说是至关重要的，因为它们可以搜索和跟踪在视野中总是以小模糊斑点的小斑点的配偶或猎物。一类特定的神经元，称为小**目标**运动探测器 (stmd)，其特点是对小目标运动具有敏锐**的**灵敏度。了解和分析 stmd 神经元的视觉路径，有利于设计用于小**目标**运动检测的人工视觉**系统**。反馈回路在视觉神经电路中得到了广泛的识别，在**目标检测**中发挥着重要作用。然而，如果 stmd 视觉通路中存在反馈回路，或者反馈环路可以显著提高 stmd 神经元的**检测**性能，目前还不清楚。本文提出了一种针对自然杂乱背景的小**目标**运动**检测**的反馈神经网络。为了形成反馈回路，模型输出被临时延迟，并作为反馈信号转发到以前的神经层。大量实验表明，与现有的基于 stmd 的小**目标**运动检测模型相比，所提出的反馈神经网络**有**了显著的改进。少

2018 年 7 月 10 日提交;v1 于 2018 年 5 月 1 日提交;最初宣布 2018 年 5 月。

评论:10 页, 5 个数字

180. 第 1804 4.10361[pdf,其他] Cs。简历

基于位置优先学习的网页元素敏感显著模型

作者:张杰,张亚,王燕峰

摘要: 了解人类的视觉注意力对于多媒体应用很重要。许多研究试图从眼动追踪数据中学习，并建立计算显著性预测模型。然而，在网页的显著性预测方面所做的努力有限，网页的特点是内容要素和空间布局更加多样化。本文提出了一种新的 web 页端到端深层生成显著性模型。为了捕获页面布局引入的位置偏差，提出了一个位置优先学习子网络，该子网利用变分自动编码器将位置偏差建模为多元高斯分布。为了对网页的不同元素进行建模，引入了多判别区域**检测**(mdrd) 分支和文本区域**检测**(trd) 分支,**旨在**提取判别本地化和 "突出"可能分别与人类关注相对应的文本区域。我们用公共网页数据集 fiwi 验证了所提出的模型，并表明所提出的模型优于最先进的网页显著性预测模型。少

2018 年 4 月 27 日提交;最初宣布 2018 年 4 月。

评论:15 页, 9 个数字, 2 个标签

181. 第 1804. 10159[pdf,其他] si

滥用嗅探: 自动检测和防御滥用 facebook 朋友

作者:sajedul talukder, bogdan carbunar

摘要: 转化符利用社交网络好友关系从用户那里收集敏感数据，并以包括假新闻、网络欺凌、恶意软件和宣传在内的滥用行为作为攻击他们的目标。例如，在 80 名用户研究参与者中，有 71 人至少有 1 名脸谱朋友，无论是在脸谱还是现实生活中，他们都从未与之互动，或者他们认为这些朋友有可能滥用发布的照片或状态更新，或发布攻击性、虚假或恶意照片内容。我们引入 abusiniff，这是一个识别被视为陌生人或虐待者的 facebook 朋友的系统，并通过不友好、不关注或限制此类朋友访问信息来保护用户。我们开发了一个调查问卷来**检测**被感知到的陌生人和朋友虐待。我们介绍了 facebook 的相互活动功能，并表明他们可以训练监督学习算法来预测调查问卷的反应。我们通过几项用户研究对 AbuSniff 进行了评估，共有来自 25 个国家的 263 名参与者参加了研究。在回答问卷后，参与者同意分别在 91.6 和 91.6 的个案中取消对滥用者的关注和限制，在 92.45% 的个案中，有 92.45% 的个案同意不跟踪和限制滥用者，并在 92.45 宗的个案中，有沙箱或非朋友的非虐待者。在未回答调查问卷的情况下，参与者同意对预计是陌生人或虐待者的朋友采取 abusinff 建议的行动，在 78.2% 的案件中。abusinff 增加了参与者自我报告的拒绝陌生人和虐待者的邀请的意愿，他们对朋友虐待的影响的认识，以及他们认为可以保护免受朋友虐待的感觉。少

2018 年 4 月 26 日提交;最初宣布 2018 年 4 月。

评论:第 12 届国际阿拉伯网络和社交媒体会议 (icwsm-18), 10 页

182. 第 xiv:1804. 09988[pdf] Cs。铬

基于蜜罐的安全方法: 保护在线社交网络免受恶意配置文件的攻击

作者:fatna elmendili, nisrine maqran, younes el bouzekri el idrissi, habiba chaoui

摘要: 近年来，社会网络的快速发展和指数化利用促使社会计算的扩张。在社交网络中，用户通过边缘或链接相互联系, facebook、twitter、linkedin 是最受欢迎的社交网络网站。由于这些网站越来越受欢迎，它们成为网络犯罪和攻击的**目标**。这主要是基于用户如何使用推特等这些网站。攻击者可以轻松地访问和收集个人和敏感用户的信息。用户对安全设置的了解程度较低，也最不关心安全设置。而且他们很容易成为身份侵犯的受害者。为了**检测**恶意用户或假配置文件，不同的技术已被提出像我们的方法，这是基于使用社交蜜罐发现恶意配置文件。在安全研究人员的启发下，该方法使用蜜罐观察和

分析网络中的恶意活动，使用社交蜜罐捕获恶意用户。该方法的两个关键要素是: (1) 部署社交蜜罐，以获取恶意配置文件的信息。(2) 分析这些恶意配置文件的特征以及用于创建分类器的已部署蜜罐的特征，以便筛选现有配置文件并监视新配置文件。少

2018 年 4 月 26 日提交;最初宣布 2018 年 4 月。

评论:7 页 10 图

日记本参考:科学、技术和工程系统研究进展杂志，第 2 卷，第 3 期，198-204 (2017) www.astesj.com 关于工程系统最新进展的特刊

183. 第 1804. 09466[pdf,其他] Cs。简历

模糊监督对象检测的锯齿形学习

作者:张小鹏,冯嘉志,熊洪凯,齐田

文摘: 本文解决了在训练阶段只进行图像级监控的弱监督对象**检测**问题。以前的方法训练**检测**模型与整个图像一次，使模型容易被困在子优化由于引入假阳性的例子。与它们不同的是，我们提出了一个锯齿形学习策略，以同时发现可靠的对象实例，并防止模型过度拟合初始种子。为了实现这一目标，我们首先开发了一个名为 "能量积累分数" (eas) 的标准，以自动测量包含**目标**对象的图像的定位难度并对其进行排名，并据此逐步通过以下方式学习探测器:喂养的例子越来越困难。这样，通过对容易学习的例子进行培训，使模型做好充分准备，从而更有效地获得更强的**检测**能力。此外，我们还在高层卷积地形图上引入了一种新的掩蔽正则化策略，以避免初始样本的过度拟合。这两个模块形成了一个曲折的学习过程，在这个过程中，渐进式学习努力发现可靠的对象实例，而掩蔽正则化增加了正确查找对象实例的难度。我们在 pascal voc 2007 上实现了 48.6% 的 map，大大超过了艺术的现状。少

2018 年 4 月 25 日提交;最初宣布 2018 年 4 月。

评论:被 cvpr 2018 年接受

184. 第 1804. 09352[pdf,其他] cs.PL

基于图形的数据结构的形状中性分析

作者:gregory j. duck, joxan jaffar , roland h. c. yap

摘要: 格式错误的数据结构可能会导致运行时错误，如任意内存访问或损坏。尽管如此，对于低级堆操作程序的数据结构属性的推理仍然具有挑战性。本文提出了一种基于约束的程序分析，该分析检查数据结构的**完整性**，并给出目标数据结构属性，因为堆是由程序操作的。我们的方法是使用**目标**程序中的类型定义自动生成属性的求解器。生成的求解器是使用内置堆、整数和相等求解器的约束处理规则 (chr) 扩展实现的。我们的程序分析的一个关键属性是目标数据结构属性是形状中性的，即分析不会检查与给定数据结构图形形状相关的属性，例如双链接列表与树。然而，分析可以**检测到**各种数据结构中操作程序的错误，包括使用列表、树、dag、图形等的程序。我们提出了一个使用可满足的模块约束处理规则 (smchr) 系统的实现。实验结果表明，我们的方法适用于实际的 c 程序。少

2018 年 5 月 2 日提交;v1 于 2018 年 4 月 25 日提交;最初宣布 2018 年 4 月。

评论:2018 年 7 月 14 日至 17 日在英国牛津举行的第 33 届国际逻辑编程会议 (iclp 2018) 上发表的论文

185. 建议: 1804. 09323[pdf] Cs。简历

基于多帧光流跟踪器的卫星视频目标跟踪

作者:杜波,蔡世汉,陈武,张良培,陶大成

摘要: 目标跟踪是计算机视觉中的一个热门话题。由于甚高分辨率遥感技术的蓬勃发展,现在可以跟踪卫星视频中的兴趣目标. 然而,由于卫星视频中的**目标**通常与整个图像相比太小,与背景也太相似,因此最先进的算法未能用令人满意的精度。由于光学流显示出即使**是目标**轻微运动的巨大潜力,我们提出了一种多帧光流跟踪器 (moft),用于卫星视频中的目标跟踪。将 lukas-kanade 光流法与 hsv 颜色系统和积分图像融合在一起,对卫星视频中的**目标**进行跟踪,同时在光流跟踪器中采用多帧差分法,以获得更好的解释。对三种 vhr 遥感卫星视频数据集进行的实验表明,与最先进的目标跟踪算法相比,该方法能够更准确地跟踪**目标**。少

2018 年 4 月 24 日提交;最初宣布 2018 年 4 月。

186. 建议: 1804. 09[pdf,其他] Cs。CI

seq2seq-vis: 用于序列到序列模型的可视化调试工具

作者:hendrik strobelt, sebastian gehrmann, michael behrisch, adam perer, hanspeter pfister,亚历山大 m.拉什

摘要: 神经序列到序列模型已被证明是准确和稳健的许多序列预测任务,并已成为自动转换文本的标准方法。这些模型在五个阶段的黑匣子过程中工作,该过程涉及将源序列编码到矢量空间,然后解码到新的**目标**序列。这个过程现在是标准的,但和许多深度学习方法一样,仍然很难理解或调试。在这项工作中,我们提出了一个可视化的分析工具,允许在翻译过程的每个阶段与训练有素的序列到序列模型进行交互。目的是确定学习了哪些模式,并**检测**模型错误。我们通过几个真实世界的大规模序列序列使用案例来演示我们的工具的效用。少

2018 年 10 月 16 日提交;v1 于 2018 年 4 月 24 日提交;最初宣布 2018 年 4 月。

评论:vast-ieee vis 2018

187. 第 1804.08910[pdf,其他] Cs。Sd

年龄改变对语音伪装有效性的感知评价

作者:rosa gonzález Hautamäki, anssi kanervisto, ville Hautamäki, tomi kinnunen

摘要: 语音伪装,有目的地修改一个人的扬声器身份,以避免被识别为自己,是一种低努力的方式来愚弄说话人识别,无论是由人执行还是自动使用扬声器验证 (asv) 系统。我们提出了对年龄陈规定型观念作为一种语音伪装战略的有效性的评价,作为我们最近工作的后续行动,在这些工作中, 60 名芬兰语母语者试图听起来像老年人和儿童。在这项研究中,我们提出的证据表明, asv 和人类观察者都很容易错过**目标**发言人,但我们没有解决所呈现的声场时代陈规定型观念有多可信的问题;这项研究有助于填补这一空白。有趣的案例将是那些成功被 asv 系统错过的人,一个典型的听众无法**发现**这是一种伪装。我们进行了一个感性的测试,以研究伪装语音样本的质量。听力测试是在当地进行的,并得到了亚马逊机械土耳其人 (mt) 的帮助。共有 91 名听众参加了测试,并被指示估计发言者的时间顺序和预期年龄。结果表明,女性说话者的预期老年和儿童声音的年龄估计是针对**目标**年龄组的,而男性说话者的年龄估计仅与**目标**声音的方向相对应。老年人的声音。就预定的儿童声音而言,听众估计大多数发言者的男性说话者年龄超过其年龄,而不是预期的**目标**年龄。少

2018 年 5 月 28 日提交;v1 于 2018 年 4 月 24 日提交;最初宣布 2018 年 4 月。

评论:接受《2018 年奥德赛演讲者: 演讲者和语言识别研讨会》

188. 第 xiv:1804. 00719[pdf,其他] si

多伊 10.1109/TKDE.2018.2820010

局部驱动的多样性在有针对性的影响最大化及其在社交网络中的应用

作者:antonio calio , roberto interdonato, chiara pulice, andrea tagarelli

摘要: 关于影响力最大化的研究往往要满足与向特定用户传播信息有关的营销需求。然而，人们很少注意到，信息传播运动的成功不仅可能取决于**要检测的**最初影响者的数量，而且还取决于他们的多样性. 运动。我们的主要假设是，如果我们学习的种子不仅能够影响，而且与更多样化的 (群体) 用户联系在一起，那么影响触发因素也会多样化，因此**目标**用户获得更高的生存机会经营。根据这一直觉，我们定义了一个名为多样性敏感目标影响最大化 (dtim) 的新问题，它假定仅通过利用社交图中的拓扑信息来模拟用户多样性。据我们所知，我们首先将拓扑驱动的多样性概念引入有**针对性**的 im 问题中，为此我们定义了两个备选定义。因此，我们提出了 dtim 的近似解决方案，它**检测出**一组规模 k 的用户，最大限度地发挥对多样性敏感的资本目标函数，为特定的**目标**用户选择。我们根据用户参与在线社交网络的特殊情况来评估我们的 dtim 方法，该案例涉及的用户没有积极参与社区生活。对实际网络的实验评估证明了我们方法的意义，也突出了进一步开发 dtim 应用解决方案的机会。少

2018 年 4 月 20 日提交;最初宣布 2018 年 4 月。

评论:与 ieee 知识与数据工程 (tkde) 交易一起出版。出版日期: 2018 年 3 月 27 日

189. 第 1804. 0781[pdf,其他] Cs。CI

使用端到端内存网络的自动姿态检测

作者:mitra mohtarami, ramy baly, james glass, preslav nakov, lluis marquez, alessandro moschitti

摘要: 我们提出了一个新的端到端内存**网络**的姿态检测，其中 (i) 共同预测文档是否同意、不同意、讨论或与特定**目标**声明无关，并且 (ii) 提取证据片段为该预测。该网络在段落级别运行，并集成卷积和递归神经网络，以及一个相似矩阵作为整体架构的一部分。对虚假新闻挑战数据集的实验评估显示了最先进的性能。少

2018 年 4 月 20 日提交;最初宣布 2018 年 4 月。

评论:naacl-2018;姿态检测;面部检查;准确性;内存网络;神经网络;分布式表示

msc 类: 68t50 类: I.2。7

190. 第: 1804. 07474[pdf,其他] Cs。铬

d 物联网: 一种用于检测受影响的物联网设备的自学习系统

作者:thien duc nguyen, samuel marchal , markus miettinen, n.asokan, ahad-reza sadeghi

摘要: 物联网设备正在被广泛部署。由于不安全的实现和配置，他们中的许多人很容易受到攻击。因此，许多网络已经有了容易破坏的易受攻击的设备。这导致了一个新的类别的恶意软件，专门**针对**物联网设备。现有的入侵**检测**技术在检测受威胁的物联网设备方面并不有效，因为在涉及不同类型的设备和制造商的数量方面，问题的规模巨大。本文介绍了一种有效**检测**受损物联网设备的系统--diot。与以前的工作不同, d 联网使用一种新的自学习方法将设备分类为设备类型，并为每个设备构建正常的通信配置文件，这些配置文件随后可用于**检测**通信模式中的异常偏差。d 联网是完全自主的，可以以分布式众包的方式进行培训，而无需人工干预或标记培训数据。因此，物联网可以应对新

设备类型的出现以及新的攻击。通过使用 30 多台现成物联网设备进行的系统实验，我们证明了 dot 在**检测**受到臭名昭著的米拉伊恶意软件危害的设备方面是有效的 (94% **的检测**率) 和快速 (2 秒)。在实际部署环境中评估时，物联网不会报告任何错误警报。少

2018 年 5 月 11 日提交;v1 于 2018 年 4 月 20 日提交;最初宣布 2018 年 4 月。

评论:18 页, 7 个数字, 9 个表

191. **第 xiv:1804. 07056[pdf,其他] Cs。简历**

现在你看到我了：评估长期视觉跟踪中的性能

作者:alan lukežič, luka cechovin zajc, tomášvojibu, jii matas, matej ksten

摘要: 我们提出了一种新的长期跟踪绩效评估方法，并提出了一个新的具有挑战性的数据集精心挑选的序列与许多**目标**失踪。我们对 6 个长期和 9 个短期最先进的跟踪器进行了广泛的评估，使用新的性能指标，适合评估长期跟踪精度、召回和 f-分数。评价表明，良好的模型更新策略和全图像重新**检测**能力对长期跟踪性能至关重要。我们将该方法集成到 vot 工具包中，以实现实验分析和基准测试的自动化，并促进长期跟踪器的开发。少

2018 年 4 月 19 日提交;最初宣布 2018 年 4 月。

192. **第 1804. 06750[pdf,其他] Cs。铬**

基于 sdn 辅助网络的慢 ddos 攻击缓解

作者:thomas lukaseder, lisa maile, benjamin erb, frank kargl

摘要: 针对网络应用程序的运行缓慢的攻击通常不容易**检测**到，因为攻击者的行为符合规范。许多网络应用程序的服务器没有为此类攻击做好准备，这可能是由于缺少对策，也可能是因为它们的默认配置忽略了此类攻击。保护网络服务免受此类攻击的压力越来越大地从服务运营商转移到受到攻击的服务器的网络运营商。最近的技术，如软件定义的网络，提供了灵活性和可扩展性，可以在**没有目标**操作员帮助的情况下分析和影响网络流。基于我们以前在基于网络的缓解方面的工作，我们扩展了一个框架，以**检测**和缓解网络基础结构中运行缓慢的 ddos 攻击，但不需要访问受到攻击的服务器。我们开发并评估了几种识别方案，仅基于网络流量信息来识别网络中的攻击者。我们表明，通过测量数据包速率和数据包距离的一致性，可以在部署网络的训练期内建立一个可靠的识别器。少

2018 年 4 月 18 日提交;最初宣布 2018 年 4 月。

评论:20 页, 3 个数字，接受安全委员会 18

193. **第 1804. 06732[pdf,其他] cs. ne**

dprd:d. 在深度学习计算中，使典型的激活值变得重要

作者:alberto delmas, sayeh sh 门 fy, patrick judd, kevin siu, milos nikolic, and 列 as moshovos

摘要: 我们表明，在卷积神经网络中为所有值选择固定精度，即使每个层的精度不同，也相当于最坏的情况设计。我们表明，如果我们可以**针对**普通的情况，而不是在比层更精细的粒度上定制精度，那么就可以使用更低的精度。虽然这一观察可能并不奇怪，但迄今为止，没有任何设计在实践中利用它。我们提出动态预测减少 (dpradd)，其中硬件动态检测精度激活需要在一个更精细的粒度**比**整个层。此外，我们使用每个组的相应动态和静态**检测**的精度对激活和权重进行编码，以减少片外和片上的存储和通信。我们

展示了 dprd 与 dprd 条纹 (dprs) 的实际实现，这是一种数据并行硬件加速器，可实时调整精度，以适应其同时处理的激活值。dprs 加速卷积层，并执行未经修改的卷积神经网络。dprs 忽略了芯片外通信，比一组卷积神经网络的固定精度加速器快 2.61x，能效提高 1.84x。我们进一步扩展了 dprs，以利用完全连接层的激活和重量精度。增强的设计分别将平均性能和能效提高了 2.59 x 和 1.19 x，而对于更广泛的神经网络集，固定精度加速器。最后，我们考虑一种成本更低的变种，它只支持即使是精确宽度，从而提供更好的能源效率。考虑到片外通信，dprd 压缩将片外流量平均减少到近 35%，而不是无压缩，从而能够在提高能量的同时，为给定的片外内存接口保持更高的性能效率。少

2018 年 5 月 15 日提交;v1 于 2018 年 4 月 16 日提交;最初宣布 2018 年 4 月。

评论:本文件最初于 2017 年 8 月提交给 hpca-24，随后进行了修订，以包括激励部分。它还于 2017 年 11 月提交给 isca-18。当前版本已更新，以包括外部带宽分析。arxiv 管理说明: 文本与 arxiv:1707. 09068 重叠

194. 第 1804. 05287[pdf,其他] Cs。简历

视频商店: 完全匹配视频中的衣服到在线购物图片

作者:程志琪,吴晓武,刘阳,华贤生

摘要: 近年来，在线零售和视频托管服务都呈指数级增长。在本文中，我们探索了一个新的跨域任务, video2shop，目标匹配的衣服出现在视频中完全相同的项目在网上商店. 提出了一种新的深部神经网络--"不对称网"，对这一问题进行了探讨。对于图像方面，采用建立良好的方法来**检测**和提取任意尺寸的服装补丁的特征。对于视频方面，从每个帧中**检测到的**对象重子中提取深层视觉特征，并进一步输入用于序列建模的长期短期内存 (lstm) 框架，该框架捕获视频中的时间动态。为了实现视频与在线购物图像的精确匹配，在具有可重构深树结构的相似网络下，对表示视频的 lstm 隐藏状态和表示静态对象图像的图像特征进行了联合调制.此外，还提出了一种近似的训练方法，以达到训练时的效率。在大型跨域数据集上进行的大量实验证明了拟议的无古网的有效性和效率，优于最先进的方法。少

2018 年 4 月 14 日提交;最初宣布 2018 年 4 月。

评论:ieee 计算机视觉和模式识别国际会议 (cvpr), 2017

195. 第 xiv:1804. 006604[pdf,其他] Cs。简历

图像中关节注意的发现与应用

作者:daniel harari, joshua b. tenenbaum, shimon ullman

摘要: 关节视觉注意的特点是两个或两个以上的人同时看一个共同**的目标**。能够在场景、相关人员及其共同**目标**中确定共同关注，对于理解社会交往，包括他人的意图和目标至关重要。在这项工作中，我们讨论了联合注意力事件的提取，以及使用这些事件进行图像描述。这部作品有两个新颖的贡献。首先，我们的提取算法是识别单个静态图像中联合视觉注意力的第一个算法。它计算三维凝视方向，通过将凝视方向与为图像计算的三维深度图相结合来识别**凝视目标**，并识别常见的凝视**目标**。其次，我们用人类的研究来证明人类对共同关注的敏感性，这表明在图像中检测这样的配置有助于理解图像，包括物剂及其关节的目标活动，因此可以为图像字幕和相关任务做出贡献。少

2018 年 4 月 10 日提交;最初宣布 2018 年 4 月。

评论:6 页, 3 个数字

196. 第 1804.04273 [pdf,其他] Cs。简历

维生素：通过对抗学习进行病毒跟踪

作者:宋宜兵,马，吴晓河,龚丽君，鲍林超，左王蒙，沈春华，刘瑞生，杨明轩

文摘：检测跟踪框架由两个阶段组成，即在第一阶段围绕**目标**对象绘制样本，并在第二阶段将每个样本分类为**目标**对象或背景。现有的使用深度分类网络的跟踪器的性能受到两个方面的限制。首先，每个帧中的阳性样本在空间上是高度重叠的，它们无法捕获丰富的外观变化。其次，正样本和负样本之间存在着极端的阶级不平衡。本文提出了通过对抗性学习来解决这两个问题的 vital 算法。为了增加阳性样本，我们使用生成网络随机生成掩码，这些掩码用于自适应丢失输入功能，以捕获各种外观变化。通过使用对抗学习，我们的网络识别掩码，在很长的时间跨度内保持**目标**对象最强大的特征。此外，为了解决班级不平衡问题，我们提出了一种高阶成本敏感损失，以减少容易的负样本的影响，方便培训分类网络。对基准数据集的大量实验表明，所提出的跟踪器在最先进的方法下表现良好。少

2018 年 4 月 11 日提交;最初宣布 2018 年 4 月。

评论:cvpr 2018 聚焦

197. 第 1804.04257 [pdf,其他] Cs。CI

仇恨灵戈：基于目标的社交媒体仇恨言论语言分析

作者:mai elsherief, vivek kulkarni, dana nguyen, williamyang wang, elizabeth belding

摘要：虽然社交媒体赋予了言论自由和个人声音的力量，但它也促成了反社会行为、网络骚扰、网络欺凌和仇恨言论。在本文中，我们加深了我们对网络仇恨言论的理解，重点是仇恨言论的一个基本被忽视但至关重要的方面----其**目标**：要么 "针对" 特定的个人或实体，要么 "概括" 于共享共同保护的特性。我们对这两种形式的仇恨言论进行了首次语言和心理语言学分析，并揭示了区分这两种仇恨言论的有趣标记的存在。我们的分析显示，定向仇恨言论，除了更个人化和定向，是更非正式的，愤怒的，往往显着攻击目标 (通过点名) 少分析**词**和更多的词暗示权威和影响。另一方面，普遍仇恨言论以宗教仇恨为主，其特点是使用杀人、消灭和杀戮等致命词语;和数量字，如百万和许多。总之，我们的工作对网络仇恨言论的细微差别进行了数据驱动分析，不仅能够加深对仇恨言论及其社会影响的了解，而且能够发现仇恨言论。少

2018 年 4 月 11 日提交;最初宣布 2018 年 4 月。

评论:10 页，7 个数字。icwsm-2018 年被接受

198. 第 1804.03461 [pdf, ps,其他] si

虚假信息网：谣言、假新闻、骗局、点击诱饵和各种其他申纳尼根

作者:savvas zannettou, michael sirivianos, jeremy blackburn, nicolas kourtellis

摘要：A new era of Information Warfare has arrived. Various actors, including state-sponsored ones, are weaponizing information on Online Social Networks to run false information campaigns with **targeted** manipulation of public opinion on specific topics. These false information campaigns can have dire consequences to the public: mutating their opinions and actions, especially with respect to critical world events like major elections. Evidently, the problem of false information on the Web is a crucial one, and needs increased public awareness, as well as immediate

attention from law enforcement agencies, public institutions, and in particular, the research community. In this paper, we make a step in this direction by providing a taxonomy of the Web's false information ecosystem, comprising various types of false information, actors, and their motives. We report a comprehensive overview of existing research on the false information ecosystem by identifying several lines of work: 1) how the public perceives false information; 2) understanding the propagation of false information; 3) **detecting** and containing false information on the Web; and 4) false information on the political stage. In this work, we pay particular attention to political false information as: 1) it can have dire consequences to the community (e.g., when election results are mutated) and 2) previous work show that this type of false information propagates faster and further when compared to other types of false information. Finally, for each of these lines of work, we report several future research directions that can help us better understand and mitigate the emerging problem of false information dissemination on the Web. △ Less

Submitted 1 October, 2018; v1 submitted 10 April, 2018; originally announced April 2018.

199. arXiv:1804.03124 [pdf, other] cs.CL

Leveraging Intra-User and Inter-User Representation Learning for Automated Hate Speech Detection

Authors: Jing Qian, Mai ElSherief, Elizabeth M. Belding, William Yang Wang

Abstract: Hate speech **detection** is a critical, yet challenging problem in Natural Language Processing (NLP). Despite the existence of numerous studies dedicated to the development of NLP hate speech… ▽ More

Submitted 13 September, 2018; v1 submitted 9 April, 2018;originally announced April 2018.

200. arXiv:1804.02864 [pdf, other] cs.CV

Semantic Edge Detection with Diverse Deep Supervision

Authors: Yun Liu, Ming-Ming Cheng, JiaWang Bian, Le Zhang, Peng-Tao Jiang, Yang Cao

Abstract: Semantic edge **detection** (SED), which aims at jointly extracting edges as well as their category information, has far-reaching applications in domains such as semantic segmentation, object proposal generation, and object recognition. SED naturally requires achieving two distinct supervision… ▽ More

Submitted 9 April, 2018; originally announced April 2018.

201. 第 xiv:1804. 01488[pdf,其他] Cs。铬

使用区块链开发 k-ary 恶意软件

作者:joanna moubarak, eric filiol, maroun chamoun

摘要: 如今，网络攻击正在迅速发展。它们是自定义的、多矢量的、在多个流中暂存的，并且**是有针对性**的。此外，新的黑客攻击游乐场似乎到达了移动网络、现代建筑和智慧城市。为此，恶意软件使用不同的入口点和插件。此外，他们目前正在部署几种用于混淆、伪装和分析阻力的技术。另一方面，抗病毒保护正在定位创新方法，暴露恶意指标和异常，揭示抗病毒机制的局限性的假设。本文首先介绍了计算机病毒学的最新发展现状，然后引入了基于区块链技术创建无法检测到的恶意软件的新概念。它总结了恶意软件为避免用于病毒**检测**而采用的技术，并介绍了利用区块链网络的新病毒技术的实现。少

2018 年 4 月 4 日提交;最初宣布 2018 年 4 月。

评论:作为 2018 年 4 月在台湾举行的 ieeeeifip man2block 会议的海报，提供 6 页, 6 位数字，扩展版

202. 第十四条: 1804. 01472[pdf,其他] Cs。铬

电网运动目标防御的成本效益分析

作者:subhash lakshminarayana, david k. y. yau

文摘: 我们研究了运动**目标**防御 (mtd)，它主动干扰输电线路反应，以阻止对电网状态估计的隐蔽虚假数据注入 (fdi) 攻击。此前关于这个主题的工作已经提出了基于随机选择的电抗扰动的 mtd，但这些扰动不能保证有效的攻击**检测**。为了解决这个问题，我们提出了正式的设计标准来选择真正有效的 mtd 电抗扰动。然而，基于关键的最佳潮流 (opf) 公式，我们发现有效的 mtd 可能会产生一个不重要的操作成本，而这一点迄今尚未受到关注。因此，我们描述了 mtd 检测能力与其相关所需成本之间的重要权衡。广泛的仿真，利用 matpower 模拟器和基准 ieee 总线系统，验证和说明了所提出的设计方法，首次解决了 mtd 的成本和有效性的关键方面。少

2018 年 4 月 4 日提交;最初宣布 2018 年 4 月。

评论:可信赖的系统和网络国际会议 (dsn)-2018 年

203. 第十四条: 1804. 01468[pdf,其他] Cs。镍

p4k:p4 和应用的形式化语义

作者:ali kheradmand , grigore rosu

摘要: 可编程分组处理器和 p4 作为此类设备的编程语言已获得极大的兴趣，因为它们的灵活性使各种应用能够快速发展，这些应用以线速工作。但是，这种灵活性，再加上设备和网络的复杂性，增加了引入难以手动发现的细微错误的机会。更糟糕的是，这是一个错误可能会带来灾难性后果的领域，但 p4 程序/网络的正式分析工具却缺失。我们认为，正式的分析工具必须基于**目标**语言的正式语义，而不是其非正式的规范。为此，我们在 k 框架中提供了 p4 语言的可执行形式语义。基于此语义, k 提供了解释器和各种分析工具，包括一个符号模型检查器和一个 p4 的演绎程序验证器。本文概述了 p4 的正式 k 语义，以及我们在形式化过程中发现的几个 p4 语言设计问题。我们还讨论了 k 为 p4 程序员和网络管理员以及语言设计人员和编译器开发人员提供的工具所产生的一些应用程序，如**检测**不可移植的代码、p4 程序的状态空间探索和网络，使用符号执行的错误查找，数据平面验证，程序验证，和翻译验证。少

2018 年 4 月 4 日提交;最初宣布 2018 年 4 月。

204. 第 xiv:1804. 01226[pdf,其他] Cs。操作系统

多伊10.114/3192366. 323380

ireplayer: 多线程应用程序的就地和相同的记录和重播

作者:刘宏宇, sam silvestro, wei wang, chen tian, 刘同平

摘要: 由于许多内在和外部的非确定性因素，复制多线程程序的执行非常具有挑战性。现有的 rr 系统在性能开销方面取得了重大进展，但没有**一个系统**针对现场设置，在现场设置中，重播发生在与记录过程相同的过程中。此外，大多数现有的工作不能实现相同的重播，这可能会阻止复制一些错误。本文介绍了 ireplayer，其目的是在原始过程中 (在 "就地" 设置下) 相同地重播多线程程序。ireplayer 的新颖原位和相同的重播使其更有可能重现错误，并允许它直接使用调试机制 (例如观察点) 来帮助故障诊断。目前, ireplayer 平均只产生 3% 的性能开销，这使得它始终可以在生产环境中启用。ireplayer 提供了一系列可能性，本文提供了三个示例:**两个用于检测**缓冲区溢出和使用后无 bug 的自动工具，以及一个与 gdb 集成的交互式调试工具。少

2018 年 4 月 3 日提交;最初宣布 2018 年 4 月。

评论:16 页, 5 个数字，将在 pldi18 出版

205. 第 1804.00777[pdf,其他] Cs。简历

dock: 通过传输常识知识来检测对象

作者:krishna kumar singh, santosh divvala, ali farhadi, yong jae lee

摘要: 我们提出了一种通过将常识知识 (dock) 从源类别转移到**目标**类别来**检测**对象的可扩展方法。在我们的设置中，源类别的培训数据具有边界框批注，而**目标**类别的培训数据仅具有图像级批注。目前最先进的方法侧重于图像级的视觉或语义相似性，以使在源类别上训练的探测器适应新的**目标**类别。相反，我们的关键思想是 (i) 不在图像级别使用相似性，而是在区域级别使用相似性，以及 (ii) 利用更丰富的常识性 (基于属性、空间等) 来指导算法学习正确**的检测.**我们从现成的知识库中自动获得这样的常识性提示，而无需任何额外的人力努力。在具有挑战性的 ms coco 数据集上，我们发现常识性知识可以显著提高现有传输学习基线的**检测**性能。少

2018 年 7 月 31 日提交;v1 于 2018 年 4 月 3 日提交;最初宣布 2018 年 4 月。

日记本参考:eccv, 2018

206. 第 xiv:18004.0002[pdf,其他] Cs。直流

rolp: 大数据内存管理的运行时对象生存期分析

作者:rodgo bruno, duarte Patrício, josésimo, Patrício veiga, paulo ferreira

摘要: 低延迟服务 (如信用卡欺诈**检测**和网站**定向**广告) 依赖于大数据平台 (例如 lucene、graphchi、cassandra)，这些平台在内存管理的运行时 (如 jvm) 之上运行。但是，由于内存管理决策不足 (例如，将生存期非常不同的对象彼此分配，导致内存碎片化)，这些平台的暂停时间可能会变得不可预测且令人无法接受。这将导致长时间和频繁的应用程序暂停时间，破坏服务级别协议 (sla)。这个问题已经被发现，结果显示，当前的内存管理技术不适合保存在内存中的大量中长寿命对象的应用程序 (大数据的范围就是这种情况应用)。以前的工作试图通过在堆外或在特殊分配区域中分配对象来减少此类应用程序的暂停，从而减轻内存管理的压力。但是，所有这些解决方案都需要程序员的努力和知识、源代码访问或离线分析的组合，这对程序员的工作效率和/或应用程序性能产生了明显的负面影响。本文介绍了运行时对象生存期分析系统 rolp。rop 配置文件应用程序代码在运行时，以确定哪些分配上下文创建具有中长生存期的对象，因为此类对象需要以不同的方式处理 (对于短期对象)。此分析信息极大地改善了内存管理决策，导致 lucene 的长尾延迟减少 51%, graphchi 减少 85%, cassandra 减

少 60%，吞吐量和内存开销可以忽略不计。rop 是为 openjdk8 热点 jvm 实现的，它不需要任何程序员的努力或源代码访问。少

2018 年 3 月 9 日提交;最初宣布 2018 年 4 月。

207. 第 xiv:1804.00540[pdf,其他] Cs。CI

英语语言中自动语法检查的系统研究

作者:madhvi soni, jitendra singh thakur

摘要: 语法检查是对文本中语法错误进行**检测**和纠正的任务。英语是科学和技术领域的主导语言。因此，非英语母语的人在阅读、写作或口语时必须能够使用正确的英语语法。这就产生了自动语法检查工具的需要。迄今为止，已经提出并实施了许多办法。但在过去十年中，在调查文献方面所做的努力较少。这一系统审查的目的是审查现有文献，突出当前的问题，并提出今后研究的潜在方向。本系统综述是对在设计搜索策略以选择网络上的论文后获得的 12 项初步研究进行分析的结果。我们还提出了一个可能的语法错误分类方案。在主要观察中，我们发现实时应用程序缺乏高效、可靠的语法检查工具。我们提出了几个有用的插图-最突出的是原理图，我们提供了每种方法和一个表，总结这些方法沿不同的维度，如**目标**错误类型，使用的语言数据集,该方法的优势和局限性。这有助于更好地理解、比较和评价以前的研究。少

2018 年 3 月 29 日提交;最初宣布 2018 年 4 月。

评论:23 页

208. 第 xiv:1204.00776[pdf,其他] Cs。简历

人员搜索的端到端检测和重新识别集成网络

作者:何振伟,张磊,魏佳

文摘: 本文提出了一种端到端学习框架下的行人**检测**和重新识别（重新识别）集成网(i-net)。i-net 用于真实世界的视频监控场景，在这些场景中，需要在整个场景视频中搜索**目标**人员，而行人边界框的注释则不可用。通过与作为联合**检测**和重新识别的 oim 相比，我们有三个不同的贡献。首先，我们介绍了 i-net 的暹罗体系结构，而不是 1 流，这样就可以实现验证任务。其次，提出了一种新的在线配对损耗（olp）和硬实例优先软最大损失（hep），使损失计算中只对硬底片引起了极大的关注。第三，在 i-net 中设计了一个负样本存储在线词典，但不对阳性样本进行了记录。我们在人员搜索数据集上显示我们的结果,**缩小了检测**和重新识别之间的差距。可实现卓越的性能。少

2018 年 4 月 1 日提交;最初宣布 2018 年 4 月。

209. 第 xiv:1803 3.11365[pdf,其他] Cs。简历

通过逐行域适应进行跨域弱监管对象检测

作者:naoto inoue, ryosuke furuta, toshihiko yamasaki, kiyoharu aizawa

摘要: 我们是否可以在没有实例级注释的情况下**检测**各种图像域中的公共对象？本文提出了一个新任务--跨域弱监督对象检测的框架,解决了这一问题。对于本文，我们可以访问源域中具有实例级批注的图像（例如，自然图像）和**目标**域中具有图像级批注的图像（例如，水彩）。此外，要在**目标**域中**检测到**的类是源域中的所有类或子集。从在源域上预先训练的完全受监督的对象检测器开始，我们提出了一种两步递进域适应技术，对两种类型的人工和自动生成的样本的检测器进行微调。我们在包含三个图像域的新收集的数据集上测试我们的方法，并在平均平均精度（map）方面与性能最佳的基线相比，实现了大约 5 至 20 个百分点的改进。少

2018 年 3 月 30 日提交;最初宣布 2018 年 3 月。

评论:将出现在 cvpr2018 (海报) 上，包括补充材料

210. 第 1803.11254[pdf,其他] 反渗透委员会

使用机器学习技术和 2d 范围数据检测、定位和跟踪托盘

作者:ihab s. mohamed, alessio capitanelli, fulvio mastrogiovanni, Stefano roovetta, renato zacaria

摘要: 工业环境中的自主运输问题正受到新的关注，因为它可以彻底改变内部物流，特别是在非结构化环境中。本文提出了一种新的架构，允许机器人使用基于机载 2d 激光测距仪的机器学习技术检测、定位和跟踪多个托盘。该体系结构由两个主要部分组成:第一阶段是采用具有 cnn 分类器的更快的基于区域的卷积神经网络 (r-cnn) 检测器的托盘检测器;第二阶段是用于定位和跟踪**检测到的**托盘的卡尔曼滤波器，我们还使用它来推迟对第一步**检测到**的托盘的承诺，直到通过顺序数据采集获得足够的信心过程。为了微调 cnn，使用包含 340 个标记的 2d 扫描的真实世界数据集对该体系结构进行了系统评估，这些扫描已在在线存储库中免费提供。**检测**性能是根据 k 倍交叉验证的平均精度进行评估的，在我们的测试中得分为 99.58。关于托盘的定位和跟踪，已经进行了实验，在一个场景中，机器人接近托盘到叉子。虽然最初只需考虑一个托盘就能获得数据，但也生成了人工数据，以模拟机器人工作空间中存在多个**目标**的情况。我们的实验结果证实，该系统能够识别、定位和跟踪托盘，成功率很高，同时对误报具有鲁棒性。少

2018 年 3 月 29 日提交;最初宣布 2018 年 3 月。

评论:本文已提交给神经计算和应用 (ncaa).

msc 类: 68t40

211. 第 xiv:1803.11175[pdf,其他] Cs。Cl

通用句子编码器

作者:daniel cer, yinfei yang, shen-yi kong, nan hua, nicole limtiaco, rhomnist. john, noah, mario guajardo-cst 佩 des, steve yuan,chris tar, yy-hsuansung, brian st 横, ray kurzweil

摘要: 我们提出了将句子编码为嵌入向量的模型，这些向量专门**针对**其他 nlp 任务的转移学习。这些模型是高效的，可在不同的传输任务中获得准确的性能。编码模型的两个变体允许在准确性和计算资源之间进行权衡。对于这两种变体，我们都会调查并报告模型复杂性、资源消耗、传输任务培训数据的可用性和任务性能之间的关系。与使用通过预先训练的单词嵌入进行的单词级别迁移学习的基线进行比较，并且基线不使用任何转移学习。我们发现，使用句子嵌入的转移学习往往优于单词级转移。通过句子嵌入进行迁移学习，我们观察到了惊人的良好性能，为转移任务提供了最少数量的监督训练数据。我们在**针对检测**模型偏差的单词嵌入关联测试 (weat) 上获得了令人鼓舞的结果。我们预先训练的句子编码模型可免费下载和在 tf 集线器上使用。少

2018 年 4 月 12 日提交;v1 于 2018 年 3 月 29 日提交;最初宣布 2018 年 3 月。

评论:7 页; 清单 1 中的固定模块 url

212. 第 xiv:1803.09733[pdf, ps,其他] Cs。Lg

域传输卷积属性嵌入

作者:苏芳,王景燕

文摘: 本文研究了利用属性数据进行迁移学习的问题。在转移学习问题中，我们希望利用辅助域和**目标**域的数据，为**目标**域中的分类问题建立一个有效的模型。同时，属性在不同的领域自然是稳定的。这强烈的动机，我们学习有效的领域转让属性表示。为此，我们建议利用强大的卷积神经网络 (cnn) 模型，将数据的属性嵌入到一个公共空间中。数据点的卷积表示形式映射到相应的属性，以便它们能够有效地嵌入属性。我们还通过一个独立领域的 cnn，蚂蚁一个特定领域的 cnn 来表示不同领域的数据，并将它们的输出与属性嵌入结合起来，建立分类模型。构建了一个联合学习框架，以最大限度地减少不同域的分类误差、属性映射误差、独立表示的不匹配，并鼓励邻域平滑度。**表示.** 利用一种基于梯度下降的迭代算法求解最小化问题。通过对人的再识别、破产预测和垃圾邮件**检测**等基准数据集的实验，验证了该方法的有效性。少

2018 年 4 月 1 日提交;v1 于 2018 年 3 月 26 日提交;最初宣布 2018 年 3 月。

213. 第 xiv:1800.9659[pdf,其他] Cs。简历

一种多层反向传播显著性检测算法及其应用

作者:朱春标,葛丽

摘要: 唾液**检测**是多媒体领域的一个活跃课题。以往大多数关于显著性**检测**的工作都集中在二维图像上。但是，对于包含多个对象或复杂背景的复杂场景，这些方法并不可靠。最近，深度信息为显著**性检测**提供了强大的线索。本文提出了一种基于深度挖掘的多层反向传播显著**性检测**算法，利用三层不同图像的深度提示。该算法具有良好的性能，在复杂情况下保持了鲁棒性。实验结果表明，该框架优于现有的其他显著性方法。此外，我们还给出了该算法的两个创新应用，即从多个图像中重建场景和视频**中**的小**目标**目标目标检测。少

2018 年 3 月 26 日提交;最初宣布 2018 年 3 月。

评论:发布版本可以在 https://link.springer.com/article/10.1007/s11042-018-5780-4 下载。源代码可以在 https://github.com/ChunbiaoZhu/CAIP2017 下载

214. 第 xiv:1803. 09668[pdf,其他] Cs。Lg

针对人工神经网络的无剪切攻击

作者:boussad addad, jerome kdjabachian , christophe meyer

摘要: 在过去的几年里，由于人工深层神经网络在计算机视觉、自然语言处理、语音识别、恶意软件**等许多机器学习任务中取得了巨大的成功，在人工智能领域取得了显著突破检测**等。然而，它们极易受到容易制作的对抗性例子的影响。许多调查都指出了这一事实，并提出了不同的方法来制造攻击，同时对原始数据增加有限的扰动。到目前为止，已知的最可靠的方法是所谓的 c & amp; w 攻击 [1]。尽管如此，一个被称为功能挤压加上整体防御的对策表明，这些攻击的大部分可以被摧毁 [6]。在本文中，我们提出了一种新的方法，我们称之为中心初始攻击 (cia)，其优点是双重的: 首先，它通过构造确保最大扰动小于事先固定的阈值，而不降低的裁剪过程攻击的质量。其次，它对最近引入的防御措施 (如功能压缩、jpeg 编码，甚至针对投票组合的防御) 都是稳健的。虽然它的应用并不局限于图像，但我们使用 imagenet 数据集上当前最好的五个分类器来说明这一点，其中两个是针对攻击的强健进行的对手重新训练。在任何像素上的固定最大扰动仅为 1.5%，大约 80% 的攻击 (**有针对性**) 愚弄投票合奏防御，当扰动只有 6% 时，几乎 100% 的攻击。虽然这表明了抵御中情局攻击是多么困难，但本文的最后一节给出了一些限制其影响的指导方针。少

2018 年 3 月 28 日提交;v1 于 2018 年 3 月 26 日提交;最初宣布 2018 年 3 月。

评论:12 页

215. 第 xiv:1803 09043[pdf, ps,其他] Cs。毫米

基于 cnn 的图像隐写术中的微对抗性嵌入式最小变化

作者:唐伟轩,李斌,谭顺泉,毛罗·巴尔尼, 黄继武

摘要: 从历史上看, 隐写方案的设计是为了保存图像统计或隐写特征。由于大多数最先进的隐式方法都采用基于机器学习 (ml) 的分类器, 因此可以通过欺骗 ml 分类器来考虑对抗隐身分析。然而, 简单地将摄动应用于 stego 图像作为对抗示例, 可能会导致数据提取失败, 并引入其他分类器**检测到**的意外人工制品。本文提出了一种新的隐藏式方法--对抗嵌入, 实现了隐藏 stego 信息的目的, 同时愚弄了一个基于卷积神经网络 (cnn) 的隐式分析仪。该方法适用于传统的畸变最小化框架。根据攻击**所针对**的 cnn 分类器的渐变反传播, 调整图像元素修改的成本, 实现了对抗性嵌入。因此, 修改方向具有与渐变符号相同的更高概率。这样, 就产生了所谓的对抗性 stego 图像。实验表明, 所提出的隐写方案对**目标**对手不知道的隐式分析仪是安全的。此外, 它还恶化了其他具有对抗性的隐式分析仪的性能, 为能够克服强大的 cnn 型隐形分析的新型现代隐写方法开辟了道路。少

2018 年 3 月 23 日提交;最初宣布 2018 年 3 月。

评论:提交给 ieee 信息取证和安全事务

216. 第 1803.08983[pdf, ps,其他] Cs。Cl

上下文外错误的自动评估

作者:patrick huber, jan niy 色调, alex waibel

文摘: 提出了一种利用上下文外错误**检测**的方法来评估文本理解任务的计算模型的新方法。通过我们自动化修改过程的新颖设计, 现有的大规模数据源可以被大量的文本理解任务所采用。因此, 数据在语义层面上进行了修改, 允许对模型进行测试, 以应对一组具有挑战性的修改后的文本段落, 这些段落需要包含更广泛的叙事话语。我们新引入的任务通过插入真实的非上下文错误来**解决**转录和翻译系统的实际实际问题。自动修改过程适用于 2016 年 tedtalk 语料库。通过完全自动化流程, 可以以低成本采用完整的数据集, 从而促进监督学习过程和更深入的网络进行培训和测试。为了评价修改算法的质量, 在修改后的数据集上对语言模型和监督二进制分类模型进行了训练和测试。对人类基线评价进行了审查, 以将结果与人类表现进行比较。评估任务的结果表明, 很难**检测**机器学习算法和人的语义错误, 这表明, 当只限于一个句子时, 这些错误是无法识别的。少

2018 年 3 月 23 日提交;最初宣布 2018 年 3 月。

评论:lrec 2018, 5 页, 上下文外错误识别, 自动评估数据集, 文本理解, tedtalk

217. 第 1803.08910[pdf, ps,其他] Cs。Cl

推特上的姿态检测: 一种基于 svm 的方法

作者:dilek küçük, fazli can

摘要: 姿态**检测**是情绪分析的一个子问题, 探讨了某一特定**目标**的自然语言文本作者的立场 (要么在文本中明确说明, 要么没有明确说明)。立场输出通常被给作为赞成、反对或不。在本文中, 我们**针对**与体育相关的推特上的姿态**检测**, 并在此类推特上介绍了基于 svm 的姿态分类器的性能结果。首先, 我们描述了三个版本的我们专有的推特数据集附加的立场信息, 所有这些都是公开提供的研究目的。接下来, 我们使用不同的功

能集对此数据集的姿态**检测**来评估 svm 分类器。所使用的功能基于非迁移项、bigrams、哈希标签、外部链接、表情符号以及最后命名的实体。结果表明，支持向量机分类器联合使用基于 unigrams、hashtags 和命名实体的功能是解决体育相关推特位置**检测**问题的一种可行方法。少

2018 年 3 月 23 日提交;最初宣布 2018 年 3 月。

评论:13 页

218. 第 1803.08359[pdf,其他] Cs。铬

在故障攻击存在的情况下保护条件分支

作者:robert schilling, mario werner , stefan manchard

摘要: 在典型的软件中，许多比较和随后的分支操作在安全性方面非常关键。示例包括密码检查、签名检查、安全启动和用户权限检查。对于嵌入式设备，这些安全关键分支是故障攻击的首选**目标**，因为单个位翻转或跳过单个指令可能会导致对系统的完全访问。过去，为了提供控制流完整性 (cfi) 并对处理后的数据进行错误**检测**，提出了许多冗余方案。但是，目前通用软件的对策并不为有条件分支提供保护机制。因此，关键分支在实践中往往只是重复。我们提出了一种保护条件分支的通用方法，该方法将基于编码的比较结果与 cfi 保护机制的冗余联系起来。该方法可用于所有类型的数据编码和 cfi 机制，并在条件分支的所有步骤中保持其错误**检测**能力。我们通过实现基于 an-code 的编码比较来演示我们的方法，该方法是一种常用的编码方案，用于**检测**算术运算过程中的数据错误。我们扩展了 llvm 编译器，以便标准代码和条件分支可以自动保护并分析其安全性。我们的设计表明，在大小和运行时方面的开销低于最先进的复制方案。少

2018 年 3 月 22 日提交;最初宣布 2018 年 3 月。

评论:2018 年 5 月接受

219. 第 1803.08319[pdf,其他] Cs。简历

学习在虚拟世界中检测和跟踪可见和闭塞的身体关节

作者:matteo fabbri, fabio lanzi, simone calderara, andrea palazzi, roberto vezzani, rita cucchiara

摘要: 在开放世界环境中的多人跟踪需要在精确**检测**方面做出特殊的努力。此外，当场景杂乱引入了遮挡**目标**的挑战性问题时,**检测**阶段的时间连续性变得越来越重要。为此，我们提出了一个深入的网络体系结构，该体系结构可以共同提取人的身体部位，并将其联系在较短的时间范围内。我们的模型通过产生不可见关节的可信解，明确地处理被闭塞的身体部位。我们提出了一个新的端到端架构，由四个分支 (可见热图、遮挡热图、部分亲和力场和时间亲和力场) 组成，由时间链接器特征提取器提供支持。为了克服监控数据的缺乏与跟踪，身体部分和遮挡注释，我们创建了最广阔的计算机图形数据集，为人们跟踪在城市场景中利用照片逼真的视频游戏。到目前为止，它是人类身体部位中最丰富的数据集 (约 50 万帧，近 1, 000 万个身体姿势)，供人们在城市场景中跟踪。我们在虚拟数据方面接受过培训的架构在图像分辨率和清晰度足够高的情况下，也表现出良好的泛化能力，从而产生了可靠的跟踪，可用于进一步的批处理数据关联或重新编码模块。少

2018 年 9 月 18 日提交;v1 于 2018 年 3 月 22 日提交;最初宣布 2018 年 3 月。

评论:2018 年 eccv 会议接受

220. 决议: 1803.07268[pdf,其他] Cs。简历

学习用于目标跟踪的动态内存网络

作者:杨天宇,陈天丽 b.

摘要: 用于视觉跟踪的模板匹配方法由于其具有可比的性能和较快的速度，近年来越来越受欢迎。然而，它们缺乏有效的方法来适应**目标**物体外观的变化，使它们的跟踪精度与最先进的距离仍然很远。在本文中，我们提出了一个动态内存网络，以适应目标在跟踪过程中**的**外观变化。lstm 用作内存控制器，其中输入是搜索要素映射，输出是内存块读取和写入过程的控制信号。由于在搜索要素图中,**目标**的位置最初是未知的，因此采用了一种注意机制，将 lstm 输入集中在潜在**目标上**。为了防止积极的模型适应性,我们应用门控剩余模板学习来控制与初始模板结合使用的检索内存量。与逐行**可检测**方法不同，在这种方法中，对象的信息由神经网络的权重参数维护，这需要昂贵的在线微调才能适应，我们的跟踪器完全向前运行，并适应**通过**更新外部内存更改目标的外观。此外，与其他跟踪方法不同的是，模型容量在离线训练后是固定的--我们的跟踪器的容量可以很容易地随着任务的内存要求的增加而扩大，这有利于记忆长期对象信息。在 otb 和 vot 上进行的大量实验表明，我们的跟踪器 memtrack 在最先进的跟踪方法上表现良好，同时保持 50 fps 的实时速度。少

2018 年 9 月 2 日提交;v1 于 2018 年 3 月 20 日提交;最初宣布 2018 年 3 月。

评论:eccv2018 相机准备就绪。代码可在 https://github.com/skyoung/MemTrack

221. 第 xiv: 180006605[pdf,其他] Cs。Lg

tbd: 深度神经网络培训的标杆与分析

作者:朱宏宇, mohamed akrout, bojian zheng, andrew pelegris, amar phanishayee, bianca schroeder, gennady pekhimenko

摘要: 近年来，深部神经网络 (dnn) 的普及，对有效地进行 dnn 相关计算产生了很大的研究兴趣。然而，主要重点通常非常狭窄，仅限于 (一) 推断----即如何有效执行已经训练过的模型, (二) 图像分类网络作为评价的主要基准。我们在这项工作中的主要目标是打破这种短视的观点，通过 (i) 提出一个新的 dnn 培训基准，称为 tbd (tbd 是 dnn 的培训基准的简称)，使用一套具有代表性的 dnn 模型，涵盖广泛的机器学习应用: 图像分类、机器翻译、语音识别、目标**检测**、对抗网络、强化学习，以及 (ii) 通过对三个主要领域的这些不同应用进行广泛的性能分析跨不同硬件配置 (单 gpu、多 gpu 和多机) 的深度学习框架 (ensorflow、mxnet、cntk)。tbd 目前涵盖六个主要应用领域和八个不同的最先进的模型。我们为这些模型提供了一个新的性能分析工具链,该工具结合**了现有**性能分析工具的目标使用、仔细选择新的和现有的度量标准和方法来分析结果以及 dnn 训练的领域特定特征。我们还在所有三个主要框架中构建了一组用于内存分析的新工具;急需的工具，最终可以阐明 dnn 培训中不同数据结构 (权重、激活、渐变、工作区) 消耗了多少内存。通过使用我们的工具和方法，我们就 dnn 培训的未来研究和优化应集中在哪里提出了一些重要的意见和建议。少

2018 年 4 月 13 日提交;v1 于 2018 年 3 月 16 日提交;最初宣布 2018 年 3 月。

222. 建议: 18006798[pdf,其他] Cs。简历

野生动物图像中对象变形的关注

作者:陈新元,徐昌,杨晓康,陶大成

文摘: 本文研究了野生图像中的物体变形问题。经典的物体变形的生成网络往往承担着双重责任: 检测利益对象,**将**对象从源域转换为**目标**域。相反，我们将生成网络分解为

两个分离网络，每个网络只专用于一个特定的子任务。关注网络预测图像的空间注意力图，转换网络的重点是翻译对象。鼓励关注网络制作的注意地图稀疏，以便对利益对象给予主要关注。无论在物体变形之前或之后，注意图都应保持不变。此外，考虑到图像的可用分割注释，学习关注网络可以收到更多的指令。实验结果表明，研究物体变形过程中的注意事项是必要的，该算法可以准确地学习注意力，提高生成图像的质量。少

2018 年 3 月 19 日提交;最初宣布 2018 年 3 月。

223. 第 1803.06121 [pdf,其他] 反渗透委员会

复杂城市激光雷达数据集

作者:jeong jyong, young-gun cho, young-sik shin, hyunchul roh, ayoung kim

文摘: 本文提出了**一种针对**复杂城市环境的光**探测**和测距 (lidar) 数据集。高层建筑和交通拥堵的城市环境对许多机器人应用构成了重大挑战。所提供的数据集是独特的，因为它能够捕捉城市环境的真正特征 (例如大都市地区、大型建筑综合体和地下停车场)。数据集中提供了二维 (2d) 和三维 (3d) lidar 的数据，它们是 lidar 传感器的典型类型。两个 16 射线 3d lidars 在两侧倾斜，以获得最大覆盖。一个 2d 激光雷达向后面对，而另一个正面是向前收集道路和建筑物的数据。来自光纤陀螺仪 (fog)、惯性测量单元 (imu) 和全球定位系统 (gps) 的原始传感器数据以文件格式呈现，用于车辆姿态估计。应用图形同步定位和映射 (slam) 算法，给出了估计为 100 赫兹的车辆姿态信息。为了便于开发，机器人操作系统 (ros) 环境中的文件播放器和数据查看器也通过网页发布。完整的数据集可在: http://irap.kaist.ac.kr/dataset。在本网站中，使用 webgl 提供每个数据集的 3d 预览。少

2018 年 3 月 16 日提交;最初宣布 2018 年 3 月。

评论:被接受参加 icra2018

224. 第 xiv:1800 5845 [pdf,其他] Cs。简历

一种用于视觉跟踪的结构相关滤波器与多任务高斯粒子滤波器的结合

作者:戴曼娜,程淑英,何祥建,王大东

摘要: 本文提出了一种新的结构相关滤波器，该滤波器与多任务高斯粒子滤波器 (kcf-gpf) 模型相结合，用于鲁棒视觉跟踪。我们首先提出了一个组装结构，其中几个 kcf 跟踪器作为弱专家提供了一个初步的决定，高斯粒子滤波器作出最终的决定。该方法旨在利用和补充 kcf 和高斯粒子滤波器的强度。与现有的基于相关滤波器或粒子滤波器的跟踪方法相比，该跟踪器具有一些优点。首先，它可以通过弱 kcf 跟踪器在大规模搜索范围内**检测**跟踪目标，并评估高斯粒子滤波器做出强决策的弱跟踪器 \ rq 决策的可靠性，从而快速处理运动、外观变化、遮挡和重新**检测**。其次，它可以通过高斯粒子滤波器有效地处理大规模的变化。第三，它可以在不重新采样的情况下使用重要性采样完全并行实现，从而方便了 vlsi 的实现，降低了计算成本。在包含 50 个具有挑战性序列的 otb-2013 数据集上进行的大量实验表明，该算法在 16 个最先进的跟踪器上表现良好。少

2018 年 3 月 3 日提交;最初宣布 2018 年 3 月。

评论:10 页. arxiv 管理说明: 文本与 arxiv:170005020 的文本重叠由其他作者

225. 建议: 18005482 [pdf,其他] Cs。简历

遥感图像中的目标变化检测

作者:vladimir ignatiev，亚历克谢·特雷金, viktorlobachev, georgy potapov, evgeny burnaev

文摘: 遥感系统和图像处理的最新发展使得有可能提出一种新的方法，对卫星地球图像系列的具体变化进行物体分类和**探测**(所谓**的目标**)更改**检测**)。本文提出了一种形式化的问题陈述，可以有效地利用深度学习方法来分析遥感图像的时间依赖性序列。我们还介绍了一个新的框架，用于**开发用于有针对性**的更改**检测的**深度学习模型，并演示了它可以用于的一些业务应用程序案例。少

2018 年 3 月 14 日提交;最初宣布 2018 年 3 月。

评论:10 页, 1 个数字, 1 个表

226. 第 xiv:1803. 04856[pdf,其他] Cs。哦

一种综合广域空中监视图像的生成系统

作者:elias j griffith, chinmaya mishra, jason f. ralph, simon maskell

摘要: 航空持久性监视 (ps) 算法的开发、基准测试和验证需要访问专门的广域空中监视 (waas) 数据集。这类数据集很难获得，而且在空间分辨率和时间持续时间方面往往非常大。本文概述了一种复杂城市环境的模拟方法，并演示了使用这种方法生成模拟传感器数据的可行性，这与使用广域成像系统进行监视和侦察应用。这为生成车辆跟踪算法和异常**检测**方法的数据集提供了一种经济高效的方法。该系统将城市交通仿真模拟器 (sumo) 与 matlab 控制器和图像生成器融合在一起，创建包含跨城市大区域不间断的门到门行程的场景。这种 "生命模式" 方法提供了具有自然运动和交通流的三维视觉信息。然后，这可用于提供模拟传感器测量 (例如视觉波段和红外视频图像)，并自动访问地面真相数据，以评估多**目标**跟踪系统。少

2018 年 3 月 13 日提交;最初宣布 2018 年 3 月。

评论:v1 (可用于模拟建模实践和理论中的发布)

227. 第 xiv:180004610[pdf,其他] Cs。简历

目标驱动的实例检测

作者:phil ammirato, cheng yangfu, mykhailo shvets, jana kosecka,亚历山大 c. berg

摘要: 虽然最先进的通用对象探测器越来越好，但没有多少系统是专门为利用实例**检测**问题而设计的。对于许多应用，如家用机器人，系统可能需要一次识别几个非常具体的实例。速度在这些应用程序中可能至关重要，识别以前看不见的实例的需要也是如此。我们引入**了一个目标**驱动实例检测器 (tdid)，它修改了用于实例识别设置的现有常规对象检测器。tdid 不仅提高了在训练过程中看到的实例的性能，运行时间较快，而且还能够进行泛化以**检测**新实例。少

2018 年 7 月 17 日提交;v1 于 2018 年 3 月 12 日提交;最初宣布 2018 年 3 月。

228. 第 1803. 04173[pdf,其他] Cs。铬

对抗软件恶意软件二进制文件：在可执行文件中进行恶意软件检测的深层学习

作者:bojan k 洛斯 naji, ambra demottis, battista biggio, davde Maiorca, giorgio giacinto, clica eckert, fabio roli

摘要: 机器学习方法已被用作**检测**恶意可执行文件的有用工具。他们利用从恶意软件示例 (如标头字段、指令序列甚至原始字节) 中检索到的数据来学习区分良性和恶意软件的模型。然而，也有证据表明，机器学习和深层神经网络可能会被逃避攻击 (也称为对抗性例子) 所愚弄，即输入数据的微小变化导致测试时的错误分类。在本工作中，我们

调查了恶意软件**检测**方法的漏洞，这些方法使用深层网络从原始字节中学习。我们提出了一种基于梯度的攻击，它能够通过在每个恶意软件示例的末尾只更改几个特定字节来规避最近提出的适合此目的的深层网络，同时保留其侵入性功能。有希望的结果表明，我们的对抗性恶意软件二进制文件以很高的概率避开**目标**网络，尽管修改的字节数不到 1%。少

2018 年 3 月 12 日提交;最初宣布 2018 年 3 月。

229. **第 xiv:18004048[pdf,其他] Cs。简历**

遥感应用中的多实例球团积分经典器融合与回归

作者:du xiao , alina zare

摘要: 在分类器 (或回归) 融合的目的是结合几个算法的输出，以提高整体性能。标准的监督融合算法通常需要准确和精确的训练标签。然而，在许多遥感应用中，可能很难获得准确的标签。本文提出了新的分类和回归融合模型，可以在训练数据的模糊和不准确标记下进行训练，其中训练标签与数据点集 (即 "袋子") 相关联，而不是单个数据点 (即 "实例")。在遥感数据的基础上，根据所提出的合成数据和目标检测 、作物**产量**预测等应用的算法进行了实验。所提出的算法具有有效的分类和回归性能。少

2018 年 3 月 11 日提交;最初宣布 2018 年 3 月。

230. **第 xiv:180003965[pdf, ps,其他] Cs。Lg**

bbp: 一种基于 ids 的机器学习中毒方法

作者:潘丽,刘强,赵文涛, 王东旭,王思琪

摘要: 在大数据时代，机器学习是入侵**检测**系统 (ids) 的基本技术之一。然而，实际的 ids 通常通过提供新的数据，然后以定期的方式对学习模型进行再培训，从而更新其决策模块。因此，构成训练或测试分类器数据的一些攻击对基于机器学习的 ids 的**检测**能力提出了重大挑战。中毒攻击是对基于机器学习的 ids 最公认的安全威胁之一，它将一些对抗样本注入训练阶段，导致训练数据数据漂移，目标性能显著下降测试数据上的 ids。本文采用边缘模式**检测**(epd) 算法，设计了一种针对 ids 中使用的几种机器学习算法的中毒方法。具体而言，我们提出了一种边界模式**检测**算法，以有效地生成接近异常数据但被当前分类器认为是正常点的点。然后，我们引入了批处理-epd 边界模式 (bebp)**检测**算法，克服了 epd 生成的边缘模式点数量的限制，得到了更多有用的对抗样本。在 bebp 的基础上，我们进一步提出了一种中度但有效的中毒方法，称为慢性中毒发作。在合成和三个实际网络数据集上进行了大量实验，证明了该中毒方法对几种著名的机器学习算法和一种实用的入侵检测方法--入侵**检测**方法的性能。fmifs-lssvm-ids。少

2018 年 3 月 11 日提交;最初宣布 2018 年 3 月。

评论:7 页 5 图，会议

231. **第 xiv:18003662[pdf,其他] Cs。CI**

仇恨言语检测: 一个已解决的问题? 微博上的长尾挑战案

作者:张子琪,罗磊

摘要: 近年来，仇恨言论在社交媒体上的传播日益增多，迫切需要采取有效的对策，吸引了政府、公司和研究人员的大量投资。已经开发了大量的方法，用于在线自动仇恨言论**检测**。其目的是将文字内容分为非仇恨或仇恨言论，在这种情况下，该方法还可能确定仇恨言论中的**针对性**特征 (即仇恨类型，如种族和宗教)。然而，我们注意到两者的表

现有很大的不同 (即非仇恨 v. s. 仇恨)。在这项工作中，出于实际原因，我们主张把重点放在后一个问题上。我们表明，这是一项更具挑战性的任务，因为我们对典型数据集中语言的分析表明，仇恨言论缺乏独特的、有鉴别力的特征，因此在难以发现的数据集中的 "长尾" 中可以找到。然后，我们提出了深层神经网络结构作为特征提取器，这对于捕获仇恨言论的语义特别有效。我们的方法是在基于 twitter 的最大的仇恨言论数据集集合上进行评估的，并被证明能够在宏观平均 f1 中超过最佳性能的方法，在更具挑战性的情况下，表现最好的方法可达 5 个百分点。识别可恨的内容。少

2018 年 10 月 25 日提交;v1 于 2018 年 2 月 27 日提交;最初宣布 2018 年 3 月。

评论:接受 @ 语义 web 日志

232. 第 18003448[pdf,其他] Cs。铬

机器人家族--通过行为建模进行 android 恶意软件检测：静态与动态分析

作者:幸运的 onwuzurike, mario almeida, enrico mariconti, jeremy blackburn, gianlucastringhini, emiliano de cristofaro

摘要: 随着移动生态系统的日益普及，网络犯罪分子越来越多地**将目标作为目标**，设计和分发窃取信息或对设备所有者造成伤害的恶意应用。针对这些问题，提出了基于基于静态或动态分析的 android 恶意软件模型检测技术。虽然这些分析技术的利弊是已知的，但它们通常是在其局限性的背景下进行比较的，例如，静态分析无法捕获运行时行为，动态分析期间通常无法实现完整的代码覆盖率等。本文对静态和动态分析方法在 android 恶意软件**检测**中的性能进行了分析，并尝试采用相同的建模方法对其**检测**性能进行比较。为此，我们构建了 mamadroid，这是一个最先进的**检测**系统，它依靠静态分析，从抽象的 api 调用序列中创建行为模型。然后，为了在动态分析设置中应用同样的技术，我们修改了 chimp，这是最近建议用于应用测试的众包人类输入的一个平台，以便从在 chimp 上执行应用时产生的跟踪中提取 api 调用的序列虚拟设备。我们将此系统称为 auntiedroid，并使用自动 (猴子) 和用户生成的输入实例化它。我们发现，将静态和动态分析结合起来，可以获得最佳的性能，f-测量达到 0.92。我们还表明，静态分析至少与动态分析一样有效，这取决于在执行过程中如何刺激应用，最后，调查方法之间分类不一致的原因。少

2018 年 7 月 13 日提交;v1 于 2018 年 3 月 9 日提交;最初宣布 2018 年 3 月。

评论:本文的初稿发表在第 16 届隐私、安全和信任年度会议 (pst 2018) 上。这是完整版

233. 第 xiv:18003347[pdf,其他] Cs。简历

预测跟踪：一种用于人的定位和跟踪的深层生成模型

作者:tharindu fernando, simon denman, sridha sridharan, clinton fookes

摘要: 目前的多人本地化和跟踪系统过度依赖于使用外观模型重新识别目标，几乎没有任何方法为这两个目标使用完整的深度学习解决方案。我们提出了一个新颖、完整的深度学习框架，用于多人本地化和跟踪。在此上下文中，我们首先引入了一个轻量级的顺序生成对抗网络架构，用于人员定位，它克服了与遮挡和噪声**检测**相关的问题，通常在多人环境中发现。在所提出的跟踪框架中，我们在行人轨迹预测方法的最新进展的基础上，提出了一种基于预测轨迹的数据关联方案。这就消除了对基于外观特征的计算成本高昂的人员重新识别系统的需求，并以最小的碎片生成类似人类的轨迹。该方法在包括静态和动态摄像机在内的多个公共基准上进行了评估，能够产生出色的性能，特别是在最近提出的其他基于深度神经网络的方法中。少

2018 年 3 月 8 日提交;最初宣布 2018 年 3 月。

评论:将出席 ieee 计算机视觉应用冬季会议 (wacv), 2018 年

234. 第 xiv:18002700[pdf,其他] Cs。铬

多伊10.114/3134600. 3134622

基于同处理器的行为监控: 在系统管理模式攻击检测中的应用

作者:ronny chevalier, maugan villatel , david plakin, guillaume hiet

摘要: 高度特权的软件, 如固件, 是一个有吸引力的**目标**, 攻击者。因此, bios 供应商使用加密签名来确保在启动时的固件完整性。然而, 这种保护并不妨碍攻击者在运行时利用漏洞。为了**检测**此类攻击, 我们建议使用依赖于独立协处理器的基于事件的行为监视方法。我们检测在主 cpu 上执行的代码, 以便向监视器发送有关其行为的信息。此信息有助于解决语义差距问题。我们的方法不依赖于行为的特定模型, 也不依赖于特定**的目标**。我们应用此方法来**检测针对系统**管理模式 (smm) 的攻击, 该模式是一种在运行时执行固件代码的高度特权的 x86 执行模式。我们使用 smm 的控制流和相关 cpu 寄存器 (cr3 和 smbase) 的不变量对 smm 的行为进行建模。我们检测两个开源固件实现: edk ii 和核心引导。我们通过模拟 x86 系统和 arm cortex a5 协处理器来**评估**我们的方法检测最先进的攻击及其运行时执行开销的能力。结果表明, 我们的解决方案**检测来自**最先进状态的入侵, 没有任何误报, 同时在 smm 的上下文中, 在性能开销方面保持可接受 (即小于 150Ⅿ由英特尔定义的阈值)。少

2018 年 3 月 7 日提交;最初宣布 2018 年 3 月。

评论:本文件的定稿已在 2017 年第 33 届计算机安全应用年度会议论文集上发表.

235. 第 xiv:18001819[pdf,其他] cs. it

亚尼奎斯特雷达: 原理和原型

作者:kumar vijay mishra, yina c. eldar

文摘: 在过去几年中, 采用了新的雷达信号处理方法, 使雷达能够从比 nyquist 采样所需的测量少得多的情况下进行信号**检测**和参数估计。这些系统----称为亚 nyquist 雷达----将接收到的信号建模为具有有限的创新率, 并利用 xamlling 框架获取信号的低速率样本。亚尼奎斯特雷达利用目标场景稀疏的事实, 促进了**压缩**传感 (cs) 方法在信号恢复中的使用。在本章中, 我们回顾了几种基于这些原理的脉冲多普勒雷达系统。与其他基于 cs 的设计相反, 我们的配方直接解决了空间和时间的低功耗模拟采样问题, 避免了令人望而却步的字典大小, 并且对噪声和杂波具有鲁棒性。我们首先引入时间子 nyquist 处理, 以估计目标位置使用比传统系统更少的带宽。这为认知雷达铺平了道路, 这些雷达与其他通信服务共享其传输频谱, 从而为在光谱拥挤的环境中共存提供了可靠的解决方案。接下来, 在不影响多普勒分辨率的情况下, 我们通过在相干处理间隔或 "慢速" 内以稀缺的方式传输交错雷达脉冲来减少停留时间。然后, 我们考虑了多输入多输出阵列雷达, 并演示了空间子 nyquist 处理, 它允许使用少量天线元件, 而不会降低角度分辨率。最后, 我们展示了子尼奎斯特和认知雷达在合成孔径雷达等成像系统中的应用。对于每个设置, 我们都提供了一个最先进的硬件原型, 旨在展示亚尼奎斯特雷达的实时可行性。少

2018 年 3 月 5 日提交;最初宣布 2018 年 3 月。

评论:48 页, 26 个数字, 2 个表, 书章节

236. 第 xiv:180001555[pdf,其他] Cs。简历

超越语境: 探索微小人脸检测的语义相似性

作者:岳熙,郑江斌,何向健,贾文静,李汉辉

摘要: 微小的人脸**检测**的目的是在杂乱的场景中发现在尺度、分辨率和遮挡方面变化程度较高的人脸。由于在微小的表面上可用的信息很少，仅仅根据微小边界框内提供的信息或它们的上下文**来检测**它们是不够的。在本文中，我们建议利用每个图像中所有预测**目标**之间的语义相似性来提升当前的人脸探测器。为此，我们提出了一个新的框架，将语义相似性建模为度量学习方案中的对等约束，然后利用图形切割技术，利用语义相似度来细化我们的预测。在三个广泛使用的基准数据集上进行的实验表明，应用这一想法比最新情况有所改善。少

2018 年 3 月 5 日提交;最初宣布 2018 年 3 月。

237. **第 xiv:18001529[pdf,其他] Cs。简历**

用于目标检测的低镜头传输检测器

作者:陈浩,王亚丽,王国友,于巧

文摘: 目标**检测**的最新进展主要是由具有大规模**检测基准的**深度学习推动的。但是，对于**目标检测任务,**完全注释的训练集通常是有限的，这可能会降低深度探测器的性能。为了应对这一挑战，本文提出了一种新的低镜头传输检测器 (lstd)，利用丰富的源域知识构建了一个有效的**目标**域检测器，仅有很少的训练实例。主要捐款说明如下。首先，我们设计了一个灵活的 lstd 深部体系结构，以减轻低镜头**检测**中的传输困难。该架构可以将 ssd 和更快 rcnn 的优势集成到一个统一的深层框架中。其次，我们引入了一个新的低镜头**检测**的正则转移学习框架，在该框架中，提出了转移知识 (tk) 和背景抑郁 (bd) 的正则化，分别利用源和源的对象知识。**目标**域，以便进一步加强微调与几个**目标**图像。最后，我们在一些具有挑战性的低镜头检测实验中检查我们的 lstd **,**其中 lstd 的性能优于其他最先进的方法。结果表明, lstd 是一种较好的低拍摄场景深度检测器。少

2018 年 3 月 5 日提交;最初宣布 2018 年 3 月。

评论:由 aaai2018 接受

238. **第 xiv:18000047[pdf,其他] 反渗透委员会**

内窥镜胶囊机器人的无监督测深和深度学习

作者:mehmet turan, evin pinar ornek,钉子易卜拉希姆利 , can giracoglu, yalmalioglu, mehmet fatih yanik,metin sitti

摘要: 在过去的十年里，许多医学公司和研究小组试图将被动胶囊内窥镜作为一种新兴的微创诊断技术转化为主动操纵内窥镜的内窥镜胶囊机器人，这将提供更直观的疾病**检测**、**靶向给药**和胃肠道类似生物的手术。在本研究中，我们介绍了一个完全无监督的，实时的气味和深度学习者的单目内窥镜胶囊机器人。我们建立了对视图序列的监控，并将重投影最小化分配给损失函数，并在多视图姿态估计和单视图深度估计网络中采用了这种方法。对建议的非刚性变形前猪胃数据集框架进行了详细的定量和定性分析，证明了该方法在运动估计和深度恢复方面的有效性。少

2018 年 3 月 2 日提交;最初宣布 2018 年 3 月。

评论:提交给 2018 年国际能源协会

239. **第 xiv:1803.00[pdf] Cs。镍**

多伊 10.5121/ijwmn.2018.10101

基于插槽的 cmaca/ca 节能 mac 协议设计

作者:suk jin lee, h 行 sik choi, sungun kim

摘要: 支持信标的网络中的设备使用开槽的 csmasa/ca 来争夺通道使用情况。网络中的每个节点在准备传输数据时都会争夺通道。基于超帧结构的开槽 csmas-ca 机制为每个节点提供了通信机会，并合理利用了支持信标的 zigbee 网络中的可用能量。当无线纳米传感器节点植入**目标**人体区域以**检测**疾病症状或病毒存在时，每个节点在信道共享和事件驱动传输方面也需要类似的特性较短的数据。本文提出了一种具有纳米传感器节点的无线网络模型，用于体内应用。提出了一种新的 mac 协议，该协议基于现有的 zigbee mac 协议方案，并分析了可变超帧持续时间和数据包大小的能量消耗性能。少

2018 年 3 月 2 日提交;最初宣布 2018 年 3 月。

评论:12 页, 9 个数字，期刊

日记本参考:2018 年国际无线和移动网络杂志

240. 建议: 1802. 10019[pdf,其他] Cs。简历

多伊 10 . 1109 / . 2018 . 2801560

基于卷积神经网络的同时交通标志检测与边界估计

作者:hee seoklee, kang kim

文摘: 提出了一种利用卷积神经网络 (cnn) 同时估计交通标志位置和精确边界的新型交通标志**检测**系统。在智能车辆导航系统中，估计交通标志的精确边界是很重要的，因为在这些系统中，交通标志可以作为道路环境的三维地标。以前的交通标志**检测**系统，包括最近基于美国有线电视新闻网的方法，只提供交通标志的边界框作为输出，因此需要轮廓估计或图像分割等额外的过程来获得精确的标志边界。在这项工作中，交通标志的边界估计被表述为一个二维姿态和形状类预测问题，这可以通过一个 cnn 有效地解决。利用输入图像中**目标**交通标志的预测二维姿态和形状类，将相应模板符号图像的边界投影到输入图像平面上，估计**目标**符号的实际边界。通过将边界估计问题表述为基于 cnn 的姿态和形状预测任务，我们的方法是端到端可训练的，比其他依赖等高线估计的边界估计方法更具有鲁棒性和小**目标**。图像分割。该方法的结构优化提供了一种准确的交通符号边界估计，在计算上也是有效的，在低功耗移动平台上的**检测**帧速率高于每秒 7 帧。少

2018 年 2 月 27 日提交;最初宣布 2018 年 2 月。

评论:可在 ieee 智能交通系统交易中发布

241. 第 1802.09990[pdf,其他] Cs。简历

视频监控中人脸识别的深度学习体系结构

作者:saman bashbaghi, eric granger, robert sabourin, mostafa parchami

文摘: 用于视频监控 (vs) 应用的人脸识别 (fr) 系统试图在分布式摄像机网络上准确**检测目标**个人的存在。在基于视频的 fr 系统中，目标个体的面部模型在注册过程中使用数量有限的参考静止图像或视频数据进行了先验设计。由于照明、姿势、比例、遮挡、模糊和相机互操作性的差异，这些面部模型通常不能代表在操作过程中观察到的面部。具体而言，在静止视频到视频的 fr 应用程序中，使用在受控条件下使用静止相机捕获的单个高质量参考静止图像，以生成面部模型，以便在以后与视频拍摄的低质量面孔进行匹配摄像机在不受控制的条件下。当前基于视频的 fr 系统可以在受控方案上很好地执行，而它们在不受控制的方案中的性能并不令人满意，主要原因是源 (注册) 和**目标**(操作) 域之间的差异。这一领域的大部分工作都是在不受限制的监视环境中设计可

靠的基于视频的 fr 系统。本章概述了通过深层卷积神经网络 (cnn) 在静态视频到视频的 fr 场景中的最新进展。特别是，文献中提出的基于三重损失函数 (例如，交叉相关匹配 cnn、树干分支合奏 cnn 和 haarnet) 和监督自动编码器 (如规范的人脸表示 cnn) 的深度学习架构是在准确性和计算复杂度方面进行了审查和比较。少

2018 年 6 月 27 日提交;v1 于 2018 年 2 月 27 日提交;最初宣布 2018 年 2 月。

242. **第 1802.09972[pdf,其他] Cs。简历**

基于照明感知深神经网络的多光谱数据融合，用于行人检测

作者:关大安,曹延鹏,梁俊荣,曹艳龙,杨英

文摘: 近年来，多光谱行人**检测**作为一个很有希望的解决方案受到广泛关注，可促进全天候应用 (如安全监视和监控) 的强大的人**的目标检测**。自动驾驶)。本文证明了多光谱图像中编码的光照信息可以用来显著提高行人**检测**的性能。提出了一种新的照明感知加权机制，用于准确描述场景的照明状况。这种照明信息被集成到双流深层卷积神经网络中，以了解不同光照条件 (白天和夜间) 下的多光谱与人类相关的特征。此外，我们利用照明信息和多光谱数据生成更准确的语义分割，用于提高行人**检测**的准确性。将所有的部分放在一起，我们提出了一个强大的框架，多光谱行人**检测**的基础上，多任务学习的照明感知行人**检测**和语义分割。我们提出的方法采用精心设计的多任务损失函数进行端到端训练，在 kaist 多光谱行人数据集上优于最先进的方法。少

2018 年 2 月 27 日提交;最初宣布 2018 年 2 月。

243. **第 1802.09961[pdf, ps,其他] Cs。CI**

用主题模型和情绪强度对习语和文学表达进行分类

作者:jing peng, anna feldman, ekaterina vylomova

摘要: 我们描述了一种习语和文字表达式自动分类的算法。我们的出发点是，特定文本段中的词语，如段落，如果是一个共同讨论议题的高级代表，就不太可能成为习语表达的一部分。我们的另一个假设是，习语发生的语境，通常是更有感情的，因此，我们纳入了一个简单的分析的强度表达的上下文。我们调查一到三个段落的单词主题表示包，其中包含应归类为习语或文字表达式 (**目标**短语)。我们使用无监督聚类方法 "潜在的 dirichlet 分配 (lda)" (blei 等人, 2003 年)，从包含习语的段落和包含文本的段落中提取主题。由于习语表达式表现出非组合性的性质，我们假设它们通常会呈现与局部主题中使用的词不同的语义。我们将习语视为语义异常值，并将语义转换标识为异常值检测. 因此，这个主题表示允许我们使用本地语义上下文将习语与文本区分开来。我们的结果令人鼓舞。少

2018 年 2 月 27 日提交;最初宣布 2018 年 2 月。

评论:emnlp 2014

244. **建议: 1802.09088[pdf,其他] Cs。简历**

在新颖性检测中的兼职分类器

作者:mohammad sabokrou, mohammad kalooei, mahood fathy, ehsan adeli

摘要: 新颖性检测是识别在某些方面不同于训练观察 (**目标**类) 的观察的过程。在现实中，新奇的阶层往往是缺席的培训，抽样差或没有很好的定义。因此，一类分类器可以有效地对此类问题进行建模。然而，由于无法获得新奇类的数据，培训端到端深度网络是一项繁琐的任务。本文在生成对抗网络成功的启发下，在无监督和半监督环境中训练深层模型，提出了一类分类的端到端体系结构。我们的体系结构由两个深层网络组成，

每个深度网络都经过相互竞争的训练，同时协作了解**目标**类中的基本概念，然后对测试样本进行分类。一个网络作为新奇的探测器工作，而另一个网络通过增强输入样本和扭曲异常值来支持它。直觉是，增强的初始化器和扭曲的异常值的可分性远远好于决定原始样本。该框架适用于图像和视频中异常和异常点**检测**的不同相关应用。mnist 和 caltech-256 图像数据集的结果，以及具有挑战性的 ucsd ped2 视频异常**检测**数据集，表明我们提出的方法有效地学习**了目标**类，优于基线和最先进的方法。少

2018 年 5 月 24 日提交;v1 于 2018 年 2 月 25 日提交;最初宣布 2018 年 2 月。

评论:cvpr 2018 论文

245. **第 xiv:1802. 09070[pdf,其他] Cs。简历**

注意感知生成对抗性抗网络 (ata-gan)

作者:dimitris kastaniotis, ioanna ntinou , dimitrios tsourounis, george economou, spiros fotopoulos

摘要: 在这项工作中，我们提出了一种新的方法来培训生成对抗性网络 (gans)。利用教师网络生成的注意图，我们能够提高生成图像的质量，并对生成的图像执行弱对象定位。为此，我们生成了使用间接不氟化 (iif) 捕获的 hep-2 细胞的图像，并研究了我们的网络执行细胞弱定位的能力。首先，我们证明了虽然有机遗传组织能够有效地了解输入域和**目标**分布之间的映射，但鉴别器网络无法**检测到**感兴趣的区域。其次，我们提出了一种新的注意力转移机制，它使我们能够通过转移学习来加强判别器对感兴趣的区域的重视。第三，我们表明，这导致了更现实的形象，因为鉴别器学会了强调感兴趣的领域。第四，该方法允许生成图像和注意力图，这对数据注释 (如在物体**检测**) 很有用。少

2018 年 2 月 25 日提交;最初宣布 2018 年 2 月。

246. **建议: 1802.08937[pdf,其他] Cs。简历**

利用形状和运动检测恶劣天气预报中的共状云

作者:郑新业,叶建波,陈玉坤,斯蒂芬·维斯塔尔,贾丽 , 何塞·pibera-fernandez, michael a. steinberg, james z.wang

摘要: 气象学家使用卫星图像中的云的形状和运动作为几种主要类型的严重风暴的指标。卫星虚拟数据在空间和时间上的分辨率都越来越高，这使得人类无法充分利用其预测中的数据。需要自动卫星图像分析方法，以便在**发现**与风暴有关的云模式后立即找到这些模式。我们提出了一种基于机器学习和模式识别的方法来**检测**卫星图像中的 "逗号形" 云，这些云是与旋风配方密切相关的特定云分布模式。为了使用**目标**运动模式**检测**区域，我们的方法在由形状和运动敏感特征表示的手动注释云示例上进行了培训。不同尺度的滑动窗口被用来确保密集的云被捕获，我们实施有效的选择规则来缩小这些滑动窗口之间的兴趣区域。最后，我们对一个保留带注释的逗号形云数据集的方法进行了评估，并将结果与恶劣天气数据库中记录的风暴事件进行了交叉匹配。我们的方法的有效性和准确性表明，在协助气象学家天气预报的潜力很大。少

2018 年 6 月 5 日提交;v1 于 2018 年 2 月 24 日提交;最初宣布 2018 年 2 月。

评论:正在提交

247. **建议: 180008857[pdf,其他] 反渗透委员会**

视觉操纵关系网络

作者:张汉波,兰旭光,周新文, 田志强,张洋, 郑南宁

文摘: 机器人抓取**检测**是机器人技术中最重要的领域之一，近年来在卷积神经网络 (cnn) 的帮助下取得了长足的进步。但是，在一个场景中包含多个对象可能会使现有的基于 cnn 的抓取检测算法失效,因为不考虑对象之间的操作关系，这是指导机器人在正确的顺序。本文提出了一种新的 cnn 体系结构，称为视觉操纵关系网络 (vmrn)，以帮助机器人**实时检测** 目标和预测操纵关系。为了实现端到端培训并满足机器人任务中的实时要求，我们提出了对象配对池层 (op2l)，以帮助预测一个正向过程中的所有操作关系。此外，为了训练 vmrn，我们收集了一个名为 "可视操作关系数据集" (vmrd) 的数据集，该数据集由 5185 张具有 17000 对象实例的图像组成，以及每个图像中所有可能的对象对之间的操作关系,它由操作关系树标记。实验结果表明，新的网络体系结构能够同时**检测**对象，预测操纵关系，满足机器人任务的实时性要求。少

2018 年 3 月 2 日提交;v1 于 2018 年 2 月 24 日提交;最初宣布 2018 年 2 月。

248. 建议: 1802.08755[pdf,其他] Cs。简历

无盲点: 使用相机和 lidars 的自主车辆的全环绕多目标跟踪

作者:akshay rangesh, mohan m. trivedi

摘要: 在线多目标跟踪 (mot) 对于自主和自动化车辆的高级空间推理和路径规划具有极其重要的意义。在本文中，我们提出了一个模块化框架，用于跟踪多个对象 (车辆)，能够接受来自不同传感器模式 (视觉和范围) 和可变数量的传感器的对象建议，以产生连续的物体轨迹。这项工作的灵感来自于计算机视觉中传统的逐检方法，但有一些关键的区别--首先，我们跨多个摄像机和不同的传感器模式跟踪对象。这是通过在传感器之间准确、高效地融合对象建议来实现的。其次，在现实世界中直接跟踪感兴趣的对象 (**目标**)。这与传统技术不同，传统技术中的对象只是在图像平面中被跟踪。这样做可以使轨道易于使用的自治代理导航和相关的任务。为了验证我们方法的有效性，我们在现实世界的高速公路上测试它，这些数据是从一个非常敏感的测试台收集的，能够捕获全环绕信息。我们证明，我们的框架非常适合通过自我驾驶的整个机动跟踪物体，其中一些需要几分钟以上的时间才能完成。我们还通过比较包括/排除不同传感器、更改传感器总数以及对象建议的质量对最终跟踪结果的影响，利用我们方法的模块化。少

2018 年 9 月 10 日提交;v1 于 2018 年 2 月 23 日提交;最初宣布 2018 年 2 月。

249. 建议: 1802.08701[pdf,其他] Cs。简历

基于机器学习的高光谱图像分析研究

作者:utsav b. gewali, sildomar t. monteiro, eli saber

摘要: 高光谱传感器能够远程研究场景材料的化学特性，以便对环境中的物体进行识别、**检测**和化学成分分析。因此，从地球观测卫星和飞机上捕获的高光谱图像在农业、环境监测、城市规划、采矿和防御方面越来越重要。机器学习算法以其出色的预测能力已成为现代高光谱图像分析的关键工具。因此，对机器学习技术的扎实了解已成为遥感研究人员和从业人员的关键。本文回顾和比较了文献中最新发表的基于机器学习的高光谱图像分析方法。通过图像分析任务和机器学习算法的类型对这些方法进行组织，并给出了图像分析任务与可应用于图像学习算法的机器学习算法类型之间的双向映射。本文全面介绍了高光谱图像分析任务和机器学习算法。所考虑的图像分析任务包括土地覆盖分类、**目标检测**、解混和物理参数估计。机器学习算法包括高斯模型、线性回归、逻辑回归、支持向量机、高斯混合模型、潜在线性模型、稀疏线性模型、高斯混合模型、集成学习、定向图形模型、无方向的图形模型、聚类、高斯过程、dirichlet 过程和深度学习。我们还讨论了高光谱图像分析领域的开放挑战，并探讨了未来可能的方向。少

2018 年 2 月 23 日提交;最初宣布 2018 年 2 月。

评论:在 isprs 摄影测量和遥感杂志上审查

250. 建议: 1802.07957[pdf,其他] Cs。简历

基于深层多尺度时空判别显著性图的非刚性目标跟踪

作者:张平平,王东,湖川路,王洪宇

文摘: 本文提出了一种基于时空一致性**显著性检测**的有效的非刚性目标跟踪方法。与大多数使用边界框指定跟踪**目标**的现有跟踪器不同，该方法可以提取**目标**的准确区域作为跟踪输出，从而更好地描述非刚性对象同时减少对**目标**模型的背景污染。此外，我们的模型有几个独特的特点。首先，开发了一种定制的深完全卷积神经网络 (tfcn)，用于模拟给定图像区域的局部显著性，它不仅提供像素级输出，而且集成语义信息。其次，提出了多尺度多区域机制，以生成局部区域显著性图，有效地考虑具有不同空间布局和尺度变化的视觉感知。随后，这些显著性映射融合在一起，通过加权熵方法，最终得出了一个判别显著性映射。最后，我们提出了一种基于所提出的显著性**检测**方法的非刚性目标跟踪算法，该算法利用时空一致性显著性映射 (stcsm) 模型进行**目标**背景分类，并使用简单的在线更新微调方案。大量的实验结果表明，与最先进的显著性**检测**和视觉跟踪方法相比，该算法具有较高的性能，尤其是优于其他相关算法。非刚性目标跟踪数据集上的跟踪器。少

2018 年 2 月 22 日提交;最初宣布 2018 年 2 月。

评论:提交给 ieee 图像处理事务，包括 12 页、9 个数字和 1 个表格。现在在视图中

251. 建议: 1802 07770[pdf,其他] Cs。简历

基于二模型决策不匹配的可推广对抗性算例检测

作者:joao monteiro, zahid akhtar, tiago h. falk

摘要: 深度神经网络 (dnn) 在广泛的应用中取得了惊人的成功。然而，最近的研究发现，他们很容易受到对抗性的例子，即，原始样品与添加微妙的扰动。这样的扰动往往太小，人类无法察觉，但它们很容易愚弄神经网络。针对对抗性实例提出的辩护技术很少，但它们需要修改**目标**模型或事先了解对抗性实例生成方法。同样，他们在遇到培训阶段没有使用的对抗性例子类型时的表现也明显下降。在本文中，我们提出了一个新的框架，可以用来通过**检测**对抗的例子来提高 dnn 的鲁棒性。特别是，我们使用独立训练模型的决策层作为后验**检测**的功能。拟议的框架不需要事先了解对抗示例生成技术，并且可以直接使用未经修改的现成模型进行增强。在标准 mnist 和 cibar10 数据集上的实验表明，它不仅很好地概括了不同的对抗示笔生成方法，而且还具有不同的加法扰动。具体来说，在我们建议的功能之上训练的不同的二进制分类器可以在一组白盒攻击中实现较高的**检测**率 (& gt;90%)，并在针对看不见的攻击进行测试时保持这种性能。少

2018 年 3 月 6 日提交;v1 于 2018 年 2 月 21 日提交;最初宣布 2018 年 2 月。

252. 建议: 1802. 06926[pdf,其他] Cs。简历

全成像 cnn 车辆检测的规模优化

作者:杨高,郭守炎,黄凯民, 陈嘉新, 钱公,杨祖,童白,加里·奥韦韦特

文摘: 许多最先进的一般目标检测方法利用共享的全图像卷积功能 (如在更快 r-cnn)。这在享受大卷积神经网络 (cnn) 模型所提供的判别能力的同时，实现了合理的测试相位计算时间。这种设计擅长包含自然图像但具有非常不自然分布的基准，即它们具有不自然的目标类高频，倾向于 "友好" 或 "主导" 的对象尺度。本文进一步研究了快速

r-cnn 目标检测方法在具有自然尺度分布和无偏置现实世界目标频率的数据集中的应用和适应性。特别是，我们表明，更好地将探测器的尺度灵敏度与现有的分布对齐，可以提高车辆**的检测**性能。我们通过修改区域建议的选择，并在 cnn 模型中使用更适合比例的全图像卷积功能来做到这一点。通过在区域建议输入中选择更好的比例，并通过对卷积神经网络的仔细设计组合要素图，提高了较小对象的性能。我们显著地将 kitti 数据集汽车类的**检测** ap 从基线上的 76.3% 更快 r-cnn 检测器提高到改进后的检测器中的 83.6%。少

2018 年 2 月 19 日提交;最初宣布 2018 年 2 月。

评论:被 2017 年 ieee 智能车辆研讨会 (iv) 所接受。链接:
http://ieeexplore.ieee.org/stamp/stamp.jsp？ arnumber=7995812

253. 建议: 1802.06515[pdf,其他] Cs。简历

图像取证: 检测具有操纵不变图像相似性的科学图像重复

作者:m. cicconet, h. elliott, d.l . 里士满, d. wainstock, m. walsh

文摘: 科学出版物中对图像的操纵和重用是一个值得关注的问题，目前缺乏可扩展的解决方案。目前用于**检测**图像重复的工具大多是手动或半自动的，尽管基于学习的方法提供了大量的**目标**数据集。本文通过复制、旋转、平移、缩放、透视变换、直方图调整或部分擦除等方式，解决了确定两个图像是否为另一个图像的操纵版本的问题。提出了一种基于 3 分支暹罗卷积神经网络的数据驱动解决方案。convnet 模型被训练将图像映射到一个 128 维空间中，在该空间中，重复图像之间的欧几里得距离小于或等于 1，唯一图像之间的距离大于 1。我们的研究结果表明，这种方法有可能改进对已发表和同行评审文献的图像处理监控。少

2018 年 8 月 22 日提交;v1 于 2018 年 2 月 18 日提交;最初宣布 2018 年 2 月。

评论:11 页; 5 个数字; 关键词: siamese 网络、相似度度量、图像取证、图像处理

254. 建议: 1802. 05196[pdf,其他] Cs。铬

社交媒体上 spear 网络钓鱼帖子的生成模型

作者:john seymour , phillip tully

摘要: 从历史上看，计算机安全中的机器学习优先考虑防御: 考虑入侵**检测**系统、恶意软件分类和僵尸网络流量识别。犯罪也可以从数据中受益。社交网络可以访问广泛的个人数据、方便植物的 api、口语语法以及缩短链接的流行，是传播机器生成的恶意内容的绝佳场所。我们的目标是发现对手在这样的领域中可能会使用哪些功能。我们提出了一个长期的短期记忆 (lstm) 神经网络，学习社会工程特定的用户点击欺骗性的 url。该模型使用社交媒体帖子的单词矢量表示进行训练，为了更有可能进行点击，它使用从**目标**时间线中提取的主题进行动态种子处理。我们通过聚类来扩展模型，根据高价值**目标**的社会参与程度对其进行分类，并使用 ip 跟踪链接的点击率来衡量 lstm 网络钓鱼探险的成功与否。我们实现了最先进的成功率，将历史电子邮件攻击活动的成功率提高了两倍，并且比手动执行相同任务的人表现要好。少

2018 年 2 月 14 日提交;最初宣布 2018 年 2 月。

评论:在 NIPS 机器欺骗研讨会 (2017) 上发表, 4 页限制加上参考资料, 2 个数字

255. 特别报告: 18004822[pdf,其他] Cs。Lg

通过对深层预测模型的对抗攻击识别医学记录中的易感位置

作者:孙梦英,唐凤仪,易金峰,王飞,周嘉宇

摘要: 电子病历 (ehr) 的激增导致了医学预测建模研究兴趣的增加。最近，许多基于深度学习的预测模型也为 ehr 数据开发，并显示出令人印象深刻的性能。然而，最近的一系列研究表明，这些深刻的模型并不安全：它们存在某些脆弱性。简而言之，训练有素的深网络可以对具有可忽略不计的变化的输入极为敏感。这些投入被称为对抗性的例子。在医学信息学的背景下，这种攻击可以通过稍微扰乱病人的病历来改变高性能深度预测模型的结果。这种不稳定性不仅反映了深层体系结构的弱点，更重要的是，它为检测输入上**的**易感部件提供了指导。在本文中，我们提出了一个高效和有效的框架，学习**时间优先的**攻击针对 lstm 模型与 ehr 输入，我们利用这种攻击策略来筛选患者的医疗记录，并识别易感事件和测量值。有效的筛选程序可以帮助决策者对如果测量不正确可能造成严重后果的地点给予额外关注。我们对现实世界中的紧急护理队列进行了广泛的实证研究，并展示了所建议的筛查方法的有效性。少

2018 年 2 月 13 日提交;最初宣布 2018 年 2 月。

256. 建议: 18004431[pdf,其他] Cs。Lg

多伊 10.11145/32198198445

利用 lstm 和非参数动态阈值检测航天器异常

作者:kyle hundman, valentino constantinou, christopher laporte, ian colwell, tomsoderstro

摘要: 随着航天器发送越来越多的遥测数据，需要改进异常**探测**系统，以减轻作业工程师的监测负担，降低运行风险。目前的航天器监测系统只**针对**一类异常类型，由于涉及规模和复杂性的挑战，往往需要昂贵的专家知识来开发和维护。我们展示了长期短期存储器 (lstm) 网络 (一种递归神经网络 (rnn)) 在利用土壤水分主动被动 (smap) 卫星和火星的专家标记遥测异常数据克服这些问题方面的有效性科学实验室 (msl) 探测器，好奇。我们还提出了一种在 smap 异常**检测**系统试点实施过程中开发的互补的无监督和非参数异常阈值方法，并与其他关键指标一起提供了错误的正缓解策略。改进和发展过程中吸取的经验教训。少

2018 年 6 月 6 日提交;v1 于 2018 年 2 月 12 日提交;最初宣布 2018 年 2 月。

评论:kdd 2018 相机就绪版本

257. 建议: 1802. 03916[pdf,其他] Cs。Lg

黑盒预测器标签移位的检测与校正

作者:zachary c. lipton, yi--h 强 wang, alex smola

抽象: 面对训练和测试集之间的分布转移，我们希望**检测**和量化这种转变，并在没有测试集标签的情况下纠正我们的分类器。在医疗诊断的推动下，疾病 (**目标**) 引起症状 (观察)，我们关注标签转移，其中标签边缘 P(Y)变化，但有条件的 p(x|Y)不。我们建议黑盒移位估计 (bbse) 来估计测试分布 P(Y).bbse 利用任意黑匣子预测因子来减少移位校正之前的维数。虽然更好的预测值给出了更严格的估计，但 bbse 即使在预测值有偏差、不准确或未校准的情况下也能工作，只要它们的混淆矩阵是可逆的。我们证明了 bbse 的一致性，约束了它的错误，并引入了一个统计测试，使用 bbse **来检测**移位。我们还利用 bbse 来纠正分类器。实验证明了准确的估计和改进的预测，即使在自然图像的高维数据集上也是如此。少

2018 年 7 月 26 日提交;v1 于 2018 年 2 月 12 日提交;最初宣布 2018 年 2 月。

评论:在 2018 年机器学习国际会议 (icml) 上发表

258. 建议: 1802.03714[pdf,其他] Cs。铬

基于图像识别的物联网恶意软件轻量级分类

作者:su jalwei, danilo vasconcellos vargas, sanjiva prasad, daniele sgandurra, yaokai feng, kouichi sakurai

摘要: 物联网 (iot) 是传统互联网的延伸，它允许大量智能设备 (如家用电器、网络摄像机、传感器和控制器) 相互连接，以共享信息和改善用户体验.当前的物联网设备通常是用于特定于域的计算的微型计算机，而不是传统的特定于功能的嵌入式设备。因此，**针对**连接到互联网的传统计算机的许多现有攻击也可能针对物联网设备。例如，ddos 攻击在物联网环境中变得非常普遍，因为这些环境目前缺乏基本的安全监视和保护机制，最近的 mirai 和 brickerbot 物联网僵尸网络就表明了这一点。本文提出了一种检测物联网环境中 ddos 恶意软件的新的轻量级方法。首先提取从二进制文件转换的单通道灰度图像，然后利用轻量级卷积神经网络对物联网恶意软件家族进行分类。实验结果表明，该系统对好软件和 ddos 恶意软件的分类可以达到 94.0% 的准确率，对好软件和两个主要恶意软件家族的分类可以达到 81.8 的准确率。少

2018 年 2 月 11 日提交;最初宣布 2018 年 2 月。

259. 建议: 1802.03269[pdf,其他] Cs。简历

用于行人检测的无监督深域适应

作者:刘丽航,林伟耀,吴丽生,于勇，迈克尔·英阳

文摘: 本文讨论了拥挤场景中行人**检测**任务中的无监督域适应问题。首先，我们利用迭代算法，以高可信度的方式对正行人样本进行迭代选择和自动注释，作为**目标**域的训练样本。同时，我们还重用源域中的负样本，以弥补阳性样本和阴性样本数量之间的不平衡。其次，基于深度网络，我们还设计了一个无监督的规则器，以减轻数据噪声的影响。更具体地说，我们将最后一个完全连接的图层转换为两个子图层--元素上的乘法层和和层，并添加无监督的正则器，以进一步提高域适应精度。在行人**检测**实验中，该方法在精度保持几乎不变的情况下，将召回值提高了近 30%。此外，我们还在监督和非监督环境中执行标准域适应基准的方法，并获得最先进的结果。少

2018 年 2 月 9 日提交;最初宣布 2018 年 2 月。

评论:2016 年 eccv 研讨会

260. 建议: 180002312[pdf,其他] cse

基于机器学习的移动应用图形用户界面原型设计

作者:kevin moran, carlos bernal-cárdenas, michael curcio, richard bonett, denys poshyvanyk

摘要: 面向用户的软件的开发人员通常会将图形用户界面 (gui) 的模型转换为代码。这个过程既发生在应用程序的初始阶段，也发生在进化的上下文中，因为 gui 更改与不断发展的功能同步。不幸的是，这种做法具有挑战性，也很耗时。在本文中，我们提出了一种通过检测、分类和组装三个任务实现 gui 精确原型设计的自动化此过程的方法。首先，使用计算机视觉技术或模型元数据从模拟工件中**检测到** gui 的逻辑组件。然后，利用软件存储库挖掘、自动动态分析和深层卷积神经网络将 gui 组件准确地分为特定于域的类型 (例如，切换按钮)。最后，一种数据驱动的 k-近邻邻域算法生成了一个合适的分层 gui 结构，可以从中自动组装原型应用程序。我们在一个名为 "重绘制" 的系统中为 android 实现了这种方法。我们的评估表明，重新绘制实现了平均 gui 组件分类精度 91%，并在显示合理代码的同时，在视觉相关性方面组合了**紧密**镜像目标模

型的原型应用程序结构。与工业从业者的访谈说明了重新绘制在改进实际开发工作流程方面的潜力。少

2018 年 6 月 4 日提交;v1 于 2018 年 2 月 7 日提交;最初宣布 2018 年 2 月。

评论:接受 ieee 软件工程交易

261. **建议: 18002181[pdf,其他] Cs。简历**

基于图理论的聚类分析框架在计算机视觉和模式识别中的应用

作者:yenatan tariku tesfaye

摘要: 最近，一些聚类算法被用来解决来自不同学科的各种问题。本文旨在将问题作为一个聚类问题来解决计算机视觉和模式识别中的不同挑战问题。我们提出了一种新的方法来解决多目标跟踪、视觉地理定位和异常**点检测**问题，使用一个统一的下划线聚**类**框架，即显性集聚类及其扩展，并提出了一个新的方法。比几种最先进的方法更高的结果。少

2018 年 1 月 7 日提交;最初宣布 2018 年 2 月。

评论:博士论文

262. **建议: 1802. 01235[pdf] Cs。简历**

利用无香味卡尔曼滤波技术跟踪多个运动物体

作者:陈西,小王,宣建华

文摘: 可靠地**检测**和跟踪多个运动物体进行视频监控是一项重要任务。然而，当在非线性运动场景中发生遮挡时，许多现有的方法往往无法连续跟踪多个感兴趣的运动对象。本文提出了一种检测和跟踪具有遮挡的多个运动目标的有效方法。移动**目标**最初是使用简单而高效的块匹配技术检测的，为多个对象跟踪提供了粗略的位置信息。然后通过非线性跟踪算法估计每个运动物体更准确的位置信息。考虑到多个运动物体之间的遮挡所造成的模糊性，我们应用了无香味卡尔曼滤波 (ukf) 技术进行可靠的目标**检测**和跟踪。与传统的卡尔曼滤波 (kf) 不同，在非线性跟踪场景中, ukf 不能实现最优估计，它可以用于跟踪非线性运动和非线性运动，因为这是无香味变换造成的。此外，还对每个物体的速度信息进行了估计，以帮助实现目标**检测**算法，有效地描述了多个遮挡运动物体。实验结果表明，该方法能够正确**地检测**和跟踪具有非线性运动模式和遮挡的多个运动物体。少

2018 年 2 月 4 日提交;最初宣布 2018 年 2 月。

评论:2012 工程与应用科学国际会议 (iceas 2012)

263. **建议: 1801. 09969[pdf,其他] Cs。简历**

滑线点回归在形状鲁棒场景文本检测中的作用

作者:朱宜兴,杜军

摘要: 传统的文本**检测**方法主要集中在四边形文本上。在本研究中，我们提出了一种新的方法，称为滑动线点回归 (slpr)，以**检测**任意形状的文本在自然场景。slpr 在文本行的边缘对多个点进行回归，然后利用这些点绘制文本的轮廓。拟议的 slpr 可以适应许多对象**检测**架构，如更快 r-nnn 和 r-fcn。具体来说，我们首先生成最小的矩形框，包括具有区域建议网络 (rpn) 的文本，然后使用垂直和水平滑动线对文本边缘的点进行等距回归。为了充分利用信息，减少冗余，我们通过矩形箱形位置计算**目标**点的 x 坐标或 y 坐标，只需回归剩余的 y 坐标或 x 坐标。因此，我们不仅可以减少系统的参

数，而且可以抑制生成更多规则多边形的点。我们的方法在传统的 icdar2015 相景文本基准和曲线文本**检测**数据集 ctw1500 上取得了竞争的成果。少

2018 年 1 月 30 日提交;最初宣布 2018 年 1 月。

264. **建议: 1801. 09292[pdf,其他] 反渗透委员会**

大型 3d 地图中的多目标检测、跟踪和长期动态学习

作者:nils bore, p 小儿 jensfelt, john folkesson

摘要: 在这项工作中，我们提出了一种在大型机器人环境中跟踪和学习所有物体动态的方法。一个移动机器人在环境中巡逻，一个接一个地访问不同的地点。可移动对象通过更改检测被**发现**，并在整个机器人部署过程中进行跟踪。为了进行跟踪，我们扩展了以前工作的 Rao-Blackwellized 粒子滤波器与出生和死亡过程，使该方法能够处理任意数量的对象。使用吉布斯抽样对**目标**出生和关联进行抽样。然后，使用预期最大化算法以无监督的方式学习系统的参数。因此，该系统可以了解特定环境的动态及其对象。该算法根据移动机器人在实际部署过程中在办公环境中自主收集的数据进行评估。我们证明，该算法自动识别和跟踪 3d 地图中的运动物体，并推断合理的动力学模型，显著降低了我们以前的工作的建模偏差。与以往的环境动力学学习方法相比，该方法是一种改进，因为它允许学习细粒度的过程。少

2018 年 1 月 28 日提交;最初宣布 2018 年 1 月。

评论:提交同行评审

265. **建议: 1801 1.08558[pdf,其他] Cs。简历**

从合成孔径雷达图像中深入学习端到端自动目标识别

作者:古河秀俊

文摘: 合成孔径雷达 (sar) 自动**目标**识别 (atr) 的标准体系结构包括**检测**、判别和分类三个阶段。近年来，人们提出了 sar atr 的卷积神经网络 (cnn)，但大多将从 sar 图像中提取的**目标**芯片中提取**的目标**芯片中的目标类分类，作为 sar atr 第三阶段的分类。在本报告中，我们提出了一个新的 cnn 端到端 atr 从 sar 图像。cnn 命名的验证支持网络 (versnet) 端到端执行 sar atr 的所有三个阶段。versnet 输入具有多个类和多个**目标**的任意大小的 sar 图像，并输出表示每个**检测到** 的目标的位置、类和姿势的 sar atr 图像。本报告描述了 versnet 的评估结果，该评估结果训练输出了所有 12 个类的分数: 10 个**目标**类、**1 个目标**前班和 1 个后台类，每个像素使用移动和固定**目标**公共数据集。少

2018 年 1 月 25 日提交;最初宣布 2018 年 1 月。

评论:技术报告, 6 页, 7 个数字, 7 个表, Copyright(C)2018 ieice

日记本参考:ieice 技术报告，第 117 卷，第 403 卷, sane2017-92，第 35-40 页, 2018 年 1 月

266. **建议: 1801 1.08535[pdf,其他] Cs。铬**

指挥歌曲: 实用的对抗性语音识别的系统方法

作者:袁学静,陈玉轩，赵悦,云辉龙，刘晓刚, 陈凯，张胜志，黄和清,王晓峰,卡尔 a .冈特

摘要: 像谷歌语音、cortana 这样的 asr (自动语音识别) 系统的普及带来了安全隐患，最近的攻击就证明了这一点。然而，这种威胁的影响并不那么明显，因为它们要么不那么隐蔽 (产生类似噪音的语音命令)，要么需要攻击装置的物理存在 (使用超声波)。本

文证明了这种攻击不仅更实用，而且是更隐蔽的攻击是可行的，甚至可以自动构造。具体而言，我们发现语音命令可以秘密嵌入到歌曲中，在播放时，可以通过 asr 有效地控制**目标**系统，而不会被人注意到。为此，我们开发了解决关键技术挑战的新技术：在背景噪音不被发现的情况下，将命令集成到歌曲中，这种方式可以让 asr 通过空气有效地识别出来由人类的听众。我们的研究表明，这可以自动地实现对现实世界 asr 应用。我们还证明，此类突击队歌曲可以通过互联网（如 youtube）和广播传播，有可能影响数百万 asr 用户。我们进一步提出了一种控制这种威胁的新的缓解技术。少

2018 年 7 月 1 日提交;v1 于 2018 年 1 月 24 日提交;最初宣布 2018 年 1 月。

评论:2018 年被 usenix 安全公司接受

267. 建议: 1801 1.08439[pdf,其他] Cs。红外

数学内容的相似性分析提高学术抄袭的检测能力

作者:mauriciroman isele

摘要: 尽管**在侦查**学术抄袭方面付出了努力，但这仍然是一个贯穿所有学科的普遍存在的问题。开发了各种工具，通过自动识别可疑文件来协助人类检查员。然而，据我们所知，这些工具目前都没有使用数学内容进行分析。这是有问题的，因为数学内容有可能代表学术文献中的大量科学贡献。因此，忽视数学内容会极大地限制对剽窃的**检测**，尤其是在经常使用数学的学科中。本文旨在通过概述现有的数学信息检索方法和分析这些方法在不同可能的数学抄袭案例中的适用性来帮助弥补这一差距。我发现，基于语法的方法在**检测**毫不掩饰的剽窃方面表现特别好，而基于结构的和混合的方法也有望**检测**出伪装的数学剽窃形式，如剽窃重命名的标识符。然而，需要在这一领域进行更多的研究，以便**能够发现**更复杂的数学抄袭：目前方法的范围仅限于公式一级，需要向分区一级扩展。此外，对等价变换的一般**检测**目前是不可行的。尽管存在这些剩余的问题，但我的结论是，所提出的方法已经可以用于**针对**数学剽窃的基本自动化**检测**系统，从而增强当前的剽窃**检测能力.**系统。少

2018 年 1 月 25 日提交;最初宣布 2018 年 1 月。

268. 建议: 1801. 08116[pdf,其他] Cs。艾

心理实验室：深层强化学习剂的心理学实验室

作者:joel z. leibo, cyen de mason d ' autume, daniel zoran, david amos, charles beattie , keith anderson, antonio garcía castañeda,
manuel sanchez, simongreen, audrunas gruslys, shane legg, demis husabis,
matthewm . botvinick

摘要: 心理实验室是深度思维实验室（beattie 等人, 2016 年）第一人称 3d 游戏世界内的一个模拟心理学实验室。心理实验室能够实现经典的实验室心理实验，使它们与人和人造药物一起工作。心理实验室有一个简单而灵活的 api，使用户能够轻松地创建自己的任务。作为示例，我们发布了一些经典实验范式的心理学实验室实现，包括视觉搜索、变化**检测**、随机点运动判别和多目标跟踪。我们还贡献了一项关于特定的最先进的深层强化学习剂--unreal（jaderberg 等人, 2016 年）的视觉心理物理学研究。这项研究得出了一个令人惊讶的结论，即 unreal 比它对更小的刺激更快速地学习更大的**目标**刺激。反过来，这种洞察以简单的小窝视觉模型的形式进行了具体的改进，结果是显著提升 unreal 在心理实验室任务和标准的 deepmind 实验室任务方面的表现。通过开放采购的心理实验室，我们希望促进一系列未来的此类研究，同时推进深度强化学习，改善其与认知科学的联系。少

2018 年 2 月 4 日提交;v1 于 2018 年 1 月 24 日提交;最初宣布 2018 年 1 月。

评论:28 页, 11 位数字

269. 建议: 1801 1.07495[pdf] Cs。CI

我们之间的敌人: 基于威胁的仇恨言论 "基于" 接受 "语言嵌入

作者:wafa alorainy, pete burnap, han liu, matthew williams

摘要: 针对个人和社会群体的攻击性或对立语言基于其个人特征 (也称为网络仇恨言论或网络仇恨) 经常被张贴并广泛流传到万维网上。这可被视为个人和社会紧张关系的一个关键风险因素。基于网络的自动网络仇恨**检测**对于观察和理解社区和区域社会紧张关系十分重要----特别是在可以迅速广泛查看和传播帖子的在线社交网络中。虽然以前的工作涉及使用词汇、词袋或概率语言解析方法, 但它们往往遇到类似的问题, 即网络仇恨可能会变得困惑和间接----因此取决于个别单词或短语的发生情况可能会导致大量的虚假否定, 提供不准确的代表网络仇恨的趋势。这个问题促使我们对微妙语言使用的表现进行思考, 例如提到来自 "他者" 的威胁, 包括在可恨的背景下移民或工作繁荣。我们提出了利用语言使用的框架, 围绕 "其他" 和群体间威胁理论来识别这些微妙之处, 并实现了一种新的分类方法, 使用嵌入学习来计算各部分之间的距离被认为是 "其他" 叙事的一部分。为了验证我们的方法, 我们对不同类型的网络仇恨, 即宗教、残疾、种族和性取向进行了几次实验, 使用 f-措施分数对通过我们的模型 0.93、0.93、0.93 获得的仇恨事例进行了评分。和 0.98, 使分类器的精度比最先进的 "

2018 年 3 月 8 日提交;v1 于 2018 年 1 月 23 日提交;最初宣布 2018 年 1 月。

270. 建议: 1801 1.07 215[pdf,其他] Cs。艾

按顺序处理您的工作: 数据库审核的博弈理论优先级

作者:赵燕,李波,叶夫根尼·沃罗比奇克,阿隆·拉兹卡,丹尼尔·法布里, 布拉德利·马林

摘要: 为了加强数据库的隐私保护, 在存储和处理越来越多的详细个人数据的情况下, 开发了多种机制, 如审计日志记录和警报触发器, 通知管理员可疑情况活动;但是, 两个常见的主要限制是: 1) 此类警报的数量通常大大超过资源受限的组织的能力, 2) 战略攻击者可能会掩盖自己的行为或仔细选择哪些记录他们接触, 使不称职的统计**检测**模型。为了解决这些问题, 我们引入了一种新的数据库审核方法, 它明确地考虑了对抗行为, 1) 确定调查警报类型的顺序, 2) 提供了为每种类型分配多少资源的上限.我们将数据库审核员和潜在攻击者之间的交互建模为 stackelberg 游戏, 在该游戏中, 审核员选择审核策略, 攻击者选择**要定位的记录**。提出了一种将线性规划、列生成和启发式搜索相结合的相应方法来推导审计策略。为了测试策略搜索性能, 采用了公开的信用卡应用程序数据集, 表明我们的方法产生了高质量的混合策略作为数据库审核策略, 我们的一般方法显著地优于非游戏理论基线。少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

类:D.4.6;H.2.0;K.6.5;j.1;i 。2

271. 建议: 1801. 06687[pdf,其他] Cs。简历

多伊 10.1109/TCYB.2018.2869384

一种直接选择性小目标运动检测杂乱背景下的视觉神经网络

作者:王宏新,彭继根,岳世刚

摘要: 区分在杂乱背景下移动的**目标**是一个巨大的挑战, 更不用说**检测一个**小到一个或几个像素的**目标**, 并在飞行中跟踪它了。在苍蝇的视觉系统中, 一类被称为小**目标**运

动探测器 (stmd) 的特定神经元被确定为对小**目标**运动表现出微妙的选择性。一些 stmd 还表现出方向选择性，这意味着这些 stmd 只对其首选运动方向有强烈的响应。定向选择性是这些 stmd 神经元的一个重要特性，有助于跟踪飞行中的配偶等小**目标**。然而，在系统地模拟这些定向选择性 stmd 神经元方面做得很少。本文提出了一种基于定向选择性 stmd 的神经网络 (dstmd)，用于杂乱背景下的小**目标检测**。在所提出的神经网络中，引入了一种新的通过从两个像素中继的相关信号实现方向选择性的相关机制。然后，在空间场上实现 stmd 神经元大小选择性的侧向抑制机制。大量实验表明，该神经网络不仅符合当前的生物学发现，即表现出方向性偏好，而且在检测小目标时也能可靠地**检测**杂乱**的**目标。背景。少

2018 年 9 月 29 日提交;v1 于 2018 年 1 月 20 日提交;最初宣布 2018 年 1 月。

评论:14 页, 21 个数字

272. **xiv:1801. 06482[pdf,其他] Cs。红外**

深入学习检测跨多个社交媒体平台的网络欺凌

作者:sweta Agrawal, amit awekar

摘要: 网络欺凌的骚扰是社交媒体上的一个重要现象。网络欺凌**检测的**现有工作至少有以下三个瓶颈之一。首先，它们只**针对**一个特定的社交媒体平台 (smp)。其次，它们只涉及网络欺凌的一个话题。第三，他们依靠精心打造的数据特征。我们表明，基于深度学习的模型可以克服这三个瓶颈。这些模型在一个数据集中学到的知识可以转移到其他数据集。我们使用三个真实世界的数据集进行了广泛的实验: formspring (12k 帖子)、推特 (16k 帖子) 和 Wikipedia(100k 帖子)。我们的实验提供了一些关于网络欺凌**检测的**有用见解。据我们所知，这是首次使用基于深度学习的模型和转移学习，系统地分析多个 smp 中各种主题的网络欺凌**检测**。少

2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

评论:接受 2018 年 ecir

273. **xiv:1801. 06428[pdf,其他] cse**

多伊 10.1109/ICSE-C.2017.16

防撞范围: 用于安卓应用自动化测试的实用工具

作者:kevin moran, mario linares-vasquez, carlos bernal-cardenas, christopher vendome , denys poshyvanyk

摘要: 在测试移动应用程序时，由于其普遍的事件驱动性质和复杂的上下文功能 (如传感器、通知)，出现了独特的挑战。由于所需的检测或平台依赖，目前 android 应用的自动输入生成方法通常不适合开发人员使用，并且通常无法有效地发挥上下文功能。为了更好地支持开发人员执行移动测试任务，在此演示中，我们展示了一个名为 crashscope 的新颖的自动化工具。该工具根据静态和动态分析的几种策略，探索使用系统输入生成的给定 android 应用程序，其内在目标是触发崩溃。当**检测到**崩溃时，crashscope 将生成增强型崩溃报告，其中包含屏幕截图、详细的崩溃重现步骤、捕获的异常堆栈跟踪以及在**目标**设备。初步研究的结果表明, crashscope 能够发现与其他最先进的工具一样多的崩溃，同时向开发人员提供详细有用的崩溃报告和测试脚本。网站: www.crashscope-android.com/crashscope-home 视频网址: https://youtu.be/ii6S1JF6xDw

2018 年 1 月 17 日提交;最初宣布 2018 年 1 月。

评论:4 页，在第 39 届 ieeeicm 软件工程国际会议 (icsea17) 会议上接受.

274. 建议: 1801 1.06 353[pdf, ps,其他] Cs。简历

转移学习提高语音情绪分类的准确性

作者:siddique latif, rajib rana , shahzad younis,junaid qadir, julien epps

文摘: 现有的大多数语音情感识别研究都集中在利用在相同条件下从同一语料库收集的训练和测试数据进行自动**情绪检测**。事实证明，在交叉语料库和跨语言场景中，这类系统的性能显著下降。为了解决这一问题，本文利用转移学习技术，提高了跨语言和交叉语料库场景中新颖的语音情感识别系统的性能。对三种不同语言的五种不同语料库的评价表明，与以往的交叉体情感识别方法相比，深度信仰网络 (dbs) 提供了更好的准确性，这相对于稀疏自动编码器和 svm 基线系统而言。结果还表明，使用大量语言进行培训，并在培训中使用一小部分**目标**数据，与基线相比，对于培训实例有限的语料库来说，也能显著提高准确性。少

2018 年 3 月 26 日提交;v1 于 2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

275. 建议: 1801. 06270[pdf, ps,其他] Cs。铬

对动态云存储中的高级持久性威胁的防御: blotto 上校游戏方法

作者:明辉敏,梁晓,谢彩霞,穆罕默德·哈吉米尔萨代吉, 纳拉扬 b. mandayam

摘要: 高级持久威胁 (apt) 攻击者应用多种复杂的方法，不断地、秘密地从**目标**云存储系统窃取信息，甚至可以诱使存储系统应用特定的防御策略和相应地攻击它。本文将 apt 攻击者和防御者之间的交互分配给云存储系统中的多个存储设备 (cpu)，形成了 blotto 上校游戏。在 apt 攻击者和防御者之间的对称和非对称 cpu 中，为 cpu 分配游戏的纳什均衡 (nex) 导出，以评估有限的 cpu 资源、日期存储大小和存储设备数量对预期数据的影响保护级别和云存储系统的效用。提出了一种基于 "热启动" 策略提升 (phc) 的 cpu 分配方案，该方案利用类似情况下的经验，初始化质量值，以加快提高学习速度，从而实现最佳的 apt 防御在不了解 apt 攻击模型和数据存储模型的情况下实现动态游戏中的性能。基于深度 q 网络 (dqn) 的 cpu 分配方案进一步提高了大量 cpu 和存储设备的 apt **检测**性能。仿真结果表明，与基于 q 学习的 cpu 分配针对 apt 相比，我们提出的基于强化学习的 cpu 分配可以提高数据保护水平和云存储系统的效用.

2018 年 1 月 18 日提交;最初宣布 2018 年 1 月。

276. 建议: 1801 1.05938[pdf, ps,其他] Cs。镍

wilad: 通过异常检测实现无线定位

作者:cam ly nguyen, aftab khan

摘要: 我们提出了一种基于 rss (接收信号强度) 的无线本地化的新方法，在这种情况下，只需要对象在特定区域内部或外部的信息，而不是对象的绝对定位。这是通过许多应用来推动的，包括但不限于安全性:**检测**物体是否从安全位置被移出; (b) 无线传感器网络:**检测**传感器在网络区域外的移动(c) 计算行为分析:**检测**离开零售店的客户。这种**检测**系统的结果自然可以用于建立对系统或用户行为的更高级别的上下文理解。我们使用监督学习方法来克服与基于 rss 的本地化系统相关的问题，包括多路径淡入淡出、隐藏和不正确的模型参数 (如在无监督方法中)。此外，为了降低收集培训数据的成本，我们采用了一种称为 "一类支持向量机 (oc-svm)" 的**检测**方法，该方法只需要一类数据 (正数据或**目标**类数据) 即可进行培训。我们利用无线信号和 oc-svm 的特性，推导出精度的数学近似值。在此基础上，我们提出了一个新的数学公式，以找到设备的最佳

位置。这使我们能够优化放置，而无需执行任何昂贵的实验或模拟。在模拟实验和实际实验的基础上，验证了所提出的数学框架。少

2018 年 1 月 18 日提交;最初宣布 2018 年 1 月。

日记本参考:ieee globeecom 2017

277. 建议: 1801. 05124[pdf,其他] Cs。简历

用于对象检测的定位感知主动学习

作者:高志志,李登宇,普拉迪普·森，刘明宇

摘要: 主动学习--一类迭代搜索要包含在训练数据集中的信息最丰富的样本的算法--已被证明可以有效地注释数据以进行图像分类。然而，由于确定对象定位假设的信息性更加困难，利用主动学习进行目标检测在很大程度上仍未得到探索。本文讨论了这一问题，并提出了两个衡量对象假设信息的指标，使我们能够利用主动学习来减少**实现目标**对象检测所需的注释数据量性能。我们的第一个度量度量测量对象假设的 "本地化紧密性"，它基于区域建议和最终预测之间的重叠比率。我们的第二个度量度量测量对象假设的 "本地化稳定性"，它基于输入图像被噪声破坏时预测对象位置的变化。我们的实验结果表明，通过使用建议的指标来扩展为分类而设计的传统主动学习算法，所需的标记培训数据量最多可以减少 25%。此外，在 pascal 2007 和 2012 数据集上，我们的本地化稳定性方法比仅使用分类的基线方法平均有 96.5 和 81.9% 的相对改进。少

2018 年 1 月 16 日提交;最初宣布 2018 年 1 月。

278. 建议: 1801. 03074[pdf,其他] Cs。铬

无人机游戏-从加密的 fpv 通道检测流 poi

作者:ben nassi, raz Ben-Netanel, adi shamir, yuval elovici

摘要: 无人机对人们的隐私造成了新的威胁。我们现在正处于一个时代，任何配备了摄像机的无人机都可以通过加密的第一人称视图 (fpv) 频道将主体流式传输流式传输，从而侵犯主体的隐私。虽然已经建议**了许多**方法来检测附近的无人机，但它们都有同样的缺点: 它们无法准确地识别捕获的是什么，因此它们无法区分无人机的合法使用 (例如,使用无人机从空中拍摄自拍) 和侵犯他人隐私的非法使用 (当同一运营商使用无人机将视线流进邻居公寓的窗户时)，在某些情况下，这种区别取决于无人机的摄像机，而不是无人机的位置。在本文中，我们打破了人们普遍持有的信念，即使用加密来保护 fpv 通道，阻止拦截器提取正在流式传输的 poi。我们展示了利用物理刺激来**检测**无人机相机是否实时指向**目标**的方法。我们研究了像素变化对 fpv 通道 (在实验室设置中) 的影响。根据我们的观察，我们展示了拦截器如何执行侧信道攻击，通过分析从真正的无人机 (dji mavic) 两次使用传输的加密 fpv 通道来**检测目标**是否正在流式传输情况: **当目标**是私人住宅，当**目标**是一个主体。少

2018 年 1 月 9 日提交;最初宣布 2018 年 1 月。

评论:https://www.youtube.com/watch? v=4icQwducz68

279. 建议: 1801. 03049[pdf,其他] Cs。简历

元跟踪器: 视觉对象跟踪器的快速、可靠的在线适应

作者:eunbyung park,亚历山大 c. berg

摘要: 本文改进了使用在线适应的最先进的视觉对象跟踪器。我们的核心贡献是一种基于离线元学习的方法，用于调整在线适应跟踪中使用的初始深度网络。元学习是由深度网络的目标驱动的，深度网络可以快速适应在未来框架中的特定**目标**的有力模型。理想

情况下，生成的模型侧重于对未来框架有用的功能，并避免过度拟合背景杂波、目标的小部分或噪音。通过在元学习过程中强制实施少量更新迭代，生成的网络训练速度显著加快。我们在高性能跟踪方法的基础上演示了这种方法：基于跟踪的基于 mdnet 的检测和基于相关的 crest.关于标准基准的实验结果，otb2015 和 vot2016 表明，我们的两个跟踪器的元学习版本提高了速度、准确性和鲁棒性。少

2018 年 3 月 19 日提交;v1 于 2018 年 1 月 9 日提交;最初宣布 2018 年 1 月。

评论:代码: https://github.com/silverbottlep/meta_trackers

280. **建议: 1801.02686** **Cs。简历**

多伊 10.572/000670610101560167

不确定性条件下城市情景的多目标检测与跟踪

作者:achim kampker, mohsen sefati, arya abdul rachman, kai kreisköther , pascual campoy

摘要: 面向城市的自主车辆需要可靠的感知技术来应对大量的不确定性。最近推出的紧凑型 3d 激光雷达传感器提供了一种环绕空间信息，可用于增强车辆感知。我们提出了一个实时集成框架的多**目标**目标目标**检测**和跟踪使用三维 lidar 为城市使用。我们的方法将传感器遮挡感知**检测**方法与计算效率高的启发式基于规则的滤波和自适应概率跟踪相结合，以处理 3d 激光雷达和**目标**对象移动的复杂性。使用真实世界的预录 3d 激光雷达数据进行的评估结果以及与最先进作品的比较表明，我们的框架能够在城市环境中实现有希望的跟踪性能。少

2018 年 2 月 3 日提交;v1 于 2018 年 1 月 8 日提交;最初宣布 2018 年 1 月。

评论:在审查时发现了一些重要的编辑问题。纸张在重新提交前将经过语言复卷

日记本参考:第 4。vehits. proc . 109 (2018) 156-167

281. **建议: 1801.01828[pdf, ps,其他]** **Cs。CI**

屏蔽谷歌对抗攻击的语言毒性模型

作者:nestor rodriguez, sergio rojas-galeano

摘要: 网络社区缺乏节制使参与者能够遭受个人侵犯、骚扰或网络欺凌，这些问题在当代后真相政治情景中因极端主义激进化而加剧。这种敌意通常是通过有毒的语言、亵渎或辱骂性的言论来表达的。最近，谷歌开发了一种基于机器学习的毒性模型，试图评估评论的敌意;不幸的是 ，有人认为 ，上述模式可能会纵评论文本序列的对抗性攻击所欺骗。本文首先将这种对抗性攻击描述为使用混淆和极性变换。前者通过排版编辑来腐蚀有毒触发内容，而后者则通过对有毒内容的语法否定来欺骗。然后，我们提出了一个两阶段的方法来对抗这些异常，在最近提出的文本去混淆方法和毒性评分模型的基础上。最后，我们进行了一个实验，约 24000 条扭曲的评论，展示了如何以这种方式恢复对抗变种的毒性是可行的，同时导致处理时间的大约增加了两倍。尽管新的对手挑战将不断地来自于书面语言的多才多艺，但我们预计，将机器学习和文本模式识别方法结合起来的技术，每一种**技术都针对**不同层次的语言特征，将需要实现对有毒语言的可靠**检测**，从而促进无侵略的数字交互。少

2018 年 1 月 5 日提交;最初宣布 2018 年 1 月。

282. **建议: 1801.01228[pdf,其他]** **Cs。艾**

多伊 10.1109/IROS.2017.8206423

一种基于无人机的检测目标搜索决策理论方法

作者:aayush gupta, daniel bessonov, patrick li

摘要: 搜救任务和监视需要在大片地区找到**目标**。这些任务往往使用带有摄像头的无人驾驶飞行器 (uav) 来**探测**和走向**目标**。然而，常见的无人机方法有两个简化的假设。首先，他们假设从不同高度进行的观测是确定正确的。实际上，观测是嘈杂的，随着用于观测的高度的增加，噪声也会增加。其次，他们假设运动命令正确执行，这可能不会发生由于风和其他环境因素。为了解决这些问题，我们提出了一种顺序算法，该算法使用部分可观测的马尔可夫决策过程 (pomdp)，根据观测结果实时确定动作。我们的配方既处理观测，也处理运动的不确定性和误差。我们运行离线模拟并学习策略。此策略在无人机上运行，以有效地找到**目标**。我们采用一种新的紧凑型来表示无人机相对于**目标**坐标的坐标。与启发式策略相比，我们的 pomdp 策略的目标速度提高了 3.4 倍。少

2018 年 1 月 3 日提交;最初宣布 2018 年 1 月。

评论:发布于 ieee iros 2017. 6 页

日记本参考:a. gupta, d. bessonov 和 p. li, "用无人机进行基于探测的目标搜索的决策理论方法", 2017 ieeeee/rsj 智能机器人和系统国际会议，加拿大温哥华, bc, 2017, pp. 5304-5309

283. 建议: 1801 1.00554[pdf,其他] Cs。CI

你听到了吗？自动语音识别的对抗实例

作者:moustafa alzantot, bharathan balaji, mani srivastava

摘要: 语音是一种常见而有效的人与人之间的沟通方式，智能手机和家庭集线器等现代消费设备配备了基于深度学习的精确自动语音识别功能，以实现人与人之间的自然互动。机器。最近，研究人员展示了对机器学习模型的强大攻击，这些攻击可能会愚弄他们产生不正确的结果。然而，以前几乎所有关于对抗性攻击的研究都集中在图像识别和物体**检测**模型上。在这篇简短的论文中，我们首次展示了针对语音分类模型的对抗性攻击。我们的算法通过添加小背景噪声来执行**有针对性**的攻击，成功率为 87%，而无需了解基础模型参数和体系结构。我们的攻击只改变音频剪辑样本子集中最不重要的位，噪声不会改变 89% 的人类听众对音频剪辑的感知，在我们的人类研究中评估。少

2018 年 1 月 2 日提交;最初宣布 2018 年 1 月。

评论:发表于 NIPS 2017 年机器欺骗研讨会

284. 建议: 1801. 00235[pdf,其他] Cs。铬

利用深度学习早期发现交叉火力攻击

作者:Saurabh misra, mmmxuantan , mostafa rezazad, matthias r. brust, ngai-man cheang

摘要: 交叉火力攻击是最近提出的一种威胁，旨在切断城市或州等整个地理区域与互联网的连接。在多个阶段的协调下，攻击使用大规模分布式僵尸网络生成低速率的良性通信，旨在填充选定的网络链接 (即所谓**的目标**链路)。采用良性流量，同时**针对**多个网络链接，使得检测交叉火力攻击成为一个严重的挑战。本文提出了一个早期**探测交叉火力**攻击的框架，即在攻击的预热期进行**探测**。我们建议监控潜在诱饵服务器的流量，并讨论与其他监控方法相比的优势。由于低速率攻击流量很难与后台流量区分开来，我们研究了几种深度学习方法来挖掘攻击检测的时空特征. 我们研究了自成管器、卷积神经网络 (cnn) 和长期短期存储器 (lstm) 网络，以**检测**其预热期间的交叉火力攻击。我们报告令人鼓舞的实验结果。少

2018 年 4 月 19 日提交;v1 于 2017 年 12 月 30 日提交;最初宣布 2018 年 1 月。

评论:5 页, 5 个数字。在新加坡 2017 年深度学习安全研讨会上发表。增加了第 2 节和第 4 节的参考资料。添加了新作者

285. xiv:1801. 00025[pdf] Cs。铬

一种基于深度信念网络的风险主机检测机器学习系统

作者:冯王燕,吴顺宁,李晓丹,凯文·昆克

摘要: 为了确保企业的网络安全, 通常是 siem (安全信息和事件管理) 系统, 以规范来自不同预防技术的安全事件并标记警报。安全运营中心 (soc) 的分析师会调查警报, 以确定它是否真正是恶意的。但是, 警报的数量通常是压倒性的, 其中大多数是假阳性, 超过了 soc 处理所有警报的能力。非常需要尽可能地降低假阳性率。以往的研究大多集中在网络入侵**检测**上, 重点研究了风险**检测**, 并提出了一种智能深信念网络机器学习系统。该系统利用警报信息、各种安全日志和分析人员在真实企业环境中的调查结果来标记极有可能被破坏的主机。文本挖掘和基于图形的方法用于生成**目标**和创建机器学习的功能。实验中, 将深度信念网络与其他机器学习算法进行了比较, 包括多层神经网络、随机林、支持向量机和逻辑回归。实际企业数据的结果表明, 深度信念网络机器学习系统在我们的问题上比其他算法表现更好, 比目前基于规则的系统有效六倍。我们还实现了从数据收集、标签创建、特征工程到在真实的企业生产环境中承载分数生成的整个系统。少

2017 年 12 月 29 日提交;最初宣布 2018 年 1 月。

评论:10 页, 10 人。该论文被 ieee 通信和网络安全会议 2017 年所接受。然而, 它没有公布, 因为这两位作者都出现在会议上

286. 决议: 1712.09162[pdf] 反渗透委员会

redbee: 一种用于实时运动目标检测的可视化惯性无人机系统

作者:黄,陈鹏, 杨新阳, 广亭,程

文摘: 空中监视和监测需要从移动摄像机进行实时和可靠的运动**检测**。大多数现有的无人机技术都涉及到将视频数据流发送回使用高端台式计算机或服务器的地面站。这些方法有一个共同的主要缺点: 数据传输受到相当大的延迟和可能的损坏。机载计算不仅可以克服数据损坏问题, 而且可以增加运动范围。遗憾的是, 由于承载能力有限, 为无人机配备高加工能力的计算硬件是不可行的。因此, 对于计算能力有限的无人机, 开发一种实时性能、高精度的运动**检测**系统是非常可取的。本文提出了一种用于实时运动**检测**的视惯性无人机系统, 即 redbee, 该系统有助于克服具有强视差和动态背景的拍摄场景中的挑战。redbee 可以在最先进的商用低功耗应用处理器 (例如, 用于我们的原型无人机的 snaprong 飞行板) 上运行, 可实现实时性能和高**检测**精度。redbee 系统通过惯性辅助双平面同源估计克服了具有强视差的拍摄场景中的障碍;通过基于空间、时间和熵一致性的概率模型对运动目标进行识别, 解决了动态背景拍摄场景中的问题。实验表明, 与最先进的实时机载**检测**系统相比, 该系统在室外环境下**检测**运动**目标**时具有更高的精度。少

2017 年 12 月 25 日提交;最初宣布 2017 年 12 月。

评论:8 页, ieeee® rsj 智能机器人和系统国际会议 (iros 2017)

287. 第: 1712.08996[pdf,其他] Cs。铬

基于 api 方法序列的深度学习的 android 恶意软件检测

作者:elmouatez billah karbab, mourad debbabi , abdelouahid derhab, djedjiga mouheb

摘要: 自过去几年以来, android 操作系统经历了极高的人气。这一占主导地位的平台不仅在移动世界中站稳脚跟，而且在物联网 (iot) 设备中也确立了自己的地位。然而，这种人气是以牺牲安全性为代价的，因为它已经成为恶意应用的**诱人目标**。因此，对复杂、自动和便携式恶意软件**检测**解决方案的需求日益增加。在本文中，我们提出 maldozer，一个自动 android **恶意软件检测**和家庭归因框架，依赖于使用深度学习技术的序列分类。从应用程序的 api 方法调用的原始序列开始, maldozer 会自动从实际示例中提取并学习恶意和良性模式，以**检测** android 恶意软件。maldozer 可以作为一个无处不在的恶意软件**检测**系统，它不仅部署在服务器上，还部署在移动设备甚至物联网设备上。我们评估 maldozer 在多个 android 恶意软件数据集上的评估，范围从 1k 到 33k 恶意软件应用程序，以及 38k 良性应用。结果表明, maldozer 能够正确**检测**恶意软件，并将其归因于其实际家庭的 f1 分数为 96%-99%，假阳性率为 0.06%-2%，在所有测试的数据集和设置下。少

2017 年 12 月 24 日提交;最初宣布 2017 年 12 月。

评论:17 页，提交给 elsevier 数字调查杂志

288. **第 1712.08062[pdf,其他] Cs。铬**

关于带有对抗性贴纸的攻击对象检测器的说明

作者:kevin eykholt, ivan evtimov, earlence fernandes, bo li, dawn song, tadayoshi kohno, amir rahmati, atul prakash, florian tramer

摘要: 深度学习已被证明是计算机视觉的强大工具，并已被广泛用于许多任务。然而，众所周知，深度学习算法容易受到对抗实例的影响。创建这些对抗性输入时，当提供给深度学习算法时，它们很可能会被错误地标记。当深度学习被用来协助安全关键决策时，这可能是有问题的。最近的研究表明，在各种物理条件下，分类器可以被物理对抗的例子所攻击。鉴于最先进的反对**检测**算法更难被同一套对抗示例所愚弄，我们在这里展示了这些检测器也可能受到物理对抗示例的攻击。在本文中，我们简要展示了静态和动态测试结果。我们设计了一种产生物理对抗性输入的算法，它可以愚弄 yolo 目标探测器，还可以基于可转移性以相对较高的成功率攻击 f 极 mcn。此外，我们的算法可以将对抗输入的大小压缩到贴纸上，当贴纸附加到**目标**对象时，会导致检测器错误地标记或在很高的时间内**无法检测**到目标。本说明提供了一小部分结果。我们即将发表的论文将包含对其他对象探测器的全面评估，并将介绍算法。少

2018 年 7 月 23 日提交;v1 于 2017 年 12 月 21 日提交;最初宣布 2017 年 12 月。

评论:简短说明: 本论文的全文已被 usenix woot 2018 所接受，可在 arxiv:8707 7769 上查阅

289. **第: 1712.07721[pdf,其他] Cs。简历**

一种多模态数据中人员检测的订单保留双线性模型

作者:oytun ulutan, benjamin s.riggan, nasser m. nasrabadi, b . s. manjunath

文摘: 我们提出了一个新的顺序保持双线性框架，利用低分辨率视频在多模态环境中使用深度神经网络进行**人的检测**。在这种设置中，摄像机的战略位置使不太坚固的传感器，例如监测地震活动的检波器，位于摄像机的视场 (fov) 内。主要的挑战是能够利用目标上不到 40 像素的视频中的足够信息，同时也利用地震等其他模式中的歧视性信息较少。与最先进的方法不同，我们的双线性框架在计算对要素之间的矢量外部产品时保

留时空顺序。尽管这些外部产品的维度很高，但我们证明，我们的保序双线性框架比最近的无阶双线性模型和替代融合方法产生更好的性能。少

2018 年 1 月 11 日提交;v1 于 2017 年 12 月 20 日提交;最初宣布 2017 年 12 月。

290. **第: 1712.06920[pdf] Cs。红外**

使用线性分类器进行大规模的破坏性检测-2017 年 wsdm 杯上的康克伯里破坏检测器

作者:阿列克谢·格里戈列夫

摘要: 目前，许多人工智能系统依靠知识库来丰富它们所处理的信息。这样的知识库通常很难获得，因此它们是众包: 它们可供互联网上的每个人建议编辑和添加新的信息。不幸的是，他们有时成为将不准确或攻击性信息放在那里的破坏者的**目标**。这对使用这些知识库的系统尤其不利: 对他们来说，使用可靠的信息做出正确的推断是很重要的。其中一个知识库是维基数据，为了打击破坏者，2017 年 wsdm 杯的组织者要求参与者建立一个检测不信任编辑的模型 。本文提出了杯的第二个解决方案: 我们证明了用简单的线性分类来实现竞争性能是可能的。通过我们的方法，我们可以在测试数据上达到 0.938 的 au roc。此外，与其他方法相比，我们的方法要快得多。该解决方案可在 github 上使用。少

2017 年 12 月 19 日提交;最初宣布 2017 年 12 月。

评论:2017 年 wsdm 杯上的 Vandalism 探测器，见 arxiv:1712. 0556

类:h。3

291. **第 1712.06417[pdf,其他] Cs。Sy**

一种基于自动生成控制的网络攻击在线检测框架

作者:tonghuang, bharadwaj satchidanandan, p. r.kumar, le zie

文摘: 我们提出了一个在线框架来**检测**对自动生成控制 (agc) 的网络攻击。基于动态水印的方法，设计了一种基于网络策略的检测算法。**该检测**算法为复杂攻击者对目标电力系统的物理和统计模型有广泛的了解，从而**为网络**攻击的检测提供了理论保障。建议的框架实际上是可以实现的，因为它不需要对发电单元进行硬件更新。该框架在四域系统和 140 总线系统中都得到了验证。少

2018 年 4 月 20 日提交;v1 于 2017 年 12 月 15 日提交;最初宣布 2017 年 12 月。

评论:本文已被接受在未来一期的 ieee 电力系统事务中发表，但尚未完全编辑。内容可能会在最终发布前更改

292. **建议: 1712.05647[pdf,其他] Cs。简历**

多伊 10.1016/j.compag.2013.11.008

利用条件随机场进行葡萄浆果尺寸高通量测定的自动图像分析框架

作者:riana roscher, katja herzog, annemarie kunkel, anna kicherer, reinhard töpfer, wolfgang förstner

摘要: 浆果大小是葡萄育种中最重要的果实性状之一。无创的、基于图像的表型有望快速、精确地监测葡萄浆果的大小。本研究开发了一个自动图像分析框架，以估计葡萄浆果的大小从图像的高通量的方式。该框架包括: (一)**检测**可能是浆果的圆形结构，以及 (二) 利用条件随机场将这些结构分类为 "浆果" 或 "非浆果" 类。该方法使用了一类分类的概念，因为只有**目标**类 "berry" 是感兴趣的，需要建模。此外，分类是使用自动主动学习方法进行的，即在分类过程中不需要用户交互，此外，该过程还自动适应不断

变化的图像条件，例如照明或浆果色。该框架在三个数据集上进行了测试，这些数据集共有 139 张图像。这些图片是根据 bbch 量表在葡萄生长不同阶段的实验葡萄园拍摄的。框架估计的植物的平均浆果大小与手工测量的浆果大小相关。0.88. 少
2017 年 12 月 15 日提交;最初宣布 2017 年 12 月。

日记本参考:农业中的计算机和电子 100 (2014), 148-158

293. **第: 1712.04823[pdf,其他] si**

用于局部社区检测的克里洛夫子空间近似

作者:kunhe, pan shi, david bindel, john e . hopcroft

文摘: 社区**检测**是计算机科学、社会科学、生物学、物理学等多个领域的重要信息挖掘任务。对于越来越常见的大型网络数据集，全球社区**检测**的费用高得令人望而却步，注意力已转移到挖掘当地社区的方法上，即从很少有标记的种子成员。为了解决这一半监督采矿任务，我们提出了一种称为 lsp 的局部光谱亚空社区**检测**方法。首次在种子周围应用采样技术，以显著缩小搜索规模。然后，我们基于 krylov 子空间定义了一个局部光谱子空间家族，并通过 krylov 子空间上的一个范数最小化为**目标**社区寻求稀疏指示器。losp 的变化取决于不同扩散速度的随机游走类型、规则随机游走或逆随机游走、局部光谱子空间的维数和扩散的步骤。根据瑞利商数对所提出的 losp 方法的有效性进行了理论分析，并在社会、生产和生物领域的各种现实世界网络以及广泛的合成 lfr 基准数据集。少

2017 年 12 月 13 日提交;最初宣布 2017 年 12 月。

评论:提交给 ieee 知识和数据工程事务 (tkde) (正在审查中)

294. **第 1712.02824[pdf, ps,其他] Cs。简历**

堆叠去噪自动编码器和转移学习用于免疫金粒子检测与识别

作者:ricardo gamelas sousa,豪尔赫 m. santos, luís m.silva, luis a.亚历山大, tiago esteves, sara rocha, paulo monjardino, joaquim marques de sá, franciscofigueiredo, pedro quelhas

文摘: 本文提出了一种检测免疫金颗粒的**系统**和用于识别这些免疫型颗粒的转移学习 (tl) 框架。免疫金粒子是一种高放大方法的一部分，用于在亚细胞水平上选择性定位生物分子，只有通过电子显微镜才能看到。细胞壁中免疫金颗粒的数量允许评估其成分的差异，为分析不同植物的质量提供了一个工具。对于它的量化，你需要一个费尽周万尽的手动标记 (或注释) 的图像包含数百个粒子。本文提出的系统可以显著利用这一人工任务的负担。对于粒子**检测**，我们使用与 sda 耦合的 log 滤波器。为了提高识别能力，我们还研究了 tl 设置在免疫原识别中的适用性。tl 在包含不同大小粒子的其他数据集 (**目标**问题) 上重用源问题的学习模型。该系统是为解决玉米细胞的一个特殊问题而开发的，即确定胚乳转移细胞中细胞壁生长物的组成。这个新颖的数据集以及复制我们实验的代码是公开的。我们确定，仅 log 检测器就能达到 f 测量精度的 84% 以上。与基准模型相比，利用 tl 开发免疫型识别也提供了卓越的性能，使准确率提高了 10\%。少

2017 年 12 月 7 日提交;最初宣布 2017 年 12 月。

295. **第: 1712.02560[pdf,其他] Cs。简历**

无监督域适应的最大分类器差异

作者:kuniaki saito, kohei watanabe, yoshitaka ushiku, tatsuya harada

文摘: 在本文中，我们提出了一种无监督域适应的方法。许多对抗学习方法训练域分类器网络来区分作为源或**目标**的特征，并训练一个特征生成器网络来模拟鉴别器。这些方法存在两个问题。首先，域分类器只尝试将要素区分为源或**目标**，因此不考虑类之间特定于任务的决策边界。因此，受过训练的生成器可以在类边界附近生成不明确的特征。其次，这些方法旨在完全匹配不同域之间的特征分布，这是很困难的，因为每个域的特点。为了解决这些问题，我们引入了一种新的方法，它试图通过利用特定于任务的决策边界来调整源和**目标**的分布。我们建议最大限度地扩大两个分类器输出之间的差异，以**检测**远离源支持的**目标**样本。功能生成器学习在支持附近生成**目标**要素，以最大限度地减少差异。在图像分类和语义分割的多个数据集上，我们的方法优于其他方法。这些代码可在 \ urlhttps://github.com/mil-tokyo/MCD_DA}

2018 年 4 月 3 日提交;v1 于 2017 年 12 月 7 日提交;最初宣布 2017 年 12 月。

评论:接受 cvpr2018 口头，代码可在 https://github.com/mil-tokyo/MCD_DA

296. 第 1712.01877 [pdf,其他] cs. it

基于信道冲孔的大型 mimo 检测方案: 性能与复杂性分析

作者:h. sarieddeen, m. m. mansour, a. chehab

文摘: 针对大型多输入多输出 (mimo) 系统，提出了一种基于信道矩阵刺穿的低复杂度**检测**方案。众所周知，基于 qr 分解的 mimo **检测**的计算成本与三角化信道矩阵中反向替换和切片操作所涉及的非零条目的数量成正比，这可以对于涉及大型 mimo 尺寸的低延迟应用，效率过高。通过系统地刺穿通道以具有特定的结构，证明了通过采用追逐**检测**、列表**检测**、 空消除检测，以及变换矩阵上的子空间**检测**。对这些方案的性能进行了数学表征和分析，推导了可实现的分集增益和位误差概率的边界。令人惊讶的是，这表明刺穿不会对硬输出探测器的接收多样性增益产生负面影响。将分析扩展到计算每层位对数似然比的软输出**检测**;结果表明，通过命令感兴趣的层在刺穿通道时处于根部，可以实现显著的性能提升。编码和未编码方案的模拟证明，在天线数量和星座大小以及相关通道的存在下，所建议的方案都能有效地扩展。特别是，每层空间的软输出**检测**被证明实现了 2.5 db 信噪比增益。10^{-4} 个中的位错误率。
256-qam 16 x16mimo，同时节省 77% 空和取消计算。少
2017 年 12 月 5 日提交;最初宣布 2017 年 12 月。

297. 第 1712.01531 [pdf] cs. it

用于压缩分布式稀疏信号恢复的高效高效传感器监测

作者:吴俊宇,杨明勋,王向义

摘要: 为了在能效和数据质量控制之间取得平衡，提出了一种基于压缩传感的无线传感器网络分布式稀疏信号恢复的传感器审查方案。在该方法中，每个传感器节点采用已知支持数据压缩的稀疏传感向量，同时对感兴趣的稀疏信号向量的未知支持进行局部推断。这自然会导致一个三元审查协议，根据该协议，每个传感器 (i) 直接传输实值压缩数据，如果**检测到**传感矢量支持与信号支持重叠, (ii) 发送一个位位艰难的决定，如果空的支持重叠推断, (iii) 保持沉默，如果测量被判断为没有信息。然后，我们的设计旨在最大限度地减少空支持重叠已决定的错误概率，但在其他情况下是正确的，但必须根据一个可容忍的假警报概率的约束，即非空支持重叠已决定，但**否则为真,目标**审查率。我们推导出最优审查规则的闭式公式;还开发了一种使用双部分搜索的低复杂性实现。此外，还对平均通信成本进行了分析。为了在所提出的审查框架下，我们提出了一种改进的基于 l_1 最小化的全局信号重建算法，该算法利用了在融合中心接收的硬决

策向量的某些稀疏性。还推导了以受限等距特性为特征的分析性能保证。通过计算机仿真说明了该方案的性能。少

2018 年 1 月 15 日提交;v1 于 2017 年 12 月 5 日提交;最初宣布 2017 年 12 月。

评论:30 页, 9 个数字

298. 第 1712.01511[pdf,其他] Cs。简历

sar 目标识别中的联合嵌入与分类

作者:王嘉云,帕特里克·德德,余思拉

文摘: 深度学习可以是自动检测合成孔径雷达 (sar) 图像中**的目标**并对其进行分类的一种有效和高效的方法，但训练有素的神经网络必须对合成孔径雷达 (sar) 图像之间存在的变化保持鲁棒性至关重要。培训和测试环境。神经网络中的层可以理解为输入图像连续转换为嵌入特征表示，并最终转化为语义类标签。为了解决 sar **目标**分类中的超拟合问题，我们训练神经网络来优化嵌入式空间中点的空间聚类，并对最终的分类分数进行优化。我们证明了使用这种双重嵌入和分类丢失训练的网络的性能优于仅具有分类丢失的网络。研究了在不同网络层后放置嵌入损耗的问题，发现将嵌入损耗应用于分类空间可以获得最佳的 sar 分类性能。最后，我们对网络的十维分类空间的可视化支持了我们的说法，即嵌入损耗鼓励目标类集群之间的更大分离，用于 mstar 数据集的训练和测试分区。少

2017 年 12 月 16 日提交;v1 于 2017 年 12 月 5 日提交;最初宣布 2017 年 12 月。

299. 第 1712.00108[pdf,其他] Cs。简历

基于特权模式的动作检测的图形提取

作者:罗泽伦,谢俊婷,姜陆江,胡安·卡洛斯·涅布尔斯,李飞飞

摘要: 我们提出了一种在现实和具有挑战性的条件下处理多式联运视频中的动作检测的技术,在这种情况下，只有有限的训练数据和部分观测的模式可用。转移学习中的常用方法并不利用源域中可能存在的额外模式。另一方面，以前关于多式联运学习的工作只侧重于一个领域或任务，并不处理培训和测试之间的模式差异。在这项工作中，我们提出了一种称为图形蒸馏的方法，它将来自源域中大型多模式数据集的丰富特权信息整合在一起，并改进了在训练数据和模式所在**的目标**域中的学习稀缺。我们评估了我们在多模式视频中的行动分类和**检测**任务的方法，并表明我们的模型在 ntu rgb + d 和 pku-mmd 基准上的性能大大优于最先进的。代码在 http://alan.vision/eccv18_graph/ 发布。少

2018 年 7 月 27 日提交;v1 于 2017 年 11 月 30 日提交;最初宣布 2017 年 12 月。

评论:eccv 2018

300. 第 xiv:1711. 09985[pdf] Cs。铬

一种针对外部基于云的拒绝服务 (dos) 攻击的身份验证协议的形式化分析

作者:marwan darwish, abdelkader ouda, luiz fernando capretz

摘要: 拒绝服务 (dos) 攻击被认为是对云计算服务可用性的最大威胁之一。由于云计算系统的独特架构,**检测**和防止 dos 攻击的方法与传统网络系统中使用的方法有很大的不同。dos 攻击者的主要**目标**是身份验证协议，因为它被视为访问云资源的网关。在这项工作中，我们提出了一种基于云的身份验证协议--一种安全地对云用户进行身份验证并通过让用户参与高计算过程来有效防止云计算系统的 dos 攻击的协议。然后，

我们通过 syverson 和 van orschot (svo) 逻辑对协议进行了分析，以验证该协议在云计算系统中的身份验证过程。少

2017 年 11 月 22 日提交;最初宣布 2017 年 11 月。

评论:arxiv 管理说明: 文本与 arxiv:1511.08839 重叠

日记本参考:《国际信息安全研究杂志》，第 3 卷，半期，第 400-407 页, 2013 年 3 月至 6 月

301. **建议: 1711. 09822[pdf,其他] Cs。简历**

典型化对象的可扩展对象检测

作者:aayush garg, thilo will, william darling, willi richert, clemens marschner

摘要: 继卷积神经网络和单片模型架构最近取得突破之后，最先进的目标**检测**模型可以可靠、准确地扩展到多达数千个类的领域。然而，当扩展到数万，或者最终扩展到数百万个或数十亿的独特对象时，情况很快就会崩溃。此外，边界盒培训的端到端模型需要大量的培训数据。尽管--使用层次结构的一些技巧--有时可以扩展到数千个类，但干净图像注释的人工要求很快就会失控。本文提出了一种针对存在原型图像的品牌标识和其他程式化对象的两层对象**检测**方法。它可以扩展到大量的唯一类。我们的第一层是美国有线电视新闻网从单次拍摄多盒探测器系列的模型，学习提出一些程式化的对象可能会出现的区域。然后，对针对手头检索任务的图像索引运行建议的边界框的内容 。拟议的体系结构可扩展到大量对象类，允许在无需再培训的情况下连续添加新类，并在风格化的对象检测任务(如徽标识别) 上表现出最先进的质量。少

2017 年 11 月 29 日提交;v1 于 2017 年 11 月 27 日提交;最初宣布 2017 年 11 月。

评论:9 页, 7 个数字

302. **建议: 1711. 09728[pdf,其他] cs. cy**

评价孟加拉国电视台的性别形象

作者:md. naimul hoque, rawshan e fatima, manash kumar manal, nazmus saquib

摘要: 计算机视觉和机器学习方法以前被用来揭示电视和电影中性别的屏幕存在。在这项工作中，利用头部姿势、性别**检测**和肤色估计技术，我们证明了孟加拉国等南亚国家电视中的性别差异表现出独特的特点，有时甚至与流行的看法。我们在孟加拉国电视广告和政治脱口秀节目中显示出明显的女性银幕存在差异。此外，与流行的假设相反，我们证明，浅色肤色的肤色不如深色肤色流行，此外，可量化的肢体语言标记并不能提供关于性别动态的结论性见解。总体而言，这些性别描述参数揭示了屏幕上性别政治的不同层面，有助于直接激励措施以细致入微和**有针对性**的方式解决现有的差距。少

2017 年 11 月 14 日提交;最初宣布 2017 年 11 月。

评论:在2017年为发展中世界举办的机器学习研讨会上发表。答复作者: nazmus saquib

303. **第: 1711. 09994[pdf,其他] Cs。简历**

fclt-一个完整的相关长期跟踪器

作者:alan lukežič, luka cechovin zajc, tomášvojibu, jii matas, matej ksten

摘要: 我们建议 fclt-一个完全相关的长期跟踪器。fclt 的两个主要组件是一个短期跟踪器，用于定位每个帧中的**目标**，以及一个探测器，它在目标丢失时**重新检测目标**。短期跟踪器和检测器都基于相关滤波器。该探测器利用了最近约束滤波器学习的特性，能够有效地**重新检测**整个图像中**的目标**。提出了一种基于相关响应质量的故障**检测**机制。

fclt 是在最近的短期和长期基准上进行测试的。它在短期基准上实现了最先进的结果，在长期基准上的表现优于当前表现最好的跟踪器 18% 以上。少

2017 年 11 月 27 日提交;最初宣布 2017 年 11 月。

304. 第 (xiv:1711. 09539)[pdf,其他] Cs。简历

热红外目标跟踪的分层暹罗网络

作者:刘桥,何振宇,王洪志,李新力

文摘 大多数热红外跟踪方法都是判别的，将跟踪问题作为分类任务。然而，分类器 (标签预测) 的目标并不与跟踪器的目标 (位置估计) 相结合。分类任务的重点是任意对象的类间差异，而跟踪任务主要处理相同对象的类内差异。本文将 tir 跟踪问题作为一个相似性验证任务，与跟踪任务的目标很好地结合在一起。我们提出了一个 tir 跟踪器，通过分层 siamese 卷积神经网络 (cnn)，名为 hsnet。为了获得 tir 对象的空间和语义特征，我们设计了一个暹罗 cnn 聚成多层卷积层。然后，在将网络传输到 tir 域之前，我们在一个大型可见视频**检测**数据集中对此网络端到端进行训练，以了解配对对象之间的相似性。接下来，这个预先训练的 siamese 网络用于评估**目标**模板和**目标**候选模板之间的相似性。最后，我们找到了最相似的**一个跟踪的目标**。关于基准的大量实验结果: vot-tir 2015 和 vot-tir 2016，表明我们提出的方法与最先进的方法相比，取得了良好的性能。少

2017 年 11 月 27 日提交;最初宣布 2017 年 11 月。

评论:11 页, 6 个数字

305. 建议: 1711. 09509[pdf,其他] Cs。简历

开放式词汇对象检索的辨析性学习及负短语增强的本土化

作者:ryota hinami, shin ' ichi satoh

摘要: 由于对象**检测**技术的成功，我们甚至可以从巨大的图像集合中检索指定类的对象。但是，目前最先进的对象探测器 (如更快 r-cnn) 只能处理预先指定的类。此外，培训还需要大量的积极和消极的视觉样本。本文讨论了开放词汇对象检索和本地化的问题，即目标对象由文本查询 (例如,**单词**或短语) 指定。我们首先提出了一个简单的扩展更快 r-cnn 适应开放词汇查询，通过转换文本嵌入向量到对象分类器和本地化回归。然后，对于判别训练，我们提出了负短语扩充 (npa) 来挖掘视觉上类似于查询的硬负样本，同时在语义上相互排斥查询。该方法可以在 0.5 秒内检索和本地化由文本查询指定的对象，只需 0.5 秒即可获得 100 万张图像的值。少

2018 年 9 月 4 日提交;v1 于 2017 年 11 月 26 日提交;最初宣布 2017 年 11 月。

评论:2018 年加入 emnlp

306. 第 711. 09414[pdf,其他] Cs。简历

记忆增强视频对象跟踪

作者:刘伯宇,王燕照，泰玉荣,唐志强

摘要: 我们介绍了一种用于视频对象跟踪的一次性学习方法。该算法只需要查看一次要跟踪的对象，并使用外部内存来存储和记住在跟踪过程中随着时间的推移前景对象的不断变化的特征以及背景。通过在每次跟踪中检索和更新相关内存，我们的跟踪模型能够保持对象的长期内存，因此可以自然地处理硬跟踪场景，包括部分和全部遮挡、运动变化和大缩放和形状变化。在我们的实验中，我们使用 imagenet ilsvrc2015 视频**检测**数据集来训练和使用 vot-2016 基准来测试和比较我们的记忆增强视频对象跟踪

(majot) 模型。从研究结果来看, mavot 在设计上具有非常高的性能和简单性，它是一种极具吸引力的视觉跟踪方法，因为它在 vot-2016 基准上表现良好，在准确性和鲁棒性方面是前 5 名表现之一。闭合、运动变化和空**目标**。少

2017 年 11 月 26 日提交;最初宣布 2017 年 11 月。

评论:提交给 cvpr2018

307. 第 1711. 09:05[pdf,其他] Cs。简历

学习具有旋转边框的旋转不变检测器

作者:刘磊,潘宗旭,斌雷

摘要: 由于多角度物体的定位和从背景中有效分离的困难，任意旋转物体的**检测**是一项具有挑战性的任务。由于采用传统的边界框 (用于定位旋转物体的旋转变型结构)，现有的方法对物体的角度变化不具有鲁棒性。本文提出了一种新的检测方法，该方法应用了新定义的可旋转边界框 (rbox)。所提出的检测器 (drbox) 可以有效地处理物体的方向角度是任意的情况。drbox 的训练迫使**检测**网络学习对象的正确方向角度，从而实现旋转不变的特性。drbox 与 "更快的 r-cnn" 和 ssd 相比，在卫星图像上**检测**车辆、船只和飞机，后者被选定为传统边界箱方法的基准。结果表明, drbox 在给定任务上的性能远远优于传统的基于边界框的方法，对输入图像和**目标**对象的旋转具有更强的鲁棒性。此外，结果表明, drbox 正确地输出了物体的方向角度，这对有效地定位多角度物体非常有用。代码和模型可在 https://github.com/liulei01/DRBox。少

2017 年 11 月 26 日提交;最初宣布 2017 年 11 月。

308. 第: 1711. 0752[pdf,其他] Cs。简历

排斥损失: 在人群中发现行人

作者:王新龙、肖泰特、姜云宁、 邵帅、孙健、沈春华

摘要: **在**人群中检测个别行人仍然是一个具有挑战性的问题，因为行人经常聚集在一起，在现实世界中相互遮挡。在本文中，我们首先探讨了最先进的行人探测器如何通过实验受到人群遮挡的伤害，从而深入了解人群遮挡问题。然后，我们提出了一个新的边界框回归损失专门设计的人群场景，称为排斥损失。这种损失是由两个动机造成的:**目标**的吸引力和周围其他物体的排斥。排斥术语阻止了建议转移到周围的物体，从而导致更强大的人群鲁棒性定位。我们的检测器由排斥损失训练优于所有最先进的方法，在遮挡情况下有显著改善。少

2018 年 3 月 26 日提交;v1 于 2017 年 11 月 21 日提交;最初宣布 2017 年 11 月。

评论:2018 年参加 ieee 计算机视觉和模式识别会议 (cvpr)

309. 第: 1711.07659[pdf] 反渗透委员会

基于 lidar 的环路闭合检测实现稳定的对抗性特征学习

作者:徐凌云,尹鹏,罗海波,刘云辉,韩建达

摘要: 在同时定位和映射 (slam) 框架中，稳定的特征提取**是环路闭合检测**(lcd) 任务的关键。在本文中，特征提取是通过使用基于无监督学习的生成对抗性网络 (gans) 来操作的。有机遗传组织是一种强大的生成模型，然而，基于甘肃的对抗性学习存在训练不稳定的问题。我们发现，在对抗性学习中的数据代码联合分布是一个比原始的有机遗传要复杂的流形。而驱动综合和**目标**分布之间吸引力的损耗函数无法有效地进行 lcd 任务的潜在代码学习。为了解决这个问题，我们将原来的对抗性学习与一个内循环限制模块和一个侧面更新模块结合起来。据我们所知，我们首先从基于光**检测**和测距 (lidar)

的输入中提取对抗特征，这对照明和外观引起的变化是不变的，就像在视觉输入中一样。我们使用 kitti 气味测量数据集来研究我们的方法的性能。大量的实验结果表明，在相同的 lidar 投影图下，所提出的特征在训练中更加稳定，与其他最先进的方法相比，可以显著提高观点差异的鲁棒性。少

2017 年 11 月 21 日提交;最初宣布 2017 年 11 月。

评论:向 2018 年 icra 提交了 8 页, 14 位数字

310. **第: 1711.07618[pdf,其他] Cs。简历**

S4 个网络: 单级实例细分

作者:范若辰,侯启斌,程明明, 穆泰江, 胡世民

摘要: 在本文中，我们考虑了一个有趣的视觉问题--突出的实例分割。除了生产近似边界盒，我们的网络还输出高质量的实例级段。考虑到每个**目标**的分类无关特性，我们设计了一个单阶段突出的实例分割框架，并给出了一个新的分割分支。我们的新分支不仅考虑每个**检测**窗口内的本地上下文，还考虑其周围的上下文，使我们能够区分相同范围内的实例，即使是在阻塞的情况下。我们的网络可进行端到端培训，并以快速运行(在处理分辨率图像时需要 40 fps320x320).我们根据公开的基准评估我们的方法，并表明它优于其他替代解决方案。此外，我们还提供了对设计选择的透彻分析，以帮助读者更好地了解我们网络每个部分的功能。为了促进这一领域的发展，我们的代码将在 \url{https://github.com/RuochenFan/S4Net} 上提供。少

2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

311. **第: 1711.07520[pdf,其他] Cs。简历**

通过本地化的第一层深层网络删除激活输出，以增强用户隐私和数据安全

作者:郝东,赵武,魏震,郭一柯

文摘: 深度学习方法在异常**检测**、预测和支持个人健康、全身身体传感等应用决策方面发挥着至关重要的作用。但是，当前深层网络的体系结构会遇到隐私问题，用户需要将其数据提供给模型 (通常托管在服务器或云上的群集中)，以便进行培训或预测。对于那些敏感的医疗保健或医疗数据 (例如 fmri 或身体传感器测量，如脑电图信号)，这个问题变得更加严重。除此之外，在从用户到模型的数据传输过程中 (尤其是通过 internet 传输的情况下)，也存在将这些数据传输的安全风险。**针对**这些问题，本文提出了一种新的深度网络体系结构，用户在深度网络中不向模型公开自己的原始数据。在我们的方法中，前馈传播和数据加密被组合到一个过程中: 我们将第一层深网络迁移到用户的本地设备，并在本地应用激活函数，然后使用 "丢弃激活输出" 方法使输出不可倒。由此产生的方法能够在不访问用户敏感原始数据的情况下进行模型预测。本文进行的实验表明，该方法达到了理想的隐私保护要求，并证明了与传统的加密/解密方法相比，具有多项优点。

2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

评论:信息取证和安全 (tifs)

312. **第: 1711.07510[pdf,其他] Cs。马**

基于移动传感器网络的可靠环境映射

作者:玄州公园,刘金孙,马修·约翰逊-罗伯森,拉姆·瓦苏德万

摘要: 构建环境参数空间图是防止危险化学品泄漏、森林火灾或估算地形高程等空间分布物理量的关键一步。尽管以前的方法可以通过调度一组自治代理有效地执行此类映射任务，但当任何代理发生故障时，它们无法确保以分散的方式以分散的方式令人满意地收敛到基础地线真理分布。由于用于执行此类映射的代理类型通常价格低廉，容易发生故障，这导致实际应用中的总体映射性能较差，在某些情况下可能危及人类安全。本文提出了一种贝叶斯方法，通过部署一组移动机器人，在出现硬件故障的情况下，配备短距离传感器的临时通信，实现环境参数的鲁棒空间映射。我们的方法首先使用 voronoi 图的变体来划分要映射到每个与至少一个机器人关联的不相交区域的区域。然后以分散的方式部署这些机器人，以最大限度地增加至少一个机器人检测其关联区域中**每个目标**的可能性，尽管失败的概率为零。通过仿真结果，验证了该方法与现有技术相比的有效性和鲁棒性。少

2018 年 3 月 20 日提交;v1 于 2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

评论:接受 icra 2018

313. **第: 1711.07477[pdf,其他] Cs。铬**

maamdroid: 通过构建行为模型的马尔可夫链检测 android 恶意软件 (扩展版)

作者:lucky onwuzurike, enrico mariconti, panagiotis Panagiotis, emiliano de cristofaro, gordon ross, gianluca stringini

摘要: 随着 android 越来越流行，恶意软件**也**越来越以它为目标，这促使研究社区提出许多不同的**检测**技术。然而, android 生态系统和恶意软件本身的不断发展使得很难设计出强大的工具，这些工具可以长时间运行，而无需修改或昂贵的再培训。为了解决这个问题，我们设置为从行为的角度**检测**恶意软件，建模为抽象 api 调用的序列。我们介绍了 madroid，这是一个基于静态分析的系统，它提取应用程序对其类、包或家族的 api 调用，并从应用程序的调用图中作为 markov 链获取的序列构建模型。这可确保模型对 api 更改具有更强的弹性，并且功能集具有可管理的大小。我们使用六年来收集的 8.5 k 良性和 35.5 万恶意应用的数据集对 madroid 进行评估，显示它可以有效**地检测**恶意软件 (高达 0.99 f-计量)，并将其**检测**功能长期保持(训练两年后最高为 0.87 f-测量)。我们还表明，与 droidapiminer 相比, mamadroid 显著提高，droidapiminer 是一个最先进的**检测**系统，它依赖于 (原始) api 调用的频率。为了评估 mamadroid 的有效性主要来自 api 抽象还是来自排序建模，我们还评估了它的一个变体，该变体使用抽象 api 调用的频率 (而不是序列)。我们发现它并不那么准确，在对恶意软件样本 (包括良性应用同样或更频繁地使用的 api 调用) 进行培训时，它没有捕获恶意。少

2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

评论:本文的初稿发表在第 24 届网络和分布式系统安全研讨会 (ndss 2017) 的论文集 [arxiv:1612.04433]。这是扩展版本

314. **第: 1711.07319[pdf,其他] Cs。简历**

多人姿势估计的级联金字塔网络

作者:陈一伦,王志成，彭玉祥，张志强,余刚, 孙健

摘要: 近年来，多人姿态估计的话题有了很大的改进，特别是随着卷积神经网络的发展。然而，仍然存在着许多具有挑战性的案例，如被遮挡的关键点、无形的关键点和复杂的背景，这些都无法很好地解决。本文提出了一种新的网络结构，称为级联金字塔网络 (cpn),**其目标**是从这些 "硬" 关键点中缓解问题。更具体地说，我们的算法包括两个阶

段: 全球网络和完善网。globalnet 是一个功能金字塔网络，它可以成功地本地化 "简单" 的关键点，如眼睛和手，但可能无法准确识别被遮挡或看不到的关键点。我们的足联网试图通过集成来自 globalnet 的所有级别的特征表示以及在线硬关键点挖掘损失来明确处理 "硬" 关键点。一般情况下，为了解决多人姿态估计问题，首先采用自上而下的管道来生成一组基于检测器的人边界框，然后是我们的 cpn，用于每个人边界框中的关键点定位。在该算法的基础上，我们在 coco 关键点基准上实现了最先进的结果，在 coco 测试开发数据集上的平均精度为 73.0，在 coco 测试挑战数据集上的平均精度为 73.0，与来自 coco 2016 关键点挑战。代码 (https://github.com/chenyilun95/tf-cpn.git) 和**检测**结果可公开提供，以供进一步研究。少

2018 年 4 月 8 日提交;v1 于 2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

评论:10 页，被 cvpr 2018 年接受

315. 第: 1711.07278[pdf, ps,其他] Cs。铬

软件分发透明度和可审核性

作者:benjamin hof, georg carle

摘要: 大型用户群依赖于通过包管理器提供的软件更新。这为提高软件更新过程的安全性提供了一个独特的杠杆。我们提出了一个透明系统的软件更新，并实现了它的广泛部署的 linux 包管理器，即 apt。我们的系统能够**检测有针对性**的后门，而不会为维护人员产生开销。此外，在我们的系统中，还确保了源代码的可用性，使用可重现的生成验证了源代码和二进制代码之间的绑定，并可以识别负责分发特定包的维护人员。我们描述了一种针对当前软件透明度系统的新的 "隐藏版本" 攻击，并提出并整合了合适的防御措施。为了解决透明度日志服务器的等价攻击，我们引入了树根交叉日志，其中日志的 merkle 树根被提交到单独操作的日志服务器中。与其他系统相比，这大大放松了运营商之间的合作要求。我们的实施是通过在两年内重播超过 3000 个 debian 操作系统的更新来评估的，显示了其可行性，并发现了许多违规行为。少

2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

316. 第 xiv:1711. 05954[pdf,其他] Cs。简历

基于 web 知识转移的零表示法对象检测

作者:陶庆义,杨浩,蔡建飞

文摘: 目标**检测**是计算机视觉中的主要问题之一，并得到了广泛的研究。现有的**大多数检测**工作都依赖于劳动密集型的监督，例如地面真相边界框的对象或至少图像级注释。相反，我们提出了一种对象检测方法，通过利用免费提供的 web 图像,不需要对**目标**任务进行任何形式的人工注释。为了促进网络图像的有效知识转移，我们引入了一个多实例多标签域适应学习框架，并进行了两项关键的创新。首先，我们提出了一个关注前景对象的实例级对抗性域适应网络，将对象外观从 web 域转移到**目标**域。其次，为了保持传输对象特征的类特定语义结构，我们提出了一种通过伪强标签生成跨域传输监督的同时传输机制。通过我们的端到端框架，我们同时学习弱监督检测器并跨域传输知识，因此，我们实现了对基准数据集基准方法的显著改进。少

2018 年 8 月 1 日提交;v1 于 2017 年 11 月 16 日提交;最初宣布 2017 年 11 月。

评论:在 2018 年 eccv 中被接受

317. 第 xiv:1711. 05929[pdf,其他] Cs。简历

对普遍对抗扰动的防御

作者:naveed akhtar, jian liu, ajmal mian

摘要: 深度学习的最新进展表明，图像无关的准潜移默化的扰动的存在，当应用于 ' 任何 ' 图像可以愚弄一个最先进的网络分类器，以改变其预测的图像标签。这些 "普遍的对抗摄动" 对深度学习在实践中的成功构成了严重威胁。我们提出了第一个专门的框架，以有效地保护网络免受这种干扰。我们的方法将摄动校正网络 (prn) 学习为**目标**模型的 "预输入" 层，因此**目标**模型无需修改。prn 是从真实的和合成的图像无关摄动中学习的，在这种情况下，还提出了一种有效的计算后者的方法。在 prn 投入产出差的离散余弦变换上分别训练了摄动检测器。查询图像首先通过 prn 并由检测器进行验证。如果**检测到**扰动，prn 的输出将用于标签预测，而不是实际图像。严格的评估表明，我们的框架可以在实际场景中保护网络分类器免受看不见的对抗干扰，成功率高达 97.5。prn 还很好地概括了一个**目标**网络的培训为另一个具有可比成功率的网络辩护。少

2018 年 2 月 28 日提交;v1 于 2017 年 11 月 16 日提交;最初宣布 2017 年 11 月。

评论:被纳入 ieee cvpr 2018

318. 第: 1711. 05817[pdf] Cs。Lg

以协位为中心的强化学习模型

作者:bita behrouzi, xufei liu, douglas tweed

摘要: 许多最近的强化学习算法是无模型的，并建立在贝尔曼方程。本文提出了一种基于状态动力学的协态方程和模型的方法。我们使用共同状态----与国家有关的成本梯度----来改进政策，并 "集中" 模型，培训它**检测**和模仿与其任务最相关的环境特征。我们证明了该方法能够处理困难的时间最优控制问题，将确定性或随机机械系统快速推向**目标**。在这些任务上，它与最近的 bellman 方法--深层确定性政策梯度相比，效果很好。而且因为它创造了一个模型，所以协体方法也可以从心理实践中学习。少

2018 年 10 月 2 日提交;v1 于 2017 年 11 月 15 日提交;最初宣布 2017 年 11 月。

评论:7 页, 7 个数字, 1 个表

319. 第: 1711. 05220[pdf, ps,其他] cs. it

多伊 10.1109/TSP.2018.2847648

面向双功能雷达通信系统: 最优波形设计

作者:范刘,周龙飞, christos masouros, ang li, 吴罗, athina petroulu

摘要: 我们专注于双功能多输入多输出 (mimo) 雷达通信 (radcom) 系统，在该系统中，单个发射机与下行蜂窝用户通信，并同时**检测**雷达**目标**。为了最大限度地减少下行多用户干扰，考虑了几个设计标准。首先，我们考虑了全方位和定向的电池设计问题，在这些问题中，得到了闭式全局最优解。基于这些波形，我们进一步考虑了加权优化，以实现雷达和通信性能之间的灵活权衡，并引入了一种低复杂度算法。上述三种设计的计算成本与传统的零强迫 (zf) 预编码相似。此外，为了解决更实用的恒模波形设计问题，我们提出了一种分支绑定算法，该算法得到全局最优解，并将其最坏情况的复杂性导出为最大迭代数的函数。最后，我们通过数值结果对所提出的波形设计方法的有效性进行了评估。少

2017 年 11 月 14 日提交;最初宣布 2017 年 11 月。

评论:13 页, 10 个数字。这项工作已提交 ieee，以便可能出版。版权可以在不通知的情况下转让，之后这个版本可能不再可以访问

320. 第: 1711. 04901[pdf,其他] Cs。简历

利用逆合成孔径雷达实现飞机目标自动识别的多雷达方法

作者:carlos pena-caballero, elifaleth cantu, jesus rodriguez, adolfo gonzáales, osvaldo castellanos, angel cantu , meegan 海峡, jae son, dengchul kim

文摘: 随着雷达技术的进步，利用合成孔径雷达 (sar) 和逆 sar (isar) 进行自动**目标**识别 (atr) 已成为一个活跃的研究领域。sar isar 是一种雷达技术，用于生成**目标**的二维高分辨率图像。与使用卷积神经网络 (cnn) 来解决这个问题的其他类似实验不同，我们使用了一种不寻常的方法，从而提高了性能并缩短了训练时间。我们的美国有线电视新闻网使用模拟生成的复杂值来训练网络;此外，我们采用多雷达方法来提高培训和测试过程的准确性，从而比其他在 sarisar 上的论文具有更高的精度。我们用我们开发的雷达模拟器生成了我们的数据集，其中包括 7 个不同的飞机模型，称为 radarpixel;它是一个使用 matlab 和 java 编程实现的 windows gui 程序，模拟器能够准确地复制真正的 sarsisar 配置。我们的目标是利用我们的多雷达技术，确定**检测**和分类**目标**所需的雷达的最佳数量。少

2018 年 3 月 12 日提交;v1 于 2017 年 11 月 13 日提交;最初宣布 2017 年 11 月。

评论:8 页, 9 个数字，数据情报和安全国际会议 (icdis)

321. 第: 1711.04808[pdf,其他] Cs。铬

多核实时系统中安全任务分配的设计空间探索

作者:monowar h 大人, sibin mohan, roudolfo pellizzoni, rakesh b. bobba

摘要: 现代实时系统 (rts) 功能的增强使它们面临各种安全威胁。最近，有人提出了在不干扰实时任务的情况下集成安全任务的框架，但它们只**针对**单个核心系统。然而，现代 rts 正在向多核平台迁移。这使得集成安全机制的问题更加复杂，因为设计人员现在有多种选择来分配安全任务的位置。本文提出了一种利用机会执行的概念来查找多核 rts 安全任务分配的空间探索设计算法--hydra。hydra 允许安全任务在不干扰系统参数或正常执行模式的情况下处理现有的实时任务，同时仍然满足入侵**检测**所需的监视频率。我们的评估使用具有代表性的实时控制系统 (以及用于更广泛探索的合成任务集) 来说明 hydra 的有效性。少

2017 年 11 月 13 日提交;最初宣布 2017 年 11 月。

评论:2018 年第 21 届 (欧洲设计、自动化和测试) 会议接受出版

322. 第 (xiv:1711. 04150)[pdf,其他] si

多伊 10.114/315244.3152512

stwalk: 时间图中的学习轨迹表示

作者:supriya pandhre, himangi mittal, manish gupta, vineeth n balasubramanian

文摘: 分析时变图中节点的时间行为对于**目标**广告、社区进化和异常**值检测**等许多应用都很有用。本文提出了一种新的方法 stwalk，用于学习时间图中节点的轨迹表示。该框架利用当前和以前时间步长图的结构特性来学习有效的节点轨迹表示。stwalk 在给定的时间步长 (称为太空行走) 上对图形执行随机遍历，并在过去时间步长 (称为时间行走) 上执行图形上的随机遍历，以捕获节点的时空行为。我们提出了两个变种的 stwalk 学习轨迹表示。在一个算法中，我们执行太空行走和时间行走作为单步的一部

分。在另一个变种中，我们分别执行太空行走和时间行走，并将学习的表示组合在一起，以获得最终的轨迹嵌入。在三个真实世界的时间图数据集上进行的大量实验验证了与三种基线方法相比，学习的表示的有效性。我们还展示了学习轨迹嵌入的优点，用于变化点**检测**，并证明了这些轨迹表示上的算术运算产生了有趣且可解释的结果。少

2017 年 11 月 11 日提交;最初宣布 2017 年 11 月。

评论:10 页, 5 个数字, 2 个表

323. **第: 1711.03892[pdf,其他] Cs。艾**

多伊 10.22489/CinC.2017.166-054

短单铅心电图记录的诱发线分类

作者:tomás tejeiro, constantino a. garcía, daniel castro, paulo félix

摘要: 在这项工作中，我们提出了一个新的方法，节奏分类短单铅心电图记录，使用一组高水平的和临床意义的特点提供的绑架解释的记录。这些功能包括用于构建两个分类器的形态和节奏相关功能: 一个用于使用每个特征的聚合值对记录进行全局评估;和另一个评估记录作为一个序列，使用一个重新**神经**网络提供的每个检测信号的个别功能。这两个分类器最终结合使用堆叠技术，通过四个**目标**类提供答案: 正常窦性心律，心房颤动，其他异常，和噪音。该方法已与 2017 年植物/cinc 挑战数据集进行了验证，最终获得 0.83 分，并在比赛中排名第一。少

2017 年 11 月 10 日提交;最初宣布 2017 年 11 月。

评论:4 页, 3 个数字。在 2017 年心脏病计算会议上发表

msc 类: 68t10

324. **第: 1711. 03677[pdf,其他] Cs。简历**

动态区域生长中的自我中心手部检测

作者:邵黄,王伟强,何胜峰,刘瑞森 w. h.

摘要: 以自我为中心的视频主要记录了佩戴相机用户开展的活动，近年来引起了大量的研究关注。由于其冗长的内容，大量与 ego 相关的应用程序被开发出来，以抽象捕获的视频。由于用户习惯于使用自己的手与**目标**对象交互，而他们的手通常在交互过程中出现在他们的视觉领域中，因此在手势等任务中涉及到一个自我中心的手**检测**步骤识别、行动识别和社会交往理解。在这项工作中，我们提出了一个动态区域增长的方法，在自我中心视频的手区域**检测**，通过共同考虑手的运动和自我中心线索。我们首先通过分析连续帧的运动模式来确定最有可能属于手的种子区域。然后，可以根据为相邻超级像素计算的分数，通过从种子区域延伸来定位手区。这些分数来自四个自我中心的线索: 对比度、位置、位置一致性和外观连续性。我们讨论如何在现实生活中应用拟议的方法，在这种情况下，多只手不规则地出现并从视频中消失。公共数据集的实验结果表明，与最先进的方法相比，该方法具有较好的性能，特别是在复杂的场景中。少

2017 年 11 月 9 日提交;最初宣布 2017 年 11 月。

325. **第: 1711.02856[pdf,其他] Cs。简历**

基于煤种到精细相似度挖掘的转导零射击哈希

作者:赖汉江,潘燕

摘要: 零拍摄哈希 (zsh) 是在没有训练数据的情况下学习小说/**目标**类的哈希模型，这是一个重要且具有挑战性的问题。大多数现有的 zsh 方法都是通过 seen/source 类和承担/**目标**类之间的中间共享语义表示来利用迁移学习。但是，由于具有不相交性，

从源数据集中获得的哈希函数在直接应用于**目标**类时具有偏差。本文研究了传感器 zsh，即我们对新类的未标记数据进行了研究。通过粗到细相似挖掘，提出了一种简单而高效的联合学习方法，将知识从源数据转移到**目标**数据。它主要由建议的深层体系结构中的两个构建块组成：1）共享的双流网络，第一个流对源数据运行，第二个流对未标记的数据运行，以了解有效的通用图像表示⑵ 一个粗到细的模块，从**从目标**类中找到最具代表性的图像，然后进一步**检测**这些图像之间的相似性，将源数据的相似性传递给**目标**以贪婪的方式提供数据。对多个基准数据集的大量评价结果表明，所提出的哈希方法比最先进的方法有了显著的改进。少

2017 年 11 月 8 日提交;最初宣布 2017 年 11 月。

326. **第: 1711. 01791[pdf,其他] Cs。简历**

具有统计过滤功能的超级网络，用于防御对抗示例

作者:孙准,小泽谷,冈谷隆行

摘要: 在图像分类等各种任务中，深度学习算法被认为容易受到对抗摄动的影响。通过使用多种防御方法来**检测**和拒绝特定类型的攻击，解决了此问题。然而，根据特定的防御方案训练和操作网络增加了学习算法的计算复杂性。在本工作中，我们提出了一种简单而有效的方法，利用数据相关的自适应卷积核，提高卷积神经网络 (kernels) 对对抗攻击的鲁棒性。为此，我们提出了一种新型的超网络，以便利用输入数据的统计属性和特征来计算统计自适应映射。然后，利用所学习的统计图对 kernels 的卷积权重进行滤波，计算动态核。因此，权重和内核进行了集体优化，以便在不使用额外的**目标检测**和拒绝算法的情况下，学习对对抗攻击具有鲁棒性的图像分类模型。我们的经验证明，该方法使 cnn 能够自发地防御不同类型的攻击，例如由高斯噪声产生的攻击，快速梯度符号方法 (good 同类等人, 2014) 和黑匣子攻击 (narodytska & amp;Kasiviswanathan, 2016 年)。少

2017 年 11 月 6 日提交;最初宣布 2017 年 11 月。

327. **第: 1711. 01656[pdf,其他] Cs。简历**

全运动视频和宽空中运动图像的空间金字塔上下文感知运动目标检测与跟踪

作者:mahdieh poostchi

文摘: 一个强大而快速的自动运动目标**检测**和跟踪系统对于**确定目标**对象的特征和提取不同功能的时空信息至关重要，包括城市视频监控系统、城市交通监控和导航，机器人。在本文中，我提出了一个协同空间金字塔上下文感知运动目标**检测**和跟踪系统。所提出的视觉跟踪器由一个通常依赖于视觉对象特征的主跟踪器和两个基于对象时间运动信息的辅助跟踪器组成，这些跟踪器将被动态调用，以帮助主跟踪器。spct 利用不同层次的图像空间上下文，使视频跟踪系统具有抗遮挡、背景噪声的能力，提高**了目标**定位的准确性和鲁棒性。我们选择了预先选择的七通道互补特征，包括 hog 的 rgb 颜色、强度和空间金字塔，对对象的颜色、形状和空间布局信息进行编码。我们利用积分直方图作为构建块，以满足实时性能的要求。提出了一种利用积分直方图方法的扩展法，在恒定时间复杂度下准确地评价空间加权局部直方图的快速算法。探讨了在 gpu 体系结构上有效计算积分直方图的不同技术，并将其应用于快速时空中值计算和三维人脸重建纹理。提出了一种基于运动信息语义融合的多组件框架和投影建筑足迹图，以显著降低多层结构城市场景中的虚警率。在广泛的 votc2016 基准数据集和空中视频上的实验证实，将互补跟踪线索结合在智能融合框架中，可以实现对全运动视频和宽空中运动图像的持久跟踪。少

2017 年 11 月 5 日提交;最初宣布 2017 年 11 月。

评论:博士论文 (162 页)

328. 第: 1711. 01575[pdf,其他] Cs。简历

对抗性退出规范化

作者:kuniaki saito, yoshitaka ushiku, tatsuya harada,kate saenko

文摘: 我们提出了一种将神经表示从具有标签的源域转移到未标记的**目标**域的方法。最近为这一任务提出的对抗方法通过愚弄一个特殊的领域评论网络，学会了跨领域的功能对齐。但是，这种方法的一个缺点是，评论家只是将生成的要素标记为域内或不域内，而不考虑类之间的边界。这可能会导致在类边界附近生成不明确的特征，从而降低**目标**分类的准确性。我们提出了一种新的方法，即对抗性退出正则化 (adr)，以鼓励生成器输出更多的目标域的判别特征 。我们的主要想法是用**一个检测**非判别特征的词处理来取代评论家，在分类器网络上使用辍学。然后，生成器学习以避免这些区域的功能空间，从而创建更好的功能。我们将 adr 方法应用于图像分类和语义分割任务的无监督域适应问题，并展示了对最新技术的显著改进。我们还表明，我们的方法可以用来培训生成性对抗性网络的半监督学习。少

2018 年 3 月 1 日提交;v1 于 2017 年 11 月 5 日提交;最初宣布 2017 年 11 月。

评论:iclr2018 上的 tba

329. 第: 1711.01369[pdf,其他] Cs。Sd

基于卷积神经网络的声音事件和场景弱标音频知识转移

作者:anurag kumar, maksim khadkevich, christian fugen

摘要: 在这项工作中，我们提出了有效地从弱标记的网络音频数据的知识转移的方法。我们首先描述了一个卷积神经网络 (cnn) 框架，用于声音事件检测和分类使用弱标记的音频数据。我们的模型从可变长度的音频高效训练;因此，它非常适合于转移学习。然后，我们提出了使用该模型学习表示的方法，可以有效地用于解决**目标**任务。我们研究了传感器和归纳转移学习任务，展示了我们的领域和任务适应方法的有效性。我们表明，利用所提出的 cnn 模型，所学的学习表示可以很好地概括 esc-50 声音事件数据集的人体水平精度，并在该数据集上设置最先进的结果。我们进一步将它们用于声学场景分类任务，并再次表明我们提出的方法也很适合这一任务。我们还表明，我们的方法也有助于捕捉语义意义和关系。此外，在这一过程中，我们还依靠平衡的训练集，在音频集数据集上设置了最先进的结果。少

2018 年 9 月 7 日提交;v1 于 2017 年 11 月 3 日提交;最初宣布 2017 年 11 月。

评论:icassp 2018

330. 第: 1711.01293[pdf, ps,其他] cs. it

具有相同雷达特征的多个目标在具有相关阻塞的多路径环境中的定位

作者:sundar aditya, and 列 as f. molisch , naif rabeah, hatim behay

文摘: 本文通过由无法确定出发方向和发射方向的单天线发射机和接收机组成的分布式 mimo 雷达，解决了将数量不详的目标本地化的问题，这些目标都具有相同的**雷达**特征。到来。此外，我们还考虑了多径传播的存在，以及直接路径可能的 (相关) 阻塞 (从发射器进入，并将**目标**反射到接收机)。在其最一般的形式中，这个问题可以被转换为贝叶斯估计问题，其中考虑到了每个多路径分量。但是，当环境映射未知时，此问题就不正确了，因此，在只考虑直接路径的情况下，导出了可跟踪的近似值。特别是，我

们考虑了环境中的散射体的相关阻塞，这在贝叶斯估计框架中作为一个先验出现。提出了一种次优多项式时间算法，解决了具有相关阻塞的贝叶斯多**目标**定位问题，并利用仿真对其性能进行了评价。我们发现，当相关阻塞是严重的，假设阻塞事件是独立的，并具有恒定的概率 (如在以前的论文中所做的那样) 导致**检测**性能不佳，错误警报更有可能发生**比检测.**少

2017 年 11 月 3 日提交;最初宣布 2017 年 11 月。

评论:出现在有关无线通信的 ieee 事务中

331. **第 1711.00214[pdf,其他] Cs。马**

异构无人机网络协调任务分配的联盟方法

作者:fatemeh afghah, mohammad zaeri-amirani, abolfazl razi, jacob chakareski, elizabeth bentley

摘要: 考虑了利用资源受限的无人机**异构**网络**进行目标检测**和后续任务完成的问题。无人机事先没有关于地点和确定这些**目标**所需资源的知识。在提出的领导-追随者联盟组建模型中，首先定位**目标**的无人机充当联盟领导人，并选择一组追随者无人机来完成与确定的目标相关的任务. 联盟组建的目标是以最少的资源利用率完成指定的任务。联盟成员的另一个作用是通过分布式合作中继方案将信号转发到地面站，使地面站了解**检测到**的对手**目标.**我们还提出了一个以联盟形成为基础的联盟机制，以监测无人机在一段时间内的合作行为，并排除潜在的不可信任的无人机。仿真结果表明，与替代方法相比，该方法在形成最优联盟方面是有效的。少

2017 年 11 月 1 日提交;最初宣布 2017 年 11 月。

评论:向行政协调会 2018 年提交 8 页, 5 个数字

332. **第 1710.10766[pdf,其他] Cs。Lg**

像素防御: 利用生成模型来理解和防御对抗示例

作者:杨松,金调秀,塞巴斯蒂安·诺沃津,斯特凡诺·埃尔蒙,内特·库什曼

摘要: 正常图像的对抗性扰动通常是人类无法察觉的，但它们会严重混淆最先进的机器学习模型。是什么让它们在图像分类器眼中如此特殊？本文从经验上表明，对抗性的例子主要在于训练分布的低概率区域，而不考虑攻击类型和**目标**模型。通过统计假设检验，我们发现现代神经密度模型在检测潜移默化的**图像**扰动方面具有惊人的性能。基于这一发现，我们设计了 pixeldefend，这是一种新的方法，通过将图像移回训练数据中看到的分布来净化恶意不安的图像。然后通过一个未经修改的分类器运行纯化后的图像，使我们的方法既不符合分类器的诊断方法，也不知道攻击方法。因此, pixeldefend 可用于保护已部署的模型，并与其他特定于模型的防御相结合。实验表明，我们的方法大大提高了各种最先进的攻击方法的恢复能力，将最强攻击的准确性从时尚 mnist 的 63% 提高到 84%，对 cifar-10 的准确率从 32% 提高到 70%。少

2018 年 5 月 21 日提交;v1 于 2017 年 10 月 30 日提交;最初宣布 2017 年 10 月。

评论:iclr 2018

333. **建议: 1710.02692[pdf,其他] Cs。铬**

隐藏时钟: 模拟控制器区域网络中的时钟偏移

作者:sang ux s 合 ong, xuhang ying, andrew clark, linda bushnell, radha poovendran

摘要: 汽车配备了电子控制单元 (ecu)，通过车载网络协议标准 (如控制器局域网 (can)) 进行通信。这些协议是在将车载通信与外部网络分离足以防范网络攻击的假设下设计的。然而，最近的攻击表明，这一假设是无效的，在这些攻击中，对手能够渗透进车内网络。在这些攻击的推动下，针对车载网络，提出了入侵**检测**系统 (ids)，这些网络利用 ecu 的时钟倾斜等特性，利用设备指纹来**检测**攻击。在本文中，我们提出了隐形攻击，一种智能伪装攻击，在这种攻击中，对手修改传输消息的时间，以匹配**目标** ecu 的时钟偏移。攻击利用这样一个事实，即虽然时钟偏移是每个 ecu 的物理属性，对手无法更改，但其他 ecu 对时钟偏移的估计是基于网络流量的，而网络流量仅是网络组件，可以由攻击者修改阿里我们实现了所提出的隐形攻击，并在两个 ids 上进行了测试，即当前最先进的 ids 和基于广泛使用的网络时间协议 (ntp) 开发的新 ids。我们在两个硬件试验台、一个原型和一个真正的连接车辆上进行了隐身攻击，并表明它总是可以欺骗这两个 ids。我们还引入了一个新的度量指标，称为 "最大倾斜指数"，用于量化隐藏攻击的有效性，即使对手无法精确匹配目标 ecu 的时钟偏差. 少

2018 年 3 月 21 日提交;v1 于 2017 年 10 月 7 日提交;最初宣布 2017 年 10 月。

评论:11 页, 13 位数字，这项工作已被第九届 acm/ieee 网络物理系统国际会议 (iccps) 所接受

msc 类: 68w01

334. 第 1710.01507[pdf,其他] Cs。红外

多伊 10.114/3209978 8.3210144

识别点击诱饵: 一种基于神经网络的多策略方法

作者:vaibhav kumar, dhruv khattar, Siddhartha gairola, yash kumar lal, vasudeva varma

摘要: 为了扩大覆盖面，并随后通过广告货币化增加收入，网络媒体已开始采用点击诱饵技术，以吸引读者点击文章。这篇文章没有兑现标题所作的承诺。传统的点击诱饵**检测**方法在很大程度上依赖于特征工程，而特征工程又依赖于它所构建的数据集。神经网络在这一任务中的应用只进行了部分探讨。考虑到社交媒体帖子中的所有信息，我们提出了一种新的方法。我们训练一个双向的 lstm，它有一个注意机制，以了解一个词在多大程度上以不同的方式对帖子的点击诱饵得分做出了贡献。我们还使用了一个暹罗网来捕获源信息和**目标**信息之间的相似性。以前的方法没有考虑从图像中收集到的信息。我们使用卷积神经网络从大量数据中学习图像嵌入，为我们的模型增加另一层复杂性。最后，我们将三个独立组件的输出连接在一起，作为完全连接层的输入。我们在 195338 个社交媒体帖子的测试语料库上进行了实验，在改进以前最先进的数据集上获得了 26.37% 的 f1 分数，以及其他拟议的方法、功能工程或其他。少

2018 年 8 月 1 日提交;v1 于 2017 年 10 月 4 日提交;最初宣布 2017 年 10 月。

评论:在 2018 年信号会上被接受为短纸

日记本参考:" 识别点击诱饵: 一种基于神经网络的多策略方法"。在第 41 届国际信息检索研究与开发会议论文集上。页数: 1225-1228

335. 第: 1710.00925[pdf,其他] Cs。简历

没有关键点的细粒度头姿势估计

作者:nataniel ruiz, eunji chong, james m. rehg

摘要: 估计一个人的头部姿势是一个关键的问题，它有大量的应用，如帮助凝视估计、建模注意力、将 3d 模型与视频相拟合以及执行人脸对齐。传统上，头部姿势是通过从

目标面估计一些关键点，并用平均人头模型解决二维到三维对应问题来计算的。我们认为，这是一个脆弱的方法，因为它完全依赖于地标性检测性能，无关的头部模型和一个临时拟合步骤。我们提出了一种优雅而稳健的方法来确定姿势，方法是在 300w-lp 上训练一个多损失的卷积神经网络，这是一个大型的综合扩展数据集，通过关节直接从图像强度预测固有的欧拉角 (yaw、俯仰和滚动)绑定的姿势分类和回归。我们对常见的野外姿势基准数据集进行了实证测试，显示了最先进的结果。此外，我们还在通常用于使用深度估计的数据集上测试我们的方法，并开始用最先进的深度姿势方法缩小差距。我们提供开源的培训和测试代码，以及发布我们的预培训模型。少

2018 年 4 月 13 日提交;v1 于 2017 年 10 月 2 日提交;最初宣布 2017 年 10 月。

评论:参加 2018 年 ieee 计算机视觉和模式识别研讨会 (cvprw)。ieee, 2018

日记本参考:ieee 计算机视觉和模式识别 (cvpr) 会议研讨会, 2018 年, 2074-2083 页

336. 第: 1710.00551[pdf,其他] Cs。铬

罗哈默防御墙上的又一次翻转

作者:daniel gruss, moritz lipp, michael schwarz, daniel genkin, jonas juffinger, sioli o ' connell , wolfgang schoechl, yuval yarom

摘要: rowhamjar bug 允许从无特权软件对 dram 单元中的位进行未经授权的修改，从而实现强大的特权升级攻击。提出了复杂的罗锤对策，旨在减轻罗锤错误或其利用。然而，最先进的技术没有提供足够的洞察这些防御的完整性。本文提出了一种新颖的罗哈默攻击和开发原语，表明即使是所有防御的组合也是无效的。我们的新攻击技术，一个位置锤击，打破了以前的假设，以触发 rowhamer bug 的要求，即，我们不锤击多个 dram 行，但只保持一个 dram 行不断打开。我们的新开发技术, opcode 翻转，通过在用户空间二进制文件中以可预测和**有针对性**的方式翻转位，绕过最近的隔离机制。我们用一种新的可靠技术--记忆方式取代了引人注目的记忆喷涂和梳理技术。内存跟踪利用系统级优化和侧通道来哄操作系统将目标页放置在攻击者选择**的**物理位置。最后，我们滥用英特尔 sgx 来向用户和操作系统完全隐藏攻击，使对攻击的任何检查或**检测都**不可行。我们的 rowhamer 飞地可用于云中协调拒绝服务攻击和个人计算机上的特权升级。我们表明，我们的攻击逃避了以前提出的商品体系的所有对策。少

2018 年 1 月 31 日提交;v1 于 2017 年 10 月 2 日提交;最初宣布 2017 年 10 月。

评论:2018 年第 39 届 ieee 安全与隐私研讨会接受的作品预印

337. 第 1709.09323[pdf,其他] Cs。简历

动态视觉传感器数据监控学习的伪标签，应用于情绪运动下的目标检测

作者:陈志强

摘要: 近年来，动态视觉传感器 (dvs)，也被称为基于事件的相机或神经形态传感器，由于与传统的基于框架的相机相比的各种优势，使用量增加。利用视网膜的启发原则，它的高时间分辨率克服运动模糊，它的高动态范围克服极端的照明条件和低功耗使它成为理想的嵌入式系统，如无人机和自驾游。但是，基于事件的数据集很少，对于对象检测等任务,标签甚至更罕见。我们通过中间伪标签将判别知识从最先进的基于框架的卷积神经网络 (cnn) 转移到基于事件的模式，作为监督学习的**目标**。我们首次展示了在实际环境中以每秒 100 帧的情况进行自我运动的基于事件的汽车**检测**，与我们的注释地面真理相比，测试平均精度为 40.3。基于事件的汽车探测器处理运动模糊和恶劣的照明条件，尽管没有明确的培训，甚至补充基于框架的 cnn 探测器，这表明它已经学会了广义的视觉表现。少

2018 年 3 月 14 日提交;v1 于 2017 年 9 月 26 日提交;最初宣布 2017 年 9 月。

338. 第 xiv:170 9.09 6916[pdf,其他] si

烟雾筛选器或直射手：在用户审查社交网络中检测精英 sybil 攻击

作者:郑海忠、薛敏辉、浩路、双浩、朱浩进、梁晓辉、 基思·罗斯

摘要: 流行的用户评论社交网络 (ursn)--如 dianping、yelp 和 amazon--通常是声誉攻击的**目标**，在这些攻击中，为了提高或降低上市产品和服务的评级，发布虚假评论。这些攻击往往来自于一组名为 sybils 的帐户集合，这些帐户由一组真正的用户集体管理。一个新的先进计划，我们称之为精英 sybil 攻击，招募有机高评级的帐户，以产生似乎值得信赖和逼真的评论。这些精锐的 sybil 账户综合起来形成了一个庞大的稀疏的 sybil 网络，现有的 sybil 假审查防御系统不可能成功。在本文中，我们进行了第一次研究，以定义、描述和**检测**西比尔的精英攻击。我们展示了现代精英赛比尔袭击有一个混合架构，第一级招募精锐的西比尔工人，并分配由西比尔组织者的任务，第二层张贴假评论盈利的精英 sybil 工人。我们设计了 ElsieDet，这是一个三阶段的 sybil **检测**计划，首先将可疑用户组排除在外，然后确定广告系列窗口，最后确定参加该活动的 sybil 精英用户。我们对中国最受欢迎的 ursn 服务--电平的一千万条评论进行了大规模的实证研究。我们的研究结果表明，来自优秀的 sybil 用户的评论是更分散的时间，工艺更有说服力的审查，并有更高的过滤旁路率。我们还衡量了 sybil 营销活动对各个行业 (如影院、酒店、餐馆) 以及连锁店的影响，并证明随着时间的推移监控 sybil 精英用户可以提供针对 sybil 营销活动的宝贵的早期警报。少

2017 年 12 月 4 日提交;v1 于 2017 年 9 月 20 日提交;最初宣布 2017 年 9 月。

339. 第 xiv:1709.06668[pdf,其他] 反渗透委员会

采用两相校准程序，采用电缆驱动机器人进行快速、可靠的自主手术清配

作者:daniel seita , sanjay krishnan, roy fox, stephen mckinley, john canny , ken goldberg

摘要: 使用机器人手术助理 (rsa) (如达·芬奇研究套件 (dvrk)) 进行清创 (去除死亡或患病的组织碎片) 等精确子任务具有挑战性，因为电缆驱动系统存在固有的非线性。提出并评价了一种新的两相粗化标定方法。在第一阶段 (粗)，我们在末端效应器上放置一个红色校准标记，并让它随机移动到一组开环轨迹中，以获得大量相机像素和内部机器人末端执行器配置的样本集。然后，这些粗糙的数据被用来训练深神经网络 (dnn) 来学习粗变换偏差。在第二阶段 (罚款) 中，第一阶段的偏差用于将末端效应器移动到打印工作表上的一小部分特定**目标**点。对于每个**目标**，人工操作员通过直接接触 (而不是通过远程操作) 手动调整末端执行器位置，并记录剩余补偿偏差。然后，这些精细数据被用来训练随机森林 (rf)，以学习精细变换偏差。随后的实验表明，如果不进行校准，位置误差平均为 4.55 mm。第一阶段可以将平均误差减少到 2.14 mm，第一阶段和第二阶段的组合可以将平均误差降低到 1.08 mm。我们将这些结果应用于葡萄干和南瓜籽作为碎片幻影的清创。使用具有标准边缘**检测**的内窥镜立体摄像机，120 项试验的实验实现了平均成功率 94.5，超过了以前的结果，碎片大得多 (8. 9.4%)，加速了 2.1 倍，减少了每台的时间。片段从 15.8 秒到 7.3 秒。源代码、数据和视频可在 https://sites.google.com/view/calib-icra/。少

2018 年 2 月 24 日提交;v1 于 2017 年 9 月 19 日提交;最初宣布 2017 年 9 月。

评论:代码、数据和视频可在 https://sites.google.com/view/calib-icra/。icra 2018 年最终版本

340. 第: 1708. 06145[pdf,其他] Cs。铬

敲门声，谁来了？聚合位置数据的成员资格推理

作者:Apostolos pyrgelis, carmela troncoso , emiliano de cristofaro

摘要: 聚合位置数据通常用于支持智能服务和应用程序，例如，生成实时交通地图或预测对企业的访问。本文首次研究了成员资格推理攻击在聚合位置时间序列上的可行性。我们引入了对抗任务的基于游戏的定义，并将其转换为分类问题，在该问题中，可以使用机器学习来区分**目标**用户是否为聚合的一部分。我们使用两个移动数据集对这些攻击对原始聚合和不同私有聚合的能力进行了经验评估。我们发现成员资格推断是一种严重的隐私威胁，并说明其有效性如何取决于对手的先验知识、基础位置数据的特征以及用户数量和聚合的时间框架执行。尽管不同的私人机制确实可以减少攻击的程度，但它们也造成了巨大的效用损失。此外，模仿防御机制行为的战略对手会极大地限制他们提供的保护。总体而言，我们的工作提出了一种新的方法，旨在评估现实环境中聚合位置数据的隶属度推断，供应商可以在数据发布前评估隐私保护的质量，监管机构也可以使用**它来检测**侵犯。少

2017 年 11 月 29 日提交;v1 于 2017 年 8 月 21 日提交;最初宣布 2017 年 8 月。

日记本参考:第 25 届网络和分布式系统安全研讨会论文集 (ndss 2018)

341. 建议: 170 08.06 128[pdf,其他] Cs。简历

重新审视训练对象类探测器的知识转移

作者:jisper uijlings, stefan popov, vittorio ferrari

摘要: 我们建议在弱监督训练图像的目标类上重新审视**训练**对象探测器的知识转移，并在一组带有边界框注释的源类的帮助下进行帮助。我们提出了一个统一的知识转移框架，该框架基于在所有源类上训练单个神经网络多类对象检测器，该模型按语义层次结构进行组织。这就产生了在层次结构中具有多个层次分数的建议，我们使用这些建议来探索广泛的知识转移，从特定于类 (自行车到摩托车) 到类通用 (从对象到任何类)。在 ilsvrc 2013 检测数据集中**的** 200 个对象类上进行的实验表明，我们的技术: (1) 比手动使用的弱监督基线在**目标**类上的性能要好得多 (70.3 corloc, 36.9% map) 工程客观性 [11] (50.5% corloc, 25.4% map)。(2) 提供**目标**对象探测器，达到完全受监督的对应方 80% 的 map。(3) 在此数据集上优于报告的最佳传输学习结果 (在 [18, 46] 上 + 41% corloc 和 + 3% map，在 [32] 上 + 16.2% map)。此外，我们还进行了几个跨数据集知识转移实验 [27, 24, 35]，发现 (4) 我们的技术在所有数据集对中的性能优于弱监督基线 1.5x-1.9x，从而确定了其普遍适用性。少

2018 年 3 月 28 日提交;v1 于 2017 年 8 月 21 日提交;最初宣布 2017 年 8 月。

评论:cvpr 18

342. 建议: 1708.03 307[pdf,其他] Cs。简历

深卷神经网络微博中的细胞检测与压缩传感

作者:姚雪,尼兰詹雷

摘要: 在显微镜图像中自动检测某些类型的细胞或细胞亚基的能力对广泛的生物医学研究和临床实践具有重要意义。细胞**检测**方法已从采用手工制作的功能发展到基于深度学习的技术。这些方法的基本思想是，它们的单元器或检测器在像素空间中进行训练，在像素空间中标记目标单元的位置。本文寻求一种不同的路径，并提出了一种基于卷积神经网络 (cnn) 的基于卷积神经网络 (cnn) 的细胞**检测**方法，该方法采用输出像素空

间的编码方法。对于单元检测问题，输出空间是指示单元格中心的标记稀疏的像素位置。我们使用随机投影将输出空间编码为固定维度的压缩向量。然后，美国有线电视新闻网从输入像素中回归这个压缩的向量。此外，还可以从预测的压缩向量中稳定地恢复输出像素空间上的稀疏单元位置，使用我 1-范数优化。过去，使用压缩传感 (cs) 进行输出空间编码已与线性和非线性预测因子结合使用。据我们所知，这是首次成功使用美国有线电视新闻网基于 cs 的输出空间编码。我们在几个基准数据集上进行了大量实验，与其他最先进的方法相比，拟议的 cnn + cs 框架 (称为 cncs) 在 f1 分数方面取得了最高或至少前三名的成绩。少

2018 年 2 月 20 日提交;v1 于 2017 年 8 月 10 日提交;最初宣布 2017 年 8 月。

343. 第 1708.03105[pdf,其他] Cs。CI

使用基于地名的统计语言模型从目标文本流中提取位置名称

作者:hussein s. al-olimat, krishnaprasad thirunarayan, valerie shalin, amit shth

摘要: 从非正式和非结构化社交媒体数据中提取位置名称需要标识引用边界和划分复合名称。变异性，特别是位置名称的系统变异性 (carroll, 1983 年)，对识别任务提出了挑战。其中一些可变性可以作为统计语言模型内的操作来预见，在这种情况下，来自地名录，如 openstreetmap (osm)、geonames 和 dbpedia。这允许从同一位置上下**文**中对推特目标文本中观察到的 n-gram 作为合法位置名称变体进行评估。使用 n-gram 统计信息和与位置相关的词典，我们的位置名称提取工具 (lnex) 处理缩写，并自动筛选和扩充地名录中的位置名称 (处理名称收缩和辅助内容)，以帮助**检测**多字位置名称的边界，从而在文本中对其进行分隔。我们评估了来自三个**目标**流的 4500 条特定于事件的推特的方法，以比较 lnex 的性能与依赖于标准语义、句法和/或正交功能的十个最先进的标记器的性能。lnex 的平均 f 分提高了 33-179%，表现优于所有的匕首。此外，lnex 还能够进行流处理。少

2018 年 6 月 7 日提交;v1 于 2017 年 8 月 10 日提交;最初宣布 2017 年 8 月。

msc 类: 68t50 类: I.2。7

日记本参考:第 27 届计算语言学国际会议 (coling 2018)

344. 第 xiv:170 08.02975[pdf,其他] Cs。Lg

图时序列中的异常检测

作者:许志强

文摘: 本文利用变分递归神经网络研究了图时间序列中的异常**检测**问题。时间相关性是由递归神经网络 (rnn) 和变分推理 (vi) 相结合的方法建模的，而空间信息则是由图形卷积网络捕获的。为了纳入外部因素，我们使用特征提取器来增强潜在变量的转换，从而了解外部因素的影响。以**目标**函数为累积 elbo，很容易将该模型推广到在线方法。对交通流数据的实验研究表明了该方法的**检测**能力。少

2017 年 11 月 1 日提交;v1 于 2017 年 8 月 9 日提交;最初宣布 2017 年 8 月。

345. 第 xiv:170 7.06786[pdf,其他] Cs。简历

野外深度图像的头部检测

作者:diego ballotta, guido borghi, roberto vezzani, rita cucchiara

摘要: 头部**检测**和定位是一项艰巨的任务，也是许多计算机视觉应用 (如视频监控、人机交互和人脸分析) 的关键要素。在 rgb 图像上**检测**人脸所做的大量工作，以及巨大

的人脸数据集的可用性，使得在该域上建立了非常有效的系统。但是，由于照明问题，在实际应用中可能需要红外或深度摄像机。本文介绍了一种利用深度学习方法的分类能力的深度**图像头部检测**新方法。除了减少对外部照明的依赖之外，深度图像隐式嵌入了有用的信息来处理**目标**对象的比例。利用了两个公共数据集：第一个数据集称为 pandora，用于训练具有人脸和非人脸图像的深层二进制分类器。第二种是康奈尔大学收集的，用于在不受限制的环境中的日常活动中执行交叉数据集测试。实验结果表明，该方法克服了最先进的深度图像方法的性能。少

2017 年 11 月 8 日提交;v1 于 2017 年 7 月 21 日提交;最初宣布 2017 年 7 月。

评论:在 2018 年 visapp 会议上作为全文 (口头) 接受

346. 第 077.0777[pdf, ps,其他] 反渗透委员会

搜索机器人的更低的边界，一些错误

作者:and 列 y kupavskii, emo welzl

抽象: 假设我们发送 K 机器人从 0 以恒定的速度 (有回合) 搜索真实的线，以在未知的位置找到**目标**;F 机器人的故障，这意味着他们没有报告的目标，虽然访问**其**位置 (称为崩溃类型)。我们的目标是在最多的时间找到**目标**|D|，如果**目标**位于 D, |D|≥1，用于尽可能小。我们表明，这是不可能实现的

& lt;2，好了，好，好了，好(，好了，好--1)，好了，好$_{-1}$+1，了，好:=2(F+1)K ，

由于先前的工作，这是很紧张的 (见 j. czyzowitz, e. kranakis, d. krizanc, l. narayanan, j. Opatmy, pod c16，在那里引入了这个问题)。这也为所谓的拜占庭式故障机器人提供了一些比以前已知更好的下限，这些机器人实际上可能会错误地报告**目标**。在论文的第二部分，我们讨论了米-射线泛化的问题，其中隐藏**的目标**将**被检测到**米光线在同一点上发出。使用我们的方法的推广，以及对原始问题的有益的缓解，我们也为这个设置建立了一个严格的较低的 (如上图，，好了，好::= 米(F+1)/k).当专门处理案件时

F=0，这解决了在米射线，由大约 15 至 30 年前的三组科学家提出: baeza-ytt、culberson 和 rawlins;由高、马、西普瑟、尹;还有伯恩斯坦、芬克尔斯坦和齐尔伯斯坦中。米-射线泛化已知与其他看似无关的问题有联系，包括在线问题的混合算法和所谓的合同算法。少

2018 年 5 月 21 日提交;v1 于 2017 年 7 月 17 日提交;最初宣布 2017 年 7 月。

评论:出现在 pod ' 18 的诉讼程序中。与以前的版本相比，添加了 m 射线的泛化

347. 第 077.0. 03816[pdf,其他] Cs。简历

通过分层卷积特征进行稳健的视觉跟踪

作者:马超,黄家斌，杨晓康,杨明轩

文摘 本文提出利用深卷积神经网络的丰富层次特征，提高视觉跟踪的准确性和鲁棒性。在目标识别数据集上训练的深层神经网络由多个卷积层组成。这些图层使用不同级别的抽象对**目标**外观进行编码。例如，最后一个卷积层的输出对**目标**的语义信息进行编码，这种表示对显著的外观变化是不变的。但是，它们的空间分辨率过于粗糙，无法精确地定位**目标**。相反，早期卷积图层中的要素提供了更精确的本地化，但对外观更改的不变

程度较低。我们将卷积层的层次特征解释为图像金字塔表示的非线性对应，并显式利用这些多层次的抽象来表示**目标**对象。具体来说，我们学习每个卷积层的输出上的自适应相关筛选器，以对**目标**外观进行编码。我们推断每一层的最大响应，以粗到细的方式定位**目标**。为了进一步处理规模估计和重新检测目标对象的问题，跟踪故障所造成的重遮挡或视图外**移动**，我们保守地学习了另一个相关滤波器，该筛选器维护了**目标**外观的长期记忆，作为一个判别分类器。我们将分类器应用于两种类型的对象建议: (1) 小步长的建议，并紧紧围绕规模估计的估计位置;(2) 具有较大步长的建议，并在整个图像中进行**目标重新检测**。大规模基准数据集的大量实验结果表明，该算法在最先进的跟踪方法下具有较好的效果。少

2018 年 8 月 11 日提交;v1 于 2017 年 7 月 12 日提交;最初宣布 2017 年 7 月。

评论:出现在 t-pami 2018 中，项目页面
https://sites.google.com/site/chaoma99/hcft-tracking

348. **第 077.00772[pdf, ps,其他] Cs。Sy**

制定相关指标，识别电网的协同网络攻击

作者:christian moya, jiang wang

摘要: 对信息和通信技术 (ict) 的日益依赖使电网面临网络攻击。特别是，协调网络攻击被认为具有高度的威胁，难以防御，因为它们 (i) 通过整合来自多个攻击实体的更多资源而具有更大的破坏性，并且 (ii) 呈现异质性通过命中多个**目标**来实现攻击目标，从而实现网络空间和物理网格中的特征。因此，与独立攻击 (其严重性受到电网冗余的限制) 不同, cca 可能会造成灾难性的后果，如停电。本文提出了一种在静态控制应用中开发相关指标的方法，以防范 cca。这些建议的指标将 cca 的**目标**与电网上的攻击目标联系起来。与相关工作相比，建议的索引提供了部署简单的优点，并能够**检测**更复杂的攻击，如测量攻击。我们演示了使用测量攻击来攻击安全受限经济调度的方法。少

2018 年 5 月 29 日提交;v1 于 2017 年 7 月 3 日提交;最初宣布 2017 年 7 月。

评论:9 页, 6 个数字

349. **特别报告: 1706. 07342[pdf,其他] Cs。简历**

一种用于心脏结构和功能自动测定及二维超声心动图检测疾病的计算机视觉管道

作者:jeffrey zhang , sravani gajjala, pulkit Agrawal , geoffreyh. tison , laura a. hallock, lauren beussink-nelson, eugene fan, mandar a.aras, charandlejordan, kirsten e. fleischmann, michelle melisko , atif qasim, aletei efros , sanjiv j.shah, ruzena bajcsy, rahul c. deo

摘要: 自动心脏图像解释有可能通过多种方式改变临床实践，包括在初级保健和农村环境中实现低成本的心功能序列评估。我们假设计算机视觉的进步可以建立一个完全自动化的，可扩展的分析管道，超声心动图 (回声) 解释。我们的方法包括: 1) 预处理;2) 卷积神经网络 (cnn)，用于视图识别、图像分割和心脏周期的阶段划分;3) 房间体积和左心室质量的定量;4) 颗粒跟踪计算纵向应变;和 5)**有针对性**的疾病**检测**。cnn 准确识别视图 (例如，根尖 4 室的景观为 99%) 和分割的单个心房。心脏结构测量与研究报告值一致 (例如，左心室舒张体积指数的平均绝对偏差 (mad)，为左心室舒张体积指数，2918 项研究)。我们计算了自动射射分数和纵向应变测量 (在 2 个队列内)，这与商业软件衍生值一致 [用于射血分数, mad 下属 5.3%, n 增幅 3101 研究; 对于应变, mad 增幅 1.5% (n 何 s19.197) 和 1.6% (n 闸门 110)],证明了对乳腺癌患者氨蝶单抗的连续监测的适用性。总体而言，我们发现，与手动测量相比，自动测量在七个内部一致性指标中

具有优异的性能，一直以来的相关系数平均增加 0.05 (pcs0.02)。最后，我们开发了肥厚性心肌病和心脏淀粉样变的疾病**检测**算法，c 统计分别为 0.93 和 0.93。我们的管道为使用自动解释来支持护理点手持式心脏超声和对医疗系统中存档的数百万回声进行大规模分析奠定了基础。少

2018 年 1 月 12 日提交;v1 于 2017 年 6 月 22 日提交;最初宣布 2017 年 6 月。

评论:9 个数字，2 张桌子

350. 第 079/02499[pdf,其他] Cs。Hc

切片类型：使用合并键盘快速看头键入

作者:burak benligiray, cihan topal , cuneyt Akinlar

摘要: 抖动是凝视**检测**的必然副产品。正因为如此，凝视打字往往是一个缓慢而令人沮丧的过程。在本文中，我们提出了一个屏幕键盘，针对凝视输入进行了优化。我们的主要目标是更有效地使用屏幕区域。我们通过确定不会用于下一个输入的键，并使用合并动画将它们的空间分配给相邻的键，来实现这一目标。我们相邻地放置频繁和很少使用的密钥对，以方便合并功能。在**瞄准**较大按键时，眼动仪引入的抖动会减少阻碍。这将使用户键入更快、更舒适。每个键上都显示一个字符和一个相关的预测。住在钥匙处进入性格，双人居住进入预测。当停留在输入字符的键上时，用户可以毫不费力地读取相关的预测。这些功能所提供的改进是使用 fitts 定律量化的。将拟议键盘的性能与另外两个为凝视打字而设计的软键盘--dasher 和 gazestalk 进行了比较。37 位新手用户用所有三个键盘输入了一段文字。实验结果表明，所建议的键盘允许更快的打字，是用户更好的首选。少

2018 年 3 月 18 日提交;v1 于 2017 年 6 月 8 日提交;最初宣布 2017 年 6 月。

351. 第 07:170 6.001091[pdf,其他] si

聚类技术在个性化网页排名估计中的作用

作者:daniel vial , vijay subramanian

抽象: 个性化的 paragrank (ppr) 是从另一个节点的角度衡量节点重要性的一个指标(我们将这些节点称为目标和源，分别)。ppr 已被用于许多应用程序，例如提供推特用户 (来源) 关于谁应遵循的建议 (ppr 认为重要的**目标**);此外，ppr 还被用于社区**检测**等图形理论问题。然而，对于 twitter 这样的大型网络来说，计算 ppr 是不可行的，因此高效的估计算法是必要的。在本文中，我们分析了 ppr 估计复杂度与聚类的关系。首先，我们设计了估计许多源/**目标**对的 ppr 的算法。特别是，我们提出了现有单对估计器的增强版本双向 ppr 这对于许多对估计来说是更有用的。然后，我们证明，可以利用共同的基础图来有效地联合估计多个对的 ppr，而不是使用原始算法分别处理每个对。接下来，我们展示了联合估计方案的复杂性与手边源和**目标**之间的聚类程度密切相关，表明当聚类发生时，估计多个对的 ppr 更容易。最后，我们考虑在有几台机器可用于并行计算的情况下估算 ppr，并设计出一种利用我们的聚类研究结果，特别是计算的数量的方法就地，以减少计算时间的方式将任务分配给计算机。这表明，复杂性和聚类之间的关系在实际分布式环境中具有重要的影响。少

2018 年 7 月 23 日提交;v1 于 2017 年 6 月 4 日提交;最初宣布 2017 年 6 月。

352. 第 xiv:1706. 00672[pdf,其他] Cs。简历

一种 n 型 gm-phd 滤波器的研制，用于多目标、多类型视觉跟踪

作者:nathanael l. baisa , andrew wallace

抽象: 我们提出了一个新的框架，扩展了标准概率假设密度 (phd) 滤波器的多个**目标**具有 n 不同类型的 n≥2 基于随机有限集 (rfs) 理论，不仅要考虑背景误报 (杂波)，还要考虑不同**目标**类型的**检测**，这些目标类型在性质上与背景的性质一般不同杂 波。在高斯和线性的假设下，我们的框架扩展了标准 phd 滤波器的现有高斯混合 (gm) 实现，以创建 n 型 gm-phd 滤波器。该方法通过将对象探测器的信息集成到此滤波器中，将两个场景应用于真实的视频序列。在第一种情况下，三 gm-phd 滤波器 (n=3 个) 应用于真实的视频序列，其中包含三种类型的多个**目标**在同一场景，两支足球队和一个裁判，使用单独的，但混乱的**检测**。在第二种情况下，我们使用双 gm-phd 滤波器 (n=2)，用于追踪同一场景中的行人和车辆，处理其探测器的混乱。对于这两种情况，munkres 的匈牙利赋值算法的变体用于关联帧之间的跟踪**目标**标识。使用最佳子模式分配 (ospa) 指标和判别率对此方法进行了评估，并将其与原始检测和独立的 gm-phd 滤波器进行了比较。这表明了我们在真实视频序列上的策略性能的提高。少

2018 年 9 月 6 日提交;v1 于 2017 年 5 月 31 日提交;最初宣布 2017 年 6 月。

评论:arxiv 管理说明: 文本与 arxiv:1705.0 4757 重叠

353. 第 07:170 5.11175[pdf,其他] Cs。简历

在稀疏和密集环境中使用多层混合特征的长期相关跟踪

作者:nathanael l. baisa , deepayan bhowmik, andrew wallace

摘要: 在稀疏和拥挤的环境中跟踪感兴趣的**目标**是一个具有挑战性的问题，在文献中尚未成功解决。本文提出了一种新的长期视觉跟踪算法，学习判别相关滤波器，并使用在线分类器，对稀疏和拥挤视频序列中的目标进行跟踪。首先，我们学习了一个翻译相关滤波器使用多层混合卷积神经网络 (cnn) 和传统的手工制作的功能。我们将较低卷积层的优点结合起来，前者保留了更多的空间细节，可实现精确定位，后者还结合了较高的卷积层，后者对语义信息进行编码以处理外观变化，然后将其与这些信息集成在一起定向梯度 (hog) 直方图和颜色命名传统特征。其次，我们包括一个重新**检测**模块，通过使用手动设计功能在最自信的帧上培训增量 (在线) 支持向量机，克服长期遮挡导致的跟踪故障。只有当对象的相关响应低于某个预定义的阈值时，才会激活此重新**检测**模块。这就产生了高分**检测**方案，并使用高斯混合概率假设密度 (gm-phd) 滤波器进行临时过滤，以找到以最大权重为**目标**状态的**检测**方案通过删除其他**检测**建议作为杂乱的估计。最后，我们学习了一个尺度相关滤波器，通过使用 hog 特征围绕估计或重新**检测**的位置构建**目标**金字塔来估计**目标**的规模。我们在稀疏和密集的数据集上进行了广泛的实验，结果表明我们的方法明显优于最先进的方法。少

2018 年 9 月 6 日提交;v1 于 2017 年 5 月 31 日提交;最初宣布 2017 年 5 月。

354. 第 17f: 170 5.08778[pdf,其他] Cs。铬

自适应降噪深网中对抗图像实例的检测

作者:梁斌,李洪成,苏苗强,李锡荣, 史文昌,王晓峰

摘要: 最近，许多研究表明，深度神经网络 (dnn) 分类器可以通过对抗示例来愚弄，该示例是通过在原始示例中引入一些扰动而制作的。因此，提出了一些强有力的防御技术。但是，现有的防御技术通常需要修改**目标**模型或依赖于事先了解的攻击。在本文中，我们提出了一种检测对抗图像示例的简单方法，该方法可以直接部署到未经修改的现成

dnn 模型中。我们认为图像的摄动是一种噪声，并介绍了两种经典的图像处理技术，即标量量化和平滑空间滤波器，以降低其效果。利用图像熵作为度量，对不同类型的图像实现自适应降噪。因此，可以通过比较特定样本的分类结果及其被剥夺的版本，而不提及事先对攻击的任何了解，有效**地检测**到对抗性的例子。与一些最先进的 dnn 模型相比，使用了 20, 000 多个对抗示例来评估所提出的方法，该方法采用了不同的攻击技术。实验表明，我们**的检测**方法能达到 9. 3 9% 的高 f 1 总分，肯定提高了防御意识攻击的门槛。少

2018 年 6 月 3 日提交;v1 于 2017 年 5 月 23 日提交;最初宣布 2017 年 5 月。

355. 建议: 1705 5.07663[pdf,其他] Cs。铬

对生成模型的成员推理攻击

作者:jamie hayes, luca melis , george danezis , emiliano de cristofaro

摘要: 生成模型估计数据集的基础分布，以便根据该分布生成逼真的样本。本文提出了第一个针对生成模型的隶属度推理攻击: 给定一个数据点，对手确定它是否被用来训练模型。我们的攻击利用生成对抗性 (gans)，该网络结合了鉴别和生成模型，利用鉴别器的学习能力，检测过度拟合并识别作为培训数据集一部分的输入分布的统计差异。我们提出的攻击基于白盒和黑匣子访问**目标**模型，针对几个最先进的生成模型，在复杂的表示面 (lfw)，对象 (cifar-10) 和医学图像 (糖尿病视网膜病变)。我们还讨论了攻击对不同训练参数的敏感性，以及它们对缓解策略的鲁棒性，发现防御要么无效，要么导致生成模型在以下方面的性能明显恶化:训练稳定性和样品质量。少

2018 年 8 月 21 日提交;v1 于 2017 年 5 月 22 日提交;最初宣布 2017 年 5 月。

日记本参考:《加强隐私技术论文集》，第 2019 卷，第 1 期

356. 第 1705. 00349[pdf,其他] Cs。燃气轮机

检测战略攻击的网络检测

作者:mathieu dahan, lina sela, Saurabh amin

文摘: 我们研究了战略网络检查的一般问题，其中一名防御者 (检查机构) 负责**检测**网络中存在的多次攻击。这名后卫可以接触到数量有限的探测器，她可以随机在网络中定位，以监控其组件。我们将解决使用最少数量的检测器来确定随机检测策略的问题，以确保**目标**预期攻击检测率。为了解决这个问题，我们制定了一个包含纳什均衡的数学程序，该模型涉及到后卫和攻击者之间大规模战略博弈的纳什均衡。我们提出了一种新的方法，利用最小集盖和最大集包装问题的解，构造了博弈的近似均衡策略轮廓。这种结构可以被看作是安全游戏中一些以前已知的结果的概括，可以扩展到大规模网络。重要的是，通过使用博弈论和组合参数，我们在检测器数量和攻击**检测**率方面为检测问题的解决提供了最佳保证。我们还推导了平衡中攻击**检测**率的结构结果，可用于通过柱生成过程进一步改善这些保证。少

2018 年 10 月 11 日提交;v1 于 2017 年 4 月 30 日提交;最初宣布 2017 年 5 月。

357. 第 1704. 07333[pdf,其他] Cs。简历

人与对象相互作用的检测与识别

作者:georgia gkioxari, ross girshick , piotr dollár, k 对准 he

摘要: 要了解视觉世界，机器不仅要识别单个对象实例，还要识别它们之间的交互方式。人类往往是这种相互作用的中心,**检测**人与物体的相互作用是一个重要的实际和科学问题。本文讨论了在挑战日常照片中**检测**& lt; 人、动词、对象 & gt; 三胞胎的任务。

我们提出了一个新的模型，它是由以人为中心的方法驱动的。我们的假设是，一个人的外表--他们的姿势、衣着、动作--是本地化他们正在与之互动的物体的有力线索。为了利用这个提示，我们的模型学习根据**被检测到**的人的外观来预测目标对象位置上的特定于**操作**的密度。我们的模型还共同学习**检测**人和对象，并通过融合这些预测，有效地将交互三胞胎注入一个干净的、共同训练的端到端系统中，我们称之为 interactnet。我们验证了我们在 coco (v-coco) 和 hico-det 数据集中最近引入的动词的方法，在这些数据集中，我们在这些数据集中展示了令人信服的结果。少

2018 年 3 月 26 日提交;v1 于 2017 年 4 月 24 日提交;最初宣布 2017 年 4 月。

358. **第 070002402[pdf,其他] Cs。简历**

多伊 10.1016/j.imavis.2017.12.002

godp：全球优化的双重路径系统，用于野外面部地标定位

作者:吴玉航, shishir k.shah, ioannis a. kakadiaris

摘要: 人脸地标定位是后不变人脸识别的基本模块。面部地标**检测**最常见的方法是级联回归，它由特征提取和面部形状回归两个步骤组成。最近的方法采用深层卷积网络来提取每个步骤的鲁棒特征，而整个系统可以看作是一个深级联回归体系结构。在这项工作中，不使用深度回归网络，提出了一个全局优化的双路径 (godp) 深层体系结构，通过解决级联像素标记问题来识别**目标**像素，而无需诉诸高级级像素标记推理模型或复杂的堆叠架构。提出的端到端系统依赖于距离感知软最大函数和双路径建议优化体系结构。结果表明，在多个野外面对齐数据库中，它的性能优于最先进的基于级联回归的方法。该模型在 aflw 数据库上实现了 1.84 归一化均值误差 (nme)，比 3ddfa 高出 61.8。人脸识别实验表明，与具有挑战性的数据库上的 dlib 工具箱相比，godp 与 dpm 猎头一起，能够将等级 1 识别率提高 44.2。少

2017 年 12 月 19 日提交;v1 于 2017 年 4 月 7 日提交;最初宣布 2017 年 4 月。

评论:2017 年 12 月被图像和视觉计算所接受

日记本参考:图像和视觉计算, 2018

359. **第 1703.07500[pdf,其他] Cs。Sy**

有限信息的攻击者能否利用历史数据对电力系统进行成功的错误数据注入攻击?

作者:张家子,朱志刚,拉利莎·桑卡尔,奥利弗·科苏特

摘要: 本文研究了仅在电力系统子网络内使用信息设计的不可观察的虚假数据注入 (fdi) 攻击的物理后果。此攻击的目标是使选定的**目标**线超载，而不会通过测量**检测到**。为了克服有限的信息，建立了一个多元线性回归模型，从历史数据中了解外部网络与攻击子网络之间的关系。通过解决两级优化问题来评估此类 fdi 攻击可能带来的最严重后果，其中一级模拟有限的攻击资源，而第二级通过直流最佳潮流制定系统对此类攻击的响应(opf)。有限信息的攻击模型反映在 dc opf 公式中，该公式只考虑攻击子网的系统信息。ieee 24 总线 rts 和 ieee 118 总线系统说明了此攻击模型的漏洞。少

2018 年 5 月 1 日提交;v1 于 2017 年 3 月 21 日提交;最初宣布 2017 年 3 月。

评论:12 页, 7 个数字，接受 ieee 电力系统交易

日记本参考:j. zhang, z. chu, l. sankar 和 o. kosut, "具有有限信息的攻击者能否利用历史数据在电力系统上安装成功的假数据注入攻击？", ieee 关于电力系统的交易, 2018 年

360. **xiv:170 0008899[pdf, ps,其他] Cs。Ds**

重新选择的图形中的二进制搜索

作者:Argyrios deligkas, george b. mertzios, paul g.spirakis

摘要: 在路径中的经典二进制搜索中，目的是通过求尽可能少的查询**来检测**未知**目标**，每个查询都会显示目标的方向. 这种二进制搜索算法最近被 [Emamjomeh-Zadeh 等人, stoc, 2016] 扩展到在任意图形中**检测目标**的问题。与路径中的经典情况类似，Emamjomeh-Zadeh 等人的算法为**目标**保留了候选对象的设置，而每个查询都询问适当选择的顶点--"中位"，以最大限度地减少潜在的可能性Φ在候选集合的顶点之间。在本文中，我们讨论了 Emamjomeh-Zadeh 等人提出的三个未决问题，即 (a)**当**查询响应是指向**目标**的近似最短路径的方向时检测**目标**; (b)**检测到**当查询的顶点是当前候选集的近似值 (而不是精确的一个) 时的**目标**，以及 (c)**检测**多个**目标**，据我们所知，到目前为止还没有取得任何进展。我们通过提供适当的上限和下限以及新的潜力来解决 (a) 和 (b) 项问题按即使每次都查询近似值，也能保证有效的**目标检测**。关于 (c)，我们启动了一项系统的研究，用于**检测**图形中的两个**目标**，并确定了查询的充分条件，这些条件允许为查询数。我们所有的积极成果都可以用我们的新潜力来获得按允许查询近似介质。少

2018 年 8 月 16 日提交;v1 于 2017 年 2 月 28 日提交;最初宣布 2017 年 2 月。

361. 建议: 1701.04508[pdf,其他] Cs。Lg

基于规范内核的单级分类在线学习

作者:chandan gautam, aruna tiwari , sundaram suresh, kapil ahuja

文摘: 本文提出了一种基于正则内核的单类极端学习机器 (elm) 分类器在线学习，称为在线 rk-oc-elm。基线核超平面模型采用正则 elm 方法，在单类分类 (occ) 的情况下，采用正则 elm 方法对单个块中的整个数据进行离线学习。此外，本文还从训练样本的流出发，以在线方式对基本超平面模型进行了调整。提出了两个框架，即边界和重构，以**检测**在线 rkoc-elm 中**的目标**类。基于边界框架的单类分类器由单节点输出体系结构组成，分类器努力将所有数据近似为任意实数。然而，基于重建框架的一类分类器是一种自动编码器体系结构，其中输出节点与输入节点相同，分类器努力在输出层重建输入层。这两个框架都采用了基于在线学习的正则内核 elm，并采用基于一致性的模型选择来选择学习算法参数。在线 rk-oc-elm 在标准基准数据集和人工数据集上进行了性能评估，并将结果与现有的一流分类器进行了比较。结果表明，在线学习单类分类器与基于批量学习的方法稍好或相同。由于所提出的分类器所使用的基本分类器是基于 elm 的，因此，所提出的分类器也将继承基本分类器的优点，即与传统的基于一类的自动编码器相比，它将执行更快的计算。少

2018 年 4 月 9 日提交;v1 于 2017 年 1 月 16 日提交;最初宣布 2017 年 1 月。

评论:论文已提交给《系统、人和控制论 ieee 交易特别问题: 带有手稿 id 的系统: smca-16-09-1033，第 3 次提交 id: smca-18-03-0322 》

362. 第 1612.04433[pdf,其他] Cs。铬

通过构建行为模型的马尔可夫链检测 android 恶意软件

作者:enrico mariconti, lucky onwuzurike, panagiotis Panagiotis, emiliano de cristofaro, gordon ross, gianluca stringini

摘要: android 平台的普及程度上升，导致**针对它的**恶意软件威胁激增。随着 android 恶意软件和操作系统本身的不断发展，设计强大的恶意软件缓解技术是非常具有挑战性的，这些技术可以长时间运行，而无需修改或昂贵的再培训。在本文中，我们介绍了 mamadroid，这是一个依赖于应用行为的 android **恶意软件检测**系统。maamdroid 从应用执行的抽象 api 调用序列中，以马尔可夫链的形式构建了一个行为模型，并使用它来提取功能和执行分类。通过对其包或系列的抽象调用，maamdroid 保持了对 api 更改的恢复能力，并保持了功能集大小的可管理性。我们评估其在六年内收集的 8.5 k 良性和 35.5 万恶意应用的数据集上的准确性，表明它不仅能有效**地检测**恶意软件 (高达 99% 的 f 计量)，而且系统构建的模型保留了其长时间的检测能力 (平均为 86% 和 75% 的 f 测量，分别为培训后一年和两年)。最后，我们与 droidapiminer 进行了比较，这是一个最先进的系统，它依赖于应用执行 api 调用的频率，显示 maimdroid 的执行率明显优于它。少

2017 年 11 月 20 日提交;v1 于 2016 年 12 月 13 日提交;最初宣布 2016 年 12 月。

评论:本文发表在第 24 届网络和分布式系统安全研讨会 (ndss 2017) 论文集上。此版本中的一些实验略有更新

363. 决议: 1611.07218[pdf] Cs。简历

使用人为派生的上下文期望可以改进深层神经网络

作者:harish katti, marius v. peelen, s. p. arun

摘要: 实际世界中的对象发生在特定的上下文中。事实表明，这种情况通过限制搜索地点，有助于**发现**.但上下文是否能直接有利于对象**检测**呢? 为此，需要独立于**目标**功能学习上下文。这在传统的对象**检测**中是不可能的，因为分类器是在包含**目标**特征和周围上下文的图像上训练的。相比之下，人类可以分别学习上下文和**目标**功能，比如当我们看到没有汽车的公路时。在这里，我们首次展示了人为的场景期望可以用来提高机器中的对象**检测**性能。为了衡量背景期望，我们要求人类主体说明在没有这些物体的场景中发生汽车或人的规模、位置和可能性。人类表现出高度系统的期望，我们可以准确地预测使用场景特征。这使得我们能够在不需要人工注释的情况下预测人类对新场景的期望。在使用预测的人类期望增强深层神经网络方面，我们在**检测**汽车和人 (1-3%) 的准确性以及**检测**相关物体 (3-20) 方面取得了显著的进步。与此形成鲜明对比的是，用其他传统特征扩大深度网络所产生的收益要小得多。这种改善是由于极有可能在极有可能被正确地贴上目标标签的地点的比赛相对较差，而在不可能的地点的激烈比赛被正确地拒绝为假警报。总之，我们的研究结果表明，使用人为派生的上下文特征增强深层神经网络可以提高它们的性能，这表明人类与深度网络不同，分别学习场景上下文。少

2018 年 3 月 28 日提交;v1 于 2016 年 11 月 22 日提交;最初宣布 2016 年 11 月。

评论:30 页, 5 个数字, 3 个表, 2 个补充表

364. 第 1611. 05345[pdf,其他] Cs。简历

多伊 10.1109/TIP.2018.2864891

基于回溯空间金字塔池 (spp) 的图像分类器，用于弱监督的顶部高目标检测

作者:hisham cholakkal, jubin johnson, deepu rajan

摘要: 自上而下的显著性模型生成一个概率图，该概率图在任务/目标 (如对象**检测**) 指定的**目标**位置达到峰值。它们通常在完全受监督的环境中进行训练，其中涉及对象的像素级注释。我们建议使用一个弱监督的自上而下的显著性框架，仅使用二进制标签，指示图像中对象的存在。首先，通过回溯策略计算了每个图像区域对基于 cnnb 的图像

分类器的置信度的概率贡献，从而产生自上而下的显著性。从一组由快速的自下而上的显著性方法生成的图像的显著性映射中，我们选择了适合自上而下任务的最佳显著性映射。选择的自下而上的显著性映射与自上而下的显著性映射相结合。利用组合显著性较高的特征来训练线性 svm 分类器来估计特征的显著性。这与组合显著性相结合，并通过显著性映射的多尺度超级像素平均图进一步细化。我们评估了拟议的弱监督自上而下的显著性的性能，并通过完全监督的方法实现了可比的性能。对 7 个具有挑战性的数据集进行了实验，并将定量结果与 4 种不同应用中的 40 种密切相关的方法进行了比较。少

2018 年 8 月 14 日提交;v1 于 2016 年 11 月 16 日提交;最初宣布 2016 年 11 月。

评论:14 页, 7 个数字

日记本参考:h. cholakkal, j. johnson, d. rajan, "基于回溯空间金字塔池 (spp) 的图像分类器，用于薄弱监管的自上而下的突出对象检测", ieee 图像处理事务, 2018 年 8 月

365. 建议: 1611. 0333[pdf,其他] Cs。毫米

多伊 10.1109/TIFS.2017.2779446

基于混合深度学习框架的大规模 jpeg 隐身分析

作者:曾继申,谭顺泉，李斌,黄继武

摘要: 在图像隐写中采用深度学习尚处于起步阶段。本文结合丰富隐式催化模型背后的领域知识，提出了一种通用的 jpeg 隐写分析混合深度学习框架。我们提出的框架包括两个主要阶段。第一阶段是手工制作的，对应于卷积阶段和丰富模型的量化和截断阶段。第二阶段是包含多个深子网的复合深部神经网络，在训练过程中学习模型参数。我们提供了实验证据和理论思考，认为引入阈值量化器，虽然禁用了基于梯度-血统的学习底部卷积阶段，确实是具有成本效益的。我们在从 imagenet 提取的大型数据集上进行了广泛的实验。我们实验中使用的主要数据集包含 500, 000 个覆盖图像，而我们最大的数据集包含 500 万个覆盖图像。实验表明，将量化和截断集成到深度学习的隐式分析仪中，可以显著提高**检测**性能。此外，我们还证明了我们的框架对 jpeg 阻塞工件的更改不敏感，并且学习的模型可以很容易地转移到不同的攻击**目标**，甚至不同的数据集。这些特性在实际应用中至关重要。少

2017 年 11 月 24 日提交;v1 于 2016 年 11 月 10 日提交;最初宣布 2016 年 11 月。

评论:被 ieee 信息取证和安全事务所接受

366. 第 1605 5.07824[pdf,其他] Cs。简历

通过概念和属性进行操作分类

作者:amir rosenfeld, shimon ullman

摘要: 自然图像中的类倾向于遵循长尾分布。当罕见课程的培训示例不足时，这是有问题的。复合类强调了这种效果，涉及几个概念的结合，例如出现在操作识别数据集中的概念。在本文中，我们建议通过学习如何利用现成的常见视觉概念来解决这个问题。我们**检测图像**中存在的显著概念，并使用它们来推断**目标**标签，而不是直接使用视觉特征，将视觉和自然语言处理中的工具结合起来。我们验证了我们的方法，最近引入的 hico 数据集达到了 31.54% 的 map 和 standfort-40 action 数据集，其中建议的方法优于通过直接视觉特征获得的方法，获得了 83.12 的精度。此外，该方法为每个类提供了一个语义上有意义的关键字列表和将其与其组成概念相关联的相关图像区域。少

2018 年 3 月 6 日提交;v1 于 2016 年 5 月 25 日提交;最初宣布 2016 年 5 月。

367. 第 1603. 04223[pdf] cs. ne

基于事件的内存表面的研究，用于高速跟踪、无监督特征提取和目标识别

作者:saeed afshar, gregory cohen , tara julia hamilton, jonathan tapson , andre van sceik

摘要: 本文比较了基于事件的衰变和基于时间的衰变内存表面，以便使用基于事件的摄像机进行基于事件的高速跟踪、特征提取和对象分类。高速识别任务包括对自由放置在相机镜头附近的模型**飞机进行检测**和分类，从而生成具有挑战性的数据集，使**其在目标**速度上出现显著差异。这种差异促使对基于事件的衰变内存表面的研究与基于时间的衰变内存表面进行比较，以捕获基于事件的数据的时间方面。然后，这些表面用于执行无监督的特征提取、跟踪和识别。为了生成内存表面，研究了事件成皮、线性衰变的内核和指数衰减的内核，发现其性能最佳的指数衰减内核。研究发现，基于事件的衰减记忆表面在识别中的性能优于基于时间的衰减内存表面，特别是在对**目标**速度不变性的要求下。研究了各种网络和接受场大小。该系统在飞机进入视场的 156 毫秒内达到 98.75% 的识别精度，仅使用 25 个基于事件的特征提取神经元与线性分类器串联。通过将线性分类器的结果与 elm 分类器进行比较，我们发现少量基于事件的特征提取器可以有效地将数据集的复杂时空事件模式投影到几乎线性可分离的表示中。功能空间。少

2017 年 11 月 8 日提交;v1 于 2016 年 3 月 14 日提交;最初宣布 2016 年 3 月。

评论:这是以前提交的手稿的更新版本

368. 建议: 1601.0. 05585[pdf, ps,其他] Cs。Sy

多伊 10.23919/ICIF.2017.8009645

广义最优子模式分配指标

作者:abu sajana rahmathullah, angel f. garcía-fernández, lennart svensson

文摘: 本文提出了有限**目标**集空间上的广义最优次模式分配 (gospa) 度量。与公认的最优子模式分配 (ospa) 指标相比, gospa 作为基数的函数是不归一化的，它以不同的方式惩罚基数错误，这使我们能够将其表示为对赋值的优化，而不是对赋值的优化排列。这样做的一个重要后果是，正如传统**的多目标**跟踪所表明的那样, gospa 允许我们惩罚**检测到**的**目标**的本地化错误以及由于缺失和错误**目标**而产生的错误 (mtt) 以良好的方式衡量业绩。此外，我们还将 gospa 度量扩展到随机有限集的空间，这对于以严格的方式通过仿真评估 mtt 算法非常重要。少

2018 年 9 月 12 日提交;v1 于 2016 年 1 月 21 日提交;最初宣布 2016 年 1 月。

评论:在 2017 年 7 月举行的第 20 届信息融合国际会议上，该论文获得了让·皮埃尔·勒·卡雷最佳论文奖。建议的 gospa 指标的 matlab 实现可在 https://github.com/abusajana/GOSPA 还请访问 https://youtu.be/M79GTTytvCM, 了解论文的 15 分钟介绍

日记本参考:2017 年第 20 届信息融合 (融合) 国际会议论文集

369. 第 07:1506.07331[pdf,其他] cs. it

mimo 和 isi 信道迭代接收机信道缩短解调器的设计

作者:沙胡,弗雷德里克·鲁塞克

摘要: 我们考虑了使用小尺寸格子描述来描述接收信号的具有内存的线性矢量通道的解调器设计问题。我们假设一个整体的迭代接收机，对于网格描述未涵盖的信号部分，

我们使用基于外部解码器提供的软信息的干扰取消。为了达到网格的描述，采用线性滤波器作为前端，将信号结构压缩到一个小的格子上。此过程需要设计三个参数: (i) 前端筛选器, (ii) 通过其进行干扰消除的反馈滤波器，以及 (iii) 指定网格的**目标**响应。在此基础上，对这种形式的解调器进行了研究，但 cs 与干扰消除之间的相互作用在文献中没有得到充分的解决。本文分别分析了两种基于福尼和 ungerboeck **检测**模型的 cs 解调器。在广义互信息 (gmi) 函数的基础上，对参数进行了联合优化。我们还介绍了第三种类型的 cs 解调器，它一般是次优的，但对所有参数都有封闭形式的解。此外，还分析了信噪比 (snr) 的渐近特性，并从最大 gmi 的意义上证明了第三个 cs 解调器渐近收敛到最优 cs 解调器。少

2017 年 12 月 21 日提交;v1 于 2015 年 6 月 24 日提交;最初宣布 2015 年 6 月。

评论:提交; 47 页; 12 位数

370. **第 1412.4171[pdf,其他] si**

信息扩散动力学与社会传感

作者:vikram krishnamurthy, william hoiles

摘要: 使用社会传感器进行统计推断是一个取得显著进展的领域，在**有针对性**的广告、营销、自然灾害本地化和预测等应用中具有相关性金融市场投资者的情绪。本章从通信信号处理的角度对社交网络中基于传感器的信息传播的四个重要方面进行了教程描述。首先，考虑了通过推特等社交媒体网络与社交传感一起在大型社交网络中进行信息交流的传播模式。其次，考虑了贝叶斯社会学习模型和风险规避社会学习在金融和网络声誉系统中的应用。第三，利用微观经济学理论中产生的显性偏好原理对数据集进行解析，以确定社会传感器是否为效用最大化器，然后确定其效用函数。最后，利用时间序列分析方法研究了社交传感器与 youtube 频道所有者的相互作用。所有这四个主题都是在卫生网络、社交媒体和心理实验的实际实验数据集的背景下解释的。此外，还给出了利用上述模型推断基于社会感知的基础事件的算法。本章介绍的概述、见解、模型和算法源于网络科学、经济和信号处理的最新发展。在更深层次上 ，本章考虑了网络的平均场动力学、避险贝叶斯社会学习滤波和最快的变化**检测**、通过社会传感器的定向无环图进行决策中的数据。在 youtube 社交网络中，用于实用功能估计 (显性偏好) 和交互社会传感器的统计建模的优化问题。少

2018 年 8 月 14 日提交;v1 于 2014 年 12 月 12 日提交;最初宣布 2014 年 12 月。

评论:arxiv 管理说明: 文本与 arxiv:1405.1129 重叠