人脸检测一年来前沿论文最新进展

2018.11.06 方建勇

提示：采用手机 safari 微软翻译技术

1. 大规模纹身图像搜索：联合检测和紧凑型表示学习

作者:胡汉,李杰,阿尼尔 k.杰恩,石光山，陈锡林

摘要: 视频监控和社交媒体中数字图像的爆炸式增长导致非常需要在执法和法医应用中有效搜查感兴趣的人。尽管在基于人脸和指纹识别的初级生物特征（例如**面部**和指纹）方面取得了巨大进展，但在法医情景中，仅有一个单一的生物特征无法达到所需的识别精度。纹身作为重要的软生物特征之一，已被发现对协助人的识别有价值。然而，在大量无约束图像中的纹身搜索仍然是一个难题，现有的纹身搜索方法主要侧重于匹配裁剪纹身，这与实际应用场景不同。为了缩小差距，我们提出了一种有效的纹身搜索方法，能够通过多任务学习，在单个卷积神经网络（cnn）中共同学习纹身**检测**和紧凑表示。虽然主干网中的特征是由纹身**检测**和紧凑表示学习共享的，但每个子网的各个潜在层都将共享功能优化为**检测**和特征学习任务。通过随机图像拼接和前置功能缓冲，解决了联合纹身**检测**和紧凑表示学习网络内的小批量问题。我们使用多个公共领域纹身基准评估拟议的纹身搜索系统，以及从这些数据集和来自互联网的图像中编译的包含约 300k 干扰器图像

的图库集。此外，我们还介绍了一个纹身素描数据集，其中包含300 个纹身，用于基于素描的纹身搜索。实验结果表明，与几种最先进的纹身检索算法相比，该方法在纹身**检测**和纹身搜索方面具有较好的大规模性能。少

2018 年 11 月 1 日提交;**最初宣布** 2018 年 11 月。

2. 学习色彩空间中的人脸呈现攻击检测

作者:李磊,夏兆强,阿代努尔·哈迪德,姜晓月,罗立法比奥·罗立,冯晓义

摘要: **人脸**攻击**检测**(pad) 已成为生物识别系统的一个棘手问题，并提出了许多对策来解决这一问题。然而，它们中的大多数直接提取特征描述符，并区分假面孔和现有色彩空间中的真实**面孔**(如 rgb、hsv 和 ycbcr)。不幸的是，对我们来说，哪个颜色空间是最好的，或者如何将不同的空间组合在一起是未知的。更糟糕的是，真假**面孔**在现有的色彩空间中重叠。因此，在本文中，产生了一个学习的可分辨的颜色喜欢的空间来处理**人**脸 pad 的问题。更具体地说，我们提供了一个端到端深度学习网络，可以将现有的色彩空间映射到一个新的学习颜色喜欢的空间。在生成对抗性网络 (gan) 生成器的启发下，所提出的网络由一个空间生成器和一个特征提取器组成。在训练色彩型空间时，探索了一种新的点到中心组合机制，以最大限度地提高层间距离，最大限度地

减小内部距离，并在真实的假面孔和呈现的假**面孔**之间保持安全的距离。在两个标准**人**脸 pad 数据库（即继动攻击数据库和 oulu-npu）上进行的广泛实验表明，我们提出的基于颜色的空间分析对抗显著优于最先进的方法，显示出出色的性能。泛化能力。少

2018 年 10 月 31 日提交;**最初宣布** 2018 年 10 月。

3. **更有效地利用工艺和产品可追溯性数据，持续改进工业性能**

作者:thierno diallo, sébastien henry, yacine ouzrout

摘要: 如今，所有工业部门都越来越**多地面临**数据量的激增。因此，它提出了有效利用这大量数据的问题。在这项研究工作中，我们关注的是工艺和产品的可追溯性数据。在一些部门（如药品和农业食品），需要收集和储存这些数据。除了这一限制（监管和/或合同）之外，我们还对使用这些数据持续改进工业性能感兴趣。确定了两个研究轴心：产品召回和对生产危害的反应能力。对于第一轴，将提出一个过程，用于产品召回利用可追溯性数据。为第二轴设想了检测和预测功能的**发展**，将过程和产品数据结合起来。少

2018 年 10 月 31 日提交;**最初宣布** 2018 年 10 月。

4. **用于大规模目标检测的混合知识路由模块**

作者:蒋振汉,徐航,梁祥丹,梁林

摘要: 显性对象**检测**方法分别处理每个区域的识别，忽略了一个场景中对象之间的关键语义相关性。这种模式导致大量的性能下降时，面对沉重的长尾问题，其中很少的样本可用于罕见的类和大量的混乱类别存在。我们利用不同的人类常识知识对大规模的对象类别进行推理，并在一个图像中达到语义一致性。特别是，我们提出了混合知识路由模块 (hkrm)，它包含了由两种知识形式所传递的推理: 一种用于结构化约束的显式知识模块，这些模块以语言知识 (例如共享的关于概念的属性、关系);和一个隐式知识模块，它描述了一些隐式约束 (例如常见的空间布局)。通过在区域到区域的图形上运行，这两个模块都可以个性化，并在特定知识形式的指导下与每个图像中的视觉模式进行协调。hkrm 具有重量轻、通用性强、可扩展性强的特点，可以轻松地将多种知识结合起来，赋予任何**检测**网络全局语义推理的能力。关于大规模目标**检测**基准的实验表明, hkrm 在 visualgenome (1000 个类别) 上获得了约 34.5% 的改进，在 map 方面对 ade 的改善幅度为 30.4%。在 https://github.com/chanyn/HKRM 中可以找到代码和训练过的模型。少

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

5. **用于统计仪识别的特征包**

作者:吴汉洲

文摘: 传统的隐写分析算法侧重于检测单个对象中隐写的存在性。实际上，一个人可能**会面临**一个复杂的场景，其中一个或多个用户中的一个或多个也被称为演员使用隐写，这被定义为摄影师身份识别问题 (sip)。这就需要隐身分析专家设计有效、稳健的**检测**算法，以识别有罪行为者。主流作品采用聚类、集成和异常**检测**的方法，确定了演员特征之间在高维空间中的距离，以找出与统计学家相对应的异常值。但是，在高维空间中，特征点可能是稀疏的，因此特征点之间的距离可能会变得相对相似，这对**检测**没有好处。此外，在机器学习中，推广和套袋等结合技术可以有效地提高**检测**性能。这促使本文作者提出了一种 sip 的功能打包方法。拟议的工作合并了多个**检测**子模型的结果，每个特征空间都从原始的全维空间中随机采样。我们创建了一个名为 imnetease 的新数据集，其中包括从社交网站下载的 5108 张图像，以模拟真实世界的场景。我们从图像中提取 pev-274 特征，并以 nsf5 为算法进行评价。实验表明，在大多数情况下，我们的工作显著提高了对创建数据集的**检测**精度，这表明了其优越性和适用性。少

2018 年 10 月 29 日提交;**最初宣布** 2018 年 10 月。

6. **从人脸视频看人的脉搏率估计：自动分量选择与盲源分离方法的比较**

作者:vladislav ostankovich, geesara prasap, ilya afanasyev

摘要: 人类的心跳可以根据患者的情况，包括接触碱基，如使用仪器和非接触碱基，如计算机视觉辅助技术测量，可以适当地使用几种不同的方法来测量。非接触式技术的使用越来越流行，因为这些技术能够减轻接触基技术的一些限制，特别是在临床部分。然而，由于摄像机的特性、光照变化、**人脸**图像中的肤色等多种原因，现有的视觉引导方法无法证明高精度的结果。我们提出了一种使用视频作为输入并在输出中返回脉冲速率的技术。最初，关键点**检测**是在两个面部次区域进行的：额头和鼻口。删除不稳定特征后，将时间滤波应用于隔离感兴趣的频率。然后采用四组分分析方法，将心血管脉冲信号与呼吸、前庭活动和面部表情其他变化引起的外来噪声区分开来。然后，将所提出的峰值**检测**技术应用于从四种不同的分量选择算法中提取的每个分量。这将能够定位每个组件中的峰值位置。提出了一种自动选择元件的方法，以选择用于计算心跳的最佳元件。最后，我们通过四种成分分析方法（pca、fastica、jade、shibbs）的比较，对 15 名志愿者的**人脸**视频数据集进行处理，并以 ecg/ekg 工作站的验证为基础事实。少

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

7. **攻击满足可解释性：对对抗性样本的属性驱动检测**

作者:陶冠宏、马世清、刘英奇、张祥宇

摘要: 对抗性样本攻击会使良性输入受到干扰，从而诱发 dnn 的不良行为。最近的研究表明，这种袭击的广泛存在和破坏性后果。现有的防御技术要么假定事先了解特定攻击，要么由于其基本假设，在复杂模型上可能无法很好地工作。我们认为，对抗性样本攻击与 dnn 模型的可解释性密切相关：虽然对良性输入的分类结果可以根据人类可感知的特征来推理，但关于对抗性样本的结果很难被缠住。解释。因此，我们提出了一种基于可解释性的人**脸**识别模型的对抗样本**检测**技术。它具有一种新的属性和内部神经元之间的双向对应推理，以识别对单个属性至关重要的神经元。增强了临界神经元的激活值，放大了计算的推理部分，削弱了其他神经元的值，抑制了不可解释部分。将这种变换后的分类结果与原始模型的分类结果进行比较，以**检测**对手。结果表明，该技术可在7种不同的攻击中达到94% 的**检测**准确率，对良性输入的误报率为 9.91。相比之下，最先进的特征压缩技术只能在 23.3% 的误报下达到 55% 的精度。少

2018 年 10 月 26 日提交;**最初宣布** 2018 年 10 月。

8. **stairroute：使用单声道楼梯减少拥塞的早期全局路由**

作者:bapi kar , Susmita sur-kolay, chittaranjan mandal

摘要: 随着工艺技术的急剧缩减，物理设计**面临严峻**挑战，并要求及早**发现**故障。否则，它可能会导致许多迭代，从而影响上市时

间。这鼓励了设计一个反馈机制，从设计流的较低抽象级别到更高的层次。其中一些努力包括放置驱动合成、可路由性（定时）驱动放置等。在这一理念的推动下，我们提出了一种新的全局路由方法，该方法采用单调的楼梯路由区域（通道），定义在平面规划阶段。目的是通过估计路由性、路由网络长度和通集数，同时考虑整个布局中的全局拥塞场景，确定给定设计网络列表的平面图拓扑的可行性。此框架适用于无保留层以及高压保留层模型。m(≥2)金属层，并适应不同的容量配置文件的路由资源，由于在金属层之间的金属间距变化的一致或不同的情况类似于最新的技术。此算法需要 o(n2kt)给定设计的时间。n 块和 K 网有最多 t 终端。mcncsrc 平面规划基准的实验结果表明 100 元%可路由性，而路由区域中的拥塞仅限于 100 元%.所有路由的网长 t-终端（t≥2）网可与 flute 计算的蒸笔长度相媲美。还得到了不同容量分布的通孔数估计。少

2018 年 10 月 24 日提交;**最初宣布** 2018 年 10 月。

9. **dfd：双射击面检测器**

作者:李健,王亚标,王长安,应泰，钱建军，杨建安，王成杰,李吉林,黄飞月

文摘: 近年来，卷积神经网络（cnn）在**人脸检测**方面取得了巨大的成功。然而，由于规模、姿态、遮挡、表情、外观和光照等方面

的高度变异性，目前的**人脸检测**方法仍然是一个具有挑战性的问题。本文提出了一种新的**人脸检测**网络，名为双镜头人脸检测器(dsfd)，该网络继承了 ssd 的体系结构，并引入了功能增强模块(fem)，用于将原始特征图传输到将单个发射探测器扩展到双射探测器。特别是，采用两组锚点计算的渐进式锚力损失 (pal)，以有效地促进特征的实现。此外，我们还提出了一种改进的锚点匹配 (iam) 方法，将新的数据增强技术和锚定设计策略集成到 dsfd 中，以便为回归器提供更好的初始化。广泛的实验流行基准:发展经济学**所 face**(容易:0.966 中：0.9. 57 努力：0。9) 和 fdb (不连续:0.991 连续： 0.862) 展示了 dsfd 相原**出**的优越性 (如 pyramidbox 和 sm)。代码将在发布时提供。少

2018 年 10 月 24 日提交;**最初宣布** 2018 年 10 月。

10. rcanopus: 使 canopus 对失败和拜占庭故障具有复原力

作者:s. keshav, w. golab, b. wong, s. rizvi, s. gorbunov

摘要: 分布式共识是许多分布式系统 (包括分布式数据库和区块链) 的关键推动因素。canopus 是一种可扩展的分布式共识协议，可确保系统中的实时节点就有序的操作序列 (称为事务) 达成一致。与大多数先前的共识协议不同，卡诺普并不依赖于一个领导者。相反，它使用虚拟树覆盖来传播消息，以限制超订阅链接之间的网络流量。它利用机架内部和网络结构内的硬件冗余，以降低

协议复杂性和通信开销。这些设计决策使 canopus 能够支持大型部署，而不会显著降低性能。现有的 canopus 协议在**面对**节点和通信故障时具有弹性，但其重点主要放在性能上，因此不能很好地响应其他类型的故障。例如，单个服务器机架的故障会导致所有活动节点停止。该协议也容易受到拜占庭节点的攻击，这可能会导致不同的实时节点以不同的事务顺序完成协议。在本文中，我们描述了 rcanopus ("恶劣的 canopus")，它扩展了 canopus 以增加活力，即允许实时节点在可能的情况下取得进展，尽管有许多类型的失败。这就要求 rcanopus 能够准确**地检测**故障并从故障中恢复，尽管使用了不可靠的故障检测器，并且容忍拜占庭攻击。其次，rcanopus 保证安全，即在拜占庭攻击和网络分区的情况下，事务订单的实时节点之间达成协议。少

2018 年 10 月 23 日提交;**v1** 于 2018 年 10 月 22 日提交;**最初宣布** 2018 年 10 月。

11. 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: 合成性 (sl) 是新发现抗癌药物靶点的一个很有前途的概念。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，需要计算预测方法来解决这些问题。本文提出了一种新的 sl 预测方法 sl2mf，该方法利用逻

辑矩阵分解法从观测到的 sl 数据中学习基因的潜在表示。两个基因可能形成 sl 的概率是由基因潜在载体的线性组合建模的。由于已知的 sl 对比未知对更值得信任，我们设计了重要性加权方案，以便在 sl2mf 中为已知的 sl 对分配更高的重要性权重和为未知对分配更低的重要性权重。此外，我们还结合了蛋白质-蛋白质相互作用 (ppi) 数据和基因本体论 (go) 的基因生物学知识。特别是，我们根据遗传代的 go 注释和 ppi 网络中的拓扑性质来计算基因之间的相似性。通过对 synlethdb 数据库中的 sl 交互数据进行了大量实验，验证了 sl2mf 的有效性。少

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

12. 恶意软件检测中的对抗性问题实例探讨

作者:屋大维·苏丘,斯科特·e·库尔,杰弗里·约翰斯

摘要: 卷积神经网络 (cnn) 体系结构正越来越多地应用于新的领域，如恶意软件**检测**，在这些领域，它能够从从可执行文件中提取的原始字节中学习恶意行为。这些架构在不涉及功能工程工作的情况下达到了令人印象深刻的性能，但它们对活动攻击者的鲁棒性尚未得到理解。此类恶意软件检测器可能**面临**一种新的攻击媒介，其形式是对分类模型的对抗干扰。现有的规避攻击旨在导致对测试时间实例的错误分类 (图像分类器已对此进行了广泛研究) 并不适用，因为输入语义可以防止对二进制文件的任意更改。

本文探讨了恶意软件**检测**的对抗示例领域。通过在生产规模数据集上对现有模型进行培训，我们显示以前的一些攻击的效果不如最初报告的有效程度，同时突出了有助于恶意软件新攻击策略的体系结构弱点分类。最后，我们探索更通用的攻击策略，以提高规避攻击的潜在有效性。少

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

13. 深杂草：一种用于深层学习的多类杂草物种图像数据集

作者：alex olsen, dmitry a. konovalov, bronson phipha, peter ridd, jake c. wood, jamie johns, wesley banks, benjamin girgenti, owen kenny, james whinney, brendan calvert, mostafa rahimi azghadi,ronald d. white

摘要: 在过去十年中，机器人杂草控制的研究有所增加，有可能提高农业生产力。大部分工作的重点是开发耕地机器人技术，而忽视了牧场畜牧业**农民面临**的重大杂草管理问题。也许广泛吸收机器人杂草控制的最大障碍是在其自然环境中对杂草物种进行可靠**的检测**。深度学习的无与伦比的成功使其成为在高度复杂的澳大利亚牧场环境中识别各种杂草的理想选择。这项工作贡献了第一个大型的，公开的，多类的图像数据集的杂草物种从澳大利亚牧场;允许开发可靠的**检测**方法，使机器人杂草控制可行。深杂草数据集由 17 509 张贴有标签的图像组成，这些图像的主要是分布在澳大利亚北部 8 个地点的 8 种具有全国意义的杂草。本文还利用基准深度学习模型--感知 v3 和 resnet-50 给出了数据集的

分类性能基准。这些模型的平均分类性能分别为 87.9% 和 90.5。这一强劲的结果预示着未来在澳大利亚牧场实施机器人杂草控制方法的良好前景。少

2018 年 10 月 9 日提交;最初宣布 2018 年 10 月。

14. **dyverse：多租户边缘环境中的 dynamic 垂直缩放**

作者:nan wang, michail matthaiou , Dimitrios s. nikopoulos, b 江 e varghese

摘要: 资源受限环境中的多租户是边缘计算中的一个关键挑战。本文开发了 "边缘环境中的 dyaminemic 垂直缩放"，这是第一个用于管理分配给应用程序的资源以促进边缘环境中的多租户的轻量级垂直缩放机制。为了实现动态垂直扩展，提出了一种静态和三种静态优先级管理方法，分别是工作负载感知、社区感知和系统感知。本研究主张动态垂直缩放和优先级管理方法可降低服务级别目标 (slo) 冲突率。利用云边缘试验台上的在线游戏和**人脸检测**工作负载来验证这项研究。dyverse 的优点是，当在单个边缘节点上部署 32 台边缘服务器时，每个边缘服务器只有一秒的开销。与在没有动态垂直缩放的边缘服务器上执行应用程序相比，静态优先级和动态优先级可将在线游戏请求的 slo 冲突率分别降低 4% 和 12%，在这两种情况下，对于面部可降低 6% **检测**工作负载。此外，对于这两个工作负载，与其他方法相比，系统感知动态垂直缩放方法有效地减少了未被违反请求的延迟。少

2018 年 9 月 19 日提交;最初宣布 2018 年 10 月。

15. 模型报告的模型卡

作 者 :margaret mitchell, simone wu, andrew zaldivar, parker barnes, lucy vasserman, ben hutchinson, elena spitzer, inioluwa deborah raji, timnit ge 兄弟

摘要: 受过训练的机器学习模式越来越多地用于在执法、医学、教育和就业等领域执行影响大的任务。为了阐明机器学习模型的预期用例，并最大限度地减少它们在不太适合的上下文中的使用，我们建议在发布的模型中附上详细说明其性能特征的文档。在本文中，我们提出了一个我们称之为模型卡的框架，以鼓励这种透明的模型报告。模型卡是附带训练有素的机器学习模型的简短文档，可在各种条件下提供基准评估，例如跨不同的文化、人口或表型组（例如种族、地理位置、性别、与预期应用领域相关的菲茨帕特里克皮肤类型）和交叉组（例如，年龄和种族，或性别和菲茨帕特里克皮肤类型)。模型卡还披露了打算使用模型的背景、业绩评价程序的细节以及其他相关信息。虽然我们主要关注计算机视觉和自然语言处理应用领域中以人为本的机器学习模型，但这个框架可以用来记录任何训练有素的机器学习模型。为了巩固这一概念，我们为两个受监督的模型提供卡片：一个是检测图像中**笑脸**的培训，另一个是**检测**文本中有毒评论的培训。我们建议使用模型卡，作为实现机器学习和相关 ai 技术负责任民主化的一

个步骤，提高人工智能技术运作情况的透明度。我们希望这项工作鼓励那些发布训练有素的机器学习模型的人在模型发布的同时提供类似的详细评估数字和其他相关文档。少

2018 年 10 月 5 日提交;最初宣布 2018 年 10 月。

16. 外周生物鉴别技术研究综述

作者:fernando alonso-fernandez, josef bigun

摘要: 眼周是指眼睛附近的面部区域，包括眼睑、睫毛和眉毛。虽然人脸和虹膜已被广泛研究，眼周区域已成为一个有希望的特点，无约束生物识别，以下要求，提高**鲁棒性**的脸或虹膜系统。由于具有惊人的高识别能力，该区域可以很容易地获得现有的**面部**和虹膜设置，用户合作的要求可以放宽，从而促进与生物识别系统的互动。即使在虹膜纹理无法可靠获得（低分辨率）或部分面部遮挡（近距离）下，它也可以在很远的**距离**内使用。在这里，我们回顾了眼科周围生物计量学研究的最新技术。描述了若干方面，包括: (一）现有数据库, (二）眼周**检测**和分割算法, (三）用于识别的特征, (四）识别眼周地区最具鉴别力的区域(v）与虹膜和**面部**模式的比较，六）软生物鉴别技术（性别/族裔分类），以及七）性别转化和整形手术对识别准确性的影响。这项工作有望提供一个最相关的问题，在眼科周生物鉴别技术，提供一个全面的涵盖现有的文献和目前的艺术状况。少

2018 年 10 月 8 日提交;最初宣布 2018 年 10 月。

17. iritrack：使用 i 复活的活动检测，以防止人脸欺骗攻击

作者:孟申,廖泽林,朱丽黄,拉希德·密美米，杜晓江, 胡建坤

摘要: 人脸活动性**检测**已成为一种广泛使用的技术，在各种身份验证场景中，这种技术在抵御欺骗攻击方面的重要性日益增加。执行活动性**检测**的现有方法通常侧重于设计智能分类器或自定义硬件，以区分真正合法用户的图像或视频样本与模拟用户的图像或视频样本。虽然有效，但它们可以消耗资源,**检测**结果可能对环境变化非常敏感。本文将虹膜运动作为一种重要的活动性标志，提出了一种简单有效的活动性**检测**系统。用户需要移动他们的眼睛与随机生成的多线，然后使用虹膜的轨迹**作为证据,**以确定性检测。iritrack 允许通过使用在用户设备交互过程中收集的数据来检查活动。我们实现了一个原型，并进行了广泛的实验，以评估所提出的系统的性能。结果表明, iritrack 可以在中等和可调节的时间开销下抵御欺骗攻击。少

2018 年 10 月 8 日提交;最初宣布 2018 年 10 月。

18. 利用仿真识别人工智能中的偏差

作者:丹尼尔·麦克达夫,罗杰·程,阿什什·卡普尔

摘要: 机器学习模型表现出偏差，通常是因为用于训练它们的数据集是偏置的。这给这种技术的部署带来了严重的问题，因为由此产生的模式可能对培训范围内的少数群体人口表现不佳，并最终给他们带来更高的风险。我们建议使用高保真计算机模拟来询问和诊断 ml 分类器中的偏见。我们提出了一个框架，利用贝叶斯参数搜索有效地描述高维特征空间，并更快地识别性能弱点。我们将我们的方法应用于一个示例域，人脸**检测**，并表明它可用于帮助识别商业**面**应用编程接口 (api) 中的人口统计学偏差。少

2018 年 9 月 30 日提交;**最初宣布** 2018 年 10 月。

19. **科夫菲：一种估计力消耗的计算机视觉方法**

作者:vaneet Aggarwal, hamed asadi, mayank gupta, jae joong lee, denny yu

摘要: 累积暴露在重复和有力的活动可能会导致肌肉骨骼损伤，这不仅降低了工人的效率和生产力，而且影响了他们的生活质量。因此，广泛获取的技术，以可靠地**检测**不安全的肌肉力量消耗水平的人类活动是必要的，为他们的福祉。然而，测量使用力的水平是具有挑战性的，现有的技术提出了一个巨大的挑战，因为它们是侵入性的，干扰人机接口，或/或主观的性质，因此不是所有的工人的可扩展性。在这项工作中，我们使用**面部**视频和光镜像 (ppg) 信号来分类力量消耗水平为 0\%、50%% 和 100%\% (代表休息、适度的努力和高度的努力)，从而提供一种非侵入性和可

扩展的方法。研究了有效的特征提取方法，包括**不同平面**的运动的标准偏差、ppg 信号中峰值和低谷之间的距离。我们注意到，ppg 信号可以从**面部**视频中获得，从而为使用**面部**视频的力消耗水平提供了一个有效的分类算法。根据从 20 名受试者收集的数据，从**面部**视频中提取的特征在 100% 和 0\% 和 50\% 数据集的组合中的分类精度为 90%%。进一步组合 ppg 信号可提供 81.7 的精度。该方法还被证明对用户说话时正确识别的力级别是稳健的，即使此类数据集不包括在培训中。少

2018 年 9 月 24 日提交;**最初宣布** 2018 年 9 月。

20. eptrl：一种强化学习剂，促进吸血检测

作者:黄克新,罗德里格斯·诺盖拉

摘要: 认识论 (基因-基因相互作用) 是预测遗传疾病的关键。我们的工作通过将以前的工作在信差检测中**所面临**的计算挑战进行建模，将其建模为一个步骤的马尔可夫决策过程，状态是基因组数据，动作是相互作用的基因，奖励是所选操作的交互测量。然后，使用策略梯度法的强化学习代理学习发现一组高度相互作用的基因。少

2018 年 9 月 24 日提交;**最初宣布** 2018 年 9 月。

21. 自我自我：亲缘关系验证的自调整深模型

作者:elan dahan, yosi keller

文摘: 亲属鉴定是生物识别和**人脸**识别领域尚未解决的挑战之一。这个问题的目的是了解两个人是否与家庭有关，以及如何（姐妹、兄弟等)解决这个问题会产生不同的任务和应用。在国土安全领域(hls)，自动**检测**被讯问的人是否与通缉犯有关至关重要，在生物鉴别领域，亲属鉴定可以帮助通过照片区分家庭，并在预测或时尚，它可以帮助预测一个年龄较大或更年轻的模型的人的**脸**。最近，随着先进的深度学习技术，这一问题在数据和研究方面得到了研究界的关注。在本文中，我们建议使用深度学习方法来解决亲属验证问题。此外，我们还提供了一种新的自学深度模型，它从不同**的面孔**中学习基本特征。我们证明，我们的模型赢得了承认家庭在 Wild(RFIW2018,FG2018) 的挑战，并获得最先进的结果。此外，我们还表明，我们提出的模型可以在不损失性能的情况下将网络的大小减少一半。少

2018 年 9 月 22 日提交;**最初宣布** 2018 年 9 月。

22. 了解假面孔

作 者 :ryota natumo, kazukiinoue, yoshihiroHirokatsu, shintaro yamamoto, shigeo morishima, hirokatataoka

摘要: **人脸**识别研究是计算机视觉（cv）中最活跃的课题之一，深度神经网络（dnn）正在填补**人脸**验证算法中人脸水平和计算机

驱动的性能水平之间的差距。然而，尽管在基于准确性的期望方面，业绩差距似乎正在缩小，但出现了一个奇怪的问题;具体而言，"**面对**对人工智能的理解真的接近人类吗？"在本研究中，为了验证大脑驱动的概念，我们使用内部创建的假**脸**数据库进行基于图像的**检测**、分类和生成。该数据库有两种配置: (i) 使用紫百合琼斯 (vj) 方法和卷积神经网络 (cnn) 生成的假**阳性面部**检测,以及 (ii) 具有类似于**面**,但完全是人为的。结果显示了一定程度的暗示知识，表明最近基于视觉的**人脸**识别算法的能力与人的水平的性能之间仍然存在差距。然而，从积极的方面来看，我们已经获得了**能够推动面部**理解模型进步的知识。少

2018 年 9 月 22 日提交;**最初宣布** 2018 年 9 月。

23. 一种快速、准确的人脸检测、识别和验证系统

作者:rajeev ranjan, ankan bansal, jingxiaozheng, h 行 yuxu , joshua glason, boyu lu, anirudh nanduri, jun-cheng chen, carlos d. castillo, rama 切拉帕

摘要: 大型注释数据集的提供和负担得起的计算能力使 cnn 在各种物体**检测**和识别基准方面的性能有了令人印象深刻的改进。这些，再加上对深度学习方法的更好理解，也提高了机器对**人脸**理解的能力。cn 能够**检测人**脸，定位面部地标，估计姿势，并识别无约束图像和视频中的**人**脸。本文详细介绍了用于无约束**人脸**识别和验证的深度学习管道，该管道在多个基准数据集上实现了

最先进的性能。我们提出了一种新型**的人脸**检测器，深金字塔单面检测器（dpssd），它是快速和能够**检测**具有大规模变化的**人**脸(特别是微小**的脸)**。我们给出了自动**人脸**识别涉及的各个模块的设计细节:**人脸检测**、地标定位和对齐以及**人**脸识别/验证。我们提供了具有挑战性的**无约束人脸检测**数据集的人**脸**检测器的评价结果。然后，我们介绍了 iarpa janus 基准 a、b 和 c (ijb-a、jibb-b、ijb-c) 和 janus 挑战集 5 (cs5) 的实验结果。少

2018 年 9 月 20 日提交;**最初宣布** 2018 年 9 月。

24. 利用卷积神经网络研究不同隐藏层和时代手写数字识别精度变化的研究与观察

作者:rezoana bente arif, md. abu bakr siddique, mohammad mahmudur rahman khan, mahjabin rahman oishe

摘要: 如今，深度学习可以应用于医学、工程等多个领域。在深度学习中，卷积神经网络（cnn）广泛应用于模式和序列识别、视频分析、自然语言处理、垃圾邮件**检测**、主题分类、回归分析、语音识别、图像等领域。分类、目标**检测**、分割、**人脸**识别、机器人和控制。与其在大型应用中近乎人的水平准确相关的好处，导致近年来美国有线电视新闻网的接受程度越来越高。本文的主要贡献是分析美国有线电视新闻网隐藏层模式对网络整体性能的影响。为了证明这种影响，我们在修改后的国家标准与技术研究所(mnist) 数据集上应用了不同层次的神经网络。同时，观察不同数

量的隐藏层和时代的网络精度变化，并对它们进行比较和对比。利用随机梯度和反向传播算法对系统进行训练，并采用前馈算法进行测试。少

2018 年 9 月 22 日提交;**v1** 于 2018 年 9 月 17 日提交;**最初宣布** 2018 年 9 月。

25. 机器人机械手的经验排名--卷积神经网络的深度学习

作者:hai nguyen, hung manhla, matthew deans

摘要: 监督学习，更具体地说是卷积神经网络（cnn），在一些视觉识别任务中已经超过了人的能力，如**交通**标志、**面孔**和手写数字的检测。另一方面，即使是最先进的强化学习（rl）方法也很难在有稀疏和二元奖励的环境中使用。他们需要手动塑造奖励功能，这可能是一个挑战。然而，这些任务对人类来说是微不足道的。人类在这些任务中成为更好的学习者的原因之一是，我们被世界上很多先前的知识所嵌入。这些知识可能嵌入我们的基因中，也可能是从模仿中学到的--一种有监督的学习。因此，缩小机器和人类学习能力之间差距的最好办法应该是通过 rl 和监督学习相结合，模仿我们在各种任务中如何学习得如此出色。我们的方法将深度确定性政策梯度和后视体验重播（rl 方法专门处理稀疏奖励）与排名为美国有线电视新闻网的经验结合起来，在模拟机器人的学习曲线上提供了显著的加速任务。体验排名允许更频繁地重播

高回报转换，从而有助于更有效地学习。我们提出的方法还可以加快学习任何其他任务，为经验排名提供额外的信息。少

2018 年 9 月 16 日提交;最初宣布 2018 年 9 月。

26. 边界平衡 gan 在无约束面近似边缘化监测中的应用研究

作者:wazeer zulfikar, seadtin santy , sahith dambekodi, tirtharaj dash

文摘: **面**前化是在其角度的姿态下，合成人 **脸正面**视图的过程。我们实现了一个具有球面线性插值 (slerp) 的生成对抗网络 (gan)，用于无约束面部图像的正面化。我们的特别关注是为了生成从监控摄像头拍摄到的侧面图像的近似正面**面**。具体而言，本工作是对基于自动编码器**的**边界均衡 gan (begin) 的实现进行综合研究，该方法利用侧视面及其镜像视图的插值来生成正面。为了提高插值输出的质量，我们用 slerp 实现了一个 began。这种方法可以产生一个有希望的输出，以及更快和更稳定的模型培训。began 模型还具有平衡的发电机鉴别器组合，它可以防止模式崩溃以及全局收敛性。预计这种近似**的人脸**生成模型将能够取代用于监视和犯罪**侦查**的人脸复合材料。少

2018 年 9 月 14 日提交;最初宣布 2018 年 9 月。

27. 面部分析的实时系统

作 者 :janne tommola, pedram ghazi, biswo adhikari , heikki hhtunen

文摘: 本文描述了实时面部分析系统的解剖结构。该系统识别年龄, 性别和面部表情从用户出现在镜头前。所有组件都是基于卷积神经网络的, 我们研究了卷积神经网络在常用训练和评价集上的准确性。这项工作的一个关键贡献是描述了帧抓取、**人脸检测**和三种类型识别的处理线程之间的相互作用。执行该系统的巨蟒代码使用普通的库--kerasensorlox、opencv 和 dlib--and 可供下载。少

2018 年 9 月 14 日提交;最初宣布 2018 年 9 月。

28. 一种从不同领域检测面上地标的两步学习方法

作者:brana vieira frade, erickson r. nascimento

文摘: 对 在机器学习领域, 特别是在卷积网络中, 对**面**上基准点的**检测**具有重要的优势。然而, 大多数探测器的准确性在很大程度上取决于大量的注释数据。在这项工作中, 我们提出了一个领域适应方法的基础上两步学习, 以**检测**对人和动物**的**脸的基准点。我们评估我们的方法在三个不同的数据集组成不同的动物**面孔** (猫, 狗和马)。实验表明, 该方法比现有方法有较好的性能, 可以利用很少的注释数据来利用地标的**检测**, 减少对大量注释数据的需求。少

2018 年 9 月 12 日提交;**最初宣布** 2018 年 9 月。

29. **贝斯-托姆普：一种针对复杂对手的快速检测和最佳响应算法**

作者:杨天培,孟兆鹏,郝建业，张崇杰，郑燕

摘要: 多智能体算法的目的往往是准确预测其他代理的行为，并在相应的交互过程中找到最佳的反应。以前的作品通常假设对手使用固定策略或随机切换之间的几个固定的。然而，在实践中，对手可能会表现出更复杂的行为，通过采取更先进的策略，例如，使用贝叶斯推理策略。本文提出了一种新的算法--bayes-tomop，该算法可以使用平稳或更高级的推理策略**有效地检测**和处理对手。bayes-tomop 还支持**检测**以前看不见的政策，并相应地学习最佳应对策略。采用 drl 技术扩展贝-托莫普，提出了深贝-托莫普。实验结果表明，在双代理竞争游戏中，贝斯-托莫普和深贝斯- 托莫普在面对不同类型的对手时，表现均优于最先进的方法。少

2018 年 9 月 13 日提交;**v1** 于 2018 年 9 月 11 日提交;**最初宣布** 2018 年 9 月。

30. **诠释阴影、亮点和面孔："人在循环中" 对数字艺术史的贡献**

作者:maarten w. a. wijntjes

摘要: 虽然自动计算技术似乎揭示了数字艺术史上的新见解，但一种互补的方法似乎得到的关注较少：人类的诠释。我们认为并

举例说明，一个 ' 人在循环中 ' 可以揭示洞察，可能很难自动检测. 具体而言，我们专注于绘画艺术中的感性方面。使用相当简单的注释任务 (例如，划定人类长度、指示高光和对凝视方向进行分类)，我们既可以复制早期的发现，又可以揭示对图形惯例的新见解。我们发现，卡纳莱托用相当准确的视角描述了人物形象，在大约 3 米和 9 米之间的不同视点高程，以及与投影平面平行的高度首选的光方向。此外，我们发现，取左脸看脸的平均图像显示了一个女人，而对于右脸显示的**是**男性，证实了早期关于绘画艺术中横向性别偏见的说法。最后，我们确认并完善了众所周知的左灯偏差。注释、分析和结果共同体现了人类的注解如何为技术和数字艺术史做出贡献和补充。少

2018 年 9 月 10 日提交;**最初宣布** 2018 年 9 月。

31. 基于 cn 的人脸和头部检测器在实时视频监控应用中的比较

作 者 :le thanh nguyen-meidine, eric granger, madhu kiran, louis-antoine bl4is-morin

摘要: **检测**由于外观、遮挡和复杂背景的变化，视频源中出现的**面孔**和头部在实际视频监控应用中具有挑战性。最近，一些 cnn 架构被提出来提高探测器的准确性，尽管它们的计算复杂性可能是个问题，特别是在必须现场**检测**人脸和头部的实时应用中使用高分辨率摄像机。本文比较了适用于**人**脸和头部**检测**的最先进的 cnn 架构的准确性和复杂性。根据准确性以及来自多个具有挑战

性的数据集的图像的时间和内存复杂性，对单通道和基于区域的体系结构进行了经验审查和比较，并将其与基线技术进行了比较。考虑到实时视频监控应用，分析了这些架构的可行性。结果表明，尽管与传统探测器相比，cnn 架构可以实现非常高的精度水平，但它们的计算成本在许多实际实时应用中可能存在局限性。少

2018 年 9 月 10 日提交;最初宣布 2018 年 9 月。

32. 一种在野外进行实时伪装人脸识别的监督学习方法

作 者 :saumya Saumya, abhinandan dogra, abrar majeedi, hanan gani, ravi m. Vishwanath, s n omkar

摘要: 面部识别一直是计算机视觉科学家和专家面临的挑战任务。尽管由于相机参数、照明和**面部**方向的变化而产生的复杂性，但在这一领域取得了重大进展，深度学习算法现在与人级精度竞争。但与**最近**人脸识别技术的进步不同的是，伪装的面部识别在计算机视觉领域仍然是一个更严峻的挑战。现代的情况是，安全是最令人关注的问题，当**面孔**被伪装时，定期**的人脸**识别技术并不能按要求发挥作用，这就需要采取不同的方法来处理入侵者的情况他们的**脸**蒙面。同样，我们提出了一个深层学习架构的伪装面部识别 (dfr)。本文提出的算法利用单层卷积神经网络 (cnn) 对第一阶段的 20 个面部关键点进行**检测**。这些面部键点后来被支持向量机 (svm) 用于根据欧几里得距离比和不同面键点之间的角度对伪装**的人脸**进行分类。这种整体架构为我们的系统提供了基本的

智能。我们的关键点特征预测精度为 65%，分类率为 72.4。此外，该架构的工作原理为 19 fps，因此几乎是实时的。我们的方法的效率也与最先进的伪装面部识别方法进行了比较。少

2018 年 9 月 8 日提交;**最初宣布** 2018 年 9 月。

33. 高性能人脸检测的选择性细化网络

作者:程志,张世峰，邢俊良,郑磊,斯坦·李·李斯坦,邹旭东

摘要: 高性能**人脸检测**仍然是一个非常具有挑战性的问题，尤其是在存在许多微小**的人脸**时。本文提出了一种新型的单发**人脸**检测器，名为选择性细化网络 (srn)，它将新的两步分类和回归操作选择性地引入到基于锚杆**的人脸**检测器中，以减少错误积极，同时提高定位精度。特别是, srn 由两个模块组成: 选择性两步分类 (stc) 模块和选择性两步回归 (str) 模块。stc 的目标是从低层**检测层中**过滤掉最简单的负锚点，以减少后续分类器的搜索空间，而 str 的设计则是为了从较高的级别**粗化地调整锚杆的位置和大小检测**层，以便为后续回归器提供更好的初始化。此外，我们还设计了一个接收场增强 (rfe) 块，以提供更多样化的接受场，这有助于更好地捕捉**面孔**在一些极端的姿势。因此，拟议的 srn 检测器在所有广泛使用的**人脸检测**基准 (包括 afw、pascal 人脸、fddb 和 wider **face** **数据**集) 上实现了最先进的性能。我们会发出守则，以进一步研究人**脸发现**问题。少

2018 年 9 月 7 日提交;最初宣布 2018 年 9 月。

34. idsgan: 用于针对入侵检测的攻击生成的生成对抗网络

作者:林子龙,石勇,薛志岳

摘要: 入侵**检测**系统作为一种重要的安全工具，对恶意交通实施的网络攻击负有防御责任。目前，在机器学习算法的帮助下，入侵**检测**系统发展迅速。然而，当它**面临**对抗攻击时，这一制度的稳健性值得怀疑。为了改进**检测**系统，应研究更多的潜在攻击方法。本文提出了一个生成对抗网络的框架 idsan，以产生对抗攻击，从而欺骗和规避入侵**检测**系统。考虑到攻击者不知道**检测**系统的内部结构，对抗攻击示例对**检测**系统执行黑盒攻击。idsan 利用生成器将原始恶意流量转换为敌对恶意流量。鉴别器对交通示例进行分类，并模拟黑匣子**检测**系统。更重要的是，我们只修改了部分攻击的非功能性功能，以保证入侵的有效性。在数据集 nsl-kdd 的基础上，证明了该模型攻击多攻击不同攻击系统的可行性，取得了较好的效果。此外，通过改变未修改特征的数量，验证了 idsgan 的鲁棒性。少

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

35. 使用图像和文本对嘈杂数据进行命名实体识别 (1 页摘要)

作者:迭戈·埃斯特维斯

摘要: 命名实体识别（ner）是信息提取的一个重要子任务，旨在定位和识别命名实体。尽管最近取得了成就，但我们在正确**检测**和分类实体方面仍然**面临**限制，在推特等短文和嘈杂文本中尤为突出。在大多数 ner 方法中，一个重要的负面方面是高度依赖手工制作的功能和特定领域的知识，这是实现最先进的结果所必需的。因此，设计处理这种语言复杂情况的模型仍然具有挑战性。在本文中，我们提出了一个新的多层次的架构，不依赖于任何特定的语言资源或编码规则。与传统方法不同，我们使用从图像和文本中提取的要素对命名实体进行分类。在瑞特数据集上对推特最先进的净入学率进行的实验测试显示了竞争结果（0.59 f-计量），表明这种方法可能导致更好的净入学率模型。少

2018 年 9 月 3 日提交;**最初宣布** 2018 年 9 月。

36. 利用逆透视映射开发基于纯视觉的障碍物检测

作者:julian nubert, niklas funk, fabio meeer, fabrice oehler

摘要: 我们的解决方案是在达基伊镇的框架内实现的。大基镇的目标是提供一个相对简单的平台，探索、解决和解决与自主驾驶有关的许多问题。"duckietown" 在基础上很简单，但环境无限可扩展。从控制单一驾驶的 duckiebots 到完整的车队管理，每一种情况都是可能的，都可以付诸实施。到目前为止，现有的模块都无法

可靠地**检测**障碍并实时对其做出反应。我们**面临着**一个普遍的问题，检测障碍的图像从一个单目 rgb 相机安装在我们的 duckiebot 的前面，并对它们作出正确的反应，而不会崩溃或错误地停止 duckiebot。无论是检测还是反应都必须实现，必须在树莓派上实时运行。由于硬件的强大限制，我们决定不对障碍物**检测**部分使用任何学习算法。正如后来所发现的，一个工作的 "硬编码" 软件需要对给定的问题进行彻底的分析和理解。用外行人的话说，我们只是想让达基伊镇成为一个更安全的地方。少

2018 年 9 月 4 日提交;**最初宣布** 2018 年 9 月。

37. 中网络：一种紧凑型面部视频伪造检测网络

作 者 :darius afchar, vincent nozick, junichi yamagishi, isao echizen

文摘: 本文提出了一种自动检测视频中的**人脸**篡改的方法，重点介绍了用于生成超逼真的伪造视频的两种最新技术: deep 机假和 face2face。传统的图像取证技术通常不太适合视频，因为压缩会使数据严重退化。因此，本文采用了深度学习的方法，提出了两个网络，这两个网络的层数都很低，可以聚焦于图像的介观特性。我们评估现有数据集上的快速网络和我们从在线视频构建的数据集。测试证明了一个非常成功的**检测**率，超过 98% 的深度假和 95% 的脸 2 脸。少

2018 年 9 月 4 日提交;最初宣布 2018 年 9 月。

38. 基于网络语言的网络网络数据异常检测

作 者 :bartley d. richardson , benjamin j.radford, shawn e.davis, keegan hines, david pekarek

摘要: 随着网络数据量的不断增加，网络维护者**面临着**越来越多的数据，他们必须分析，以确保其网络的安全。此外，在全球范围内不断制造和执行新型攻击。当前基于规则的方法可以有效地描述和标记已知的攻击，但当出现新的攻击或新类型的数据时，这些方法通常会失败。相比之下，无监督机器学习通过不需要标记的数据来从大量网络流量中学习，提供了明显的优势。本文提出了一种应用于网络异常**检测**的基于语言的自然语言技术（后缀树)。我们说明了一种利用网络数据特征生成语言的方法，我们的实验结果说明了将该技术应用于流型数据的积极初步结果。作为这项工作的一个基本假设，我们声称恶意网络行为者在执行攻击时在数据中留下可观察到的内容。这项工作旨在识别这些文物，并利用它们来识别广泛的网络攻击，而不需要标记的地面真相数据。少

2018 年 8 月 15 日提交;最初宣布 2018 年 8 月。

39. 采矿（最大值）西班牙岩心从世俗网络

作 者 :edardo galimberti, alain barrat, francesco bonchi, ciro cattuto, francesco gullo

摘要: 在分析临时网络时，一项基本任务是识别密集的结构（即显示大量链接的顶点组）及其时间跨度（即高密度保持的时间段)。我们通过引入一个时间核心分解的概念来解决这个任务，其中每个核心都与其跨度相关：我们称之为这样的核心跨度核心。由于时间间隔的总数是时间域大小的二次值 t 在分析中，西班牙岩心的总数是二次的。|t|也是如此。我们的第一个贡献是一种算法，通过利用跨核之间的包容特性，有效地计算所有的跨领域核心。然后，我们重点研究的问题是只寻找最大的跨度核心，即不被任何其他分芯所支配的西班牙核心，同时由核心属性和跨度。我们设计了一种非常有效的算法，该算法利用关于最大值条件的理论发现，直接计算最大值，而无需计算所有的西班牙核心。在几个真实的时间网络上进行的实验证实了我们方法的效率和可扩展性。通过记录学校中面对面互动的近**端**传感基础设施收集的时间网络上的应用，突出了（最大）端核概念在分析社会动态和**检测**/纠正数据中的异常。少

2018 年 8 月 28 日提交;**最初宣布** 2018 年 8 月。

40.用于准确的人脸欺骗检测的判别表示组合

作者:肖松,徐照,方良基,林天伟

文摘 本文介绍了**人**脸攻击**检测的**三种判别表示。首先，我们设计了一个描述符称为空间金字塔编码微纹理（spmt）特征来表征局部外观信息。其次，我们利用 ssd，这是一个深入的学习框架，以检测，挖掘上下文提示，并进行端到端**的人脸**呈现攻击检测。最后，我们设计了一个描述符**称为模板面**匹配双目深度（tfbd）功能来描述真实和假**面**的立体结构。为了准确地检测演示攻击，我们还设计了两种表示组合。首先，我们提出了一个决策级级级策略，结合 spmt 与 ssd。其次，我们使用一个简单的分数融合策略，将人脸结构线索（tfbd）与局部微纹理特征（spmt）结合起来。为了展示我们设计的有效性，我们评估了 spmt 和 ssd 在三个公共数据集上的表示组合，它优于所有其他最先进的方法。此外，我们还评估了 spmt 和 tfbd 在数据集中的表示组合，并取得了优异的性能。少

2018 年 8 月 27 日提交;**v1** 于 2018 年 8 月 27 日提交;**最初宣布** 2018 年 8 月。

41. 大家现在跳舞

作者:陈嘉玲, shiry ginosar, tinghuizhou,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。

42. 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。

43. 在软件定义的网络中缓解洪水和慢 ddos 攻击

作者:thomas lukaseder, shreya ghosh,frank kargl

摘要: 分布式拒绝服务 (ddos) 攻击是 internet 中服务的持续威胁。今年，观测到的最大 ddos 攻击记录定为 1.7 tbps。同时，背后仍然缺乏**发现**和缓解机制。许多缓解系统需要受害者的援助---或者受害者的管理人本身必须积极活动，以减轻攻击。我们引入了一个系统，可以**检测**攻击、识别攻击者，并完全在网络基础结构内缓解攻击。随着软件定义网络灵活性的提高，可以实现缓解此类攻击的新可能性。除了我们关于减少对 2018 年 lcn 的反射性 ddos 攻击的简短论文外，我们还想展示我们在 2017 年 lcn 上介绍的减少洪水攻击的工作，以及我们在缓解缓慢的 ddos 攻击方面所做的工作。在我们的演示中，我们展示了如何组合这些系统，以及它们在**面对**如此不同的攻击时是如何工作的。少

2018 年 8 月 16 日提交;最初宣布 2018 年 8 月。

44. 面对面: 手术室中的匿名视频

作者:evangello flouty, oddseal zisimopoulos , danail stoyanov

摘要: 手术手术室 (or) 中的视频采集越来越有可能，并有可能用于计算机辅助干预 (cai)、外科数据科学和智能 or 集成。捕获的视频天生携带敏感信息，为了保持患者和临床团队的身份，这些信息不应该完全可见。当手术视频流存储在服务器上时，如果在医院外拍摄，则必须在存储前匿名播放视频。在本文中，我们描述了如何将深度学习模型 "更快的 r-cnn" 用于此目的，并帮助匿名处理在 or 中捕获的视频数据。该模型**检测**并模糊**面**，以保持匿名性。在测试了现有**的人脸检测**训练模型后，收集了一个适合手术环境的新数据集,**其面部**被外科口罩和帽子挡住，以便进行微调，从而实现更高的**面部-**在 or 中的**检测**率。我们还提出了一个时间正则化内核，以提高召回率。该模型在应用时间平滑前后分别实现了 8.05% 和 93.45 的**人脸检测**召回率。少

2018 年 8 月 6 日提交;**最初宣布** 2018 年 8 月。

45. 从视频中进行无监督的硬例挖掘，以改进对象检测

作 者 :souyoung jin, aruni roychowdhury, huiizu jiang, ashish singh, aditya prasad, 深 chakraborty, erik d-miller

摘要: 最近在物体**检测**方面取得了重要进展，利用了侧重于 {\em 硬阴性} 实例的培训目标，即目前被探测器评为正数或不明确的阴性例子。当训练网络对参数进行更正时，这些示例会对参数产生重大影响。不幸的是，它们在训练数据中往往很少，获取成本很

高。在这项工作中，我们通过分析视频序列上训练探测器的输出，展示了如何自动获得大量的硬底片 {\ em}。特别是，在时间上隔离的**检测** { \em}，即没有关联的前面或后面的**检测**，很可能是硬底片。我们描述了从未标记的视频数据中挖掘大量此类硬底片(以及硬 {\ em 阳性}) 的简单过程。我们的实验表明，对这些自动获得的示例进行再培训检测器通常可以显著提高性能。我们在多个体系结构和多个数据集上进行了实验，包括**人脸检测**、行人**检测**和其他对象类别。少

2018 年 8 月 13 日提交;**最初宣布** 2018 年 8 月。

46. dfternet：面向 2 位动态融合网络实现精确的人类活动识别

作者:詹扬,奥索洛·伊恩·雷蒙德,张承远,万英,龙军

文摘 深卷神经网络 (dcnn) 目前在人类活动识别应用中很受欢迎。然而,**面对**现代人工智能传感器游戏，许多研究成果无法在便携式设备上得到实际应用。dnn 通常占用大量资源，太大，无法部署在便携式设备上，因此这限制了复杂活动**检测**的实际应用。此外，由于便携式设备不具备高性能图形处理单元 (gpu)，因此在操作游戏 (act) 体验中几乎没有任何改进。此外，为了处理多传感器协作，以往所有的人类活动识别模型通常都平等地对待来自不同传感器信号源的表示。然而，不同类型的活动应采取不同的融合策略。本文提出了一种新的方案。该方案用于训练具有权

重和激活约束为 {-0.5、0、0.5} 的 2 位卷积神经网络。它考虑了不同传感器信号源与活动类型之间的相关性。这个模型，我们称之为 dfternet，旨在产生一个更可靠的推理和更好的权衡实际应用。我们的基本思想是利用在预先训练的滤波器组中直接量化权重和激活，并针对不同的活动类型采用动态融合策略。实验表明，在活动识别 (如 opop 示 ity 和 pamap2 数据集) 上，采用动态融合策略可以超过基准模型性能约 5%。利用所提出的量化方法，我们能够实现更接近全精度对应的性能。这些结果也通过 unimib-shar 数据集进行了验证。此外，该方法还能在 cpu 上实现 ~ 9x 的加速和 10 倍的内存节省。少

2018 年 9 月 29 日提交;**v1** 于 2018 年 7 月 30 日提交;**最初宣布** 2018 年 8 月。

47. 大规模词汇分类中的错误检测

作者:刘思凡,王洪志

摘要: 知识库 (kb) 是人工智能的一个重要方面。kb 构造**面临的**一个重大挑战是它包含许多噪声，这妨碍了它的有效使用。尽管提出了一些 kb 清理算法，但它们侧重于知识图的结构，而忽略了概念之间的关系，这可能有助于发现 kb 中的错误关系。在此过程中，我们通过两个概念的对应实例之间的距离来度量两个概念之间的关系，并**检测**冲突概念集交集内的错误。为了高效和有

效地清理知识库，我们首先应用基于距离的模型来确定使用两种不同方法的冲突概念集。然后，我们提出并分析了几种算法如何检测和修复的误差,基于我们的模型，我们使用哈希方法来计算距离的有效方法。实验结果表明，该方法能够有效地清理知识库。少

2018 年 8 月 5 日提交;**最初宣布** 2018 年 8 月。

48. 用于人脸对齐的深度多中心学习

作者:邵志文,朱恒良，新潭，阳阳豪,马丽庄

摘要: 面部地标彼此高度相关，因为某个地标可以通过其邻近的地标来估计。大多数现有的深度学习方法只使用一个称为形状预测层的完全连接层来估计面部地标的位置。本文提出了一种新的多中心学习框架–多形状预测层的人**脸对齐**深度学习框架。特别是，每个形状预测层都强调分别**检测**到一定的语义相关地标群。首先重点突出具有挑战性的地标，并分别对每个地标群进行进一步优化。此外，为了降低模型的复杂度，我们提出了一种模型组合方法，将多个形状预测层集成到一个形状预测层中。大量实验表明，该方法能够有效地处理具有实时性能的复杂遮挡和外观变化。我们方法的代码可在 https://github.com/ZhiwenShao/MCNet-Extension。少

2018 年 8 月 5 日提交;**最初宣布** 2018 年 8 月。

49. 用于无线物联网入侵检测的主动学习

作者:杨凯,任杰,朱燕桥，张伟义

摘要: 物联网 (iot) 在我们的日常生活中变得非常普遍，但它也**面临着独特的**安全挑战。入侵**检测**对于无线物联网网络的安全性和安全性至关重要。本文讨论了无线入侵**检测**中的人与环主动学习方法。我们首先提出了针对成功的无线物联网**网络入侵检测**系统 (ids) 的设计所面临的根本挑战。然后，我们简要回顾了主动学习的基本概念，并提出了它在无线入侵**检测**的各种应用中的应用。并通过实验实例说明了主动学习方法比传统监督学习方法有显著的性能改进。虽然机器学习技术在入侵**检测中**得到了广泛的应用，但利用机器和人的智能进行物联网入侵检测的人在式学习**中**的应用仍在其婴儿。希望本文能帮助读者理解主动学习的关键概念，促进这一领域的进一步研究。少

2018 年 8 月 3 日提交;**最初宣布** 2018 年 8 月。

50. 主动学习对 android 重新打包恶意软件的激励与检测

作者:aleldin salem

摘要: 重新打包是一种技术，已越来越多地被 android 恶意软件的作者所采用。研究界在设计检测这类恶意软件的技术方面**所面临的**主要问题是缺乏在良性应用中嫁接的恶意片段的基础事实。

如果没有这些关键知识，就很难培训能够有效地对新颖的、不打包的恶意软件进行分类的可靠分类器。为了避免此问题，我们认为，如果允许可靠的分类器请求对应用行为进行新的、更准确的表示，则可以对其**进行检测**重新打包的恶意软件。这种学习技巧被称为主动学习。在本文中，我们提出了使用主动学习来培训分类器能够应对重新打包的恶意软件的模糊性质。我们实现了一个架构, aion，连接的过程，刺激和**检测**重新包装的恶意软件使用反馈循环描绘主动学习。我们使用两个恶意软件数据集（mal 基因组和 Piggybacking）对 aion 的示例实施进行的评估表明，主动学习可以优于传统**的检测**技术，因此具有很大的检测 android 的潜力重新打包的恶意软件。少

2018 年 8 月 3 日提交;**最初宣布** 2018 年 8 月。

51. 你在排队吗？人群中基于 rssi 的队列检测

作者:吴方静, gürkan solmaz

摘要: 人群行为分析的重点是群体的行为特征，而不是个人的活动。这项工作考虑了人类排队的行为，这是群体的一种特定的人群行为。我们设计了一种即插即用系统解决队列**检测**问题的基础上，基于 wi-fi 蓝牙低功耗（ble）接收信号强度指示器（rssi）捕获的多个信号嗅探器。这项工作的目标是确定设备是否仅基于 rssi 在队列中。其关键的想法是不仅从单个设备的数据中提取特

征，而且从多个设备的数据与多个嗅探器观察到的移动相关性之间的移动性相似性。因此，我们提出了单设备特征提取、跨设备特征提取和交叉嗅探特征提取的模型训练和分类。系统地进行了模拟队列运动实验，研究了**检测**精度。最后，我们将我们基于信号的方法与现实世界中的社交活动中基于签名的人脸检测方法与真实的人**的队列进行**了比较。实验结果表明，该方法的精度最低为77%，其性能明显优于基于相机的**人脸检测**，因为人们互相遮挡可见性，而无线信号可以是**检测到**而不阻塞。少

2018 年 8 月 2 日提交;**最初宣布** 2018 年 8 月。

52. 腹腔镜手术的实时成像仪器分类

作者:sebastian bodenstedt, 安东妮亚·奥内穆斯, darko katic, anna-laura wekerle, martin wagner, hannes kenngot, bat müller-schtic, rüdiger dirmann, 斯特凡妮·斯派伊德尔

摘要: 在腹腔镜手术中，上下文感知辅助系统旨在缓解外科医生**面临**的一些困难。为确保在正确的时间提供正确的信息，必须了解干预的现阶段。目前使用的手术工具的实时定位和分类是基于活动的相位识别和辅助生成的关键组成部分。在本文中，我们提出了一种基于图像的方法，在腹腔镜干预过程中**实时检测**和分类工具。首先，使用像素级随机林分割检测潜在的仪器边界框。然后使用随机林的级联对这些边界框中的每一个进行分类。为此，从每个**检测到**的边界框中提取多个特征，如色调和饱和度上的直

方图、渐变和 surf 特征。我们从两种不同类型的程序中评估了我们的方法。我们区分了四种最常见的乐器 (LigaSure、无障碍的草，吸气器，夹子苹果) 和背景。我们的方法成功地找到了高达 86% 的所有仪器分别。在手动提供的边界盒上，我们实现了高达 58% 的仪器类型识别率，在自动检测到的边界盒上实现了高达 49% 的仪器类型识别率。据我们所知，这是第一个允许在腹腔镜设置中实时对手术工具进行基于图像的分类的方法。少

2018 年 8 月 1 日提交;**最初宣布** 2018 年 8 月。

53. 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, lililin

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。

54. 改进 3c：数据清理与货币的一致性和完整性

作者:丁晓欧·丁洪志、 王洪志、苏嘉轩、李建忠、高红

摘要: 数据质量在当今的大数据管理中发挥着关键作用。随着各种来源数据的爆炸式增长，数据质量**面临多重**问题。在此基础上，本文从完整性、一致性和通用性等方面研究了多数据质量的提高。对于建议的问题，我们引入了一个名为改进 3c 的 4 步框架，用于在没有时间戳的情况下**检测**和改进不完整和不一致数据的质量。我们计算并实现了给定货币约束产生的记录之间的相对货币顺序，根据该顺序，考虑到时间影响，可以有效地修复不一致和不完整的数据。出于有效性和效率的考虑，我们在修复不完整之前进行

不一致的修复。定义了与电流相关的一致性距离，以更准确地测量脏记录与干净记录之间的相似性。此外，货币订单被视为不完整修复培训过程中的一个重要特征。通过实例详细介绍了求解算法。对一个真实的数据和一个合成的数据进行了深入的实验，验证了该方法能够提高脏数据清理的性能，而这些问题是现有方法难以有效清理的。少

2018 年 7 月 31 日提交;最初宣布 2018 年 8 月。

55. 检测和汇总不断发展的移动应用中的 gui 更改

作者:kevin moran, cody watson, john hoskins, george purnell , denys poshyvanyk

摘要: 近年来，移动应用程序已成为一个流行的软件开发领域，部分原因是用户群庞大、硬件功能强大和可访问平台。但是，移动开发人员也**面临着**独特的挑战，包括频繁发布的压力，以跟上快速平台演进、硬件迭代和用户反馈的步伐。由于这种快速的发展速度，开发人员需要自动支持来记录对其应用所做的更改，以帮助程序理解。移动应用中对文档的更改中，最具挑战性的类型之一是由于其抽象的、基于像素的表示形式而对图形用户界面 (gui) 所做的更改。在本文中，我们提出了一种完全自动化的方法，称为 gcat，用于**检测**和总结移动应用程序演变过程中的 gui 变化。gcat 利用计算机视觉技术和自然语言生成，准确、简洁地总结了在连续提交或发布之间对移动应用的 gui 所做的更改。与开

发人员指定的更改相比，我们根据检测 gui 更改的精度和召回程度来**评估**我们的方法的性能，并在受控用户研究中调查生成的更改报告的效用。我们的结果表明，gcat 能够准确**地检测**和分类 gui 更改----优于开发人员----同时提供有用的文档。少

2018 年 9 月 4 日提交;**v1** 于 2018 年 7 月 25 日提交;**最初宣布** 2018 年 7 月。

56. 转移学习为行动单位认可

作者:yen khyelim, zukang liao, stavros petridis, maja pantic

摘要: 本文提出了一种基于转移学习模型的面部表情识别分类器集成。对利用特征提取和微调卷积神经网络(cnn) 进行面部动作单元检测的主要实验工作。对提取的 cnn 码的线性判别分析(lda)、支持向量机 (svm) 和长期短期存储器 (lstm) 等多个分类器进行了比较和评价。多模型组合也被用来进一步提高性能。我们发现，vgg-face 和 resnet 是使用特征提取和 vgg-net 变体和 resnet 集成的操作单元识别的相对最优的预训练模型。少

2018 年 7 月 19 日提交;**最初宣布** 2018 年 7 月。

57. 安全运营中心的声纳: 安全从业人员是怎么想的?

作者:louise m.acon , bushra alahmadi, jason r.c . 护士, michael goldsmith, sadie creese

摘要: 在安全操作中心 (soc) 中，安全从业人员使用一系列工具来**检测**和减少恶意计算机网络活动。在这种情况下，数据被表示为声音的声音被认为是解决 soc **所面临**的一些独特挑战的一种方法的潜力。例如，声纳化已被证明可以对过程进行外围监测，这可以帮助在繁忙的 soc 中进行多任务处理。然而，安全从业人员将声纳技术纳入其实际工作环境的观点尚未得到审查。因此，本文的目的是通过探索在 soc 中使用声纳的态度来解决这一差距。我们报告了一项研究的结果，该研究包括在线调查 (nncs20) 和采访在一系列不同 soc 中工作的安全从业人员。我们的贡献是对超声化在 soc 工作实践中可能有助于帮助的背景的深入了解，以及对超声化可能没有好处甚至可能有问题的领域的理解。我们还分析了声纳系统设计的关键要求及其与 soc 设置的集成。我们的研究结果澄清了引入声纳技术以支持在这一重要的安全监控环境中开展工作的潜在好处和挑战的见解。少

2018 年 7 月 17 日提交;**最初宣布** 2018 年 7 月。

58. 从 resnet50 提取的特征和深林的分类分析

作者:suhita ray

文摘: 在本报告中，我们提出了皮肤病变图像的分类技术，作为我们提交 isic 2018 年挑战的一部分，在皮肤病变分析黑色素瘤检测。我们的数据来自 isic 2018: 黑色素瘤**检测**的皮肤病变分析

大挑战数据集。这些特征是通过一个卷积神经网络提取的，在我们的案例中 resnet50，然后利用这些特征，我们训练一个深林，有级联层，对我们的皮肤病变图像进行分类。我们知道，卷积神经网络是图像表示学习的最先进的技术，卷积滤波器通过反向传播从图像**中学习**特征。然后，这些特征通常会被输入到分类器中，如 softmax 图层或其他此类分类器，用于分类任务。在我们的例子中，我们不使用传统的反向传播方法，并训练一个软最大层进行分类。相反，我们使用深林，这是一种新的决策树集成方法，其性能在广泛的任务中具有很强的竞争力。因此，我们使用 resnet50 从皮肤病变图像中提取特征，然后使用深林对这些图像进行分类。之所以使用这种方法，是因为在只有小规模培训数据的地区，深林被发现效率非常高。而且，由于深林网络本身决定其复杂性，它也迎合了我们在这个问题上**所面临**的数据集不平衡问题。少

2018 年 7 月 25 日提交;**v1** 于 2018 年 7 月 16 日提交;**最初宣布** 2018 年 7 月。

59. 深度学习中的目标检测：综述

作者:赵忠秋,郑鹏,徐守涛,吴新东

文摘: 由于目标检测与视频分析和图像理解**的**密切关系，近年来引起了广泛的研究。传统的对象**检测**方法建立在手工制作的特征和可扩展的浅层体系结构之上。通过构造复杂的组合，将多个低

级图像特征与对象探测器和场景分类器的高级上下文结合起来，它们的性能很容易停滞。随着深度学习的快速发展，引入了更强大的工具来解决传统体系结构中存在的问题，这些工具能够学习语义、高层次、更深层次的功能。这些模型在网络体系结构、训练策略和优化功能等方面的行为不同。本文对基于深度学习的目标**检测**框架进行了综述。我们的回顾首先简要介绍了深度学习的历史及其代表性工具，即卷积神经网络（cnn）。然后，我们重点介绍了典型的通用对象**检测**体系结构以及一些修改和有用的技巧，以进一步提高**检测**性能。由于不同的特定**检测**任务表现出不同的特征，我们还简要介绍了几个具体的任务，包括突出的目标**检测**、**人脸检测**和行人**检测**.并进行了实验分析，比较了各种方法，得出了一些有意义的结论。最后，提出了几个有希望的方向和任务，作为今后对象**检测**和相关神经网络学习系统工作的指导。少

2018 年 7 月 15 日提交;最初宣布 2018 年 7 月。

60. 面部地标的实时形状跟踪

作者:kim hyungjoon, hyeonwookim, eenjun hwang

摘要: **在**实时虚拟化妆应用程序中，检测面部地标和准确跟踪其形状是必不可少的，用户可以通过向不同方向移动面部来查看化妆效果。典型**的面部**跟踪技术**可检测**不同的面部地标，并使用点跟踪器（如 kanade-lucas-tomaasi）点跟踪器对其进行跟踪。通

常, 5 或 64 点用于跟踪人脸。尽管这些点足以跟踪面部地标的大致位置，但还不足以跟踪面部地标的确切形状。本文结合深度学习技术和点跟踪器，提出了一种能够实时跟踪面部地标精确形状的方法。我们使用 segnet 准确地检测面部地标, segnet 在深度学习的基础上执行语义分割。使用 klt 点跟踪器跟踪检测到的地标边缘点。尽管它很受欢迎，但 klt 点跟踪器还是存在点丢失问题。我们通过定期执行 segnet 来计算面部地标的形状来解决这个问题。也就是说，通过将这两种技术结合起来，可以避免 segnet 实时形状跟踪的计算开销和 klt 点跟踪器的点丢失问题。我们进行了几个实验来评估我们的方法的性能，并在此报告一些结果。少

2018 年 7 月 14 日提交;最初宣布 2018 年 7 月。

61. news/泄漏 2.0-调查新闻的多语言信息提取和可视化

作者:gregor wiedemann, seid muhie yimam, chris biemann

摘要: 调查新闻近年来面临两大挑战: (1) 大量非结构化数据来自大型文本集合，如泄露或回答信息自由请求; 2) 多语言数据，原因是加强政治、商业和民间社会方面的全球合作和沟通。面对这些挑战，记者们越来越多地在国际网络中合作。为了支持这种合作，我们提出了新版本的 new/泄漏 2.0，我们的开源软件，用于基于内容的泄漏搜索。它包括三个新的主要功能: 1) 40 种语言的

自动语言**检测**和与语言相关的信息提取; 2) 有效探索的实体和关键字可视化; 3) 用于分析来自各种格式的机密数据。我们用一个典型的案例研究来说明新的分析能力。少

2018 年 7 月 13 日提交;**最初宣布** 2018 年 7 月。

62. 无监督视听教学的深度共聚

作者:聂飞平,李学龙

摘要: 看到的鸟鸣叫，跑车伴随着噪音，人们**面对面**地交谈等.这些自然的视听对应提供了探索和了解外部世界的可能性。但是，混合的多个对象和声音使在无约束环境中执行高效匹配变得棘手。为了解决这个问题，我们建议充分挖掘视听元器件，并在它们之间进行复杂的对应学习。具体而言，提出了一种新的无监督视听学习模型，称为深度共聚类 (dcc)，该模型在不同的共享空间中与卷积映射的多模态向量同步执行聚类集，以捕获多个视听通信。这种集成的多模聚类分析网络可以在端到端的方式中有效地进行最大边距损失的训练。进行大量的特征评估和视听任务实验。结果表明, dcc 可以学习有效的单式表示，分类器甚至可以比人类更有能力。此外, dcc 在声音定位、多源**检测**和视听理解任务中表现出显著的性能。少

2018 年 7 月 10 日提交;**v1** 于 2018 年 7 月 9 日提交;**最初宣布** 2018 年 7 月。

63. 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: ..... 判别 ksvd 字典算法 (stksvd) 在在线多目标跟踪中学习目标外观。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位置/发音变化、背景部分遮挡等因素的影响。...更多

2018 年 7 月 5 日提交;**最初宣布** 2018 年 7 月。

64. 人脸变形攻击检测的反射分析

作者:clemens seibold, anna hilsmann, peter eeert

摘要: 面部变形是一种合成的**面部**图像, 看起来类似于两个不同的个体, 甚至可以欺骗生物识别系统来识别这两个个体。这种攻击被称为**人脸**变形攻击。创建这样一个面部变形的过程是有据可查的, 很多教程和软件来创建它们是免费的。因此, 它是强制性的, 能够**检测**到这种欺诈, 以确保**作为**可靠的生物特征的人脸的完整性。在这项工作中, 我们研究了**人**脸变形对照明的物理正确性的影响。我们根据眼睛中的镜面反射高光估计光源的方向, 并使用它们生成皮肤上高光的合成地图。这张地图与图像中被怀疑是欺诈的亮点进行了比较。具有不同几何形状的变形**面**、源图像的错

误对齐或使用具有不同照明的图像，可能会导致反射中的不一致，从而指示存在变形攻击。少

2018 年 7 月 5 日提交;最初宣布 2018 年 7 月。

65. 使用面部和语音识别检测和分析 youtube 视频中的内容创建者协作

作 者 :moritz lode, michael rtl, christian koch, amr rizk, ralf steinmetz

文摘: 本工作讨论并实现了说话人识别在 youtube 视频中检测协作的应用。catana 是**一个检测**和分析 youtube 协作的现有框架，它正在利用**人脸**识别来**检测**合作者，而在视频内容上的性能自然不佳，而不会出现**面**。本文提出了利用主动扬声器检测和说话人识别对 catana **进行**扩展，以提高**检测**精度。少

2018 年 7 月 5 日提交;最初宣布 2018 年 7 月。

66. 卫星数据的大范围并行中断检测

作者:malte von meren, fabian gieseke, jan verbesselt, sabina rosca, stphanie horion, achim zeileis

摘要: 目前，遥感领域**面临着**大量的数据。虽然这提供了各种令人兴奋的研究机会，但在计算时间和空间要求方面也带来了重大挑战。实际上，由于数据量的增加，现有的方法对处理和分析所有可

用数据的速度太慢。本工作旨在加速 bfast，这是一种最先进的**卫星图像时间序列断裂检测**方法。特别是，我们为 bfast 提出了一个大规模并行实现，它可以有效地利用现代并行计算设备（如 gpu)。我们的实验评估表明，建议的 gpu 实现比现有的公开实现快四个数量级，比相应的多线程 cpu 执行快十倍。运行时间的大幅减少使得对显著较大的数据集的分析可以在几秒钟或几分钟内进行，而不是数小时或数天。我们展示了在给定人工数据集和真实数据集的情况下实现的实际好处。少

2018 年 7 月 4 日提交;**最初宣布** 2018 年 7 月。

67. rt-byzcast：拜占庭弹性实时可靠广播

作者：david kozhaya，jérémie decou 若希特，paulo esteves-verissimo

摘要: 今天的网络物理系统在实现其预期目标方面**面临各种**障碍，即相对于网络和无线设备的日益整合，通信不确定性和故障阻碍了所需的同步。满足实时截止日期。此外，至关重要的是，这些系统还面临重大的安全威胁。这种威胁组合增加了身体受损的风险。本文通过研究如何建立第一个实时拜占庭可靠的广播协议（rtbrb)来应对这些问题，该协议可以容忍网络的不确定性、故障和攻击。以前的文献描述了实时可靠的广播协议，或者是异步（非实时)拜占庭语。我们首先证明，即使借助传统的分布式计算范式，也不可能使用传统的分布式计算范式来实现 rtbrb，例如，即使在广

播算法的帮助下，进程的错误/故障检测机制也会与广播算法本身分离。最强大的故障探测器。我们通过提出 rt-byzcast 来避免这种不可能，这是一种基于在滑动时间窗口中聚合数字签名的算法，以及基于具有自崩溃功能的授权进程来掩盖和绑定损失的算法。我们通过证明通过正确的进程广播的消息是在已知的有界延迟内传递的，从而实时运行 rt-byzcast (i)，并且 (ii) 通过证明使用我们的算法的正确进程会使其崩溃而可靠。即使消息丢失率高达 60%，概率也可以忽略不计。少

2018 年 7 月 3 日提交;**最初宣布** 2018 年 7 月。

68. 针对客户端特定异常检测的人脸攻击检测

作者:shervin rahimzadeh Arashloo, josef kittler

文摘: 以前发现，单类异常**检测**方法在**人脸**攻击**检测中**非常有效，尤其是在 \ texttit 拟 {unsen} 攻击场景中，系统会接触到新类型的攻击。本工作遵循同样基于异常的问题公式，并分析部署针对**人**脸欺骗**检测的**结状 {客户端特定} 信息的优点。我们建议使用从预先训练的深层卷积神经网络中获得的表示来训练一类特定于客户端的分类器 (生成类分类器和判别式分类器)。接下来，根据特定主题的分数分布，为每个客户端设置一个不同的阈值，然后将其用于有关测试查询的决策。通过使用不同的一类系统进行的广泛实验表明，在一类异常检测公式中使用特定于客户端的信息

(无论是在模型构造中还是在决策阈值调优中)，都提高了性能显著。此外，还证明了用于识别目的的同一组深层卷积特征对于类特定类异常**检测**中的**人脸**表示攻击检测是有效的范式。少

2018 年 7 月 2 日提交;**最初宣布** 2018 年 7 月。

69. 通过视频分析利用服务业有限的资源

作者:郑春鸿,伊约拉 e. Olatunji

摘要: 服务业对许多发达经济体和发展中经济体作出了重大贡献。随着业务活动的迅速扩大，由于资源短缺导致服务反应迟缓，许多服务公司难以保持客户的满意度。在资源短缺和解决方案发生之前就对其进行预测是减少对运营的不利影响的有效方法。然而，就能力和劳动力成本而言，这种积极主动的做法非常昂贵。许多公司陷入生产力难题，因为它们未能找到足够有力的论据来证明新技术的成本是合理的，但却不能不投资于新技术，以与竞争对手相匹配。问题是，是否有创新的解决办法来最大限度地利用现有资源，并大幅减少资源短缺可能导致但以低成本实现高水平服务质量的影响。这项工作通过对我们在香港国际机场 (hkia) 设计和部署的手推车跟踪系统的实际分析，说明视频分析如何帮助实现管理层通过实时检测满足客户需求的目标并利用现有视频技术而不是采用新技术，防止他们在服务消费过程中可能遇到的问题。本文介绍了商业视频监控系统与视频分析深度学习算法的集成。

结果表明，系统能在**面对**全部或部分遮挡时提供准确的决策，精度高，显著改善了日常操作。根据设想，这项工作将提高服务业资源管理综合技术的认识，并将其作为实时客户援助的措施。少

2018 年 6 月 30 日提交;最初宣布 2018 年 7 月。

70. **嵌入式系统中人脸情感识别的报告准确性、推理时间和功耗等一切都很重要**

作者:jelena milosevic, dexmont pena, andrew forembsky, david moloney, miroslaw malek

摘要: 虽然文献中提出了几种人脸情感识别任务的方法，但都没有报告在嵌入式环境中运行系统所需的功耗和推理时间。由于对这些因素没有足够的了解，不清楚我们是否真的能够在嵌入式环境中提供准确的**面部**情感识别，如果没有，我们离实现它的可行性还有多远，最大的是什么 "我们**面临的**瓶颈。本文的主要目的是回答这些问题，并传达这样的信息：不仅报告**检测**精度，不如将功耗和推理时间报告为拟议系统及其采用的真正可用性在人机交互中，很大程度上取决于它。在本文中，我们确定了最先进的**人脸**情感识别方法，这些方法可能适用于嵌入式环境，以及最常用的数据集。我们的研究表明，大多数所进行的实验使用具有摆式表达式的数据集，或在具有特殊图像收集条件的特定实验设置中使用数据集。由于我们的目标是评估在现实场景中确定的有希望的方法的性能，我们收集一个具有非夸张情绪的新数据集，我们

除了公开的数据集外，还将其用于评估**检测结果**在三种常用的嵌入式设备上具有不同的计算能力，实现了准确性、功耗和推理时间。我们的研究结果表明，灰度图像仍然比彩色图像更适合嵌入式环境，对于大多数被分析的系统来说，无论是推理时间还是能耗，或者两者都是在实际应用中应用的限制因素.少

2018 年 6 月 29 日提交;**最初宣布** 2018 年 7 月。

71. **基于概率二分法和卷积神经网络的主动查询驱动视觉搜索**

作者: Athanasios tsiligkaridis, theodoros tsiligkaridis

文摘: 提出了一种基于概率二分法的高效目标**检测**与定位框架。卷积神经网络 (cnn) 被训练并用作一个嘈杂的甲骨文，为输入查询图像提供答案。从 cnn 获得的响应以及误差概率估计被用来更新沿每个维度的物体位置的信念。我们证明，沿每个维度查询在本地化错误上实现了与联合查询设计相同的下限。最后，我们将我们的方法与现实世界中传统的滑动窗口技术进行了比较，并在保持准确定位的同时，以至少一个数量级的方式显示速度的提高。少

2018 年 10 月 28 日提交;**v1** 于 2018 年 6 月 28 日提交;**最初宣布** 2018 年 6 月。

72. **saql：一种基于流的系统实时异常系统行为检测查询系统**

作者:高鹏、肖旭盛、丁丽、志春、李康国、 吴振宇、钟欢金、三吉夫 r.库尔卡尔尼、普拉特克·米塔尔

摘要: 最近，高级网络攻击，包括一系列涉及许多漏洞和主机的步骤，损害了许多受保护良好的企业的安全。这导致了一种解决方案，即将每个主机（大数据）中的系统活动作为一系列事件无处不在地监视，并为测试危险事件搜索异常（异常行为)。由于打击这些袭击是防止进一步损害的关键时间任务，这些解决办法在纳入专家知识以对大规模来源数据进行及时异常**检测**方面**面临**挑战。为了应对这些挑战，我们提出了一个新的基于流的查询系统，该系统以企业中多个主机聚合的实时事件馈送作为输入，并提供了一个异常查询引擎，该查询引擎查询事件馈送以识别异常行为基于指定的异常。为了便于根据专业知识表达异常，我们的系统提供了一种特定于域的查询语言 saql，它允许分析人员表示模型（1）基于规则的异常，(2）基于不变的时间序列异常，(3）不变的异常，以及（4）基于异常的异常。我们在由 150 个主机组成的 nec 实验室中部署了我们的系统，并使用 1.1 tb 的实际系统监控数据（包含 330 亿次事件）对其进行了评估。我们对一系列广泛的攻击行为和微观基准的评估表明，我们的系统具有较低**的检测**延迟（和 lt;2s）和较高的系统吞吐量（110，000 事件；支持 ~ 4000 台主机），并且在内存利用率方面比现有的基于流的复杂事件处理系统。少

2018 年 6 月 25 日提交;最初宣布 2018 年 6 月。

73. 用于姿势转移的生成模型

作者:charick chai, al 阁下 li , gokul swamy

摘要: 我们研究了最近的邻居和生成模型之间的姿势转移。我们拍摄一个人执行一系列操作的视频，并尝试生成另一个人执行相同操作的视频。我们的生成模型（pix2pix）在生成相应的帧和在演示的操作集之外泛化方面的性能优于 k-nn。我们最显著的贡献是确定一个管道（姿势**检测**,**人脸检测**, k-nn 为基础的配对），是有效地执行所需的任务。我们还详细介绍了几种迭代改进和失败模式。少

2018 年 6 月 23 日提交;最初宣布 2018 年 6 月。

74. 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目标攻击，在黑盒神经网络中，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。

75. 网络档案图像数据中人的关系研究

作 者 :eric müller-budack, kader Pustu-Iren, sebastian diering, ralph ewerth

摘要: 万维网上的多媒体内容正在迅速发展，包含了不同领域许多应用的宝贵信息。因此，自 90 年代中期以来，互联网档案计划已经收集了数十亿的过时的网页。但是，大量数据很少用适当的

元数据标记，并且需要自动方法来启用语义搜索。通常情况下，互联网档案的文本内容被用来提取实体及其可能的关系跨领域，如政治和娱乐，而图像和视频内容通常被忽视。本文介绍了一种存储在互联网档案中的网络新闻图像内容中的人识别系统。因此，该系统补充了文本中的实体识别，使研究人员和分析人员能够更准确地跟踪媒体报道和人员关系。基于深度学习**人脸**识别方法，我们建议建立一个系统，自动检测感兴趣的人，并收集样本材料，随后用于在互联网档案的图像数据中识别他们。我们在适当的标准基准数据集上评估人**脸**识别系统的性能，并通过两个用例演示该方法的可行性。少

2018 年 6 月 21 日提交;**最初宣布** 2018 年 6 月。

76. 浅谈鲁棒人脸欺骗检测的深层局部特征学习

作 者 :gustavo botelho de souza, jaopaulo papa, aparecido nilceu marana

摘要: 生物识别技术成为安全系统的可靠解决方案。然而，鉴于生物识别应用程序的传播，犯罪分子正在开发技术，通过模拟合法用户的身体或行为特征 (欺骗攻击) 来规避这些应用。尽管**人脸**是一个很有希望的特点，因为它的普遍性，可接受和存在的相机几乎无处不在，人**脸**识别系统是极易受到这种欺诈，因为他们很容易被愚弄与常见的印刷面部照片。基于卷积神经网络 (cnn) 的最先进的方法，在**人脸**欺骗**检测**中具有良好的效果。然而，这些方

法并没有考虑到从每个面部区域学习深层局部特征的重要性，尽管从**面部**识别中可以知道，每个面部区域都呈现不同的视觉方面，这也可以被利用，**面部**欺骗**检测.**在这项工作中，我们提出了一个新的美国有线电视新闻网架构训练在两个步骤为这样的任务。最初，神经网络的每个部分都从特定的面部区域学习特征。之后，对整个面部图像进行了微调。结果表明，这样的预训练步骤使美国有线电视新闻网能够学习不同的局部欺骗线索，提高了最终模型的性能和收敛速度，优于最先进的方法。少

2018 年 10 月 11 日提交;**v1** 于 2018 年 6 月 19 日提交;**最初宣布** 2018 年 6 月。

77. 基于电容的动能可穿戴设备的活动传感

作者:郭豪兰,马东,徐伟涛,马布·哈桑,文虎

文摘: 我们提出了一种新的使用传统的储能组件，即电容器，在动力学动力可穿戴 iot 作为传感器，以**检测**人类的活动。由于不同的活动以不同的速率在电容器中积累能量，因此可以通过观察电容器的充电速率直接**检测**到这些活动。拟议的基于电容器的活动传感机制 (capsense) 的主要优点是，它避免了在活动**检测**期间对运动信号进行采样的需要，从而显著节省了可穿戴设备。我们**面临的**一个挑战是，电容器本质上是非线性能量蓄能器，即使对于相同的活动，这也会导致不同时间的充电速率发生显著变化，

具体取决于电容器的当前充电水平。我们通过联合配置电容器和相关能量收集电路的参数来解决这个问题，这使得我们能够在近似线性的充电周期上运行。我们设计并实施了一个动能鞋底，并对 10 个对象进行了实验。结果表明，与传统的基于运动信号**的活动检测**相比，capsense 可以对五种不同的日常活动进行分类，准确率达到 95%，同时消耗 73% 的系统功率。少

2018 年 6 月 19 日提交;**最初宣布** 2018 年 6 月。

78. **查找相似的：测量人脸相似度，而不是人脸身份**

作者:amir sadovnik, wassim gharbi, thanh vu, andrew gallagher

摘要: **人脸**图像是计算机视觉的主要重点领域之一，接收各种各样的任务。虽然**人脸**识别可能是研究最广泛的，但许多其他任务，如亲属**关系检测**，人脸表情分类和面部老化已被审查。在这项工作中，我们提出了一个新的，主观的任务，量化感知人脸相似之间的一对**面孔**。也就是说，我们预测面部图像之间的感知相似性，因为它们不是同一个人。虽然这项任务显然与**人脸**识别有关，但却有所不同，因此有理由进行单独调查。人类经常说两个人看起来很像，即使是在两个人实际上并没有混淆的情况下也是如此。此外，由于**人脸**相似度与传统图像相似性不同，在数据收集和标注以及处理人类标签人之间的主观意见不同等方面也存在挑战。我们提出的证据表明，找到面部外观相似和识别**面孔**是两个不同

的任务。我们提出了一个新的界面相似性数据集，并引入了类似的网络，针对类似的**人**脸分类，它的性能优于针对同一任务的人**脸**识别网络的临时使用。少

2018 年 6 月 13 日提交;**最初宣布** 2018 年 6 月。

79. 用于面部动作单元检测的表达式增强雷西登网络

作者:shreyank jyoti, abhinav dhall

文摘: 本文探讨了野外面部行动单元 (fau)**检测**的主题。特别是，我们有兴趣回答以下问题: (1) 密集块之间的剩余连接对**人脸**分析有多大用处？(2) 来自一个接受过分类面部表情识别 (fer) 训练的网络的信息对 fau **检测**任务有多大用处？建议的网络 (residen) 利用密集块和剩余连接，并使用来自 fer 网络的辅助信息。实验在表情网络和 disfa 数据集上进行。实验表明，面部表情信息对 au **检测**是有用的。拟议的网络在这两个数据库上取得了最新的成果。通过对跨数据库协议结果的分析，发现了该网络的有效性。少

2018 年 6 月 13 日提交;**最初宣布** 2018 年 6 月。

80. 静态恶意软件检测与借口：量化机器学习和当前防病毒的鲁棒性

作者:威廉·弗莱什曼,爱德华·拉夫,理查德·扎克,马克·麦克莱恩,查尔斯·尼古拉斯

摘要: 随着基于机器学习 (ml) 的恶意软件**检测**系统变得越来越普遍，与当今广泛使用的更传统的防病毒 (av) 系统相比，有必要量化其优势。构建一个商定的测试集，将恶意软件**检测**系统的基准测试以基于纯粹的分类性能是不实际的。相反，我们通过创建一种新的测试方法来解决这个问题，在执行对抗性修改时，我们会评估一组已知良性和恶意文件的性能变化。然后，性能的变化与规避技术相结合，量化了系统对这种方法的鲁棒性。通过这些实验，我们能够以可量化的方式展示纯粹基于 ml 的系统如何比 av 产品更强大，以**检测**恶意软件，企图通过修改逃避，但在**面对**显着新颖的攻击。少

2018 年 6 月 12 日提交;**最初宣布** 2018 年 6 月。

81. 可靠的电子邮件跟踪识别：一种机器学习方法

作者:约翰内斯·豪普特,本尼迪克特·本德尔,本杰明·法比安，斯特凡·莱斯曼

摘要: 电子邮件跟踪允许电子邮件发件人收集电子邮件收件人上的细粒度行为和位置数据，这些收件人通过其电子邮件地址是唯一可识别的。这种跟踪侵犯了用户隐私，因为电子邮件跟踪技术在未经用户同意或不知情的情况下收集数据。为了提高电子邮件通信的隐私性，本文开发了一种**检测**引擎，以三种贡献的形式作为选择性跟踪阻塞机制的核心。首先，分析了大量的电子邮件通

讯，以显示跟踪在不同国家、行业和时间的广泛使用。其次，我们提出了一套功能，旨在识别现实条件下的跟踪图像。设计了新的功能，使其在计算上可行、高效、可推广和对跟踪基础设施的变化具有弹性。第三，我们在基准实验中使用一系列最先进的分类器来测试这些特征的预测能力，以阐明基于模型的跟踪识别的有效性。我们评估的预期准确性的样本外数据，在越来越长的时间内，当**面对**未知的发件人时。少

2018 年 6 月 11 日提交;最初宣布 2018 年 6 月。

82. 绵羊身份识别、年龄和体重估计数据集

作 者 :aya salama abdelhady, aboul ella hasanenin, aly Abdelhady

摘要: 人口的急剧增加和提高生产力的冲动激发了科学家、生产者和消费者对绵羊识别的兴趣的增加。预计到 2050 年，世界人口将超过 960 万。为此，提高了对有效畜牧业生产必要性的认识。羊被认为是粮食资源的主要来源之一。现在的研究大多针对开发实时应用，方便羊的识别进行品种管理，并收集体重和年龄等相关信息。重量和年龄是评估生产有效性的关键矩阵。因此，视觉分析最近证明，它比其他方法取得了显著成功。视觉分析技术需要足够的图像来测试和完成研究。因此，收集绵羊图像数据库是实现这一目标的重要步骤。我们在这里提供了用于测试和比较正在开发的此类算法的数据集。我们收集的数据集由 416 张彩色图像

组成，用于不同姿势的绵羊的不同特征。在从三个月到六年的一年中收集了 52 只羊的图片。对于每只羊，为身体两侧拍摄了两张图像,**为面部**两侧拍摄了两张图像，从顶部视图拍摄了一张图像，为臀部拍摄了一张图像，为牙齿拍摄了一张图像。收集到的图像涵盖了不同的照明、质量水平和旋转角度。分配的数据集可用于测试羊的识别、称重估计和年龄**检测**算法。这类算法对疾病管理、动物评估和所有权至关重要。少

2018 年 6 月 8 日提交;**最初宣布** 2018 年 6 月。

83. 自适应智能蜘蛛机器人

作 者 :rozita teymourzadeh, rahim nakhli mahal, ng kengshen, kok wai chan

摘要: 本文介绍了一种自适应智能蜘蛛机器人的研制。随着传感器的加入，四足蜘蛛机器人能够无线监测环境。在智能机器人的应用中，提出了一种新的自动站适应国家仪器 (ni) 控制器。研究工作将解决现有传统机器人适应能力弱的问题。提出的项目提出了一种无需人接口即可工作的自适应智能蜘蛛机器人。拟议的设计利用国家仪器 (ni) labview 的控制方案生产出一种智能便携式系统。此外，自适应智能蜘蛛机器人在**面对**障碍物时很容易适应新的情况。设计采用反馈回路原理图 labview 与智能控制器接口进行，并采用 gh-311 超声波传感器检测机器人前方的任何障碍物，gh-312 烟雾传感器用于**检测**烟雾在特定区域和 lm35 温度传感

器，以获得周围的温度。该模块采用移动无线路由器模块 tp-link tl-mr3420 路由器进行设备通信设计和实现。对该机器人进行了测试和分析，结果表明系统效率在 95% 以上，在机器人应用中具有较好的应用能力.

2018 年 6 月 10 日提交;**最初宣布** 2018 年 6 月。

84. 社会环境中的深层好奇心循环

作者:jonatan barkan, goren gordon

摘要: 在婴儿内在学习动机的启发下，我们开发了一个深刻的好奇心循环 (dcl) 架构，他们重视以其自身为基础的信息丰富的感官渠道。dcl 由一个学习者组成，它试图学习代理的状态动作转换的正向模型，以及一个新的增强学习 (rl) 组件，即一个动卷深 q 网络，它使用学习者的预测误差作为奖励.我们的代理的环境是由视觉社交场景组成的，由情景喜剧视频流组成，因此学习者和 rl 都被构造为深层卷积神经网络。代理人的学习者学习预测视觉场景动态的零顺序，从而产生与其社会环境中的变化成正比的内在回报。情景喜剧中这些社会信息变化的来源主要是**面孔**和手的动作，导致在无人监督的情况下学习社会交往特征。**人手检测**以价值函数为代表，社会互动的光流由策略表示。我们的研究结果表明,**人脸和手的**检测是嵌入社会环境中的基于好奇心的学习的紧急属性。少

2018 年 6 月 10 日提交;最初宣布 2018 年 6 月。

85. 用于对象发现和检测的自监控信号

作者:etienne bot,亚历山大 toshev, ja kosecka

摘要: 在机器人应用中，我们经常**面临**发现新物体的挑战，而很少或根本没有贴上标签的训练数据。本文探讨了机器人穿越环境提供的自我监控的使用，以了解遇到的物体的表示。对自我运动和深度感知的了解使代理能够有效地关联多个对象建议，这些建议可作为从未标记的图像中学习对象表示的训练数据。我们通过两种方式演示了这种表示形式的效用。首先，我们可以通过在学习的嵌入空间中执行聚类来自动发现对象。每个生成的群集都包含从不同角度和比例查看的一个实例的示例。其次，考虑到少量的标记图像，我们可以有效地学习这些标签的检测器。在射弹最少的情况下，这些探测器的 map 比根据这一有限数据训练的现成标准探测器的 0.22 的 map 要高得多，为 0.22。因此，提出的自我监控在没有或非常小的人工标记成本的情况下，实现了有效的环境特定对象发现和**检测**。少

2018 年 6 月 8 日提交;最初宣布 2018 年 6 月。

86. 利用局部质量特征进行指纹识别

作者:ram prakash sharma, somnath dey

摘要: 基于指纹的识别在各种应用中得到了广泛的应用。然而，目前的识别系统很容易受到欺骗攻击，利用指纹的人造副本来欺骗传感器。在这种情况下，指纹**活动性检测**可确保真正合法的指纹的实际存在，而不是假冒的自制合成样品。本文提出了一种基于静态软件的指纹质量特征检测指纹活动的方法 。我们从单个指纹图像中提取特征，以克服动态基于软件的方法所**面临**的问题，这些方法需要更长的计算时间和用户协作。该系统在当地一级提取了 8 个传感器独立的质量特征，其中包含了真实和假指纹的山脊谷结构的微小细节。这些局部质量特征构成了一个 13 维特征向量。该系统在 livdee 2009 年竞赛的公开数据集中进行了测试。实验结果显示，与目前最先进的方法相比，该方法为 livdee 2009 年提供了 5.3% 的最小平均分类误差。此外，在 livdet 2009 上性能最佳的功能的有效性在最新的 livdet 2015 数据集上进行评估，该数据集包含使用未知欺骗材料制作的指纹。与 livde2015 获胜者获得的 4.22 相比，平均分类错误率为 4.22。此外，拟议的系统采用单一的指纹图像，从而产生更快的影响，并使其更方便用户使用。少

2018 年 6 月 8 日提交;**最初宣布** 2018 年 6 月。

87. 在 ictu oculi：通过检测眼睛闪烁暴露 ai 生成的假脸视频

作者:李月尊,张明清章,刘思伟

摘要: 深层生成网络的新发展显著提高了生成逼真的假**脸**视频的质量和效率。在这项工作中，我们描述了一种新的**方法**来揭露假脸视频产生的神经网络。我们的方法是基于**检测**眼睛闪烁的视频，这是一个生理信号，并没有很好地呈现在合成的假视频。我们的方法在眨眼式检测数据集**的**基准上进行了测试，并显示了使用 deepfake 生成的视频检测性能。少

2018 年 6 月 11 日提交;**v1** 于 2018 年 6 月 7 日提交;**最初宣布** 2018 年 6 月。

88. **发现空间. 天真的代理的传感器体验中的空间拓扑和度量规律性的接地**

作者:alban lafl 气 ière, j. kevin o ' regan,bruno gas, 亚历山大 terekhov

摘要: 根据传感器应急理论，我们从一个基本的传感器运动的角度来研究空间的感知问题。尽管空间在我们对世界的认知中普遍存在，但空间概念的起源在很大程度上仍然是神秘的。例如，在人为感知的情况下，通常通过让工程师预先定义代理必须**面对**的问题的空间结构来规避此问题。我们在这里表明，空间的结构可以由一个天真的代理以感官运动的形式自主地发现，这种特性与所谓的可赔性感官体验相对应：这些体验可以由代理人或其产生环境。通过**检测**这种可赔性体验，代理人可以推断其物体移动的外部空间的拓扑和度量结构。我们提出了这些规律性的性质的理论

描述，并说明了在一个模拟机器人手臂上配备了一个眼睛一样的传感器，并与一个对象相互作用的方法。最后，我们展示了如何使用这些规律性来构建传感器外部空间配置的内部表示形式。少

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

89. 基于 ai 的软件定义物联网网络两级入侵检测

作者:李嘉奇,赵志峰,李荣鹏,张洪刚

摘要: 软件定义的物联网 (sd-iot) 网络从集中式管理和交互式资源共享中获益，从而提高了物联网应用的效率和可扩展性。但随着服务和应用程序的快速增长，它很容易受到可能的攻击，并**面临**严峻的安全挑战。入侵**检测**已被广泛用于确保网络安全，但经典**的检测**手段通常是基于签名或基于明确行为的，无法智能**地检测到**未知攻击，这很难满足 sd-物联网网络的要求。本文提出了一种基于 ais 的两阶段入侵**检测**方法，该检测是由软件定义技术授权的。它通过全局视图灵活地捕获网络流，并通过应用 ai 算法智能地检测攻击。首先利用具有群分裂和微分突变的蝙蝠算法来选择典型特征。然后，利用加权投票机制自适应地改变样本的权重来对流量进行分类，从而开发随机林。评价结果表明，改进后的智能算法选择了更重要的特征，在流量分类方面取得了较好的性

能。并验证了智能入侵**检测**具有较好的精度，与现有的解决方案相比具有较低的开销。少

2018 年 6 月 7 日提交;**最初宣布** 2018 年 6 月。

90. 基于眼睛眨眼和头部姿势估计的睡意检测新系统

作者:m. ben dkhil, a. wali , adel m. alimi

摘要: 司机嗜睡问题被认为是增加道路事故数量的最重要原因之一。本文提出了一种新的实时驾驶嗜睡方法，以防止道路事故的发生。该系统使用智能摄像机，拍摄司机**面对**的图像，并监督眼睛眨眼 (打开和关闭) 状态和头部姿势，以**检测**不同的睡意状态。**面部**和眼睛**的检测**是通过紫百合和琼斯技术完成的。少

2018 年 5 月 31 日提交;**最初宣布** 2018 年 6 月。

91. 众筹: 基于人群的文献评论筛选平台

作 者 : 豪 尔 赫 · 拉 米 雷 斯 , evgeny krivosheev, marcos baez, fabio casati, boualem benatallah

摘要: 在本文和演示中，我们提出了一个基于人群和人群 + ai 的系统，称为 crowdrev，支持文献评论的筛选阶段，并以一小部分成本实现与作者分类相同的质量，几乎是瞬间的。crowdrev 使作者能够很容易地利用人群，并确保即使面对困难的文件或标准，也不会浪费任何金钱: 如果系统**检测到**任务对人群来说太难，它

就放弃了尝试（对于那张论文来说），或为该标准，或完全），而不浪费金钱，永远不会损害质量。少

2018 年 5 月 31 日提交;最初宣布 2018 年 5 月。

92. 基于神经网络约束优化的人脸检测器对抗攻击

作者: Avishek joey bose, parham aarabi

摘要: …… 获得机器学习模型的目标是对它们进行错误分类。虽然在图像分类模型上提出了许多不同的对抗攻击策略，但目标**检测管道的破坏**却困难得多。本文提出了一种新的策略，利用一个算法来解决约束优化问题，从而绘制出对抗性的实例。更多

2018 年 5 月 30 日提交;最初宣布 2018 年 5 月。

93. 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。与现有的只限于操纵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肖像视频一个目标演员。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。为了实现源到目标视频的重新动画，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。

94. 技术报告：关键价值商店中的乐观执行

作　者　:duong nguyen, aleksey charapko, sandeep kulkarni, murat demirbas

摘要: cap 定理的局限性意味着，如果在存在网络分区的情况下需要可用性，则必须牺牲顺序一致性，这是一种更自然的系统设计一致性模型。我们关注的问题是，如果设计人员有一个算法可以正常工作，顺序一致性，但**面临**的基础键值存储提供了较弱(例如，最终或因果) 的一致性，那么他应该做什么。我们提出了一种基于**检测**回滚的方法：设计人员识别一个正确性谓词，例如

P，并继续运行协议，因为我们的系统监视P.如果P被破坏（因为基础键值存储提供了较弱的一致性），系统回滚并恢复计算在一个状态，其中P持。我们使用在伏地魔键值存储上运行的实际图形应用程序来评估这种方法。我们在 amazon aws ec2 实例上进行部署的实验表明，使用与监视的最终一致性可以提供50--80%与顺序一致性相比，吞吐量增加。我们还表明，监视本身的开销很低（通常小于 4\%），**并且检测**冲突的延迟很小。特别是，超过99。9%在不到的情况下**检测到**的违规情况。50 在区域 aws 网络中的毫秒，并在不到5在全球 aws 网络中的秒数。少

2018年6月23日提交;**v1** 于2018年5月25日提交;**最初宣布** 2018年5月。

95. 分层一排列哈希：高效的近重复检测

作者:张成元,林云武,朱磊,新潘园,君龙,黄方

摘要: 随着多媒体技术的进步和智能手机、数码相机、存储设备的普及，在多媒体检索和管理系统等许多应用中收集的大量多媒体数据迅速增加。其中数据元素由文本、图像、视频和音频组成。因此，多媒体近重复**检测**的研究引起了研究机构和企业界的高度关注。传统的解决方案最小哈希（\ minwish）**面临**两个挑战：昂贵的预处理时间和较低的比较速度。因此，本工作首先引入一种称为 "一个排列哈希" (hashing) 的哈希方法，以避免昂贵的预处理

时间。在 \ oph 的基础上，开发了一种更有效的基于排列哈希的策略群，以应对较高的比较时间。基于大多数多媒体数据的相似度不是很高的事实，本文设计了一种新的哈希方法，即分层一排列哈希 (\ hoph)，以进一步提高性能。在实际多媒体数据集上进行的综合实验清楚地表明，具有相似精度的 \ hoph 比"更快 5 到 7 倍

2018 年 8 月 15 日提交;**v1** 于 2018 年 5 月 29 日提交;**最初宣布** 2018 年 5 月。

96. 基于监控摄像机的定制深度学习视频分析的部署

作 者 :pratik dual, rohan mahadev, suraj kothawade, kunal dargan, rishabh iyer

摘要: 本文展示了我们定制的基于深度学习的视频分析系统在以安全、安全、客户分析和流程合规性为重点的各种应用中的有效性。我们描述了我们的视频分析系统，包括搜索、汇总、统计和实时警报，并概述了其构建块。这些构建块包括目标**检测**、跟踪、**人脸检测**和识别、人**脸和人脸**子属性分析。在每种情况下，我们都演示了使用部署方案中的数据训练的自定义模型如何提供比现成模型优越得多的精度。为此，我们描述了我们的数据处理和模型培训管道，它可以在快速周转时间内从视频中训练和微调模型。最后，由于这些模型大多部署在现场，因此必须有不需要 gpu 的资源受限模型。我们演示了如何自定义资源受限模型，并将其

部署到嵌入式设备上，而不会显著降低准确性。据我们所知，这是第一份在监控视频分析的各种实际客户部署场景中全面评估不同深度学习模型的工作。通过分享我们的实施细节和为各种客户部署定制的深度学习模型所获得的经验，我们希望定制的基于深度学习的视频分析能够广泛融入世界各地的商业产品中。少

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

97. dif：醉酒人员识别中的醉酒面融合数据集

作者:devendra pratap yadav, abhinav dhall

摘要: 交通事故每年造成 100 多万人死亡，其中很大一部分是醉酒驾驶造成的。为了减少交通事故和相关的财务费用，车辆中的自动醉酒**检测**系统是必要的。现有的解决方案需要特殊的设备，如心电图、红外摄像机或呼吸分析仪。在这项工作中，我们提出了一个新的数据集称为 dif (融合面数据集) 包含 rgb 脸视频的醉酒和清醒的人**从**网上来源获得。我们分析**面部**视频，以提取与眼睛注视,**面部**姿势和面部表情相关的功能。利用递归神经网络对这些多模态面部特征的演化进行建模。我们的实验表明，眼睛注视和面部表情特征对我们的数据集特别有鉴别力。我们在 dif 数据集上实现了较好的分类精度，并表明**人脸**视频可以有效地用于**检**

测醉汉。这样的**面部**视频可以很容易地通过相机获得，用于防止醉酒驾驶事件。少

2018 年 5 月 25 日提交;最初宣布 2018 年 5 月。

98. 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) 有效的深度学习跟踪和**人脸**相关算法 (如**人脸检测**) 的结合为该领域未来的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。

99. 从颈近红外视频中估计颈动脉脉搏和呼吸率

作者:陈伟轩, javier hernandez, rosalind w. picard

摘要: 目的: 非接触式生理测量是一个不断增长的研究领域, 可以通过远程设备轻松、不显眼地捕捉心率 (hr) 和呼吸速率 (br) 等生命体征。然而, 大多数方法只在明亮的环境中工作, 在这种环境中, 微妙的光电测和超声心动图信号可以很容易地进行分析, 或者需要昂贵的定制硬件来执行测量。方法: 本工作引入了一种低成本的方法, 利用近红外 (nir) 视频成像技术测量与颈动脉脉冲和颈部呼吸运动相关的细微运动。建立了颈部皮肤反射模型, 为该方法提供了理论依据。特别是, 该方法依赖于用于颈部**检测**的模板匹配、用于特征提取的主成分分析和用于数据平滑的隐马尔可夫模型。主要结果: 我们在一项 12 人实验室研究中将估计的 hr 和 br 测量值与 fda 清除装置提供的测量值进行了比较: 在明亮和黑暗的情况下, 这些估计实现了每分钟 0.36 次和每分钟 0.36 呼吸的平均绝对误差照明。意义: 这项工作提出了在环境照明有限、人**的脸**不容易获得或需要保护的现实生活条件下进行非

接触式生理测量的可能性。由于近红外成像设备的可用性不断提高，所述方法易于扩展。少

2018 年 5 月 24 日提交;最初宣布 2018 年 5 月。

100. 基于网络优化的智能人口系统年龄估计

作者:许振珍,孙鹏,永港温

摘要: 年龄估计是一项艰巨的任务，需要对面部特征进行自动检测和解释。近年来，卷积神经网络（cnn）在基准数据集中的学习年龄模式方面取得了显著的改善。然而，对于 "野外" 的**脸**(来自视频框架或互联网）来说，现有的算法并不像正面和中性**的脸那样**准确。此外，随着野生老化数据的不断增加，现有深度学习平台的计算速度成为另一个关键问题。本文提出了一种高效的年龄估计系统，该系统具有年龄估计算法和深度学习系统的联合优化。该系统与城市监控网络配合使用，可为智能人口统计提供年龄组分析。首先，我们构建了一个三层雾计算架构，包括边缘、雾和云层，它直接处理原始视频中的年龄估计。其次，优化了基于 cnn 的具有标签分布和 k-l 发散距离的年龄估计算法，并对最新野生老化数据集的模型进行了评价。实验结果表明: 1、系统在无接触的情况下动态采集远距离人口统计数据，实现城市人口分析;和 2。年龄模型培训在不失去训练进度或模型质量的情况下加快了速度。

据我们所知，这是第一个在提高智能城市和城市生活效率方面具有潜在应用前景的智能人口统计系统。少

2018 年 5 月 21 日提交;**最初宣布** 2018 年 5 月。

101. 利用深度学习在野外进行长期的面部跟踪

作者:张昆磊,拉海拉希迪,拉海巴拉蒂，陈学文

文摘: 本文研究了一个特定的人的长期面部跟踪给出了他的**人的人的人的人的人的人的人的**脸图像在一个单一的帧作为一个查询在视频流。利用预训练的大数据深度学习模型，开发了一种新的系统，用于在不受约束的环境中进行精确的视频**人脸跟踪**，描绘了各种进出帧的人员和物体。在该系统中，我们提出了一种**检测**-验证跟踪方法（称为 "dvt"），通过**人脸检测**、**人脸**的协作完成长期**的人脸**跟踪任务验证，以及（短期)**面部**跟踪。基于级联卷积神经网络的离线训练检测器对帧中出现的所有**人脸**进行定位，基于深卷积神经网络和相似度度量学习的离线训练人脸验证器决定是否有任何**面**或哪**一张脸**对应于被询问的人。一个在线训练的跟踪器跟踪**着一个帧**之间的脸。当在情景喜剧和电视节目中验证时，dvt 方法在召回和精度方面优于跟踪学习检测（tld）和**人脸**-tld。拟议的系统还在许多其他类型的视频上进行了测试，并显示了非常有希望的结果。少

2018 年 5 月 19 日提交;**最初宣布** 2018 年 5 月。

102. 最狂野的面孔：暴力环境中的人脸检测和识别

作者:mehmet kerim yucel, yunus can bilge, oguzan oguz,nazli ikizler-cinbis , pinar duygulu, ramazan gokberk cinbis

摘要: 随着大规模数据集和能够学习复杂表示的深度学习模型的引入,**人脸检测**和识别任务取得了令人印象深刻的进展。尽管取得了这些进展，但现有数据集并没有反映出**在**最疯狂的情况下，如敌对争端或打斗中，人脸识别的困难。此外，现有数据集并不完全不受约束地表示低分辨率、高模糊和大遮挡方差的情况。为此，我们介绍了最狂野的**面孔**数据集，它侧重于通过暴力场景产生的不利影响。该数据集由电影中名人的一组广泛的暴力场景组成。我们的实验结果表明，最先进的技术并不十分适合暴力场面，因此，最狂野**的面孔**可能会引起更多的兴趣，在**人脸检测**和识别研究。少

2018 年 5 月 19 日提交;**最初宣布** 2018 年 5 月。

103. 基于纹理和姿势相关初始化的鲁棒性面部地标定位

作者:潘一云,周俊伟,高永生,熊胜武

摘要: 当**面部**部分被遮挡时，坚固的面部地标定位仍然是一项具有挑战性的任务。近年来，级联姿态回归由于其在面部地标定位和遮挡**检测方面**的优异性能，越来越受到人们的关注。但是，这种方法对初始化非常敏感，在这种情况下，不正确的初始化可能会

严重降低性能。在本文中，我们提出了一个鲁棒初始化级联姿态回归（ricpr）提供纹理和姿势相关的初始形状的测试面. 通过研究**测试面**和训练**面**之间局部二元模式直方图的相关性，选择与测试**面**最相关的训练**面**形状作为纹理相关初始化。为了使初始化对各种姿态更加稳健，我们根据基于多任务级联卷积网络的五个基准地标来估计测试**面**的粗糙姿态。然后用平均**面**的形状和粗糙的测试**面**姿势构造姿势相关的初始形状。最后，将纹理相关和姿态相关的初始形状作为鲁棒初始化连接在一起。我们评估了富有挑战性的 cofw 数据集的 ricpr。实验结果表明，该方案在面部地标定位和遮挡**检测方面**取得了比现有方法更好的性能。少

2018 年 5 月 15 日提交;**最初宣布** 2018 年 5 月。

104. 对话消失：发现早期对话失败的迹象

作者:justinezhang, jonathan p. chang , Cristian danescu-nuicu 心-mizil, lucas dixon, ya 水利 hua, nithumthain, dario taraborelli

摘要: 网络社会制度**面临**的主要挑战之一是骚扰和人身攻击等反社会行为的普遍存在。在这项工作中，我们介绍了从谈话一开始就预测它是否会失控的任务。与事后**检测**不良行为不同，此任务旨在在对话仍可能被挽救的情况下实现早期、可操作的预测。为此，我们开发了一个捕获语用手段的框架，如礼貌策略和修辞提示--用于开始对话，并分析它们与未来轨迹的关系。将此框架应用

于受控环境，我们演示了在在线讨论中**检测**反社会行为预警信号的可行性。少

2018 年 5 月 14 日提交;**最初宣布** 2018 年 5 月。

105. 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

文摘: 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 **人脸上**获得了 92.6 和 100% 的攻击成功率，同时保持了与中的无攻击模型几乎相同的准确性。正常模式。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。

106. 分布式深林及其在现金流出欺诈自动检测中的应用

作者:张亚林 ,周军，郑文豪，季峰, 李龙飞，刘子奇,李明强，张超浩, 李小龙, 周志华

摘要: 互联网公司**每天都面临着**处理大规模机器学习应用的需要，需要能够处理超大规模任务的分布式系统。深林是最近提出的以树型为基石的深层学习框架，在各任务领域取得了极具竞争力的成果。然而，它还没有在非常大规模的任务中进行测试。在本文的基础上，基于我们的参数服务器系统和人工智能平台，我们开发了一个易于使用的 gui 的分布式深林版本。据我们所知，这是首次实现分布式深林。为了满足现实世界任务的需要，对原来的深林模型进行了许多改进。我们在一个超大规模的任务中测试了深林模型，即自动检测现金流出欺诈，并提供了超过 1 亿个培训样本。实验结果表明，深林模型根据不同角度的评价指标，即使在参数调整方面做得很少，也具有最佳的性能。此模型可以阻止大

量的金钱欺诈交易 \cemetumtem 即为业务机密}。即使与最佳部署模型相比，深林模型也能带来显著的经济损失。少

2018 年 5 月 27 日提交;**v1** 于 2018 年 5 月 10 日提交;**最初宣布** 2018 年 5 月。

107. 人脸防打网卷积神经网络的性能评价

作者:chaitanya nagpal , shiv ram dubey

摘要: 在当今时代，基于生物识别的访问控制由于其简单性和易用性而越来越流行。它减少了身份识别的手动工作，方便了自动处理。人脸是最重要的生物识别视觉信息之一，在不受控制的环境中，无需用户合作即可轻松捕获。应高度优先考虑对欺骗**面**的精确**检测**，以使基于**人脸**的身份识别和访问控制对可能的攻击具有鲁棒性。最近发展起来的基于卷积神经网络 (cnn) 的深度学习技术已被证明是非常有效地处理视觉信息的优秀方法之一。美国有线电视新闻网从数据自动地学会分层特征在中间层。基于美国有线电视新闻网的几种方法，如初始和 resnet 已显示出出色的性能图像分类问题。本文对 cnn 进行了面部反欺骗的性能评价。本研究采用了初始和重置 cnn 架构。结果是通过基准 msu 移动人脸欺骗数据库计算的。实验考虑了模型的深度、随机权重初始化与重量转移、微调与零训练和不同学习速度等不同方面。利用

这些 cnn 架构在不同的环境下**进行人**脸欺骗，得到了较好的效果。少

2018 年 5 月 7 日提交;**最初宣布** 2018 年 5 月。

108. 与李力一起评估人工干预应对错误发现的挑战

作者:john galea, sean heelan, daniel neville, daniel kroening

摘要: 符号执行已显示出它能够发现软件中与安全相关的缺陷，但**面临着**重大的可伸缩性挑战。人们普遍认为，专家的人工干预有助于缓解这些限制因素。然而，对这一想法几乎没有进行正式调查。在本文中，我们介绍了我们的经验，将 klee 符号执行引擎应用到一个新的 bug 语料库，并使用手动干预，以减轻遇到的问题。我们的贡献是 (1) 半翅目，一个新的语料库超过 130 个错误在现实世界的软件, (2) 一个全面的评估 klee 符号执行引擎在半翅目与分类的经常发生的软件模式，是有问题的符号执行，以及 (3) 旨在解决符号执行的根本问题的人工缓解的评估。我们的经验表明，在许多情况下，手动干预可以提高代码覆盖率和错误**检测**。然而，这不是一颗银弹，我们讨论它的局限性和遇到的挑战。少

2018 年 5 月 9 日提交;**最初宣布** 2018 年 5 月。

109. 用于高效人脸检测的锚点级联

作者:于宝生,陶大成

摘要: **面部护理检测是**面部分析任务的关键，如面部再现和**人脸**识别。级**联面**探测器和基于锚杆的**人**脸探测器都将光辉的演示转化为实践，并受到社区的高度关注。然而，级**联人脸**探测器的**检测**精度往往很低，而基于锚杆的人脸探测器严重依赖于在 imagenet 等大规模图像分类数据集上预先训练的非常大的网络[1]，这对训练和部署都不具有计算效率。本文设计了一种高效的基于锚杆的级联框架--锚杆级联。为了通过探索上下文信息来提高检测精度，我们进一步提出了锚杆级联的**上下文**金字塔极值机制。因此，锚栅级联可以培养出非常高效的**人脸检测**模型,**具有较高的检测**精度。具体而言，与流行的基于 cnn 的级联**面**检测器 mtnnn [2] 相比，我们的锚级联**面**检测器大大提高**了检测**精度，例如，在 fddb 上的 1k 误报时，从 0.9435 提高到 0.97 04,而它仍然以类似的速度运行。在两个广泛使用**的人脸检测**基准 fddb 和 wider **face** 上的实验结果证明了该框架的有效性。少

2018 年 5 月 8 日提交;**最初宣布** 2018 年 5 月。

110. 量化模拟：面向非常微小的 cnn 的目标检测

作者:易伟,潘新宇,秦红伟,欧阳万里,严俊杰

文摘: 在本文中，我们提出了一个简单而通用的框架，用于训练非常微小的 cn 进行目标检测。由于表示能力有限，训练非常微小

的网络来完成检测等复杂任务是很有挑战性的。据我们所知，我们的方法被称为量化模拟，是第一个专注于非常微小的网络的方法。我们使用两种类型的加速方法：模拟和量化。模仿通过从教师网络传授知识，提高了学生网络的性能。量化可将全精度网络转换为量化网络，而不会显著降低性能。如果教师网络是量化的，学生网络的搜索范围就会缩小。利用量化的这一特点，我们提出了量化模拟。它首先量化大型网络，然后模拟量化的小网络。量化操作可以帮助学生网络更好地匹配教师网络中的要素图。为了评估我们的方法，我们在各种流行的 cnn 上进行实验，包括 vgg 和 resnet，以及不同的**检测**框架，包括更快的 r-cnn 和 r-fcn。在 pascal voc 和 wider **face** **上的**实验验证了我们的量化仿真算法可以应用于各种设置，并且在计算结果有限的情况下优于最先进的模型加速方法。少

2018 年 9 月 13 日提交;**v1** 于 2018 年 5 月 6 日提交;**最初宣布** 2018 年 5 月。

111. 基于骨到细深递归神经网络的面部地标定位

作 者 :shahar mahpod, rig das, Emanuele Maiorana, yosi keller, patrizio campisi

文摘 人脸地标点定位是计算机视觉中的一个典型问题，广泛应用于**提高人脸**识别、人脸表情分析、**人脸**动画等的准确性。近年来，许多研究人员为设计一个强大的面部地标**检测**系统做出了巨大的

努力。然而，由于存在极端姿势、夸张的面部表情、无约束照明等因素，它仍然是最具挑战性的任务之一。本文提出了一种新的基于粗糙到细的深递归神经网络（rnn）框架，该框架利用热图图像进行人脸地标点定位。使用热图图像允许我们使用整个**人脸**图像，而不是**人脸**初始化边界框或在地标点周围的补丁图像。我们提出的框架的性能表明，在处理遮挡程度较高 、姿势变化、大偏航角和照明较大的困难人脸图像方面，情况有了显著改善。与目前最好的最先进技术相比，300-w 私人测试装置的故障率降低45%，曲线下的面积提高 11.5，是我们建议的框架的一些主要贡献。少

2018 年 5 月 3 日提交;**最初宣布** 2018 年 5 月。

112. 面部属性分类中的级联 cnn 多任务学习

作者:ni 壮, yan yan, si chen, hanzi wang

摘要: 近年来，人脸属性分类（fac）在计算机视觉界引起了广泛的关注。随着具有挑战性的 fac 数据集的提供，已经取得了巨大的进展。然而，传统的 fac 方法通常首先对输入图像进行预处理(即执行**人脸检测**和对齐)，然后预测人脸属性。这些方法忽略了这些任务（即**人脸检测**、人脸地标定位和 fac）之间的固有依赖关系。此外，在不考虑面部属性差异的情况下，对一些采用卷积神经网络的方法进行了基于固定损失权重的训练。为了解决上述问题，

我们提出了一种新的多任务学习表壳卷积神经网络方法 mcfa，用于同时预测多个面部属性。具体而言，该方法利用三个级联子网络（即 s _ net、m _ net 和 l _ net，对应于不同尺度下的神经网络），以粗到细的方式联合训练多个任务，从而实现端到端优化。此外，该方法还基于一种新的动态加权方案，将损失权重自动分配给每个面部属性，从而使所提出的方法集中于预测更困难的面部属性。实验结果表明，该方法在具有挑战性的 celeba 和 lfwa 数据集上优于几种最先进的 fac 方法。少

2018 年 5 月 3 日提交;**最初宣布** 2018 年 5 月。

113. 基于多标签学习的面部属性分类深度传输神经网络

作者:ni zen zen, sichen, hanziwang, shen chwhua

文摘: 深神经网络（dnn）最近在包括面部属性分类在内的各种计算机视觉任务中取得了优异的性能。用 dnn 对面部属性进行分类的巨大成功往往依赖于大量的标记数据。然而，在现实世界的应用程序中，只提供了一些常用属性（如年龄、性别）的标签数据；而未标记的数据可用于其他属性（如吸引力、发际线）。针对上述问题，我们提出了一种新的基于多标签学习的人脸属性分类深度传输神经网络方法--fmtnet，它由三个子网络组成：人脸 **检测**网络（多标签学习网络（mnet）和转移学习网络（tnet）。首先，基于更快的基于区域的卷积神经网络（更快的 r-cnn），对 fnet 进行

了人脸**检测**微调。然后，由 fnet 对 mnet 进行微调，以预测具有标记数据的多个属性，并开发了一种有效的减肥体重方案，以明确利用基于属性分组的面部属性之间的相关性。最后，在 mnet 的基础上，利用无监督域适应的方法对无标记的人脸属性分类进行了培训。这三个子网紧密耦合，实现了有效的面部属性分类。所提出的 fmtnet 方法的一个显著特点是，三个子网络 (fnet、mnet 和 tnet) 是在一个相似的网络结构中构建的。关于具有挑战性**的人脸**数据集的大量实验结果表明，与几种最先进的方法相比，我们提出的方法是有效的。少

2018 年 5 月 3 日提交;**最初宣布** 2018 年 5 月。

114. 精确的框分：从数据集中提取更多信息，以提高人脸检测的性能

作者:ce qi,陈晓平,王平宇,苏飞

文摘: 对于基于 r-cnn 框架的人**脸检测**网络的培训，如果与地面真相的交叉过度结合 (iou) 高于第一个阈值 (如 0.7)，锚被指定为阳性样本;如果其 iou 低于第二个阈值 (如 0.3)，则为负样本。并通过上述标签对**人脸检测**模型进行训练。但是，不使用在第一个阈值和第二个阈值之间具有 iou 的锚点。提出了一种新的训练策略--精确盒分 (pbs) 来训练目标检测模型。提出的训练策略在第一和第二阈值之间使用带有 iou 的锚点，可以持续提高**人脸**

检测的性能。我们提出的培训策略从数据集中提取更多信息，从而更好地利用现有数据集。此外，我们还介绍了一种简单而有效的模型压缩方法（semcm），该方法可以进一步提高**人**脸检测器的性能。实验结果表明，在我们提出的方案基础上,**人脸检测**网络的性能可以得到持续的提高。少

2018 年 4 月 28 日提交;**最初宣布** 2018 年 4 月。

115. 推进无约束人脸检测的极限：一个挑战数据集和基线结果

作者:hajime nada, Vishwanath a. sindagi, he zhang , vishal m. patel

摘要: **面部护理在**过去几年中，检测工作取得了巨大进展，每年都会超过新的里程碑。虽然许多挑战，如规模、姿态、外观的巨大变化得到了成功解决，但仍然存在着一些现有方法或数据集没有具体反映的问题。在本工作中，我们确定了需要研究界关注的下一组挑战，并收集了一个新的**人脸**图像数据集，这些图像涉及这些问题，如基于天气的退化、运动模糊、焦点模糊和其他几个问题。我们证明，在最先进的探测器的性能和现实世界的要求方面存在着相当大的差距。因此，为了推动无约束**人脸检测**的进一步研究，我们提出了一个新的注释无约束**人脸检测**数据集（ufdd），提出了几个挑战和基准的最新方法。此外，我们还对这些方法的结果和失败案例进行深入分析。数据集和基准结果将在适当时候

公开。udd 数据集以及基线结果可在以下位置查阅：www.ufdd.info/

2018 年 8 月 8 日提交;**v1** 于 2018 年 4 月 26 日提交;**最初宣布** 2018 年 4 月。

116. 智能 icu 中试研究：利用人工智能技术进行患者自主监测

作者:anis davoudi, kumar rohit malhotra, benjamin sh 厂, scott siegel, seth williams, matthewrupert, emel bihorac, tezcan azrazgat-baslantt , patrick j。急躁, azra bihorac, parisa r 减退

摘要: 目前，许多危重护理指标是由不堪重负的护士重复评估和记录的，例如非语言患者的身体功能或面部疼痛表情。此外，关于患者及其环境的许多基本信息根本没有被捕获，或以非颗粒的方式捕获，例如睡眠干扰因素，如强光、巨大的背景噪音或过度访问。在这项试点研究中，我们研究了在重症监护病房 (icu) 中使用普及传感技术和人工智能对危重病人及其环境进行自主和颗粒监测的可行性。作为一个典型的流行条件，我们也描述了神志不清和不精神错乱的病人和他们的环境。我们使用可穿戴传感器、光和声音传感器以及高分辨率相机来收集病人及其环境的数据。我们使用深度学习和统计分析对收集到的数据进行了分析。我们的系统执行**人脸检测**,**人脸**识别，人脸动作单元**检测**，头部姿势**检测**，面部表情识别，姿势识别，动作分析，声音压力和光级**检测**，以及访问频率**检测**。我们能够**检测到**病人的**脸**(平均精度

(mAP)=0.94)，识别病人的**脸**(mapcs0.80)，以及他们的姿势(f1bs0.94)。我们还发现，所有面部表情、11个活动特征、白天的探视频率、夜间的探视频率、夜间的光照水平和声压水平，在神志不清和非神志不清的患者 (value<0.05)。总之，我们表明，对危重病人及其环境进行颗粒式自主监测是可行的，可用于确定危重病人病情和相关环境因素的特点。少

2018年9月26日提交;**v1** 于2018年4月25日提交;**最初宣布** 2018年4月。

117. 基于泛锐高分辨率卫星图像的鲁棒异常船舶建议检测

作者:viet hung luu, nguyen hoang hoa luong, quang hung bui , thi nhat thanh nguyen

文摘: 现在，顶级船舶探测器采用了船舶建议书的预先筛选，以避免在图像中进行详尽的搜索。在非常高的分辨率 (vhr) 光学图像中，船舶在公海杂波 (噪声样背景) 中作为异常明亮像素的集群出现。基于异常的检测器利用全色 (pan) 数据在许多研究中被广泛用于**船舶的探测**，然而，仍然面临着两个主要缺点: 1)**检**出率往往**很**低，特别是在船舶低的情况下对比度和 2) 这些模型需要一个高手动配置，以选择一个阈值最好的分离船舶从海面背景。本文旨在进一步研究基于异常的模型，以解决这些问题。首先，将泛锐化多光谱 (ms) 数据与 pan 结合在一起，以增强船舶识别。其次，结合全局强度异常和局部纹理异常图，提出了一种改进的

基于异常的模型。针对海洋杂波的现状和泛锐化过程引起的噪声，引入了基于量化理论的纹理异常抑制项。vnredsat-1 vhr 光学卫星图像的实验结果表明，泛锐化近红外（p-nir）波段可以改善对周围水域船舶的识别。与最先进的基于异常的检测器相比，我们提出的基于异常的 pan 和 p-nir 数据组合模型不仅不能实现船舶**检测的**最高召回率（在高对比度和低对比度数据集上的召回率为 91.14 和 45.9%)分别)，但也对不同的自动阈值选择技术具有鲁棒性。少

2018 年 4 月 24 日提交;**最初宣布** 2018 年 4 月。

118. 用于网络安全的自动大流量分析

作者:苗元田,阮家,潘雷潘,王宇，张军,杨祥

摘要: 网络流量分析技术是网络安全系统的基石。我们通过三种流行和当代的网络安全应用程序在入侵**检测**、恶意软件分析和僵尸网络**检测**中展示了它的用途。然而，自动流量分析**面临**着大流量数据带来的挑战。针对大数据的三大特征--体积、变化和速度，回顾了缓解实时流量分类、未知流量分类和分类器效率等关键挑战的三种最先进的技术。采用统计特征、未知发现和相关分析的新技术显示出处理大流量数据的广阔潜力。鼓励读者致力于提高网络安全中自动流量分析的性能和实用性。少

2018 年 4 月 24 日提交;**最初宣布** 2018 年 4 月。

119. 低质量图像人脸检测的研究概况

作者:周玉谦,刘丁,黄晓明

摘要: **面部护理检测**是一个很好的探索问题。在前面的工作中，研究**了面**探测器的许多挑战，如极端姿态、照明、低分辨率和小尺度。然而，以前提出的模型大多是在高质量图像上进行培训和测试的，而在监控系统等实际应用中并不总是如此。本文首先回顾了目前最先进的**人脸**检测器及其在基准数据集 fddb 上的性能，并对算法的设计协议进行了比较。其次，我们研究了它们在测试不同模糊、噪声和对比度水平的低质量图像时的性能下降。我们的研究结果表明，手工制作和深度学习的**人**脸探测器对于低质量图像来说还不够坚固。它激励研究人员为野外 **人脸检测**提供更坚固的设计。少

2018 年 4 月 19 日提交;**最初宣布** 2018 年 4 月。

120. 使用隐式 3d 特征的活动性检测

作者:j. matias di martino, qio qio, trishul n 最高, guillermo sapiro

摘要: 欺骗攻击是对现代**人脸**识别系统的威胁。在这项工作中，我们提出了一个简单而有效的活动检测方法，以增强 2d **人脸**识别方法，使其强大的攻击。我们表明，欺骗攻击的风险可以通过使用额外的光源，例如闪光灯来推断。从在不同光照下拍摄的一对输

入图像中，我们定义了隐式包含面部三维形成的判别特征。此外，我们还表明，当考虑多个光源时，我们能够验证哪个光源已经被激活。这使得设计一个高度安全的活动光身份验证框架成为可能。最后，进一步研究了在没有三维重建的情况下使用三维特征的情况，我们引入了从未校准的立体对相机中获得的一种近似的基于程度的隐式 3d 特征。有效性实验表明，在几乎没有特征提取延迟的具有挑战性的场景中，所提出的方法产生了最先进的结果。少

2018 年 4 月 19 日提交;**v1** 于 2018 年 4 月 18 日提交;**最初宣布** 2018 年 4 月。

121. 人脸：大规模变异中一种高效的人脸检测网络

作者:王建峰,叶元,李伯勋,余刚,孙健

摘要: **面部护理检测**是**人脸**识别等许多应用的基础研究课题。特别是随着卷积神经网络的发展，已经取得了令人印象深刻的进展。然而，在高分辨率图像视频中广泛存在的大规模变异问题在文献中并没有得到很好的解决。本文提出了一种新的算法--sface，该算法有效地将基于锚点的方法和无锚法集成起来，解决了规模问题。还引入了一种名为 4k-**人脸**的新数据集，用于评估具有极大规模变化的**人脸检测**性能。sface 架构在新的 4k **面**基准上显示了有希望的结果。此外，我们的方法可以以每秒 50 帧 (fps) 的速度运

行，在标准的 **wider face 数据**集上的精度为 80% ap，在速度上几乎比最先进的算法高出一个数量级，同时实现了比较性能。少

2018 年 4 月 23 日提交;**v1** 于 2018 年 4 月 18 日提交;**最初宣布** 2018 年 4 月。

122. 基于逐行校准网络的实时旋转不变人脸检测

作者:石雪鹏,石光山,明娜，吴淑哲,陈锡林

摘要: 旋转不变人**脸检测**，即**检测**具有任意平面旋转（rip）角度的**人**脸，在无约束的应用程序中被广泛需要，但仍然是一项具有挑战性的任务，因为**脸**的外观的大变化。大多数现有方法都会影响处理大型 rip 变化的速度或准确性。为了更有效地解决这一问题，我们建议进行逐行校准网络（pcn），以粗到细的方式执行旋转不变的**人脸检测**。pcn 由三个阶段组成，每个阶段不仅区分**了人**脸和非**面**，而且还逐步将每个**面候选的** rip 方向校准为垂直。通过将校准过程划分为几个渐进步骤，并且仅在早期阶段预测粗方向, pcn 可以实现精确、快速的校准。通过对与 rip 范围逐渐减小的非人**脸**进行二进制分类, pcn 可以准确地**检测出具有完整的人脸**。360◦ rip 角度。这样的设计导致了实时旋转不变的**人脸**检测器。在多定向 fddb 和一个具有挑战性的开发经济学**者脸**的子集上进行的实验表明，我们的 pcn 取得了很有前途的性能。少

2018 年 4 月 17 日提交;**最初宣布** 2018 年 4 月。

123. 主动交通管理系统中的网络安全问题研究

作 者 :zulqarnain h.khattak, hyungjun park, seongah hong, richard atta boateng, brian l. smith

摘要: 运输机构已引入主动交通管理系统，以管理经常和非经常的挤塞情况。atm 系统依赖于有线和无线网络使组件的互连。不幸的是，这种支持 atm 系统的连接还提供了潜在的系统接入点，从而容易受到网络攻击。随着 atm 系统开始集成物联网 (iot) 设备，这种情况变得越来越明显。因此，有必要严格评估 atm 系统的网络攻击漏洞，并探索在**网络攻击面前**提供稳定性和优雅退化的设计概念。在这项研究中，开发了一个原型 atm 系统和一个实时网络攻击监测系统，用于北维吉尼亚州 i-66 1.5 英里的路段。监测系统通过将 atm 系统生成的车道控制状态与监测系统认为最有可能的车道控制状态进行比较,**检测**出 atm 系统的预期运行偏差。在两组状态之间出现任何偏差的情况下，监控系统将显示由备份数据源生成的车道控制状态。在仿真实验中, atm 原型系统和网络攻击监控系统受到了仿真网络攻击。评价结果表明，在受到网络攻击时，平均速度比 atm 系统下降了 1 5%，与基线情况相似。这说明 atm 系统的有效性被网络攻击所否定。然而，监测系统使自动取款机系统恢复到预期的安全状态，并减少了网络攻击的负面影响。这些结果表明，除了传统的系统入侵防护方法外，还需要重新审视 atm 系统设计概念，以此作为防范网络攻击的一种手段。少

2018 年 4 月 16 日提交;最初宣布 2018 年 4 月。

124. 基于深度学习的 iemocap 数据集多模态情感识别

作者:samarth tripathi, homayoon beigi

摘要: 情感识别已经成为人类计算机互动的一个重要研究领域，因为我们改进了行为各个方面的建模技术。随着技术的进步，我们对情感的理解也在不断提高，对自动情感识别系统的需求也越来越大。研究的方向之一是使用神经网络，它善于估计依赖于大量和多样化输入数据来源的复杂函数。本文试图利用神经网络的这一有效性，使我们能够利用来自语音、文本和运动的数据，从**面部**表达式、旋转和手部运动中的数据，对 iemocap 数据进行多模态情感识别.此前的研究主要集中在 iemocap 数据集上的语音**检测**上，但我们的方法是首次使用 iemocap 提供的多种数据模式进行更可靠、更准确的情绪**检测**。少

2018 年 4 月 16 日提交;最初宣布 2018 年 4 月。

125. binareye: 一种始终具有能量的可扩展二元 cnn 处理器，在 28nm cmos 芯片上具有所有内存

作者:bert moons, daniel bankman, litayang, boris murmann, 玛丽安·维尔赫斯特

摘要: 本文介绍了一种用于始终在线二元卷积神经网络的数字处理器--binareye。该芯片通过神经元阵列利用局部权重触发器最大限度地实现数据重用。它存储完整的网络模型和要素映射，因此不需要片外带宽，从而达到 230 1b-TOPS/W 的峰值效率。它的 3 个层次的灵活性-(a) 重量重新配置，(b) 可编程网络深度和 (c) 可编程网络宽度-允许交易能量的准确性，这取决于任务的要求。binareye 的完整系统输入到标签能耗范围从 14.4 ujp 的 86% cifar-10 和 98% 的所有者识别度下降到 0.92 ujf，以高达每秒 1700 帧**的速度进行 94%**的**人脸**检测。这比最先进的技术更高效，精度高。少

2018 年 4 月 16 日提交;**最初宣布** 2018 年 4 月。

126. 超越交易：以更高的精度加速基于 fcn 的人脸检测器

作者:宋光禄,刘宇,姜明,王玉杰,严俊杰,标岭

摘要: 几年来，全卷神经网络 (fcn) 以其先天性的共享内核滑窗搜索能力主导着**人脸检测**任务的游戏，从而降低了所有冗余计算，以及最新的最先进的方法，如 f 发 rcn, ssd, yalo 和 fpn 使用 fcn 作为他们的骨干。因此，这里有一个问题：我们能否找到一个通用的策略，以更高的精度进一步加速 fcn，从而加快所有最近基于 fcn 的方法？为了对此进行分析，我们将**人脸**搜索空间分解为两个正交方向，即 "尺度" 和 "空间"。在由两个基向量展开的

空间中，只有几个坐标表示前景。因此，如果 fcn 可以忽略大多数其他点，搜索空间和虚警应该被显著淡化。基于这一哲学，一种新的方法，称为尺度估计和空间关注建议 (s2a 个 P) 建议注意图像金字塔中的某些特定比例和有效位置。此外，我们还在注意结果的基础上，采用了掩模卷积操作，以加速 fcn 的计算。实验表明，基于 fcn 的 rpn 方法可以通过 4 个 x 在帮助下 s2a 个 P 同时，它还可以达到最先进的 fdb, afw 和 malf **人脸检测基准.**少

2018 年 6 月 2 日提交;**v1** 于 2018 年 4 月 14 日提交;**最初宣布** 2018 年 4 月。

127. 一种人机交互的实时无监督人脸重新识别系统

作者:王玉江,沈洁,斯塔夫罗斯·佩特里迪斯,马贾·潘蒂奇

摘要: 在人机交互 (hri) 的背景下,**人脸**重新识别 (人脸重新识别) 的目的是验证机器人是否已经观察到某些**检测**到的**人**脸。在社交机器人中，区分不同用户的能力至关重要，因为它将使机器人能够根据用户的个人喜好定制交互策略。到目前为止,**人脸**识别研究取得了很大的成功，但对**人脸**重新识别在社会机器人中的现实应用却很少受到关注。在本文中，我们提出了一个有效的和无监督的**人脸**重新识别系统，同时重新识别多个**人脸**的 hri。该重新识别系统采用深层卷积神经网络提取特征，并采用在线聚类算法来确定**人脸的** id。其性能在两个数据集上进行评估: teresa 机器人收

集的 teresa 视频数据集和 youtube 人脸数据集 (ytf 数据集)。我们证明，优化的技术组合在 terra 数据集上实现了总的 93.55 的精度，在 ytf 数据集上实现了总的 901.41% 的精度。我们将该方法实现到 HCI^2 框架中的软件模块中，以便进一步集成到 teresa 机器人中，并以每秒 10 ~ 26 帧的速度实现了实时性能。少

2018 年 4 月 11 日提交;**v1** 于 2018 年 4 月 10 日提交;**最初宣布** 2018 年 4 月。

128. 宠物对幸福的影响：一种基于社会多媒体的大规模多因素分析

作者:彭雪峰，李启志,罗洁波

文摘: 从减轻压力和孤独，到提高生产力和整体福祉，宠物被认为在人们的日常生活中发挥着重要作用。许多传统研究表明，频繁与宠物互动可以让个人变得更健康、更乐观，最终享受更幸福的生活。然而，这些研究大多不仅在规模上受到限制，而且还可能以主观自我报告、访谈和问卷调查为主要方法，带有偏见。在本文中，我们利用从社交媒体收集的大规模数据和最先进的深度学习技术，对这一现象进行了深入和广泛的研究。我们的研究包括四个主要步骤: 1) 收集约 20, 000 个 instagram 用户的时间表帖子, 2) 使用**人脸检测**和识别 200 万张照片，以推断用户的人口统

计，关系状况，以及是否有孩子，3）通过微笑分类和文本情感分析，基于图像和字幕分析用户的幸福程度，3）应用转移学习技术，重新训练初始空间 3 模型的最后一层进行宠物分类，4)从用户人口统计的多种因素分析宠物对幸福感的影响。我们的主要结果已经证明了我们提出的方法的有效性与许多新的见解。我们认为，这种方法也适用于其他领域，作为一种可扩展、高效和有效的社会行为和心理健康建模和分析方法。此外，为了便于涉及人**脸的**研究，我们还发布了 700k 分析的人脸数据集。少

2018 年 3 月 24 日提交;最初宣布 2018 年 4 月。

129. 一种用于多核机器可扩展内存分配的无阻塞好友系统

作 者 :romolo marotta, mauro ianni , alessandro pellegrini, andrea scarselli, francesco quaglia

摘要: 核心内存分配组件（如 linux 好友系统）的常见实现通过自旋锁同步线程来处理并发分配/发布请求。这种方法显然不容易扩展大线程计数，这一问题已在文献中通过引入分层分配服务或复制核心分配器（分层体系结构中最底层的分配器）得到解决。这两种解决方案都倾向于减少对每个核心分配器的实际并发访问的压力。在本文中，我们探索了内存分配/释放可伸缩性的另一种方法，该方法仍然可以与这些文献建议结合起来。冲突**检测**依赖于读修改-写入（rmw）类中的常规原子机器指令。此外，除了提高可伸缩性和性能之外，它还可以避免将时钟周期浪费在线程的

自旋锁定操作上，而这些线程原则上可以在完全并发的情况下执行内存分配/释放。因此，它可以恢复性能下降--面对并发访问--独立于处理的内存块的当前碎片级别。少

2018 年 5 月 19 日提交;**v1** 于 2018 年 4 月 10 日提交;**最初宣布** 2018 年 4 月。

130. 利用自旋转双麦克风阵列对无人地面机器人进行实时有源化

作者:deepakgala, nathan lindsay, liang sun

抽象: 本工作提出了一种新的技术，只使用新开发的自旋转双麦克风产生的听觉间时差 (itd) 在三维空间中执行声源的定向和距离定位机器人平台。利用状态空间模型在球面坐标系中建立了系统动力学。状态空间模型的可观测性分析表明，当声源放置在 90 和 0 程度。该方法利用三维模型和二维模型分别产生的方位角估计之间的差异，检查零度高程条件，并使用多项式曲线拟合进一步估计高程角方法。此外，该方法还能够**检测到** 90 通过提取 "埋在" 噪声中的零 itd 信号来实现度提升。此外，距离定位是通过首先旋转麦克风阵列面向声源,然后将麦克风垂直于源机器人矢量的固定步数的预定义距离来执行的。麦克风阵列的集成旋转和平移运动仅使用 itd 提示提供完整的方向和距离定位。还开发了一个使用自旋转双麦克风阵列的新型机器人平台，用于执行声源定位的无人地面机器人。该技术首先在仿真中进行了测试，然后

在新开发的机器人平台上进行了验证。还利用安装在 kemar 虚拟头上的麦克风收集的实验数据对所提出的技术进行了测试。结果表明了该技术的有效性。少

2018 年 4 月 10 日提交;**最初宣布** 2018 年 4 月。

131. 基于概率控制的对抗性超声强象自适应

作者:西马,青小关,赵贤峰,刘亚奇

摘要: 深度学习模型容易受到对抗性攻击，从而产生对深度学习模型的特殊输入样本，从而使模型对样本进行错误分类。除了深度学习模型外，对抗攻击对基于特征的机器学习模型也是有效的。本文讨论了对抗性攻击在提高隐写方案抗隐写分析能力方面的应用。我们应用角化神经网络作为对抗生成器。我们的目标是提高典型的空间自适应隐写技术的性能，以实现丰富的模型特征和神经网络的隐身分析。通过控制梯度图之后像素的翻转方向，可以将对抗方法与自适应隐写相结合。隐式的对抗性例子可以使自己"似乎" 无辜的掩护对隐形剂。然而，生成的隐式对抗性例子只能有效地欺骗使用非对抗性例子训练的隐式分析仪。**当面对**使用对抗式实例训练的隐形剂时，可以很容易**地检测**到它们，并且检测错误率很低。对抗性方法使生成的 stego 图像与封面图像更加明显。为了改善这种情况，我们通过将 softmax 层的概率向量修改为特定向量而不是修改类别向量来调整计算梯度图的方法。因此，

生成的对抗示例由 softmax 的概率输出控制。随着调整，对抗方案的性能优于典型的自适应隐写。我们开发了一种实用的双层 stc 对抗对抗性隐写方法。实验证明了该方法在丰富的模型和神经网络上的有效性。少

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

132. 基于单目视觉的微型飞行器群协同定位

作者:sai vemprala, srikanth Saripalli

文摘: 本文提出了一种基于视觉的微型飞行器群协同定位框架。这些车辆都被认为配备了前置单眼摄像头,并能够相互通信。这种协同定位方法建立在分布式算法的基础上，将单个和相对姿态估计技术结合起来，以便组针对周围环境进行本地化。mav 最初**检测**并匹配彼此的显著特征，以创建观察到的环境的稀疏重建，作为全局地图。地图可用后，每个 mav 都执行特征**检测**和跟踪，并进行强大的异常点拒绝过程，以估计其自身的六自由度姿态。有时，mav 还可以通过特征匹配和基于多视图几何的相对姿态计算将相对测量与单个测量融合在一起。介绍了该算法在 microsoft airsim 中模拟的 mav 和环境中的实现，并讨论了协同本地化的结果和优点。少

2018 年 4 月 7 日提交;**最初宣布** 2018 年 4 月。

133. 测试科学软件：一个系统的文献综述

作者:umulee kanewala, james m. bieman

摘要: 背景：科学软件在关键决策中发挥着重要作用，例如，根据气候模型进行天气预报，以及计算研究出版物的证据。最近，由于软件故障导致的错误，科学家不得不撤回出版物。系统测试可以识别代码中的此类错误。目的：本研究旨在确定科学软件测试中**面临**的具体挑战、提出的解决方案和未解决的问题。方法：对相关文献进行系统的文献调查。我们确定了 62 项研究，这些研究提供了有关测试科学软件的相关信息。结果：我们发现，在测试科学软件时**面临**的挑战主要分为两类: (1) 测试由于科学软件的特点而出现的挑战，如甲骨文问题; (2) 测试因科学软件的特点而出现的挑战科学家和软件工程界之间的文化差异，如查看代码和它作为不可分割的实体实现的模型。此外，我们还确定了有可能克服这些挑战及其局限性的方法。最后，我们描述了尚未解决的挑战，以及软件工程研究人员和实践者如何帮助克服这些挑战。结论：科学软件对测试提出了特殊的挑战。具体而言，科学家开发人员和软件工程师之间的文化差异，以及科学软件的特点，使得测试变得更加困难。现有的技术 (如代码克隆**检测)**可以帮助改进测试过程。软件工程师在开发测试技术时，应考虑科学软件带来的特殊挑战，如甲骨文问题。少

2018 年 4 月 5 日提交;**最初宣布** 2018 年 4 月。

134. 通过概率分布预测进行端到端显著性映射

作者:saumya jetley, naila murray, eleonora vig

摘要: 大多数显著估计方法的目的是明确建模低点显著性线索，如边缘或斑点，并可能另外纳入自上而下的线索使用**人**脸或文本**检测**。使用眼睛固定数据训练显著性模型的数据驱动方法越来越流行，特别是随着大规模数据集和深层架构的引入。但是，在后一种范式中，当前的方法使用为分类或回归任务而设计的损失函数，而在地形图上评估显著性估计。在本文中，我们引入了一个新的显著性映射模型，该模型将映射公式化为广义伯努利分布。然后，我们训练一个深层的架构来预测这样的地图使用新的损失函数，配对软最大激活函数与措施设计，以计算概率分布之间的距离。我们在广泛的实验中展示了这种损失函数在四个公共基准数据集上比标准函数的有效性，并展示了比最先进的显著性方法更高的性能。少

2018 年 4 月 5 日提交;**最初宣布** 2018 年 4 月。

135. 将卡通引入生活: 改进卡通人脸检测和识别系统

作者:saurav jha, nikhil Agarwal, suneeta Agarwal

摘要: 鉴于最近在人**脸检测**和识别技术方面的深度学习进步，本文回答了 "他们在漫画中的作用如何" 这个问题--这个领域在很

大程度上仍未被探索直到最近，主要是由于大规模数据集不可用，以及传统方法在这些数据集上的失败。我们的工作研究并扩展了上述任务的多个框架。在**人脸检测**方面，我们采用了多任务级联卷积网络（mtcnn）架构，并将其与传统方法进行了对比。对于**人脸**识别，我们的双重贡献包括：(i) 归纳转移学习方法，将初始 v3 网络的功能学习能力与支持向量机（svm）的特征识别能力结合起来，(ii) 一个拟议的混合卷积神经网络（hcnn）框架训练的融合像素值和 15 个手动定位的面部关键点。所有的方法都在野外卡通**面**(iiit-cfw) 数据库中进行了评估。我们证明，hcnn 模型提供的稳定性优于初始 + 支持向量机的稳定性，而不是更大的输入变化，并探索了合理的体系结构原则。我们证明，初始 + 支持向量机模型建立了一个最先进的 f1 分数的任务性别识别卡通面孔。此外，我们还介绍了一个小型数据库，该数据库承载着卡通**面孔**上 15 点的位置坐标，属于 iiit-cfw 数据库的 50 名公众人物。少

2018 年 7 月 6 日提交;**v1** 于 2018 年 4 月 5 日提交;**最初宣布** 2018 年 4 月。

136. 比较与对比：学习显著的视觉差异

作者:steven chen, ken gruman

摘要: 相对属性模型可以根据所有**检测到**的属性或属性对图像进行比较，详尽地预测哪些图像更美观、更自然，等等，而不考虑排

序。然而，当人类比较图像时，某些差异自然会突出，首先会出现在人们的脑海里。这些最明显的差异，或突出的差异，很可能首先描述。此外，许多差异虽然存在，但可能根本没有提及。在这项工作中，我们介绍和建模突出的差异，一个丰富的新功能，用于比较图像。我们收集最显著差异的实例级注释，并构建一个基于相对属性特征的模型，该模型预测看不见的对的显著差异。我们在具有挑战性的 ut-zap50k 鞋和 lfw10 面数据集上测试我们的模型，并优于一系列基线方法。然后，我们展示了我们的突出模型如何改进两个视觉任务，图像搜索和描述生成，实现人与视觉系统之间更自然的沟通。少

2018 年 4 月 13 日提交;**v1** 于 2018 年 3 月 30 日提交;**最初宣布** 2018 年 4 月。

137. 学习匿名面，以进行隐私保护操作检测

作者:任忠正,李勇, michael s. ryoo

摘要: 人们越来越关注计算机视觉设备通过录制不需要的视频来侵犯用户的隐私。一方面，我们希望摄像系统能够识别重要事件，通过了解其视频来帮助人类的日常生活，但另一方面，我们希望确保它们不会侵犯人们的隐私。在本文中，我们提出了一个新的原则方法来学习视频 \强调 {面对匿名}。我们使用两个竞争系统战斗的对抗训练设置: (1) 视频匿名器，修改原始视频以删除隐私

敏感信息，同时仍在努力最大限度地提高空间动作**检测**性能; (2) 试图从匿名视频中提取隐私敏感信息的歧视者。最终的结果是视频匿名器执行像素级修改，以匿名每个人的**脸**，对操作**检测**性能的影响最小。与传统的手工匿名化方法（包括掩蔽、模糊和添加噪声）相比，我们实验证实了我们的方法的优势。代码、演示和更多结果可以在我们的项目页面 https://jason718.github.io/project/privacy/main.html 中找到。少

2018 年 7 月 26 日提交;**v1** 于 2018 年 3 月 30 日提交;**最初宣布** 2018 年 3 月。

138. 用于篡改人脸检测的双流神经网络

作者:周鹏,韩新通,弗拉德 i. morariu, larry s. davis

文摘: 我们提出了一个用于**人脸**篡改**检测的**双流网络。我们训练 googlenet 检测面部分类流中**的**篡改伪影，并训练基于补丁的三重网络，以利用捕获局部噪声残差和相机特征的功能作为第二流。此外，我们使用两个不同的联机**面**交换应用程序来创建一个新的数据集，该数据集由 2010 年被篡改的图像组成，每个数据集都包含一个被篡改**的面**。我们在新收集的数据集上评估建议的双流网络。实验结果表明了该方法的有效性。少

2018 年 3 月 29 日提交;**最初宣布** 2018 年 3 月。

139. 开放式身份保存人脸综合的研究

作者:简民宝,董晨,方文, 李厚强,姜华

文摘: 我们提出了一个基于生成对抗性网络的框架，将人脸的身份和属性区分开来，这样我们就可以方便地重新组合不同的身份和属性，以实现保身份人脸合成.打开的域。以前的保身份人脸合成过程主要限于合成已在训练数据集中的已知标识的人脸。为了在训练数据集之外合成具有标识的人，我们的框架要求该主体的一个输入图像生成一个标识向量，以及任何其他输入面图像来提取属性矢量捕获，例如，姿势、情感，照明，甚至背景。然后，我们重新组合同一性向量和属性向量，用提取的属性合成一个新的主体面。我们提出的框架不需要以任何方式注释人脸的属性。它具有不对称损耗功能，以更好地保存身份并稳定训练过程。它还可以有效地利用大量未标记的训练面图像，进一步提高被合成面的保真度，而这些主题在标记训练面数据集中没有显示出来。我们的实验证明了所建议的框架的有效性。我们还介绍了它在更广泛的应用中的使用，包括面前化、人脸属性变形和面对对抗示例检测。少

2018 年 8 月 9 日提交;**v1** 于 2018 年 3 月 29 日提交;**最初宣布** 2018 年 3 月。

140. 基于活动的动态人脸检测与跟踪

作者:gregor lenz, sio-hoi ieng, ryad benosman

摘要: 我们提出了第一个纯粹基于事件的方法，使用 atis，一个神经形态**相机的人脸**检测。我们通过将输入帧中的本地活动与预定义范围（定义为特定位置中每秒的事件数）来查找闪烁的眼睛对。如果在范围内，则检查信号是否有额外的约束，如持续时间、同步性和眼睛之间的距离。在注册了一个有效的闪烁后，我们等待在同一位置的第二个闪烁启动高斯跟踪器以上的眼睛。根据他们的位置，在估计**的脸**轮廓周围绘制一个边界框。然后可以跟踪**面**，直到它被遮挡。少

2018 年 3 月 27 日提交;最初宣布 2018 年 3 月。

141. 一种基于卷积神经网络的人脸快速检测方法

作者:郭冠军,王汉子,严燕,金正，李波

摘要: 目前通过卷积神经网络（如 overfeat、r-innn 和 densenet）进行的**人脸或**物体检测方法明确地提取了基于图像金字塔的多尺度特征。然而，这种策略增加了**人脸检测**的计算负担。本文提出了一种基于判别完全特征（dcfs）的人脸快速检测方法，该方法采用精心设计的卷**积神经**网络**提取**,**直接进行人脸检测**。在完整的要素地图上执行。dcfs 表现出了尺度不变性的能力，有利于快速、有希望的人**脸检测**。因此，该方法不需要在传统方法中使用的图像金字塔上提取多尺度特征，这可以大大提高**其人脸检测**效率。

在几种流行**的人脸检测**数据集上的实验结果表明了该方法的有效性 和有效性。少

2018 年 3 月 27 日提交;最初宣布 2018 年 3 月。

142. 人脸取证：一种用于人脸伪造检测的大型视频数据集

作 者 :andreas rössler, davde Cozzolino, luisa verdoliva, christian riess, justus thies, matthias nišner

摘要: 随着计算机视觉和图形的最新发展，现在可以生成具有极其逼真**合成面**的视频，即使是实时的视频也是如此。无数的应用程序是可能的，其中一些发出了合法的警报，呼吁可靠的假视频探测器。事实上，区分原创视频和操纵视频对人类和计算机都是一个挑战，特别是在视频被压缩或分辨率低的情况下，就像在社交网络上经常发生的那样。由于缺乏足够的数据集，对**人脸**操作检测的研究受到严重阻碍。为此，我们引入了一个新的**人脸**操作数据集，其中包含大约 50 万张编辑过的图像 (来自 1000 多个视频)。这些操作是用最先进的**面部**编辑方法生成的。它至少比所有现有的视频操作数据集超出一个数量级。利用我们的新数据集，我们引入了经典图像取证任务的基准，包括分类和分段，同时考虑到不同质量级别的视频压缩。此外，我们还引入了一个基准评估，用于创建具有已知地面真相的无法区分的伪造;例如，生成细化模型。少

2018 年 3 月 24 日提交;最初宣布 2018 年 3 月。

143. 生成对抗性抗性网络技术在图像创建和修改中的比较

作者: Mathijs pieters, marco wiering

摘要: 生成的敌对网络 (gans) 已证明能够成功地生成逼真的真实图像。本文比较了各种 gan 技术，包括监督技术和非监督技术。比较了不同目标功能对训练稳定性的影响。我们在网络中添加了一个编码器，从而可以将图像编码到 gan 的潜在空间。利用深卷积神经网络对发电机、鉴别器和编码器进行参数化。对于鉴别器网络，我们试验使用了一种新的胶囊网络，这是一种检测图像中全局特征的最先进的技术。实验使用数字和**人脸**数据集进行，并使用各种可视化来说明结果。结果表明，利用编码器网络可以重建图像。有了条件 gan，我们可以改变生成或编码图像的视觉属性。与标准的卷积神经网络相比，以胶囊网络为鉴别器的实验产生了质量较低的图像。少

2018 年 3 月 24 日提交;最初宣布 2018 年 3 月。

144. 在微博上描述和检测仇恨用户

作者:manoel horta ribeiro, pedro h.calais, yuri a.santos, Virgílio a. f. almeida, wagner meira jr 。

摘要: 目前描述和**检测**仇恨言论的大多数方法都集中在在线社交网络中发布的 "文本内容" 上。由于 osn 文本的不完备性和噪音性以及仇恨言论的主观性，他们在收集和注释仇恨言论方面**面临着**不足。这些限制通常会受到过度简化问题的约束，例如只考虑包含与仇恨相关的单词的推文。在这项工作中，我们部分解决了这些问题，将重点转向 \textit{users}。我们开发并采用了一种强大的方法来收集和注释可恨的用户，这种方法并不直接依赖于词典，也不依赖于用户的整个配置文件。这就产生了一个推特的转发图样本，其中包含 100 元,386 用户，其中 4 个,972 附加说明。我们还收集了数据收集后三个月内被禁止的用户。我们表明，可恨的用户在活动模式、单词使用以及网络结构方面与正常用户不同。我们获得了类似的结果，比较了可恨的邻居和普通用户的邻居，也暂停了用户和活跃用户的邻居，提高了我们分析的鲁棒性。我们注意到，仇恨用户的联系密密麻麻，因此将仇恨言论**检测**问题表述为通过图表进行半监督学习的任务，利用 twitter 上的连接网络。我们发现，利用图形结构的节点嵌入算法，在检测这两种可恨性（95%auc vs88%非盟委员会）和被停职的用户 (93%auc vs88%非盟委员会)。总之，我们提出了以用户为中心的仇恨言论观点，为更好地**发现**和理解这一相关和具有挑战性的问题铺平了道路。少

2018 年 3 月 23 日提交;**最初宣布** 2018 年 3 月。

145. 用退火对抗性的捆绑程序训练进行图像绘制

作者:杨超章,宋玉航,刘晓峰,唐庆明,郭建华

摘要: 深层生成模型的最新进展显示出具有广阔的潜力，在图像插入，这是指使用已知的上下文预测不完整图像的缺失像素值的任务。但是，现有的方法可能会变慢，或者生成不令人满意的结果，并容易**检测到**缺陷。此外，孔附近往往有可感知的不连续性，需要进一步的后处理来混合结果。我们提出了一种新的方法来解决训练一个非常深的生成模型，以合成高质量的照片写实绘画的困难。我们的模型以条件生成对抗性网络（条件甘肃）为主干，引入了一种新的块式程序训练方案，在提高网络深度的同时，稳定训练。我们还提出了一种新的策略，称为对抗性损失退火，以减少伪影。我们进一步描述了一些专门为涂装而设计的损失，并展示了它们的有效性。大量的实验和用户的研究表明，我们的方法优于现有的方法，在几个任务，如绘画,**人脸**完成和图像协调。最后，我们展示了我们的框架可以很容易地作为交互式引导画的工具，展示了它解决现实世界共同挑战的实用价值。少

2018 年 3 月 27 日提交;**v1** 于 2018 年 3 月 23 日提交;**最初宣布** 2018 年 3 月。

146. 偷偷进入魔鬼的殖民地--网络社交网络中的虚假形态与网络法研究

作 者 :mudasir ahmad wani, suraiya jabin , ghulam yazdani, nehaluddin ahmadd

摘要: 存储在在线社交网络 (osn) 上的大量用户社交、个人和职业生活内容不仅吸引了研究人员和社会分析师的关注，也吸引了网络犯罪分子的关注。这些网络犯罪分子通过建立假个人资料或设计机器人和利用 osn 的弱点进行非法活动，非法渗透到 osn。随着技术的发展，网络犯罪越来越多。每日报告的安全和隐私威胁在 osn 不仅需要智能自动**检测**系统，可以实时识别和缓解假配置文件，而且还需要加强安全和隐私法律，以减少网络犯罪。在本文中，我们研究了不同的 osn 网站上的各种类别的假配置文件，如受损的个人资料，克隆的配置文件和在线机器人 (垃圾机器人，社交机器人，类似机器人和影响机器人)，以及现有的网络法律，以减轻其威胁。为了设计假的个人资料**检测**系统，我们强调了不同类别的假个人资料功能，能够区分不同种类的假实体和真实的。研究人员在构建假个人资料**检测**系统时**面临**的另一个主要挑战是无法获得针对假用户的数据。本文通过提供极其强制的数据收集技术以及一些现有的数据来源来应对这一挑战。此外，还尝试介绍了几种机器学习技术，用于设计不同的假配置文件**检测**系统。少

2018 年 3 月 22 日提交;**最初宣布** 2018 年 3 月。

147. 基于信号游戏的 v2i 公路运营中的错误行为检测

作者:吴曼熙,李进, Saurabh amin, patrick jaillet

摘要: 车辆对基础设施（v2i）通信越来越多地支持高速公路运营，如电子收费、拼车和车辆排装。本文研究了利用 v2i 通信中的安全漏洞对公路运营产生负面影响的个别车辆战略不当行为的诱因。我们考虑 v2i 支持的高速公路段,**面对**两类车辆（代理群体），每类车辆都有对一台服务器（车道子集）的授权访问。车辆具有战略意义，因为它们可能会向系统操作员错误地报告其类（类型），并获得对专用于其他类的服务器的未经授权的访问。这种不当行为会对符合要求的车辆造成额外的拥塞外部性，因此需要加以遏制。我们关注的是一个操作人员能够检查车辆是否有不当行为的环境。检查费用昂贵，成功的**检测**会对行为不当的车辆处以罚款。我们制定了一个信号博弈来研究车辆类别与运营商之间的战略互动。我们的均衡分析提供了控制车辆行为不当或不行为的动机的成本参数的条件。我们还确定了操作人员的均衡检测策略。少

2018 年 8 月 21 日提交;**v1** 于 2018 年 3 月 22 日提交;**最初宣布** 2018 年 3 月。

148. 金字塔盒：一种上下文辅助单发面检测器

作者:徐唐,杜大丹,何泽强，刘景拓

摘要: **面部护理检测已经**研究了很多年，剩下的挑战之一就是在不受控制的环境中**检测**小的、模糊的和部分闭塞的**面孔**。本文提

出了一种新的上下文辅助**单面**检测器，名为 "\ 强调{pyramidboxx}"，用于处理硬**面检测**问题。注意语境的重要性，我们在以下三个方面提高了语境信息的利用率。首先，我们设计了一个新的上下文锚，通过半监督的方法来监督高级上下文特征学习，我们称之为 pyramidanchors。其次，我们建议将适当的高级上下文语义特征和低级面部特征结合起来，这也允许金字塔盒在一次拍摄中预测所有尺度的**人**脸。第三，引入上下文相关结构，提高预测网络的容量，提高输出的最终精度。此外，我们还使用数据锚点采样的方法来增加不同尺度的训练样本，从而增加了较小**面**的训练数据的多样性。通过利用上下文的价值, pyramidbox 在最先进的**性能**中实现了优于两个通用人脸**检测**基准 (fddb 和 wider **face)** 。我们的代码可在 paddlepaddle 中使用: \ href html://github.com/PaddlePaddle/models/tree/develop/fluid/face_detection}{\url{https://github.com/PaddlePaddle/models/tree/develop/fluid/face_detection}}。少

2018 年 8 月 16 日提交;**v1** 于 2018 年 3 月 20 日提交;**最初宣布** 2018 年 3 月。

149. 利用多区域对人脸图像进行热到可见合成

作者:benjamin s. riggan, nathaniel j. short, shuowen hu

文摘: 热面图像中可见光**谱面的**合成是一种很有前途**的异质人脸**识别方法;利用现有的**可见图像**识别软件，并使人工分析师能够更

有效地验证跨频谱匹配。我们提出了一种新的合成方法，通过利用全局（例如，整个**面部**）和局部区域（如眼睛、鼻子和嘴巴）来提高合成的可见图像的鉴别质量。在这里，每个区域提供（1）相应区域的独立表示，(2) 额外的正则化项，这影响合成图像的整体质量。我们分析了使用多个区域从热面合成可见**人**脸图像的效果. 我们证明，与最近发布的合成方法相比，我们的方法提高了跨频谱验证率。此外，利用我们的合成图像，我们报告了面部地标**检测**的结果--通常用于图像注册--这是**人脸**识别过程中的一个关键部分。少

2018 年 3 月 20 日提交;**最初宣布** 2018 年 3 月。

150. 卷积点表示：密集注释图像与三维人脸对齐之间的卷积桥梁

作者:吴玉航,黎安武哈,项旭, ioannis a. kkadadaris

摘要: 我们提出了一个可靠的方法来估计面部姿势和形状信息从一个密集的注释面部图像。该方法依靠卷积点集表示（cpr），一种精心设计的矩阵表示来汇总在带注释图像中检测到的点集中编码的不同层次的信息。cpr 分解了形状和不同姿势参数的依赖关系，并允许通过卷积神经网络和递归层连续更新不同的参数。在更新姿势参数时，我们会对重投影误差和预测方向进行采样，并根据重投影误差的模式更新参数。此技术增强了模型在具有挑战性的情况下搜索本地最小值的能力。我们还证明，来自不同来源的注

释可以在 cpr 框架下进行合并，并有助于超越目前最先进的 3d **人脸**对齐解决方案。实验表明，当密集注释的图像包含噪声和缺失值时，所提出的基于 cprfa (基于 cpr 的**人脸**对齐) 显著提高了三维对齐精度，这在 "野外" 采集方案中很常见。少

2018 年 4 月 2 日提交;**v1** 于 2018 年 3 月 17 日提交;**最初宣布** 2018 年 3 月。

151. 复杂城市激光雷达数据集

作 者 :jeong jyong, young-guncho, young-sikshin, 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。

152. 三维面部表情识别的精确定位和深度学习

作者:asm jan, huasongding, hhying meng, limingchen, huibin li

文摘: 有意义的面部部位可以传达面部动作单元**检测**和表情预测的关键线索。纹理三维**人脸**扫描可以提供详细的三维几何形状和 2d 纹理外观线索的脸，这有利于人脸表情识别 (fer)。然而，准确的面部部位提取以及融合是一项具有挑战性的任务。本文设计了一种基于精确的面部零件提取和面部零件深度特征融合的三维 fer 系统。特别是，每个纹理三维**人脸**扫描首先表示为 2d 纹理贴图和具有一对一密集对应的深度贴图。然后，利用一种新的四级过程提取纹理贴图和深度图的面部部分，包括面部地标定位、面部旋转校正、面部大小调整、面部零件边界盒提取和后处理程序。最后，分别从纹理贴图和深度图中学习了所有面部部位的深度融合卷积神经网络 (cnn) 特征，并利用非线性支持向量机进行表达式预测。在 BU-3DFE 数据库上进行了实验，证明了在相同环境下对不同的面部部位、纹理和深度提示进行梳理并报告最先进的结果的有效性。少

2018 年 3 月 4 日提交;最初宣布 2018 年 3 月。

153. vegac：基于视觉的年龄、性别和面部表情分类--基于卷积神经网络

作 者 :ayesha gurnani，vandit gajjar，viraj mavani ，yash khandhediya

摘要: 本文探讨了视觉显著性在面部图像中对年龄、性别和面部表情进行分类的方法。对于多任务分类，我们提出了基于可视化显著性的 vegac 方法。利用深度多级网络 [1] 和现成的**人脸**检测器 [2]，我们提出的方法首先**检测**测试图像中的**人**脸，并提取 cnn 对裁剪面的**预测**。vegac 的 cnn 从不同的基准对收集到的数据集进行了微调。我们的卷积神经网络 (cnn) 使用 vgg-16 架构 [3]，并在 imagenet 上进行预训练，用于图像分类。我们展示了年龄估计方法、性别分类和面部表情分类方法的有用性。我们在选定的基准上用我们的方法取得了竞争的结果。我们所有的模型和代码都将公开提供。少

2018 年 3 月 13 日提交;**最初宣布** 2018 年 3 月。

154. 深度自适应注意联合面部行动单元检测和人脸对齐

作者:邵志文,刘志雷，蔡建飞,马丽庄

摘要: 面部行动单元 (au)**检测**和**人脸对齐**是两个高度相关的任务，因为面部地标可以提供精确的 au 位置，以便提取有意义的局部特征，用于非盟**检测**。大多数现有的 au **检测**工作通常将**人脸对齐**

视为预处理，并独立处理这两个任务。本文提出了一种新的端到端深度学习框架，用于联合**非盟检测**和**人脸**对齐，这一点还没有得到探讨。特别是首先学习多尺度共享特征，将**人脸**对齐的高级特征输入到非盟**检测**中。此外，为了提取精确的局部特征，我们提出了一个自适应注意学习模块，以自适应地细化每个 au 的注意力图。最后，组装的本地特征与**人脸**对齐特征和用于 au **检测**的全局特征集成在一起。关于 bp4d 和 disfa 基准的实验表明，我们的框架明显优于最先进的 au **检测**方法。少

2018 年 7 月 24 日提交;**v1** 于 2018 年 3 月 15 日提交;**最初宣布** 2018 年 3 月。

155. 面磁：放大功能图，以检测小面

作 者 :pouya samangouei, mahyar najibi, larry davis, rama chellappa

文摘: 本文介绍了**一种基于** fsterrcn 框架的**人**脸检测器--人脸放大镜网络（**人脸**-磁网），它使小尺度**的**判别信息能够流向分类器，没有任何跳过或剩余连接。为了实现这一目标，**face**-magnet 在区域建议网络（rpn）中部署了一组卷转换层（也称为反卷积），并在 "感兴趣区域（roi）" 池图层之前部署了另一组，以便于**检测**更精细**的卷积层。面**。此外，我们还设计、培训和评估其他三个经过良好调整的体系结构，它们代表了规模问题的常规解决方案：上下文池、跳过连接和缩放分区。这三个网络中的每一个都取得

了与最先进的**人脸**探测器相当的结果。通过大量的实验，我们发现基于 vgg16 体系结构的**人脸**-磁体在发展经济学所数据集上的人脸**检测**任务上取得了比最近提出的**基于** resnet 101 的 hr 方法更好的效果。在硬盘上获得与我们的其他方法 ssh 相似的结果。少

2018 年 3 月 14 日提交;**最初宣布** 2018 年 3 月。

156. 融合双目深度和空间金字塔编码微纹理特征的人脸欺骗检测

作者:肖松,徐照,林天伟

摘要: 由于各种情况使得**特征**空间的划分极其复杂，因此强大的特征对于人脸欺骗检测至关重要。因此，本文提出了两个新的、鲁棒性强的反欺骗特征。第一个是基于双目摄像机的深度功能，称为 "模板**面**匹配双目深度" (tfbd) 功能。第二个是基于高级微纹理的特征，称为空间金字塔编码微纹理 (spmt) 特征。介绍了一种新的模板**人脸配**准算法和空间金字塔编码算法以及这两种新的特点。基于这两个鲁棒性特征，实现了多模**态人脸**欺骗**检测**。在广泛使用的数据集和由我们自己构建的综合数据集上进行实验。结果表明，与我们提出的特点融合在一起的**人脸**欺骗**检测**具有较强的鲁棒性和时间效率，同时也优于其他最先进的传统方法。少

2018 年 3 月 13 日提交;**最初宣布** 2018 年 3 月。

157. 用于面部地标检测的样式聚合网络

作者:董宣义,严燕,万里欧阳,易阳

文摘: 面部地标**检测**的最新进展通过从**面部**形状和姿势的丰富变形中学习判别特征而取得成功。除了**人**脸本身的方差，图像样式的内在差异，如灰度与彩色图像、光线与暗、强与沉闷等，也一直被忽视。这个问题变得不可避免，因为越来越多的 web 图像是从各种来源收集的训练神经网络。在这项工作中，我们提出了一种风格聚合的方法来处理大的内在方差的图像样式的面部地标检测。我们的方法通过生成的对抗模块将原始**人**脸图像转换为风格聚合图像。该方案使用风格聚合图像来维护对环境变化更稳健的**人脸**图像。然后，伴随着风格聚合的原始**人**脸图像进行二重唱，训练一个相互补充的地标性探测器。通过这种方式，对于每个**面**，我们的方法以两个图像作为输入，即一个在其原始样式中，另一个在聚合样式中。在实验中，我们观察到图像样式的大方差会降低面部地标探测器的性能。此外，我们通过与我们方法的变体相比，显示了我们的方法对图像样式的大方差的鲁棒性，在这种变体中，生成对抗模块被删除，并且不使用样式聚合图像。与最先进的基准数据集 aflw 算法和 300-w. code 相比，我们的方法表现良好，可在 github 上公开使用: https://github.com/D-X-Y/SAN 以下

2018 年 3 月 22 日提交;**v1** 于 2018 年 3 月 11 日提交;**最初宣布** 2018 年 3 月。

158. 我们建立了一个假新闻 & amp; 点击诱饵过滤器：接下来发生了什么会打击你的头脑!

作 者 :georgi karadzhov, pepa gencheva, preslav nakov, ivan koychev

摘要: 这是完全惊人的!假新闻和点击诱饵完全侵入了网络空间。让我们**面对**现实吧：每个人都恨他们有三个简单的原因。理由 #2 绝对会让你吃惊。这些在选举时能够取得的成就将完全打击你的心灵!现在，我们都同意，这不能继续下去，你知道，必须有人阻止它。所以，我们做了这个关于假新闻/点击诱饵**检测**的研究，相信我们，这是完全伟大的研究，它真的是!别搞错了这是有史以来最好的研究!说真的，来看看，我们都有：神经网络、注意力机制、情感词汇、作者分析，你给它起个名字。词汇特征，语义特征，我们绝对拥有一切。我们已经完全测试过了，相信我们!我们有结果，也有数字，真的很大的数字。有史以来最好的数字!哦，和分析，绝对一流的分析。兴趣？来阅读有关假新闻和点击诱饵在保加利亚网络空间的令人震惊的真相。你不会相信我们发现了什么!少

2018 年 3 月 10 日提交;**最初宣布** 2018 年 3 月。

159. 稳定和一致的成员资格，可快速扩展

作 者 :lalith suresh, dahlia malkhi, parik 粪 gopalan, ivan portocarreiro, zeeshan lokhandwala

文摘: 我们提出了快速，分布式会员服务的设计和评估。在 rapid 的核心是一个多进程剪切**检测**(cd) 的方案，它围绕两个关键的见解: (i) 它怀疑一个过程失败后，警报从多个来源到达，和 (ii) 当一组进程遇到问题，它**检测**整个组的故障，而不是单独总结每个进程。实现这些见解转化为简单的成员资格算法，通信开销较低。我们提供的证据表明，我们的策略几乎可以在任何地方推动一致**检测**，即使在出现复杂的网络条件 (如单向可达性问题、防火墙配置错误和数据包丢失) 时也是如此。此外，我们还提出了经验证据和分析，证明几乎无处不在的检测发生的概率很高。为了完成设计，快速包含一个无引线的共识协议，可将多进程切割**检测**转换为视图更改决策。生成的成员服务既适用于完全分散的模式，也适用于逻辑集中模式。我们提出了一个评估快速在中等可扩展的云设置。快速引导 2000 节点群集比现行工具 (如成员列表和 zookeeper) 快 2-5.8 倍,**在复杂**的故障情况下保持稳定，并提供强大的一致性保证。快速很容易集成到现有的分布式应用程序中，我们演示了其中的两个应用程序。少

2018 年 3 月 9 日提交;**最初宣布** 2018 年 3 月。

160. 2^B3^C: 2 框 3 作物的面部图像的性别分类与卷积网络

作者:vandit gajjar

摘要: 本文以深度学习的方法对面部图像中的性别分类进行了探讨。我们的卷积神经网络 (cnn) 使用 vgg-16 架构 [1], 并在 imagenet 上进行预训练, 以进行图像分类。我们提出的方法 (2^B3^C) 首先**检测面部**图像, 将**检测到的人**脸的边缘增加 50%, 用两个盒子裁剪**面部**三个裁剪方案 (左、中、右裁剪) 并摘录美国有线电视新闻网对裁剪计划的预测。我们的方法的 cnn 是微调的协助和 lfw 与性别注释。通过在 alence 上实现 90.8 的分类, 并在 lfw 数据集上实现 95.3% 的竞争分类精度, 证明了该方法的有效性。此外, 为了检查我们的方法的真正能力, 我们的性别分类系统在考虑实时场景的 gpu 上的帧速率为 7-10 fps (帧/秒)。少

2018 年 3 月 5 日提交;**最初宣布** 2018 年 3 月。

161. 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。

162. 无监督的面部表现学

作者:samyak datta, gaurav sharma, c. v. jawahar

文摘: 我们提出了一个方法，在不受监督的培训 cnn，以学习歧视性**的脸**表示。我们挖掘监督培训数据，指出同一视频帧中的多个**面必须**属于不同的人，而跨多个帧跟踪的同一**面**必须属于同一个人。我们无需使用任何手动监控即可从数百个视频中获取数百万**张面孔**对。尽管从视频中提取的人脸的**空间**分辨率低于作为标准监督**人**脸数据集（如 lfw 和 casia-webface）的一部分提供的人，但前者表示了一个更为逼真的设置，例如大多数**检测到**的人脸都很小的监控场景。我们使用从收集到的视频帧中提取的相对较低**的分辨率面对** cnn 进行培训，并在基准的 lfw 数据集上实现更高的验证精度，参见手动制作的要素（如 lbp），甚至超过了最先进的深度网络，如 vgg-**脸**，当他们被制成工作与低分辨率的输入图像。少

2018 年 3 月 3 日提交;**最初宣布** 2018 年 3 月。

163. 解开基于深度学习的人脸识别对疟疾攻击的鲁棒性

作 者 :gaurav goswami, nalini ratha,akshay agarwal, richa singh, mayank vatsa

摘要: 基于深度神经网络 (dnn) 的体系结构模型具有较高的表达能力和学习能力。然而，它们本质上是一个黑匣子方法，因为它是不容易的数学制定在其许多层表示中学习的函数。认识到这一点，许多研究人员已经开始设计方法，以利用基于深度学习的算法的缺点质疑其鲁棒性，并暴露其奇异性。在本文中，我们试图解开与人**脸**识别的 dnn 的鲁棒性相关的三个方面: (i) 评估深度架构对**人脸**识别的影响，即常见攻击的漏洞观察到现实世界中的扭曲，这些扭曲是用浅薄的学习方法以及基于学习的对手很好地处理的;(ii) 通过描述深部网络隐藏层中的异常过滤器响应行为来**检测**奇点;(iii) 对处理管道进行更正，以缓解这一问题。我们的实验评估使用多个开源的基于 dnn 的**人脸**识别网络，包括 openface 和 vgg-face，以及两个可公开使用的数据库 (meds 和 pasc)，证明了深度学习的性能基于人**脸**识别算法在这种失真的情况下可能会受到很大的影响。并将该方法与现有**的检测**算法进行了比较，结果表明，该方法能够利用中隐藏层的响应适当地设计分类器，从而非常准确地**检测**到攻击。网络。最后，我们提出了几种有效的对策，以减轻对抗攻击的影响，并提高基于 dnn **的人脸**识别的整体鲁棒性。少

2018 年 2 月 22 日提交;**最初宣布** 2018 年 3 月。

164. 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来生成面部模型，以便以后与拍摄的低质量**的面孔**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，互相关联匹配的 cnn、树干分支合奏 cnn 和 haarnet) 和监督的自动编码器 (例如，规范**面**) 的深度学习架构表示美国有线电视新闻网) 审查和比较的准确性和计算复杂度。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。

165. 百万富翁：众包的一种有指导的方法

作 者 :bo han, quming yao, yuangang pan, ivor w. tsang , xiaquuixiao, 焦强, masashisugiyama

摘要: 现代机器学习正在迁移到复杂模型的时代，这需要大量注释良好的数据。虽然众包是实现这一目标的一个有希望的工具，但现有的众包方法几乎无法获得足够数量的高质量标签。本文以百万富翁游戏节目中的 "吸引人而暗示" 的回答策略为动力，将提示引导的方法引入众包中，以应对这一挑战。我们的方法鼓励工人在不确定问题时从提示中获得帮助。具体而言，我们提出了一个混合阶段设置，包括主阶段和提示阶段。当工人在主舞台上**面临**任何不确定的问题时，他们被允许进入暗示阶段，在做出任何答案之前先寻找暗示。开发了一种独特的支付机制，满足众包的两个重要设计原则。此外，拟议的机制进一步鼓励高素质的工人减少使用提示，这有助于确定和分配更多可能的报酬。在 amazon 机械土耳其人身上进行的实验表明，我们的方法确保了足够数量的低支出的高质量标签，并**检测**到高质量的工人。少

2018 年 3 月 6 日提交;**v1** 于 2018 年 2 月 26 日提交;**最初宣布** 2018 年 2 月。

166. 从稳健锚点的角度看小脸

作者:朱晨根,兰涛,霍阿卢,马里奥斯·萨维德斯

文摘: 本文介绍了一种新的锚杆设计，以支持基于锚杆的人**脸检测**，实现卓越的尺度不变性能，特别是在微小**的人脸**上。为了实现这一点，我们明确解决了基于锚点的探测器在体积小的**面**(例如小于 16x16 像素) 上大幅下降性能的问题。在本文中，我们将调查为什么会出现这种情况。我们发现，目前的锚定设计不能保证微小**的面**和锚箱之间的高重叠，这增加了训练的难度。提出了新的预期最大重叠 (emo) 分数，可以从理论上解释低重叠问题，并激发几个有效的策略，新的锚定设计导致更高**的脸**重叠，包括锚杆的跨步减少与新的网络架构、额外的移动锚点和随机**人脸**移位。综合实验表明，我们提出的方法明显优于基于基线锚杆的检测器，同时在具有竞争力的具有挑战性的**人脸检测**数据集上不断取得最先进的结果运行时速度。少

2018 年 2 月 25 日提交;**最初宣布** 2018 年 2 月。

167. 基于社会医学的大规模自定义睡眠不足疲劳模式分析

作者:彭雪峰,罗洁波,凯瑟琳·格伦，李启志,詹景耀

摘要: 疲劳的复杂性引起了各学科研究人员的极大关注。短期疲劳可能会导致驾驶时的安全问题;因此，动态系统被设计用来跟踪驾

驶员疲劳。长期疲劳可能导致慢性综合征，并最终影响个人的身心健康。传统的疲劳评估方法不仅需要先进的设备，而且需要大量的时间。本文试图通过对人体面部暗示的审视，开发一种新的、有效的预测个体疲劳率的方法。我们的目标是根据自拍预测疲劳率。为了将疲劳率与用户行为联系起来，我们从 instagam 上的 10 480 个用户那里收集了近 100 万个时间线帖子。我们首先检测所有的**面孔**，并使用自动算法识别他们的人口统计数据。接下来，我们调查不同年龄、性别和族裔群体的疲劳分布情况。这项工作是评估睡眠不足疲劳的一种有希望的方法，我们的研究为通过社交媒体大规模用户疲劳建模提供了一个可行和有效的计算框架。少

2018 年 2 月 22 日提交;**最初宣布** 2018 年 2 月。

168. 生物信息学软件的质量保证：利用变形测试测试生物医学文本处理工具的案例研究

作者:madhusudan srinivasan, morteza pourreza shahri, umulee kanewala, indika kahanda

摘要: 生物信息学软件在包括医学和保健在内的许多领域作出关键决定方面发挥着非常重要的作用。然而，大多数研究都是针对开发工具的，很少花时间和精力测试软件，以确保其质量。在测试中，测试甲骨文用于确定测试在测试过程中是否通过或失败，不幸的是，对于大部分生物信息学软件来说，确切的预期结果并没

有得到很好的定义。因此，与对生物信息学软件进行系统测试相关的主要挑战是甲骨文问题。变形测试（mt）是一种用于测试**面临**甲骨文问题的程序的技术。mt 使用变质关系（mr）来确定测试是否已通过或失败，并指定输出应如何根据对输入所做的特定更改进行更改。在这项工作中，我们使用 mt 来测试 lingpipe，这是一种使用计算语言学处理文本的工具，通常用于生物信息学中的生物实体识别，从生物医学文献中识别。首先，我们确定了一组用于测试任何生物实体识别程序的 mr。然后，我们开发了一组测试用例，可用于使用这些 mr 测试 lingpipe 的生物实体识别功能。为了评估此测试过程的有效性，我们会自动生成一组有故障的 lingpipe 版本。通过对实验结果的分析，我们观察到我们的 mr 可以**检测**到这些错误版本的大部分，这表明这种测试技术在生物信息学软件质量保证方面的效用。少

2018 年 2 月 20 日提交;最初宣布 2018 年 2 月。

169. 使用 "不偷看" 自动编码器检测异常面

作者:anand bhattad, jason rock, david forsyth

摘要: **检测**异常**面**具有重要的应用。例如，系统可能会判断火车司机何时因医疗事件而丧失能力，并协助采取安全恢复策略。这些应用程序要求很高，因为它们需要准确**检测**只有在运行时才能看到的罕见异常。这样的设置会导致受监督的方法执行得很差。我

们描述了一种检测满足这些要求的异常**人脸**图像的方法。我们构造了一个可靠地具有大的异常图像输入的特征向量，然后使用各种简单的无监督方法根据特征对图像进行评分。明显的构造（自动编码器代码；自动编码器残差）被自动编码器中的 "窥视" 行为所击败。我们的功能结构从图像中删除矩形补丁，使用经过专门训练的自动编码器预测基于图像其余部分的修补程序的可能内容，然后将结果与图像进行比较。高分表明，自动编码器很难预测补丁，因此很可能是异常的。我们证明了我们的方法可以识别典型图像池中的真实**异常**人脸图像，这些图像来自于 celeb-a，比最先进的实验要大得多。基于我们的方法，用另一组正常的名人形象进行了控制实验--"典型的一组"，但非名人 a 并不被认定为异常;证实这不是因为庆祝 a 的特殊特性。少

2018 年 2 月 15 日提交;**最初宣布** 2018 年 2 月。

170. 通过表演表中的引文引发的不完整的锦标赛对最先进的论文进行排名

作 者 :mayank singh, rajdeep sarkar, Pawan goyal, animesh mukherjee, soumen Chakrabarti

摘要: 我们如何才能为特定的任务找到最先进的纸张？是否有可能根据标准基准的性能，以论文之间部分订单的形式自动维护排行榜？我们能否**在**一些指标改进但另一些指标降低的论文中检测到潜在的异常？引文计数是否可用于早期**检测**表现最好的论文？

在这里，我们回答这些问题，同时描述我们的经验，建立一个新的文献计量系统，有力地挖掘实验性能从论文。我们提出了一个新的性能锦标赛图，以论文为节点，边缘编码嘈杂的性能比较信息从论文中提取。这些提取类似于不完整的比赛中比赛的结果(嘈杂)。如果它们是完整和完全可靠的，编译排名将是微不足道的。**面对**嘈杂的提取，我们提出了几种方法来对论文进行排名，确定其中最好的论文，并表明商业学术搜索系统在寻找最先进的论文时惨败。在科学的稳步发展中，我们发现在表演锦标赛中广泛存在周期，这暴露了潜在的异常和重现性问题。利用计算机科学 27 个领域广泛使用的最先进论文列表，我们证明我们的系统能够有效地建立可靠的排名。我们的代码和数据集将被放置在公共领域。少

2018 年 2 月 13 日提交;最初宣布 2018 年 2 月。

171. 测试代理：自适应、自主和智能测试用例

作者:edward Enoiu, mirgita frasheri

摘要: 软件规模的增长、缺乏执行回归测试的资源以及未能更快地**检测** bug，都使人们更加依赖持续集成和测试自动化。即使有更多专门用于测试自动化的硬件和软件资源，软件测试**也面临着**巨大的挑战，导致对自动化测试用例选择和优先排序的复杂机制的依赖程度增加。持续集成框架的一部分。这些机制目前正在使用

称为测试用例的简单实体，这些实体被具体实现为可执行脚本。我们的主要想法是通过使用智能软件代理的概念，为测试用例提供更多的推理、自适应行为和学习能力。我们将此类测试用例称为测试代理。作为测试代理基础的模型能够灵活和自主地操作，以满足总体测试目标。我们的目标是通过让测试代理自己知道何时应该执行、如何更新其目的以及何时应彼此交互，来加强回归测试的分散性。在本文中，我们设想了显示这种自适应自治行为的软件测试代理。特别是在软件测试中寻求使用自适应自治代理的新研究中，探索了测试代理使用方面的新发展和挑战。少

2018 年 2 月 12 日提交;**最初宣布** 2018 年 2 月。

172. 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。

173. 深层视觉域适应：一项调查

作者:王梅,邓伟宏

文摘: 深域自适应已成为一种新的学习技术，可以解决大量标记数据不足的问题。与传统的学习共享特征子空间或使用浅层表示重用重要源实例的方法相比，深域自适应方法利用深层网络通过嵌入域来学习更多可转移的表示在深度学习的管道中进行适应。对浅域适应进行了全面的调查，但很少有人及时回顾新出现的深度学习方法。本文对计算机视觉应用的深域适应方法进行了全面的综述，得出了四大贡献。首先，我们根据定义两个域如何不同的差异化的数据属性，对不同的深域自适应方案进行分类。其次，我们将基于训练损失的深度领域自适应方法分为几个类别，并简要分析和比较了这些类别下的最新方法。第三，概述了超越图像分类的计算机视觉应用，如**人脸**识别、语义分割和目标**检测**。第四，强调了现行方法的一些潜在缺陷和今后的几个方向。少

2018 年 5 月 24 日提交;**v1** 于 2018 年 2 月 10 日提交;**最初宣布** 2018 年 2 月。

174. 对公开数据集上皮肤检测方法的公平比较

作者:alessandra 卢米尼, loris nanni

摘要: 皮肤**检测**是在数字图像中识别皮肤和非皮肤区域的过程，广泛应用于从手势分析到跟踪身体部位和**人脸检测**等多个应用。皮肤**检测**是一个具有挑战性的问题，引起了研究界的广泛关注，但由于缺乏共同的基准和统一的测试协议，很难对各种方法进行公平的比较。在这项工作中，我们研究了这一领域的最新研究，并提出了使用几种不同数据集的方法之间的公平比较。这项工作的主要贡献是一个框架，以评估和结合不同的皮肤探测器方法，其源代码将免费提供给未来的研究，并广泛的实验比较几个最近的方法也被用来定义一个在许多不同的问题上很好地工作的合奏。在 10 个不同的数据集上进行了实验，其中包括超过 10000 张标记的图像: 实验结果证实，这里提出的组合与其他独立方法相比取得了非常好的性能，而不需要临时的参数调整。本文提出的测试和集成框架的 matlab 版本将从 (https://www.dei.unipd.it/node/2357 + 模式识别和集成分类器) 免费提供。少

2018 年 2 月 7 日提交;**最初宣布** 2018 年 2 月。

175. 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%，并在显示合理代码结构的同时，在视觉亲和力方面对目标模型进行了精确镜像的原型应用程序。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。

176. 基于迁移学习的野外微笑检测

作者:xin guo, luisa f. polanía, kenneth e. barner

文摘: 来自无约束面部图像的微笑**检测**是一个专门的、具有挑战性的问题。作为最翔实的表达之一，微笑传达了基本的潜在情感，如快乐和满足，这导致了多种应用，如人类行为分析和互动控制。与**人脸**识别数据库的大小相比，用于训练微笑**检测**系统的标记数据要少得多。为了利用**人脸**识别数据集中的大量标记数据，缓解微笑**检测**的过度拟合，提出了一种有效的基于学习的微笑**检测**方法。与以前使用手工设计的功能或从零开始训练深层卷积网络的作品不同，我们探索并微调了一个训练有素的深**面**识别模型，以便在野外**检测笑容.**通过对具有不同输入的人脸识别模型进行微调，包括从 genki-4k 数据集生成的对**齐**、未对齐和灰度图像，构建了三种不同的模型。实验表明，该方法实现了最先进的性能。本文还对该模型对噪声和模糊伪影的鲁棒性进行了评价。少

2018 年 1 月 17 日提交;**最初宣布** 2018 年 2 月。

177. 使用改进的更快的 rcnn 进行人脸检测

作者:张长正,徐翔,杜丹丹

文摘: 更快的 rcnn 在通用目标检测方面取得了巨大的成功，包括 pascal 目标**检测**和 ms coco 目标**检测**。在本报告中，我们提出了一个详细设计的更快 rcn 方法，名为 fdnet1.0 的人**脸检测**。采用了多尺度训练、多尺度测试、光设计 rcnn、一些推理技巧和

基于语音的集成方法等技术。我们的方法通过发展经济学**所 face 验证**数据集 (简单设置、中集、硬集) 在三个任务中实现了两个第 1 位和一个第 2 位。少

2018 年 2 月 6 日提交;**最初宣布** 2018 年 2 月。

178. 一种遮挡堆叠沙漏定位与遮挡估计的方法

作者:kevan yuen, mohan m. trivedi

摘要: 司机安全的一个关键步骤是观察司机的活动,**脸**是这个过程中提取头部姿势、眨眼率、打哈欠、与乘客交谈等信息的关键一步，这样可以帮助获得更高层次的信息，比如分心，嗜睡，意图，和他们在哪里寻找。在行车安全的背景下，系统在恶劣的照明和遮挡下进行鲁棒估计是很重要的，但也能**检测**到遮挡发生的时间，以便从**面部**遮挡部位预测信息可以适当地考虑。本文介绍了封闭堆叠沙漏玻璃，基于原有的堆叠沙漏网的工作，身体姿态关节估计，其中重新训练，以处理**检测到的人**脸窗口和输出 68 闭塞热图，每个对应于面部地标。从这些热图中提取具有里程碑意义的位置、遮挡水平和精细**的人脸检测**分数，以消除误报。使用面部地标位置，可以提取头部姿势和张口开放等特征，以获得驾驶员的注意力和活动。对该系统进行了定量和定性的人**脸检测**、头部姿态和野外数据集遮挡估计的评估，并显示了最新的结果。少

2018 年 2 月 5 日提交;**最初宣布** 2018 年 2 月。

179. 用于监测铁路操作人员班次的人脸识别

作者:s ritika, dattaraj rao

摘要: 火车飞行员是一项非常乏味和压力很大的工作。飞行员必须时刻保持警惕，很容易忘记轮班时间。在美国这样的国家，飞行员被法律授权坚持 8 小时轮班。如果他们的班次超过 8 小时，铁路可能会因为司机过度疲劳而受到处罚。当 8 小时的轮班可能在旅途中结束时，就会出现这个问题。在这种情况下，新司机必须转移到正在运行的换班机车位置。因此，在司机轮班期间对其进行准确的监控，并确保正确安排班次，对铁路来说非常重要。在这里，我们提出了一个自动化的摄像系统，使用安装在机车驾驶室内的摄像头，以不断记录视频源。对这些源进行实时分析，以**检测**驾驶员的**面部**，并使用最先进的深度学习技术识别驱动程序。其结果是提高了火车飞行员的安全性。摄像机从驾驶室内连续捕获存储在车载数据采集设备上的视频。利用先进的计算机视觉和深度学习技术，定期对视频进行分析，以**检测**飞行员的存在并识别飞行员。使用基于时间的分析，可以确定该移位处于活动状态的时间。如果此时间超过分配的班次时间，则会向调度发送警报以调整班次时间。少

2018 年 5 月 21 日提交;**v1** 于 2018 年 2 月 5 日提交;**最初宣布** 2018 年 2 月。

180. 基于模糊逻辑和双边滤波器的图像预置

作者:mahmoud afifi

摘要: 图像后页是将具有大量色调的图像转换为具有不同平面区域和较少的色调的合成图像。在本技术报告中，我们介绍了使用模糊逻辑的实现和结果，以便以简单、快速的方式生成后置图像。图像滤波是基于模糊逻辑和双边滤波的;其中，给定的图像是模糊的，以删除小细节。然后，使用模糊逻辑将每个像素分为三个特定类别中的一个，以减少颜色的数量。此筛选器是在构建**"人脸"** 数据集上的 "规范" 时开发的，目的是为数据集中的原始**人**脸图像添加新的难度级别。此滤波器不会影响人体**检测**性能;然而，它被认为是逃避**面部检测**过程的障碍。这种滤镜通常可用于图像的后验，尤其是那些具有较高对比度的图像，以获得生动的颜色图像。少

2018 年 2 月 3 日提交;**最初宣布** 2018 年 2 月。

181. 扩展网络: 无地标, 深, 3d 面部表情

作者:chen-juchang, anh tuan tran, tal h 斯纳, iacopo masi, ram nevatia, gerard medioni

文摘: 我们描述了一种基于深度学习的三维面部表情系数估计方法。与以前的工作不同，我们的过程不会将面部地标**检测**方法作为一个代理步骤进行中继。最近的方法表明, cnn 可以直接从图

像强度中训练出准确和判别的三维可变形模型 (3DMM) 表示。通过上述面部地标**检测**，这些方法能够估计在前所未有的野外观察条件下出现的遮挡**面**的形状。我们在这些方法的基础上，表明面部表情也可以通过一个强大的，深，无地标的方法来估计。我们的 expnet cnn 直接应用于**人脸**图像的强度，并回归一个 29d 矢量的 3d 表达系数。我们提出了一种独特的数据采集方法来训练这个网络，利用深部网络对训练标签噪声的鲁棒性。我们进一步提供了一种评估估计表达系数准确性的新方法：通过测量它们在 ck + 和情感识别基准上捕捉面部情绪的程度。我们表明，我们的 expnet 产生的表达系数，更好地区分面部情绪比那些获得的状态，面部地标**检测**技术。此外，随着图像比例的下降，这一优势也在增长，这表明我们的 expnet 比具有里程碑意义的**检测**方法更易于扩展更改。最后，在相同的精度水平下，我们的 expnet 比它的替代品快了数量级。少

2018 年 2 月 1 日提交;**最初宣布** 2018 年 2 月。

182. 分裂的国家？一种利用文本和投票检测偏好亲和力块的多网络方法

作者:caleb pomeroy, niheer dasandi, slava j. mikhaylov

摘要: 本文为一个新兴的文献做出了贡献，该文献将选票和文本与投票和文本同时建模，以更好地理解所表达的偏好的两极分化。

它根据自然语言处理和网络科学文献的发展----即保留的单词嵌入----提出了一种在国际关系等多维环境中估计偏好两极分化的新方法。人类语言的宝贵的语法素质，以及多层网络中的社区**检测**，这些网络将密集连接的行为者定位在多个复杂的网络中。我们发现，同时使用这些工具有助于更好地估计各国在联合国投票和发言中表达的外交政策偏好，而超出了仅投票允许的范围。这些定位亲和力块的效用通过在国际关系中的冲突爆发的应用得到了证明，尽管这些工具将引起所有**面临**偏好测量和两极分化的学者的兴趣。多维设置。少

2018 年 2 月 1 日提交;**最初宣布** 2018 年 2 月。

183. 独立判断的一个合理的分布式过程层次的描述

作者:ardavan s. Nobandegani , ioannis n. psaromiligkos

摘要: 如果人类缺乏区分相关因素和不相关的能力--计算能力，那么面对在不确定的情况下每天做出无数决定，世界会显得多么混乱，这是不可想象的相当于处理概率独立性关系。大脑高度并行和分布式的计算机制表明，人类独立判断的一个令人满意的过程级描述也应该模仿这些特征。在这项工作中，我们提出了第一个理性的，分布式的，消息传递，过程级的独立判断的帐户，称为 D*.有趣 D*显示了一种奇怪的，但正常的倾向，快速**检测**依赖关系，只要他们持有。此外 D*在最坏情况下的运行时间方面，它的

性能优于 ai 文献中之前提出的所有算法，最近在神经科学调查贝叶斯网络可能实现的神经级工作支持了这一算法的一个显著方面。D*很好地说明了对认知合理性的追求如何能够导致发现具有吸引人的特性的最先进的算法，其简单性使 D*可能是一个很好的教学对象的候选人。少

2018 年 1 月 30 日提交;最初宣布 2018 年 1 月。

184. 使用 md5 校验和延迟云服务中的变化来增强拜占庭容错能力

作者:c sathya, s agilan, a g aruna

摘要: 云计算管理超越了典型的人类叙事。然而，如果虚拟系统不能有效地设计为容忍拜占庭故障，则可能导致执行错误的任务，而不是云崩溃。云可以从崩溃中恢复，但无法从信誉的丧失中恢复。此外，除非虚拟系统旨在**检测**、容忍和消除此类故障，否则任何数量的复制或故障处理措施都无助于**应对**拜占庭故障。然而，为解决拜占庭断层所做的研究并没有提供令人信服的解决方案，因为它们在**检测**拜占庭断层方面的能力有限。因此，本文将云系统建模为一个离散系统，以确定虚拟系统在不同时间间隔下的行为。延迟变化变量作为与虚拟节点关联的预期处理延迟偏差的度量，从 p {低、正常、高、极值} 集合中获取值。同样，检查和错误变量，甚至计算内部节点没有连接到 tcp 任何 ip 堆栈的值从

p {无错误，错误} 的集合。然后，这些条件由错误事件的发生表示，这些事件会导致特定的组件模式从安全故障转换为故障停止或拜占庭易发。少

2018 年 1 月 26 日提交;最初宣布 2018 年 1 月。

185. 预测大型网上服务供应商的可疑账户活动

作者:hassan halawa, matei ripanu, konstantin beznosov, baris coskun, mezhu liu

文摘: **面对**大规模的自动化社会工程攻击大型在线服务，快速**检测**和修复受损的帐户对于限制新攻击的传播和减轻对用户的总体损害至关重要,公司，和广大公众。我们提倡基于机器学习的全自动方法: 我们开发了一个预警系统，利用账户活动跟踪来预测哪些账户今后可能会受到损害，并产生可疑活动。我们假设，这一预警是更及时**地发现**受损账户从而加快补救的关键。我们通过在一家大型在线服务提供商的实验中展示了该系统的可行性和适用性，该测试使用了涵盖数亿用户的四个月的真实生产数据。我们证明了--即使只使用登录数据以较低的计算成本推导特征，以及基本的模型选择方法--我们的分类器可以进行调整，以实现良好的分类精度，当用于预测。我们的系统在最多一个月前正确识别帐户后来标记为可疑的精确，召回，和假阳性率，这表明该机制可能被证明是有价值的操作设置，以支持更多的层防御。少

2018 年 1 月 25 日提交;最初宣布 2018 年 1 月。

186. 提高卷积神经网络性能的手工饲养特性

作者:sedeidhsadat hosseini, seok heelee, nam ik cho

摘要: 由于卷积神经网络 (cnn) 需要为给定的问题找到正确的特征，因此对手工制作的特征的研究在目前有些被忽视。在本文中，我们表明，为给定的问题找到一个合适的功能可能仍然很重要，因为它们可以提高基于 cnn 的算法的性能。具体而言，我们表明，在年龄/性别估计、**人脸检测**和情感识别等与**人脸**有关的作品中，为美国有线电视新闻网提供适当的功能可以提高其性能。我们使用 gabor 筛选银行响应来完成这些任务，并将它们与输入图像一起提供给 cnn。图像和 gabor 响应的堆栈可以作为张量输入提供给 cnn，也可以作为融合图像的加权总和，作为图像和 gabor 响应的加权总和。gapor 筛选器参数也可以根据给定的问题进行调整，以提高性能。通过大量的实验表明，所提出的方法比传统的仅使用输入图像的基于 cnn 的方法具有更好的性能。少

2018 年 1 月 23 日提交;最初宣布 2018 年 1 月。

187. 情绪身体手势识别的调查

作 者 : Fatemeh noroozi, ciprian adrian corneanu, dorotakaminšska, tomasz Kamińska, sergio Escalera, Gholamreza anbarjafari

摘要: 自动情感识别在过去十年中已成为一个趋势性的研究课题。虽然基于面部表情或言语的作品比比皆是，但从身体手势中识别影响仍然是一个不太被探索的话题。我们提出了一项新的综合调查，希望能促进这一领域的研究。我们首先介绍情感身体手势作为通常所说的 "肢体语言" 的一个组成部分，并评论性别差异和文化依赖等一般方面。然后，我们定义了一个完整的框架，自动情感身体手势识别。我们在 rgb 和 3d 中介绍了人**的检测**和评论、静态和动态身体姿态估计方法。然后，我们从情感表达手势的图像中评论最近有关表象学习和情感识别的文献。我们还讨论了将语音或**面部**与身体手势相结合的多模态方法，以提高情感识别能力。虽然预处理方法 (如人体**检测**和姿态估计) 是当今成熟的技术，完全用于鲁棒的大规模分析，但我们表明，对于情感识别，标记数据的数量很少，因此没有关于明确定义的输出空间和表示的一致是浅薄的，在很大程度上基于天真的几何表示。少

2018 年 1 月 23 日提交;**最初宣布** 2018 年 1 月。

188. 价值存储中的乐观执行

作 者 :duong nguyen, aleksey charapko, sandeep kulkarni, murat demirbas

摘要: cap 定理的局限性意味着，如果在存在网络分区的情况下需要可用性，则必须牺牲顺序一致性，这是一种更自然的系统设计一致性模型。我们关注的问题是，如果设计人员的算法具有顺

序一致性，但却**面临**一个底层键值存储，该存储提供了较弱（例如，最终或因果）的一致性，则她应该做什么。我们提出了一种基于**检测**回滚的方法：设计人员识别一个正确性谓词（如 p），并继续运行协议，因为我们的系统监视 p。如果违反 p（因为基础键值存储提供了较弱的一致性），系统将回滚并在 p 保持的状态下恢复计算。我们在伏地魔键值存储中评估了这种方法。我们在 amazon aws 上部署伏地魔的实验表明，与顺序一致性相比，使用最终与监控的一致性可以提高 20-40% 的吞吐量。我们还表明，监视器本身的开销很小（通常小于 8%），**检测**冲突的延迟非常低。例如，在不到 1 秒的时间内**检测到** 99.9% 以上的违规情况。少

2018 年 1 月 22 日提交;**最初宣布** 2018 年 1 月。

189. 质量分类图像分析在人脸检测与识别中的应用

作者:杨飞,张谦,王妙辉,邱国平

摘要: 运动模糊、注意力不集中、空间分辨率不足、有损压缩等诸多因素都会导致图像质量低下。然而，图像质量在传统模式识别文献中却是一个基本被忽视的问题。本文以**人脸检测**和识别为例，表明图像质量是影响传统算法性能的重要因素。我们证明了最重要的不是图像质量本身，而是训练集中的图像质量应该与测试集中的质量相似。为了处理现实世界中可以将不同类型和严重程度的图像呈现给系统的实际应用场景，我们开发了一个高质量的分

类图像分析框架，以自适应地处理混合质量的图像。我们首先使用深层神经网络根据图像的质量等级对其进行分类，然后为每个质量类中的图像设计一个单独的**人脸**检测器和识别器。我们将给出实验结果，表明我们的质量分类框架能够根据图像退化的类型和严重程度对图像进行精确分类，并能显著提高最先进的**人脸**检测器的性能。识别器，以处理包含混合质量图像的图像数据集。少

2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

190. 功能相似代码片段动态检测面临的挑战

作 者 :florian deissenboeck, lars heinemann, benjamin hummel, stefan wagner

摘要: 经典的克隆**检测**方法几乎无法找到独立开发的冗余代码，即不是复制和粘贴的结果。为了自动检测这种功能类似的独立原点代码，我们尝试了一种动态**检测**方法，将随机测试应用于选定的代码块，类似于江苏和苏的方法。我们发现，这种方法在应用于不同的 java 系统时**面临着**一些限制。本文详细介绍了我们对动态检测功能相似的代码片段所面临的挑战的见解。我们的研究结果支持了关于检测方法的有根据**的讨论**，并作为未来研究的起点。少

2018 年 1 月 18 日提交;最初宣布 2018 年 1 月。

191. 降网：一种用于基于视频的人脸对齐的经常性编码解码器网络

作者:西鹏,罗杰里奥 s. 费里斯,王晓宇 , dimitris n. metaxas

文摘: 提出了一种基于递归编码器解码器网络模型的视频实时**人脸**对齐方法。我们提出的模型预测了二维面点热图通过**检测**和回归损失进行的规律性，同时独特地利用了空间和时间维度的递归学习。在空间层面，我们在组合输出响应映射和输入之间添加了反馈环路连接，以便使用单个网络模型实现迭代卷到精细的**人脸**对齐，而不是依赖于传统的级联模型集成。在时间层面，我们首先将网络瓶颈中的特征与时间变量（如姿势和表达式）以及时间不变因素（如身份信息）分离。然后将时间递归学习应用于解耦的时间变异特征。我们表明，这样的特征解对于测试时产生了更好的泛化和更准确的结果。我们进行了全面的实验分析，显示了我们提出的模型的每个组件的重要性，以及优于最先进的结果和我们的方法在标准数据集中的几个变化。少

2018 年 1 月 16 日提交;**最初宣布** 2018 年 1 月。

192. 基于分段的部分面的人脸属性检测方法

作者:upal mahbub, sayantan sarkar, rama chellappa

文摘: 从**面检测**属性的最先进方法**几乎**总是假定存在完整的、不封闭的**面**。因此，对于部分可见和遮挡的**面**，它们的性能会降低。本文介绍了一种基于深卷积神经网络的深卷积神经网络方法，该方法是为在部分遮挡**面**中执行属性**检测**而明确设计的。该方法以多个面部段和全**面作为**输入，采用数据驱动的方法来确定哪些特征是局部的。网络的独特体系结构允许由多个细分来预测每个属性，从而实现委员会机器技术，将本地和全局决策结合起来，以提高性能。通过访问基于分段的预测，splitface 可以很好地预测那些在**面部**可见部分局部化的属性，而不必依赖整个**面部**的存在。我们使用 celeba 和 lfwa 的面部属性数据集进行标准评估。我们还修改了这两个数据集，以遮挡**面**，从而评估属性**检测**算法在部分**面上的**性能。我们的评估表明，splitface 的性能明显优于其他最近的方法，特别是对于部分**面.**少

2018 年 1 月 10 日提交;最初宣布 2018 年 1 月。

193. 驱动程序嗜睡检测的长期多粒度深层框架

作者:lyu, z 子 jian yuan, dapeng chen

摘要: 对于从视频中**检测到**的现实中驾驶员嗜睡，头部姿势的变化非常大，全球**面孔**上现有的方法无法提取有效的特征，如靠边站和降低头部。不同长度的时间依赖关系也很少被前面的方法所考虑，例如打哈欠和说话。在本文中，我们提出了一个长期的多粒

度深框架，以**检测**司机嗜睡的驾驶视频包含正面面。该框架包括两个关键组成部分: (1) 多粒度卷积神经网络 (mcnn)，一个新的网络利用一组平行的 cnn 提取器在不同粒度的对齐面部补丁，并提取面部表示有效地处理了头部姿态的较大变化，并能灵活地融合主要部位的详细外观线索和局部到全局空间约束;(2) 在面部表示上应用深层长期记忆网络，探索序列帧长度可变的长期关系，能够区分具有时间依赖性的状态，如眨眼和闭上眼睛.在公共 nthu-ddd 数据集的评估集中，我们的方法的精度达到了 90.05%，速度约为 37 fps，这是驾驶员睡意**检测**的最先进方法。此外，我们还构建了一个新的数据集 fi-ddd，它对时间维度中的昏昏欲睡位置具有较高的精度。少

2018 年 1 月 8 日提交;**最初宣布** 2018 年 1 月。

194. henet：一种关于英特尔的深度学习方法®用于有效漏洞检测的处理器跟踪

作者:李晨, salmin sultana, ravi sahita

文摘: 本文介绍了一种分层集成神经网络 henet，用于对硬件生成的控制流跟踪进行分类，用于恶意软件**检测**。到目前为止，基于深度学习的恶意软件**检测**一直专注于分析可执行文件和运行时 api 调用。静态代码分析方法由于模糊代码和对抗摄动而**面临挑战**。在执行过程中收集的行为数据更难以混淆，但最近的研究表

明，针对基于 api 调用的恶意软件分类器的攻击是成功的。我们研究基于控制流的程序执行特征，以构建可靠的深度学习恶意软件分类器。henet 由一个低级行为模型和一个顶级集成模型组成。低级模型是每个应用程序的行为模型，通过对执行的控制流跟踪生成的时间序列图像进行传输学习进行训练。我们使用英特尔® 处理器跟踪启用处理器，用于低开销执行跟踪，并设计轻量级图像转换和控制流跟踪的分段。顶级集成模型聚合所有跟踪段的行为分类，并**检测**攻击。硬件跟踪的使用增加了我们系统的可移植性，而深度学习的使用消除了功能工程的人工工作。我们根据 pdf 阅读器的实际开发情况来评估 henet。与传统的机器学习算法相比, henet 在测试集中实现了 100% 的精度和 0% 的假阳性，并获得了更高的分类精度。少

2018 年 1 月 8 日提交;**最初宣布** 2018 年 1 月。

195. 人脸闪烁：一种基于光反射的安全活动检测协议

作者:唐迪,周哲,张银谦,张克环

摘要: **人脸**认证系统越来越普遍，尤其是随着深度学习技术的快速发展。然而，人类面部信息很容易被捕获和复制，这使得**面部**身份验证系统容易受到各种攻击。活动**检测**是防止此类攻击的重要防御技术，但现有的解决方案并不能提供明确而有力的安全保障，特别是在时间方面。为了克服这些限制，我们提出了一种名为 "

人脸闪烁"的新的活动检测协议，该协议大大提高了在**人脸**身份验证系统上成功发起攻击的门槛。通过在屏幕上随机闪烁设计良好的图片并分析反射光，我们的协议利用了人**脸**的物理特征：以光速进行反射处理、独特的文本特征和不均匀的 3d 形状.我们的协议与屏幕和数码相机的工作机制合作，能够**检测到**攻击过程中留下的微妙痕迹。为了演示**人**脸闪烁的有效性，我们实现了一个原型，并对从实际场景中收集的大型数据集进行了彻底的评估。结果表明，我们的时间验证能够有效地**检测**合法身份验证与恶意案例之间的时间差距。我们的**人脸**验证还可以准确地区分二维平面和 3d 对象。我们的活动**检测**系统的整体精度为 98.8%，并在不同的情况下对其鲁棒性进行了评估。在最坏的情况下，我们的系统的精度下降到仍然很高的 97.3%。少

2018 年 8 月 22 日提交;**v1** 于 2018 年 1 月 5 日提交;**最初宣布** 2018 年 1 月。

196. 基于区域的基于最佳匹配的基于虚拟现实社交媒体的 3d 人脸重建

作 者 : Gholamreza anbarjafari, rain eric haamer, iiris lusi, toomas tikk, lembit valgma

摘要: 虚拟现实 (vr) 的使用呈指数级增长，由于许多研究人员已经开始致力于开发新的基于虚拟现实的社交媒体。为此，重要的是要有一个像他们一样的用户的化身，以便很容易地由可访问的

设备，如手机生成。本文提出了一种利用手机摄像机图像或视频数据再现三维人**脸**模型的新方法。该方法更注重模型形状而不是纹理，以使**人**脸可识别。我们**检测**到 68 个面部特征点，并使用它们将**面部**分成 4 个区域。对于每个区域，都会找到最佳的拟合模型，并进一步进行变形组合，以找到每个区域的最佳拟合模型。然后将这些组合并进一步变形，以恢复原始的面部比例。我们还提出了一种对生成的模型进行纹理处理的方法，其中使用上述特征点为生成的模型生成纹理少

2017 年 12 月 12 日提交;**最初宣布** 2018 年 1 月。

197. 重温电子邮件欺骗攻击

作者:胡航,王刚

摘要: 电子邮件系统是抵御网络钓鱼和社交工程攻击的核心战场，但电子邮件提供商在对传入电子邮件进行身份验证方面**仍然面临关键**挑战。因此，攻击者可以应用欺骗技术模拟受信任的实体来进行高度欺骗性的网络钓鱼攻击。在这项工作中，我们研究电子邮件欺骗来回答三个关键问题: (1) 电子邮件提供商如何**检测**和处理伪造的电子邮件？(2) 在什么条件下伪造电子邮件可以穿透防御，到达用户收件箱？(3) 伪造的电子邮件进入后，电子邮件提供商如何警告用户？警告真的有效吗？我们通过对 35 个流行电子邮件提供商 (数十亿用户使用) 的端到端测量以及由模拟和

网络钓鱼实验组成的广泛用户研究 (n = 913) 来回答这些问题。我们有四个关键发现。首先，大多数流行的电子邮件提供商都有**必要的**协议来检测欺骗，但仍然允许伪造的电子邮件进入用户收件箱 (例如，雅虎邮件, icloud, gmail)。其次，一旦伪造的电子邮件进入，大多数电子邮件提供商对用户没有警告，特别是在移动电子邮件应用上。一些提供商 (如 gmail 收件箱) 甚至具有误导性的 ui，使伪造的电子邮件看起来真实。第三，一些电子邮件提供商 (9/35) 对未经核实的电子邮件实施了视觉安全提示，这表明对减少危险用户行为产生了积极影响。将模拟实验与现实的网络钓鱼测试进行比较，我们观察到，当用户在现实环境中措手不及时，安全提示的影响就不那么重要了。少

2018 年 1 月 2 日提交;**最初宣布** 2018 年 1 月。

198. "就像狼中的羊": 微博上仇恨用户的特征

作者:manoel horta ribeiro, pedro h.calais, yuri a.santos, Virgílio a. f. almeida, wagner meira jr 。

摘要: 在线社交网络 (osn) 中的仇恨演讲对公司和政府来说是一个关键的挑战，因为它影响到用户和广告商，而且有几个国家对这种做法有严格的立法。这促使在推特 、社交媒体的帖子和评论中发现和描述这一现象。然而，由于 osn 数据的噪音大、现象稀少、仇恨言论定义的主观性等原因，这些方法**仍存在**一些缺陷。

这项工作提出了一个以用户为中心的仇恨言论视图，为更好的**检测**方法和理解铺平了道路。我们收集推特数据集 100 元,386 用户以及高达 200 人推特从他们的时间表与一个随机步行基于爬虫在转发图，并选择一个子样本 4 个,972 手动注释为可恨或不通过众包。我们检查用户活动模式、可恨用户和普通用户之间传播的内容以及采样图中的网络中心度测量之间的差异。我们的结果显示，可恨的用户有更多的最新帐户创建日期，更多的状态，和跟踪每天。此外，他们还喜欢更多的推特，在更短的时间间隔内发微博，在转发网络中更核心，这与经常与这种行为相关的 "独狼" 定型观念相矛盾。仇恨的使用者更多的是消极的，更多的是亵渎，使用更少的词与仇恨，恐怖主义，暴力和愤怒等主题。我们还发现了仇恨的普通用户和他们的 1 邻域之间的相似之处，暗示了强烈的同音。少

2018 年 1 月 14 日提交;**v1** 于 2017 年 12 月 31 日提交;**最初宣布** 2018 年 1 月。

199. 对位酶剽窃的检测方法

作者:维克多·汤普森

摘要: 对抄袭**是抄袭侦查**系统**面临**的难题之一。当文本在词汇或句法上被改变以看起来不同，但保留其原意时，就会发生解释。大多数抄袭**检测**系统 (其中许多是商业的) 都是为了**检测**单词的同现

和光的修改而设计的，但无法**检测到**严重的语义和结构变化，例如什么是在许多学术文献中看到。因此，许多转述抄袭案件没有被发现。本文通过提出**一种检测**释义文本中最常用的技术（现象）的方法（即：词法替换、插入删除和单词和短语）来探讨转译抄袭问题。重新排序），并将这些方法组合到一个转述检测模型中。我们评估了我们提出的包含释义文本的集合的方法和模型。实验结果表明，与单独运行方法相比，组合方法（提出的模型）的性能有了显著提高。结果表明，所提出的转译检测模型的性能优于标准基线（基于贪婪的字符串倾斜），以及以往的研究。少

2017 年 12 月 29 日提交;**最初宣布** 2017 年 12 月。

200. 苦艾网络：检测和修改对抗实例

作者:陈洁峰,孟子航,孙长田，唐伟，朱英伦

摘要: 尽管深度神经网络在最近的研究和应用中取得了巨大的成功，但它仍然容易受到人类无法察觉的对抗性扰动的影响。为了解决这个问题，我们提出了一个新的网络，称为 reabsnet，以实现高分类精度面对各种攻击。该方法是用监护人网络增强现有的分类网络，以**检测**样本是否自然或受到敌对干扰。关键的是，我们不是简单地拒绝对抗性的例子，我们修改他们，以获得他们真正的标签。我们利用了这样的观察，即包含对抗性扰动的样本有可

能在修改后返回到其真正的类别。我们证明，我们的 reabsnet 在各种对抗攻击下的表现优于最先进的防御方法。少

2017 年 12 月 21 日提交;最初宣布 2017 年 12 月。

201. 铁路轨道开关一次性检测的暹罗神经网络

作者:dattaraj j rao, shruti mittal, s. ritika

文摘: 深度学习方法已被广泛用于分析视频数据，通过对图像帧进行分类和**检测**对象来提取有价值的信息。我们描述了一种独特的方法，使用视频馈送从移动机车连续监测铁路轨道和**检测**重要的资产，如开关上的轨道。这里使用的技术被称为暹罗网络，它使用两个相同的网络来学习两个图像之间的相似性。在这里，我们将使用一个暹罗网络来持续比较轨道图像，并检测轨道中**的**任何显著差异。交换机将是不同的图像之一，我们将找到一个映射，明确区分交换机与其他可能的轨道异常。然后将推广同样的方法，以**检测**铁路轨道上的任何异常。铁路运输是独特的，因为它有轮式车辆，火车由机车拉，在接近每小时 200 英里的高速上在有制导的铁轨上运行. 铁路网络上的多个轨道使用一种名为 switch 或道岔。交换机可以手动操作，也可以通过控制中心的命令自动操作，它控制列车在网络的不同轨道上的移动。这些开关的准确位置对铁路来说非常重要，在现场真实了解它们的状态很重要。现代列车使用**面向**轨道的高清摄像机，不断从轨道上录制视频。

我们使用暹罗网络并与基准图像进行比较，描述了一种监视跟踪和突出显示异常的方法。少

2017 年 12 月 21 日提交;最初宣布 2017 年 12 月。

202. 不分类时：在测试时对 dnn 分类器的异常检测攻击 (ada)

作者:david j. miller, yulia wang, george kesidis

摘要: 最近广泛部署的基于机器学习的系统 (包括深度神经网络 (dnn)) 面临的一个重大威胁是对抗式学习攻击。我们分析了可能的测试时间回避攻击机制，并表明，在某些重要情况下，当图像受到攻击时，正确分类时没有效用: i) 从攻击者的缓存中选择 (甚至是任意) 图像;ii) 当分类器决定的唯一接收者是攻击者时。此外，在某些应用程序域和方案中，检测攻击是高度可操作的，而不管它面对的是正确的分类 (如果没有**检测到**攻击，仍然会执行分类)。我们假设，即使人类无法察觉的，对抗性扰动是机器检测的.我们提出了一个纯粹的无监督异常探测器 (ad)，与以前的工作不同: i) 使用高度合适的零假设密度模型 (特别是与 rlu 层的非负支持匹配) 对深层的关节密度进行建模;ii) 利用多个 dnn 图层;iii) 利用 "源" 和 "目标" 类概念、源类不确定性、类混淆矩阵和 dnn 权重信息构建基于 kulllebleblеr 发散的新决策统计信息。在三种突出的攻击策略下，我们在 mnist 和 cifar-10 图像数据库上进行了测试，我们的方法优于以往的**检测**方法，在两次攻

击中实现了强大的 roc auc **检测**精度，并且比最近具有更好的精度报告了在最强（cw）攻击上的各种方法。我们还评估了对我们系统的完全白盒攻击。最后，我们评估了其他重要的性能度量，如分类精度，相对于**检出**率和攻击力。少

2018 年 6 月 27 日提交;**v1** 于 2017 年 12 月 18 日提交;**最初宣布** 2017 年 12 月。

203. 多任务流形深度学习的多模态人脸姿势估计

作者:洪朝群,余军

文摘: 人**脸**姿势估计的目的是用二维图像估计凝视方向或头部姿势。它给出了一些非常重要的信息，如交际手势、显著**性检测**等，近年来引起了人们的广泛关注。然而，它是具有挑战性的，因为复杂的背景，不同的方向和**面对外观**的可见性。因此,**人脸**图像的描述性表示和将其映射到姿势是至关重要的。本文利用多模态数据，提出了一种新的人**脸**姿态估计方法，该方法采用了一种新的深度学习框架--多任务流式深度学习 m2dl.它以改进的深部神经网络特征提取和多任务学习的多模态映射关系为基础。在提出的基于深度学习的框架中，流形正则化卷积层（mrcl）通过学习神经元输出之间的关系来改善传统的卷积层。此外，在提出的映射关系学习方法中，将不同的**人脸**表示模式自然结合起来，学习从**人脸**图像到姿势的映射函数。通过这种方式，改进了具有多个任务的

计算映射模型。在三个具有挑战性的基准数据集上的实验结果 dpos、hpid 和 bkhpd 显示了 m2dl. 少

2017 年 12 月 18 日提交;最初宣布 2017 年 12 月。

204. 基于深度学习的铁路轨道特定交通信号选择

作者:s ritika, shruti mittal, dattaraj rao

摘要: 随着铁路运输行业积极走向自动化，准确定位和库存路边轨道资产，如交通信号，道口，开关，里程等是至关重要的。随着新的积极列车控制 (ptc) 规定的生效，许多铁路安全规则将直接与里程和信号等资产的位置挂钩。将根据列车在路边资产方面的位置执行较新的速度规定。因此，铁路必须有一个关于这些资产的类型和地点的准确数据库。本文讨论了一个真实世界的用例，即从安装在移动机车上**的**摄像机检测铁路信号并跟踪其位置。该摄像机经过设计，可承受行驶中列车上的环境因素，并以每秒 30 帧左右的速度提供一致的稳定图像。利用先进的图像分析和深度学习技术，在这些相机图像中**检测到**信号，并创建了其位置的数据库。铁路信号与道路信号在形状和轨道放置规则方面有很大差异。由于空间限制和城市地区的交通密度，信号没有放在轨道的同一侧，多条线路可以平行运行。因此，有必要将**检测到**的信号与列车运行的轨道联系起来。我们提出了一种方法，将信号与它们所属的特定轨道联系起来，使用安装在引线机车上的前**置**摄像头

的视频馈送。一个轨道**检测**、感兴趣的区域选择、信号检测的管道**已经**实现，在覆盖 150 公里的线路上，总的精度为 94.7%，有 247 个信号。少

2017 年 12 月 17 日提交;**最初宣布** 2017 年 12 月。

205. 移动云计算中的网络攻击检测：一种深度学习方法

作 者 :khoi khac nguyen, dinh thai hoang, dusit niyato, ping wang, diep nguyen, Niyato dutkiewicz

摘要: 随着移动应用和云计算的快速增长，移动云计算引起了学术界和业界的极大兴趣。但是，移动云应用程序正**面临数据**完整性、用户机密性和服务可用性等安全问题。对此类问题的预防性方法是在网络威胁可能对移动云计算系统造成严重影响之前**对**其进行检测和隔离。在本文中，我们提出了一个新的框架，利用深度学习方法来**检测**移动云环境中的网络攻击。通过实验结果，我们表明，我们提出的框架不仅识别不同的网络攻击，而且在**检测**攻击时达到了较高的准确性 (高达 97.11%)。此外，我们还介绍了与当前基于机器学习的方法的比较，以证明我们提出的解决方案的有效性。少

2017 年 12 月 16 日提交;**最初宣布** 2017 年 12 月。

206. 深度图像头的头的面朝下估计

作 者 :guido borghi, matteo fabbri, roberto vezzani, simone calderara, rita cucchiara

摘要: 深度摄像机可以为人们的监控和行为理解建立可靠的解决方案，特别是当不稳定或照明条件差导致普通 rgb 传感器无法使用时。因此，我们提出了一个完整的框架，仅基于深度图像来估计头部和肩部的姿势。头部**检测**和定位模块也包括在内，以便开发一个完整的端到端系统。框架的核心元素是一个卷积神经网络，称为 poseidon +，它作为输入接收三种类型的图像，并提供姿势的三维角度作为输出。此外，基于确定性条件 gan 模型的面深组件能够从相应的深度图像中产生幻觉. 我们的经验证明，这对系统性能有积极的影响。我们在两个公共数据集 (biwi kinect 头姿势和 ICT-3DHP) 和潘多拉 (潘多拉) 上测试了拟议的框架，这两个数据集主要受汽车设置的启发。实验结果表明，该方法基于强度和深度输入数据，克服了近期的几项先进作品，以每秒 3 0 帧以上的速度实时运行。少

2018 年 8 月 30 日提交;**v1** 于 2017 年 12 月 12 日提交;**最初宣布** 2017 年 12 月。

207. fhedn：一种基于上下文建模的特征层次编码解码器解码器网络，用于人脸检测

作者:周泽勋,何忠石,陈子玉，贾元元，王海燕, 杜景龙,陈定定

摘要: 受天气条件、相机姿势和范围等因素的影响。在从室外监控摄像头或门禁系统收集的图像中，物体通常很小、很模糊、被遮挡和多样化。对于公安领域的**人脸**识别系统来说，准确**地检测人脸**是一个具有挑战性和重要意义的问题。本文设计了一种基于上下文建模结构的基于上下文建模结构的特征层次编码解码器网络(fhedn)，该结构可以通过层次结构**检测**小的、模糊的、遮挡的**人脸**. 从结束到开始的层次结构喜欢编码器解码器在一个单一的网络。所提出的网络由多个上下文建模和预测模块组成，用于**检测**小的、模糊的、遮挡的和多样化的姿态**面**。此外，还分析了训练组分布、默认箱的规模和收货场规模对**实施**阶段检测性能的影响。通过实验证明，我们的网络在发展经济学**所** face 和 fdb 基准上取得了很有希望的性能。少

2017 年 12 月 11 日提交;**最初宣布** 2017 年 12 月。

208. 使用级联回归重建三维面部表情

作者:吴方子,李松南,赵天浩,王恩吉恩根,吕生

文摘: 提出了一种新的单幅图像三维人脸表情重建模型拟合算法。从单一图像中**重建人脸**表情是计算机视觉中一项具有挑战性的任务。最先进的方法将输入图像与 3d 可变形模型 (3DMM) 相匹配。这些方法需要解决随机问题，不能处理表达式和姿态变化。为了解决这个问题，我们采用了三维**人脸**表达模型，并采用了一个对

缩放、旋转和不同照明条件具有鲁棒性的组合特征。该方法应用级联回归框架来估计 3DMM 的参数。**检测**到 2d 地标，并将其用于初始化 3d 形状和映射矩阵。在每次迭代中，都会估计当前 3DMM 参数与地面真相之间的残留物，然后使用以更新 3d 形状。还根据更新的形状和 2d 地标计算映射矩阵。利用了局部斑块的 hog 特征以及三维地标投影和二维地标之间的位移。与现有方法相比，该方法具有较强的表达和姿态变化，可以重建出更高的保真**三维人脸**形状。少

2018 年 8 月 17 日提交;**v1** 于 2017 年 12 月 10 日提交;**最初宣布** 2017 年 12 月。

209. 混合眼心定位，采用级联回归和手工制作的模型拟合

作者:alex levinshtein, edmund phung, parham aarabi

文摘: 我们提出了一种新的用于眼睛中心**检测**的级联回归器。以前的方法从**面部**或眼动仪开始，使用高级功能或强大的回归器进行眼睛中心定位，但不是两者兼而有之。相反，我们使用现有的面部特征对齐方法更准确地**检测**眼睛。我们通过使用高级功能和强大的回归机制来提高本地化的鲁棒性。与大多数其他不细化回归结果的方法不同，我们通过添加一个鲁棒的圆拟合后处理步骤来提高本地化的准确性。最后，使用简单的手工制作的眼睛中心定位方法，我们展示了如何训练级联回归器，而不需要手动注释训练

数据。我们对我们的新方法进行了评估，并表明它在 biid、gi4e 和 talkingface 数据集上实现了最先进的性能。在平均归一化误差为 e & lt; 0.05 时，对手动注释数据进行训练的回归器的准确率为 99.07% (biid)、99.27 (gi4e) 和 95 5.68% (talkingface)。自动训练的回归体几乎同样好，准确率为 93.9 (biid)、99.27 (gi4e) 和 954.46% (talkingface)。少

2017 年 12 月 7 日提交;最初宣布 2017 年 12 月。

210. 超级风扇：集成的面部地标定位和超分辨率的现实世界中的低分辨率的人脸在任意的姿势与 gans

作者:adrian bulat, ge 奥尔基奥斯·齐米罗普洛斯

摘要: 本文讨论了两个具有挑战性的任务：提高低分辨率面部图像的质量，并准确定位如此糟糕的分辨率图像上的面部地标。为此，我们做出以下 5 个贡献: (a) 我们提出 superfan：第一个同时处理这两个任务的端到端系统，即提高**人脸**分辨率和**检测**面部地标。新颖性或超级 fan 在于通过热图回归和优化新的热图损耗，将人脸对齐的子网络集成在基于 gan 的超分辨率算法中。(b) 我们说明联合培训这两个网络的好处，不仅在正面图像 (如以前的工作) 上报告良好的结果，而且在面部姿势的整个光谱上报告良好的结果，不仅在合成的低分辨率图像上报告，而且在现实世界中报告图像。(c) 我们提出了一种新的基于残差的架构,**从而**改进

了最先进的表面超分辨率。(d) 从数量上看，我们在**面对**超分辨率和对齐方面都显示出比最先进的技术有了很大的改进。(e) 从质量上讲，我们首次在现实世界的低分辨率图像上显示出良好的结果。少

2018 年 3 月 27 日提交;**v1** 于 2017 年 12 月 7 日提交;**最初宣布** 2017 年 12 月。

211. 规模问题：社区检测算法的比较分析

作者:paul wwen 卖方 iii, feng wang

摘要: 了解社交媒体的社区结构至关重要，因为它具有广泛的应用范围，如好友推荐、用户建模和内容个性化。现有的研究使用结构指标，如模块化和电导率和功能指标，如地面真相来衡量的资格的社区发现的各种社区检测算法，而忽略了自然和重要的维度，社区规模。最近，人类学家邓巴建议，社交媒体中稳定社区的规模应该限制在 150 个，被称为邓巴的数字。在本研究中，我们提出了一种系统的算法比较方法，通过正交化地将社区规模作为一个新的维度集成到现有的结构度量中，以一致和全面地评估社交媒体环境下的社区质量。我们设计了一种基于启发式集团的算法，该算法控制具有可调参数的社区的大小和重叠，并与 twitter 网络和 dblp 网络上的五种最先进的社区**检测**算法一起对其进行评估。具体来说，我们根据发现的社区的大小分为四个类，称为亲

密的朋友，偶然的朋友，熟人，和只是一**张脸**，然后计算的覆盖面，模块化，三角参与比，电导,传递性，以及每个类中社区的内部密度。我们发现，不同类别的社区表现出不同的结构品质，许多现有的社区**检测**算法倾向于输出非常大的社区。少

2017 年 12 月 2 日提交;**最初宣布** 2017 年 12 月。

212. 用于单级人脸检测的特征集聚网络

作者:张建良,吴雄伟,朱建科，海 c . h.

文摘: 近年来，利用深度学习进行人**脸检测**取得了可喜的成果。尽管取得了显著的进展，但野外**人脸检测**仍然是一个开放的研究挑战，特别是在检测具有截然不同的尺度和特征的**人** 脸时。本文提出了一种新的简单而有效的 "特征集聚网络" 框架 (fanet)，以构建一种新的单级**人脸**检测器，该检测器不仅实现了最先进的性能，而且运行高效。在特征金字塔网络 (fpn) 的启发下，我们框架的关键思想是利用单个卷积神经网络固有的多尺度特征，将不同尺度的高级语义特征图聚合为上下文线索，以增强上下文线索较低级别的要素地图通过分层聚集方式，以边际额外的计算成本。我们进一步提出了一个分层损失，以有效地训练 fanet 模型。我们在多个公众**人脸检测**基准上评估了拟议的 fanet 检测器，包括 pascal **人脸**、fddb 和 wider **face** **数据**集，并取得了最先进的结果。我们的探测器可以实时运行 gpu 上的 vga 分辨率图像。少

2018 年 9 月 10 日提交;**v1** 于 2017 年 12 月 3 日提交;**最初宣布** 2017 年 12 月。

213. 基于种族和性别多样性的人脸属性检测

作者:hee jung ryu, hartwigadam, margaret mitchell

文摘: 我们演示了一种**人脸**属性**检测**方法，通过在学习属性之前学习人口信息，在性别**和种族子组中保留或提高属性检测的准确性检测**任务。该系统被我们称为好人. 利用所学的人口特征，同时拒绝从下游**人脸属性检测任务中**推断人口特征，保护潜在用户的人口隐私，同时得出一些最好的报告到目前为止的**数字**属性检测中的世界和 celeba 数据**集中**。少

2018 年 7 月 17 日提交;**v1** 于 2017 年 12 月 1 日提交;**最初宣布** 2017 年 12 月。

214. 面向弱监督对象检测的多实例课程学习

作者:李思阳,朱向新,黄秦国，许浩,郭杰伦

摘要: 在使用弱标记数据监视对象检测器时，大多数现有的方法都容易被捕获在判别对象部分，例如，由于缺乏对完整程度的监督，找到猫的**脸**而不是全身。对象。为了应对这一挑战，我们将对象分割纳入检测器训练，该训练指导模型正确定位完整对象。提出了将课程学习 (cl) 注入多实例学习 (mil) 框架的多实例课程

学习 (micl) 方法。micl 方法首先自动选取简单的训练示例，其中分割掩码的范围与**检测**边界框一致。训练集逐渐扩展到包括更难的例子来训练处理复杂图像的强大探测器。在 pascal voc 数据集中，所提出的环路分割的 micl 方法的性能大大优于最先进的弱监督对象检测器。少

2017 年 11 月 25 日提交;**最初宣布** 2017 年 11 月。

215. 基于视觉的主动说话人自我监控检测是社会意识语言习得的前提

作者:kalin stefanov, jonas beskow, giampiero salvi

文摘: 本文提出了一种在多人口语交互场景中**检测**主动说话者的自我监督方法。我们认为，这种能力是任何人为的认知系统试图在社会环境中获得语言的基本前提。我们的方法能够**检测到**任意数量的可能重叠的主动扬声器，完全基于关于他们**的脸**的视觉信息。我们的方法不依赖于外部注释，从而符合认知发展。相反，他们使用听觉模式的信息来支持视觉领域的学习。在大型多人**面对面**交互数据集上对这些方法进行了广泛的评价。在多扬声器设置下，结果的精度达到 80%。我们相信这个系统是任何从事社会交往的人工认知系统或机器人平台的重要组成部分。少

2017 年 11 月 24 日提交;**最初宣布** 2017 年 11 月。

216. 服务器，云中的服务器。谁是人群中最公平的?

作者:marc böhlen, varun chandola, amol salunkhe

文摘: 本文遵循了近年来的自动化选美比赛，讨论机器学习技术，特别是神经网络，如何改变处理吸引力的方式，以及这对文化景观的影响。我们描述了在一个大型名人**面孔**数据库中，为探索两种不同的卷积神经网络架构在面部吸引力分类方面的行为而进行的实验。与其他易于定义的面部特征相比，即使是最好的分类系统，也很难有力地**检测到**吸引力。在这些实验结果的基础上，我们讨论了几种检测机器评价人的特征时起作用的因素的方法，以及在数据选择中，以及在网络体系结构中如何产生偏差;在整个过程中的多个级别上以多个形式。总体目标是用混合方法制定一个新的条件: 平台级机器学习系统产生的滑点，这些系统在被认为依赖于高水平人类智慧的领域做出判断。少

2017 年 11 月 23 日提交;**最初宣布** 2017 年 11 月。

217. 基于记忆的视频流深层表示的在线学习

作 者 :fedico pernici, fedico bartoli, matteo bruni, alberto del bimbo

文摘: 我们提出了一种新的在线无监督方法，从视频流中**进行人脸**身份学习。该方法利用深层的**人**脸描述符和基于记忆的学习机制，利用视觉数据的时间一致性。具体而言，我们引入了一种基于

反向近邻的判别特征匹配解决方案和一种特征遗忘策略，该**策略**检测冗余特征，并在时间进展时适当地丢弃这些特征。结果表明，所提出的学习过程是渐近稳定的，可以有效地应用于无约束视频流的多**面**识别和跟踪等相关应用。实验结果表明，该方法利用未来信息的离线方法，在多**人脸**跟踪任务中取得了可比的效果，在**人脸**识别方面取得了较好的性能。代码将公开提供。少

2017 年 11 月 17 日提交;**最初宣布** 2017 年 11 月。

218. 人脸注意网络：一种有效的人脸检测器

作者:王建峰,叶元,余刚

文摘: 随着卷积神经网络的发展，人**脸检测**的性能得到了很大的提高。然而，由于面膜和太阳镜引起的遮挡问题，仍然是一个具有挑战性的问题。这些被阻断的病例召回情况的改善通常会带来高误报的风险。本文提出了一种新型**的人脸**注意网络检测器，该检测器可以显著提高遮挡情况下人**脸检测**问题的召回率，同时又不影响检测速度。更具体地说，我们提出了一个新的锚级关注，这将突出从**面部**区域的特点。结合我们的锚分配策略和数据增强技术，我们获得了最先进的结果，公众**面部检测**基准，如 widerface 和 mafa。该代码将被发布以供复制。少

2017 年 11 月 22 日提交;**v1** 于 2017 年 11 月 20 日提交;**最初宣布** 2017 年 11 月。

219. 一种基于面部图像的融合性别识别方法

作 者 :benyamin Ghojogh, saeed bagheri shouraki, hodamohammadzade, ensieh iranmehr

文摘: 本文提出了一种以面部图像为输入的基于融合的性别识别方法。本文首先利用预处理和地标**性检测**方法，寻找**人**脸的重要地标。此后，提出了四个不同的框架，这些框架的灵感来自最先进的性别承认制度。第一个框架使用局部二进制模式（lbp）和主成分分析（pca）提取特征，并使用反向传播神经网络。第二个框架使用 gbor 筛选器、pca 和内核支持向量机（svm）。第三个框架使用**面**的下部作为输入，并使用内核支持向量机对其进行分类。第四个框架使用线性判别分析（lda）来对**人**脸的侧面轮廓地标进行分类。最后，使用加权表决对框架的四项决策进行融合。本文利用了面部性别识别中两种主要信息的纹理和几何信息。实验结果表明了该方法的有效性和有效性。该方法对 fei **面**数据集的中性**面**获得 94% 的识别率，相当于该数据集的最先进识别率。少

2017 年 11 月 17 日提交;**最初宣布** 2017 年 11 月。

220. 多模态抑郁严重程度的估计

作 者 :evgeny stepanov, stephane lathuiliere, shammur absar chowdhury, arindam ghosh, radu-laurentu vieriu, nicu sebe, giuseppe riccardi

摘要: 抑郁症是一种主要的衰弱疾病，可以影响到所有年龄的人。随着每年抑郁症病例的不断增加，有必要开发**检测**抑郁症存在和程度的自动技术。在这一 avec 挑战中，我们探索了不同的模式(从**面部**提取的语音、语言和视觉特征)，以设计和开发**检测**抑郁症的自动方法。在心理学文献中，phq-8 问卷已被公认为衡量抑郁症严重程度的工具。在本文中，我们的目标是自动预测 phq-8 分数从不同的模式提取的特征。我们表明，从面部地标提取的视觉特征在估计 phq-8 结果方面获得了最佳性能，在开发集上的平均绝对误差 (mae) 为 4.66。言语的行为特征提供了 4.73 的 mae。语言特征产生的 mae 稍高，为 5.17。切换到测试集时，我们从音频转录派生的 "转弯" 功能获得了最佳性能，获得了 4.11 的 mae (相当于 4.11 的 rmse)，这使得我们的系统成为 avec 2017 抑郁症子挑战的赢家。少

2017 年 11 月 10 日提交;**最初宣布** 2017 年 11 月。

221. 增强对防御性蒸馏深神经网络的攻击

作者:刘玉佳,张伟明,李少华,余能海

摘要: 深神经网络 (dnn) 在机器学习的许多任务中都取得了巨大的成功，如图像分类。不幸的是，研究人员已经证明，dnn 很容易被对抗的例子攻击，稍微不安的图像，这可能会误导 dnn 给出不正确的分类结果。这种攻击严重阻碍了 dnn 系统在安全或安

全要求严格的地区的部署，如自主汽车、**人脸**识别、恶意软件**检测**。防御蒸馏是一种旨在培养强效 dnn 的机制，它显著降低了对抗性例子生成的有效性。然而，最先进的攻击可以在蒸馏网络上成功，概率为 100%。但这是一个白盒攻击，需要知道 dnn 的内部信息。然而，黑匣子场景更为一般。本文首先提出了在白盒设置中 100% 成功率可以愚弄防御式蒸馏网络的 epsilon-neighborhood 域攻击，并迅速生成具有良好视觉质量的对抗性示例。在此攻击的基础上，我们进一步提出了基于区域的攻击，以针对在黑盒设置中进行防御性蒸馏的 dnn。我们还执行旁路攻击，间接打破蒸馏防御作为一种补充方法。实验结果表明，我们的黑匣子攻击在防御蒸馏网络上具有相当的成功率。少

2017 年 11 月 16 日提交;**最初宣布** 2017 年 11 月。

222. scada 系统的隐私保存入侵检测技术

作者:marwa keshk, nour moustafa , elena sitnikova, gideon creech

摘要: 监控控制和数据采集 (scada) 系统**面临**着缺乏一种保护技术的情况，这种技术可以在使用其他应用程序 (特别是其他应用程序) 处理这些数据时战胜不同类型的入侵并保护数据不被泄露入侵**检测**系统 (ids)。scada 系统可以管理工业控制环境中的关键基础设施。通过物理和数字系统的连接，保护敏感信息是现实中的一项艰巨任务。因此，隐私保护技术已成为有效的，以保护敏感

的私人信息和**检测**恶意活动，但它们在错误**检测**、数据的敏感性百分比方面并不准确披露。本文提出了一种新的基于相关系数和期望最大化（em）聚类机制的隐私保存入侵**检测**(ppid）技术，用于选择数据的重要部分和识别侵入性事件。此技术在电力系统数据集上进行评估，以进行多类攻击，以测量其**检测**可疑活动的可靠性。实验结果优于上述三种技术，显示了所提出的技术在当前 scada 系统中的应用效率和有效性。少

2017 年 11 月 7 日提交;最初宣布 2017 年 11 月。

223. 基于概率风险识别的 scada 系统入侵检测系统

作者:thomas marsden, nour moustafa , elena sitnikova, gideon creech

摘要: .由于监控和数据采集（scada）系统控制着几个关键的基础设施，它们已经连接到互联网。因此, scada 系统**面临着**不同类型的复杂网络对手。本文提出了一种基于概率风险识别的入侵**检测**系统（pri-ids）技术，该技术基于对 modbus tcp 账面网络流量的分析，用于识别重播攻击。人们承认, modbus tcp 由于其未经身份验证和未加密的性质，通常是易受攻击的。我们的技术通过配置测试台来使用仿真环境进行评估，测试平台是一个价格低廉、准确且可扩展的 scom scada 网络。在测试 ids 时，可以利用测试台，方法是从与 modbus 主从位于同一 lan 上的攻击者发送

单个数据包。实验结果表明，该技术能够有效、高效地识别重播攻击。少

2017 年 11 月 7 日提交;最初宣布 2017 年 11 月。

224. 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

摘要: 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。

225. 通过快速鲁棒矩阵完成的背景减法

作者:behnaz rezaei, sarah ostadabbas

摘要: 背景减法是大多数视频检测系统的首要任务。背景减法最重要的部分是背景建模，这是不同算法中常见的。在这方面，本文以一种计算效率高的方法解决了背景建模的问题，这对于当前来自高分辨率多通道视频的 "大数据" 处理的爆发具有重要意义。我们的模型基于自然图像的背景位于低维子空间上的假设。我们在一个低阶矩阵完成框架中制定并解决了这个问题。在背景建模中，我们受益于**内**视扩展的 frank-wolfe 算法，用于求解定义的凸优化问题。我们在背景模型挑战 (bmc) 和斯图加特人工背景减法 (sabs) 数据集上评估了我们的快速鲁棒矩阵完成 (frmc) 方法。将结果与鲁棒主成分分析 (rpca) 和低阶鲁棒矩阵完成 (rmc) 方法进行了比较，这两种方法均由不精确的增强拉格朗日乘法器

(ialm) 求解。结果显示，为了检测场景中的移动对象，计算速度更快，至少是使用 ialm 求解器时的两倍，而在某些挑战中具有可比的精度甚至更好。少

2017 年 11 月 3 日提交;最初宣布 2017 年 11 月。

226. 数据、深度和设计：学习黑色素瘤筛选的可靠模型

作者:爱德华多·瓦莱,米歇尔·福纳西亚利,阿丰索·梅内戈拉,朱莉娅·塔瓦雷斯,弗拉维亚·瓦斯克斯·比特坎特，林提丽,桑德拉·阿维拉

摘要: 在过去两年中，深度学习促进了黑色素瘤自动筛查的飞跃。然而，这些模型的训练成本很高，难以参数化。目的：探讨黑色素瘤**检测**深度学习模型设计与评价的方法问题。我们探讨了研究人员**面临**的十种选择：转移学习、模型架构、列车数据集、图像分辨率、数据增强类型、输入规范化、分割使用、培训持续时间、支持向量机的额外使用和测试数据扩充。方法：对 5 个不同的测试数据集进行了两个全阶乘实验，在我们的主要实验中进行了 2560 项详尽试验，在我们的转移学习评估中进行了 1280 项试验。我们用多路方差分析。我们使用详尽的试验来模拟顺序决策和组合，无论是否使用测试集中的特权信息。结果--主要实验：列车数据量具有不成比例的影响，解释了几乎一半的性能变化。在其他因素中，测试数据的增加和输入分辨率的影响最大。更深入的模

型，如果与额外的数据结合起来，也会有所帮助。-转移实验：转移学习是至关重要的，它的缺失带来巨大的性能惩罚。-模拟：模型的集合是在不使用特权信息和牺牲方法严谨性的情况下，以有限的资源提供可靠结果的最佳选择。结论和意义：推进黑色素瘤自动筛查研究需要对较大的公共数据集进行管理。间接使用测试集中的特权信息来设计模型是一个微妙但经常出现的方法错误，导致过于乐观的结果。模型的集合是一种经济高效的替代昂贵的全阶乘和不稳定的顺序设计。少

2018 年 3 月 22 日提交;**v1** 于 2017 年 11 月 1 日提交;**最初宣布** 2017 年 11 月。

227. 我们在面部欺骗检测中走了多远?

作者:luiz souza, mauricio p 人中奥纳, luciano oliveira,若昂·帕帕

摘要: 越来越多地使用**基于人脸**识别的控制访问系统，这说明需要更准确的系统来**检测人**脸欺骗攻击。本文对近十年来发表的**人**脸欺骗**检测**作品进行了广泛的分析。分析的作品按其基本部分进行分类，即描述符和分类器。这一结构化的调查还带来了**人**脸欺骗**检测**领域的时间演变，以及考虑该领域最重要的公共数据集的作品的比较分析。这项工作所遵循的方法对于观察现有方法的趋势、讨论尚未解决的问题以及为**面部**欺骗**检测的**未来提出新的前景特别相关。少

2018 年 9 月 29 日提交;**v1** 于 2017 年 10 月 26 日提交;**最初宣布** 2017 年 10 月。

228. 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。

229. 基于级联的基于区域的密集连接网络，用于事件检测：一种地震应用

作者:岳武、林友佐 、郑州、 大卫·奇斯·博尔顿、刘基 、保罗·约翰逊

文摘: 时间序列信号**的事件自动检测**具有广泛的应用，如视频监控中的异常事件**检测**和地球物理数据中的事件**检测**。传统的**检测**方法主要通过在数据中使用相似性和相关性来**检测**事件。这些方法可能效率低下，而且精度较低。近年来，由于计算能力的显著提高，机器学习技术使许多科学和工程领域发生了革命性的变化。在本研究中，我们应用了一种基于深度学习的方法来检测时间序列地震信号的**事件**。然而，从二维物体**检测**到我们的问题，对类似的想法的直接适应**面临着**两个挑战。第一个挑战是地震事件的持续时间差别很大;另一个是所产生的建议在时间上是相互关联的。为了应对这些挑战，我们提出了一种新的基于级联区域的卷积神经网络来捕获不同大小的地震事件，同时结合上下文信息来丰富每个建议的特征。为了实现更好的泛化性能，我们使用密集连接的块作为网络的主干。由于一些正事件没有正确注释，我们进一步将**检测**问题表述为噪声学习问题。为了验证我们**的检测**方法的性能，我们将我们的方法应用于岩石力学实验室的双轴 "地震机器" 生成的地震数据，并在专家的帮助下获取标签。通过数值试验表明，我们的**新检测**技术具有较高的精度。因此，我们新的基于

深度学习的**检测**方法有可能成为在各种应用中从时间序列数据中查找事件的强大工具。少

2017年11月28日提交;**v1**于2017年9月12日提交;**最初宣布**2017年9月。

230. 我们可以使用预处理来增强紫百合-琼斯面检测器的功能吗？实证研究

作 者 :mahmoud afifi, marwa nasser , mostafa korashy, katherine rohde, aly abdelrahim

摘要: 紫百合-琼斯**人脸检测**算法过去是（现在仍然是）一个相当流行的**人脸**检测器。尽管最近提出了许多**人脸检测**技术，但由于其简单性，仍有许多研究工作是基于 viola-jones 算法的。本文利用紫百合-琼斯算法研究了一组盲预处理方法对**人脸检测**率的影响。我们专注于两个方面的改进，特别是照明不良的**面孔**和模糊**的面孔**。为了提高检测精度，采用了多种照明不变和去模糊**的方法**。我们要避免使用可能会阻碍**人脸**检测器的盲目预处理方法。为此，我们进行了两套实验。第一套是为了避免任何可能伤害**人脸**探测器的盲目预处理方法。第二套是为了研究所选择的预处理方法对难受条件影响的图像的影响。在紫百合-琼斯**人脸**检测器使用之前，我们提出了将预处理方法应用于图像的两种方法。使用四个不同的数据集，对使用以前的增强图像所带来的潜在改进得出一致的结论。结果表明，某些预处理方法可能会影响紫百合人

脸检测算法的准确性。然而，其他预处理方法对**人脸**检测器的精度有明显的积极影响。总体而言，我们建议采用三种简单、快速的盲光光度归一化方法作为预处理步骤，以提高预训练的紫百合-琼斯**人脸**检测器的精度。少

2017 年 12 月 10 日提交;**v1** 于 2017 年 9 月 22 日提交;**最初宣布** 2017 年 9 月。

231. 抗逆转录酶识别人脸检测

作者:陈玉佳,宋凌晓,何然

摘要: 由于各种真实世界的遮挡会产生较大的外观变化，遮挡人**脸检测**是一项具有挑战性的**检测**任务。本文介绍了一种同时**检测**闭塞面和分割遮挡**区域**的对抗错位感知面检测器 (aofd). 具体而言，我们采用对抗训练策略来生成类似遮挡的面部特征，而**这种特征对于人脸**检测器来说是很难识别的.在检测闭塞**面的同时预测**遮挡掩模，并将遮挡区域用作辅助区域，而不是作为障碍。此外，分割分支的监控信号将对特征产生反向影响，从而有助于检测受力**遮挡的人**脸。因此, aofd 能够找到有几个暴露的面部地标的**面孔**具有非常高的信心，并保持高**检测**精度，即使是蒙面**人**脸。大量实验表明, aofd 不仅在 mafa 遮挡**人脸检测**数据集上的性能明显优于最先进的方法，而且在基准上还实现了具有竞争力的**检测精度.**用于一般**人脸检测**的数据集，如 fdb 。少

2018 年 9 月 29 日提交;**v1** 于 2017 年 9 月 15 日提交;**最初宣布** 2017 年 9 月。

232. 来自不可靠数据集的认证计算

作者:themis Gouleakis, christos tzamos, manolis zampetakis

摘要: 广泛的学习任务需要人为输入对海量数据进行标记。不过，收集到的数据通常质量较低，包含不准确和错误。因此，现代科学和商业**面临着**从不可靠的数据集学习的问题。在本工作中，我们提供了一种基于仅有少量数据集记录的通用方法，以保证各种优化目标的高质量学习结果。我们的方法，识别少量的关键记录集，并验证其有效性。我们表明，许多问题只需要波利(1/)验证，以确保计算的输出最多是一个因素(1±大)远离真相。对于任何给定的实例，我们都提供了一个具有最大可能数量的记录的 waltext{实例最优} 解决方案，以近似地验证正确性。然后利用这个实例对问题进行优化的表述，证明了我们的主要结果: "满足一些 lipschitz 连续性条件的每一个函数都可以通过少量的验证进行认证"。我们证明了所需的 lipschitz 连续性条件，即使是一些 np 完全问题也能满足，这说明了该定理的通用性和重要性。如果此认证步骤失败，将识别无效记录。删除这些记录并重复到成功，保证结果是准确的，并且仅取决于已验证的记录。令人惊讶的是，正如我们所表明的，对于几种计算任务来说，更有效的方法是可能的。这些方

法始终保证生成的结果不受无效记录的影响，因为将**检测**和验证影响输出的任何无效记录。少

2018 年 6 月 12 日提交;**v1** 于 2017 年 9 月 12 日提交;**最初宣布** 2017 年 9 月。

233. s3 个 fd：单次射击尺度不变面检测器

作者:张世峰,朱祥宇,李祥宇,史海林,王晓波,李斯坦

抽象: 本文提出了一种实时**人脸**检测器，名为单次拍摄尺度不变面检测器 (s3 个 fd)，它在具有单一深度神经网络的各种面尺度上表现出色，特别是对于小**人脸**。具体而言，我们试图解决一个常见问题，即基于锚杆的探测器会随着物体变小而急剧恶化。我们在以下三个方面做出了贡献: 1) 提出一个规模公平的**人脸检测**框架，以处理不同尺度的**人脸**。我们将锚点贴在广泛的图层上，以确保所有比例的**人**脸都有足够的特征进行**检测**。此外，我们还在有效接受场和提出的等比例区间原理的基础上设计了锚杆尺度;2) 采用规模补偿锚杆匹配策略，提高小**面**的召回率;3) 通过最大背景标签降低小**脸**的假阳性率。因此，我们的方法在所有常见的**人脸检测**基准上实现了最先进的**检测**性能，包括 afw、pascal 人脸、fddb 和 wider **face** **数据**集，以及可以在 nvidia titan x (pascal) 上运行 36 fps，用于 vga 分辨率图像。少

2017 年 11 月 15 日提交;**v1** 于 2017 年 8 月 17 日提交;**最初宣布** 2017 年 8 月。

234. 面箱：高精度的 cpu 实时面检测器

作者:张世峰,朱祥宇,李祥宇,史海林,王晓波,李斯坦

摘要: 尽管**在人脸检测**方面取得了巨大的进步，但剩下的开放挑战之一是实现 cpu 上的实时速度以及保持高性能，因为有效的**人脸检测模型**往往是计算上的令人望而却步。为了应对这一挑战，我们提出了一种新的**人脸**检测器，名为脸盒，在速度和精度上都具有卓越的性能。具体来说，我们的方法具有轻量级但功能强大的网络结构，由快速消化卷积层 (rdcl) 和多尺度卷积层 (mscl) 组成。rdcl 旨在使脸箱能够在 cpu 上实现实时速度。mscl 旨在丰富接受场和离散的锚在不同的层，以处理不同尺度的**面孔**。此外，我们提出了一种新的锚点致密化策略，使不同类型的锚点在图像上具有相同的密度，显著提高了小**脸**的召回率。因此，建议的检测器在单个 cpu 内核上以 20 fps 运行，在使用 gpu 的情况下使用 gpu 运行 vga 分辨率图像。此外，脸盒的速度与**人**脸的数量是不变的。我们对该方法进行了全面的评估，并在多个**人脸检测**基准数据集上提供了最先进的**检测**性能，包括 afw、pascal **人脸**和 fddb。少

2018 年 1 月 3 日提交;**v1** 于 2017 年 8 月 17 日提交;**最初宣布** 2017 年 8 月。

235. dock 过来面：一个易于安装和使用更快的 r-inn 人脸检测器在 docker 容器

作者:nataniel ruiz, james m. rehg

摘要: **面部护理检测**是面部地标**检测**、姿态估计、情绪分析和**人脸**识别等许多应用中一项非常重要的任务，也是必要的预处理步骤。**人脸检测**不仅是计算机视觉应用中的一个重要预处理步骤，也是计算心理学、行为成像和其他领域的研究人员可能不会在计算机视觉领域开始的一个重要的预处理步骤框架和最先进的**检测**应用程序。现有研究的很大一部分包括**人脸检测**作为预处理步骤，使用现有的开箱即用检测器，如基于 hog 的 dlib 和 opencv haar 人**脸**探测器，这些探测器已不再是最先进的---它们的使用主要是因为它们易于使用和可访问性。我们介绍 dockerface，一个非常精确的更快的 r-cnn **人脸探测器在**一个 docker 容器，不需要培训，易于安装和使用。少

2018 年 4 月 5 日提交;**v1** 于 2017 年 8 月 14 日提交;**最初宣布** 2017 年 8 月。

236. 无约束人脸检测与开放式人脸识别挑战

作者:manuel günther, peiyunhu , christian herrmann, chi ho chan, minjiang, shufan yang, akshay raj dhamija, deva ramanan, jürgen beyerer, josefkittler, mohamad al jasaery, mohammad iqbal nouyed, guodong guo, cezary Stankiewicz, terrance e. boult

摘要: **面部护理检测**和识别基准已转移到更困难的环境。本文提出的挑战是下一步从室外监控摄像头中对人的自动检测和识别。虽然**人脸检测**在从网络上收集的图像中显示出显著的成功，但监控摄像机包括更多样化的遮挡、姿势、天气状况和图像模糊。尽管**人脸**验证或闭式**人脸**识别在某些数据集中已经超过了人的能力，但开放式识别要复杂得多，因为它需要拒绝来自**人脸**检测器。我们表明，不受约束**的人脸检测**可以接近高**检**出率，尽管有中等的错误接受率。相比之下，开放式**人脸**识别目前很弱，需要更多的关注。少

2018 年 9 月 25 日提交;**v1** 于 2017 年 8 月 7 日提交;**最初宣布** 2017 年 8 月。

237. cnn 目标检测的递归量表逼近

作者:刘宇,李洪阳,严俊杰,魏方音,王晓刚, 唐晓欧

摘要: 由于卷积神经网络 (cnn) 缺乏处理大规模变化的固有机制，因此在多尺度目标**检测**中，我们总是需要多次计算地形图，这在实践中存在着计算成本的瓶颈.为了解决这个问题，我们设计了一个重复比例近似 (rsa) 来计算一次特征图，只有通过这个地图，

我们才能近似其他级别上的其余地图。rsa 的核心是递归展开机制：给定特定比例的初始映射，它将以较小的比例生成预测，该比例为输入大小的一半。为了进一步提高效率和准确性，我们 (a)：设计一个比例预测网络，以全球预测图像中的潜在比例，因为不需要计算金字塔所有级别上的地图。(b)：建议建立一个地标回溯网络，以追溯倒退地标的位置，并为每个地标产生置信度评分;lm 能有效地缓解 rsa 中累积误差引起的误报。整个系统可以在统一的 cnn 框架内进行端到端培训。实验表明，该算法在**人脸检测**基准上优于最先进的方法，并在通用生成过程中取得了可比的结果。rsa 的源代码可用于 github-comnse/comefans®对象的**检测**。少

2018 年 2 月 8 日提交;**v1** 于 2017 年 7 月 29 日提交;**最初宣布** 2017 年 7 月。

238. 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：第一个名为 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。

239. 基于多种外观模型和图形关系学习的稳健人脸跟踪

作者:tanushri chakravorty, guillaum-亚历山大·比洛多, eric 格兰杰

文摘: 本文讨论了在实际场景中进行可视**面跟踪时**，跨不同挑战的外观匹配问题。本文提出了利用具有长期和短期外观记忆的多外观模型进行高效的**人脸**跟踪的脸跟踪方法。它展示了对变形、平面内旋转和平面外旋转、刻度、干扰和背景杂波的鲁棒性。它利用了逐检**的**优点，通过**使用人**脸检测器来处理人脸的剧烈外观变化. 该探测器还有助于在漂移过程中重新初始化 facetrack。提出了一种加权计分级融合策略，通过在可能**的人脸**位置周围产生考生，获得具有最高融合分数的**人**脸跟踪输出。该跟踪器在自动启动时表现出令人印象深刻的性能，其性能优于许多最先进的跟

踪器，但 struck 的优势非常小：精度分别为 0.001 和成功 0.001。少

2018 年 8 月 30 日提交;**v1** 于 2017 年 6 月 29 日提交;**最初宣布** 2017 年 6 月。

240. 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。

241. 多视图动态面部动作单元检测

作者:andres romero, juan leon , pablo arbelaez

文摘: 针对多视点动态人脸动作单元检测的细粒度识别问题，提出了一种新的卷积神经网络**方法**。我们利用最近在大规模物体识别方面取得的进展，制定了预测特定行动单位的存在或不存在的任务，将人**脸**的静止不动的形象描述为整体分类。然后，我们通过考虑不同行动单元的共享和独立表示，以及将颜色和运动信息结合起来的不同 cnn 架构，来探索我们方法的设计空间。然后，我们进入 fera 2017 挑战赛的新设置，在这种设置中，我们建议我们的方法的多视图扩展，首先预测拍摄视频的视点，然后评估一个整体的动作单元探测器,训练的特定观点。我们的方法是整体的、高效的和模块化的，因为新的行动单元可以很容易地包含在整个系统中。我们的方法大大优于 2017 年 fera 挑战赛的基线, f1 指标的绝对改进率提高了 14%。此外，它与 2017 年 fera 挑战的获胜者相比也是有利的。代码源可在 https://github.com/BCV-Uniandes/AUNets。少

2018 年 8 月 20 日提交;**v1** 于 2017 年 4 月 25 日提交;**最初宣布** 2017 年 4 月。

242. 混合信号神经形态电路中超参数选择的微分演化与贝叶斯优化

作 者 :llewyn salt, david howard, giacomo indiveri, yulia sandamirskaya

摘要: lobula 巨型运动探测器 (lgmd) 是一种已识别的蝗虫神经元，它**能探测**到隐伏的物体并触发其逃逸反应。了解导致这些快速和稳健响应的神经原理和网络可以导致在机器人应用中设计高效的促进避障策略。在这里，我们提出了一个神经形态尖峰神经网络模型的 lgd 驱动的输出的神经形态动态视觉传感器 (dvs)，它已被优化，以产生强大和可靠的响应，面对的约束和变异性它的混合信号模数电路。由于该 lgmd 模型具有许多参数，因此我们使用微分演化 (de) 算法来优化其参数空间。我们还研究了自适应微分进化 (sade) 的使用，它已被证明可以减轻为 de 找到合适的输入参数的困难。我们探讨了两种生物机制的应用：突触可塑性和膜自适应性在 lgmd。我们应用 de 和 sade 来寻找最适合无人驾驶飞行器 (uav) 上避障系统的参数，并展示它如何优于用于比较的最先进的贝叶斯优化。少

2017 年 11 月 5 日提交;**v1** 于 2017 年 4 月 16 日提交;**最初宣布** 2017 年 4 月。

243. 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，而是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，而不需要采用高级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。

244. 你能告诉我从印度哪里来吗？对细粒度种族人脸分类的人和计算机进行比较

作者:harish katti, s. p. arun

摘要: **面孔**构成了人类丰富多样判断的基础，但其基本特征仍然鲜为人知。尽管在种族中的细粒度区分可能比在种族或性别等粗

放型的情况下更严格地限制人类可能使用的面部特征，但这种细粒度的区别的研究相对较少。细粒度的种族分类也很有趣，因为即使是人类在这些任务上也可能不是完全准确的。这使我们能够比较人类和机器所犯的错误，而标准的对象**检测**任务与人类的性能近乎完美的情况相比。我们开发了一个新的**面部数据库**，近1650不同**的印度面孔**标记为细粒度种族（南对北印度），以及年龄、体重、身高和性别。随后，我们要求近 130 名人类对象将每一**张脸**归类为属于印度北部或南部邦。然后，我们将人类在这项任务上的表现与在地面真相标签上训练的计算模型进行了比较。我们的主要结果是: (1) 人类是高度一致的（平均精度: 63.6%），有的**人脸**的分类一致，准确率 & gt; 90%，有的人脸一贯错误分类，准确率 & lt; 30%;(2) 在地面真相标签上训练的模型表现出稍差的性能（平均准确率: 62%），但在人类分类的**精度**& gt; 80% 的表面上表现出更高的精度（72.2）。对于从**人脸**中提取的简单空间和强度测量以及接受种族或性别分类培训的深度神经网络的模型来说，情况也是如此;(3) 利用从每个**面部**部位获得的过度完整的特征库，我们发现嘴形是对细粒度比赛分类的最大贡献者，而**面部**部位之间的距离是最强的性别的预测。少

2018 年 2 月 19 日提交;**v1** 于 2017 年 3 月 22 日提交;**最初宣布** 2017 年 3 月。

245. 基于图形草图的空间高效数据聚类

作 者 :anne morvan , krzysztof choromanski, cédric Gouy-Pailler, jamal atif

摘要: 在本文中，我们讨论了在**面对**\ 强调 {高空间约束} 时从数据集中恢复任意形状的数据群集的问题，例如，在许多实际应用中，当分析算法是直接的时候，情况就是这样。部署在资源有限的移动设备上收集数据。我们提出了一个新的空间高效密度的 \ 强调 {非参数 t) 方法，该方法研究从有限数量的线性测量 (即不同图的 \ 强调计划} 版本中恢复的最小生成树 (mst)G 之间的 n 要群集的对象。与 K-意思是 K-媒体或 K-medoids 算法，它不会失败区分集群与特定的形式，由于 mst 的属性表示一个图形的基础结构。dbscan 或频谱聚类方法不需要输入参数。在处理不同图时，遵循动态 \ 强调 {半流媒体} 模型，检索近似 mstG 作为边缘重量更新的流，它被勾勒出一个通过数据到一个紧凑的结构，需要 o(n 多洛格(n))空间，远远好于理论的内存成本 o(n2)的 G.恢复的近似 mstt 作为输入, dbmstclu 然后成功地**检测到**正确数量的非凸集群上执行相关的削减 t 在一个时间线性 n.我们为聚类划分的质量提供了理论保证，并展示了它在多个数据集上的优势，而不是现有的最先进技术。少

2018 年 5 月 27 日提交;**v1** 于 2017 年 3 月 7 日提交;**最初宣布** 2017 年 3 月。

246. 从单个图像中使用几何细节进行 3d 人脸重建

作者:罗江,张巨勇,邓百林,李浩丽,刘丽刚

摘要: 从单个图像进行 3d **人脸**重建是一个经典且具有挑战性的问题，在许多领域有着广泛的应用。在 rgb-d 或单目视频输入**的**面部动画的最新工作的启发下，我们开发了一种新的方法，利用粗到精细的优化策略，从无约束的二维图像中重建三维**人脸.**首先，通过将 3d 面的投影与从输入图像中**检测到**的 2d 地标对齐，从基于示例的双线性人**脸**模型生成平滑的粗三维**面**。随后，使用局部校正变形场，使用光度一致性约束对粗三维**面**进行细化，形成中等**的面**形状。最后，在中**面**上采用形状遮阳方法来恢复精细的几何细节。我们的方法在准确性和细节恢复方面优于最先进的方法，这一点在使用现实世界模型和公开数据集的大量实验中得到了证明。少

2018 年 6 月 11 日提交;**v1** 于 2017 年 2 月 18 日提交;**最初宣布** 2017 年 2 月。

247. 三维人脸纹理的组合与隐写

作者:mohsen moradi, mohamer-reza sadeghi

摘要: 人与人之间沟通的一个严重问题是向他人隐瞒信息，最好的办法就是欺骗他们。由于现在**人脸**图像大多采用三维格式，在本文中我们将隐写三维**人脸**图像,**检测**哪些由好奇的人将是不可能的。由于在**检测人脸**纹理时，只有它的纹理是重要的，我们将纹

理与形状矩阵分开，为了消除一半的额外信息，隐写只用于**面部**纹理和重建三维**人脸**，我们可以使用任何其他形状。此外，我们还将指出，通过使用两个纹理，如何组合两个 3d **面.**为了完整地描述该过程，首先, 2d **面被**用作构建 3d **面的**输入，然后 3d 纹理隐藏在其他图像中。少

2018 年 1 月 18 日提交;**v1** 于 2017 年 2 月 4 日提交;**最初宣布** 2017 年 2 月。

248. 基于手势的自我中心手分割引导

作者:yubozhang, vishnu naresh boddeti, kris m. kitani

摘要: 使用可佩戴的第一人视点摄像机，准确识别图像中的手是人类活动理解的关键子任务。传统的手部分割方法依靠大量手动标记的数据来生成可靠的手部检测器。但是，这些方法仍然**面临挑战**，因为手的外观因用户、任务、环境或照明条件而异。在许多可穿戴应用程序和接口的情况下，一个关键的观察是，只有在特定的情景上下文中准确**地检测**用户的手是唯一必要的。基于这一观察，我们引入了一种交互式方法来学习不需要任何手动标记的训练数据的特定于人的手分割模型。我们的方法分两个步骤进行，一个交互式引导步骤，用于识别移动的手区域，然后学习个性化的用户特定的手外观模型。具体而言，我们的方法采用了两个卷积神经网络: (1) 使用预定义运动信息检测手部区域的手势

网络;(2) 根据手势网络的输出学习手部区域的人特定模型的外观网络。在训练过程中，为了使外观网络对手势网络中的错误保持鲁棒性，前一个网络的丢失功能在学习时包含了手势网络的信心。实验证明，我们的方法具有鲁棒性，f1 分数超过 0.8，涵盖广泛的照明和手外观变化，超过基线方法 10% 以上。少

2018 年 6 月 11 日提交;**v1** 于 2016 年 12 月 8 日提交;**最初宣布** 2016 年 12 月。

249. 利用主动视觉进行机载传感和计算，在狭窄的间隙进行侵略性四旋翼飞行

作 者 :davandfalanga, elias mueggler, matthias faessler, davandhasamuzza

摘要: 我们解决了在复杂环境中实现自主四旋翼飞行的主要挑战之一，即通过狭窄的间隙飞行。虽然以前的工作依赖于板外定位系统或对间隙位置和方向的准确的先验知识，但我们完全依靠板载传感和计算，并通过从单个板载中融合间隙**检测**来估计完整状态相机与 imu。这个问题具有挑战性，原因有二: (一) 四旋翼对间隙的不确定性随距离的距离呈二次增加;(ii) 四旋翼必须主动控制其方向向间隙，以便能够进行状态估计 (即主动视觉)。我们通过生成考虑几何、动态和感知约束的轨迹来解决这个问题: 在接近机动过程中，四旋翼始终**面临**间隙，允许状态估计，同时尊重车辆动力学;在穿过缝隙的过程中，四旋翼与间隙边缘的距离最大化。

此外，我们还对其执行过程中的轨迹进行了重新规划，以应对国家估计的不同不确定性。我们在许多实际实验中成功地对该方法进行了评估和演示。据我们所知，这是首次通过狭窄的缝隙解决和实现自主、积极的飞行，只需在机载传感和计算中，在事先不知道差距的姿态的情况下。少

2018 年 4 月 5 日提交;**v1** 于 2016 年 12 月 1 日提交;**最初宣布** 2016 年 12 月。

250. 磁盘上的 2 个机器人搜索和提取：无线和面对面通信模型

作 者 :konstantinos georgiou，george karakostas ，evangelos kranakis

摘要: 我们开始研究一个新的问题，{\ em 搜索和提取} 在分布式环境中关于 \ 强调 {宝疏散} 从一个单位磁盘。宝藏和出口位于磁盘周长和已知弧距的未知位置。一个由两个机器人组成的团队从磁盘的中心出发，他们的目标是把宝藏带到出口。在任何时候，机器人都可以以同样的速度在磁盘上选择的任何地方移动，彼此独立。机器人只有在经过一个有趣的点（宝藏或出口）的确切位置时，**才会检测到**该点。我们有兴趣设计分布式算法，最大限度地减少最坏情况下的宝疏散时间，即任何机器人发现宝藏并将其带到出口所需的时间。机器人之间的通信协议可以是 {\em 无线}，即在任何时候共享信息，或者是 {\em 面对面} (即非无线)，只有在机器人相遇时才能共享信息。对于这两种模型，我们都获得了

将宝藏带到出口的上限。我们的主要技术贡献涉及**面对面**的模型. 更具体地说，我们展示了机器人如何在不开会的情况下交换信息，有效地实现了高效的宝排空协议，而该协议受到远距离通信不足的影响最小。最后，我们通过在**面对面**模型中提供一个下限来补充我们的积极成果.少

2018 年 10 月 11 日提交;**v1** 于 2016 年 11 月 30 日提交;**最初宣布** 2016 年 11 月。

251. 将数据驱动方法与模型驱动方法相结合，实现鲁棒的面部地标检测

作者:张洪文,李琪,孙振南,刘云帆

摘要: 面部地标**检测**是现实世界计算机视觉应用中一项重要而又具有挑战性的任务。本文结合数据和模型驱动的方法，提出了一种有效、可靠的人脸地标**检测**方法。首先，训练一个完全卷积网络（fcn）来计算所有面部地标点的响应图。这种数据驱动的方法可以充分利用面部图像中的整体信息，对面部地标进行全局估计。之后，响应映射中的最大点将安装预训练的点分布模型（pdm），以生成初始面部形状。这种模型驱动的方法能够通过考虑形状的先验信息来纠正异常值的不准确位置。最后，采用正则化地标正移（rlms）的加权版本对面部形状进行迭代微调。该估计校正优化过程完美地结合了数据驱动方法（fcn）的全局鲁棒性、模型驱动

方法 (pdm) 的异常校正能力和 rlms 的非参数优化等优点。大量实验的结果表明，我们的方法在具有挑战性的数据集上实现了最先进的性能，包括 300w、aflw、afw 和 cofw。该方法能够在面部图像中产生令人满意的检测结果，表现出夸张的**表情**、大的头部姿势和部分遮挡。少

2018 年 2 月 11 日提交;**v1** 于 2016 年 11 月 30 日提交;**最初宣布** 2016 年 11 月。

252. 场景语法、因子图和信仰传播

作者:jroen chua, pedro f. felzenszwalb

摘要: 我们描述了一个复杂场景的概率建模和模糊观测推断的一般框架。该方法是以图像分析中的应用为动力，是基于使用随机语法定义的优先点。我们定义了一类语法，它捕获场景中对象之间的关系，并为统计推断提供重要的上下文提示。由概率场景语法定义的场景上的分布可以用图形模型表示，这种结构可以用来进行具有循环信念传播的有效推理。我们给出了两种不同应用的实验结果。其中一个应用涉及二元等高线图的重建。另一个应用程序涉及**检测**和本地化图像中**的人**脸。在这两个应用程序中，相同的框架都能产生强大的推理算法，这些算法可以有效地将局部信息结合起来，对场景进行推理。少

2018 年 7 月 30 日提交;**v1** 于 2016 年 6 月 3 日提交;**最初宣布** 2016 年 6 月。

253. 特权信息下的检测

作者:z. berkay celik, patrick mcdaniel , rauf izmailov, nicolas papernot, ryan sheatsley, raquel alvarez , ananthram swami

摘要: 在四分之一个多世纪的时间里,**检测**系统一直由从实际或模拟环境中收集的输入要素中收集到的模型驱动。工件 (例如，网络事件、潜在恶意软件示例、可疑电子邮件) 在运行时与学习到的模型相似而被视为恶意或非恶意。但是，模型的培训历来仅限于运行时可用的功能。在本文中，我们考虑了一种另一种学习方法，该方法使用 "特权" 信息 (在训练时提供的功能) 训练模型，但在运行时不提供**这些**功能，以提高检测系统的准确性和恢复能力。特别是，我们调整和扩展了知识转移、模型影响和蒸馏方面的最新进展，以便能够在一系列安全域中使用运行时不可用的取证数据或其他数据。经验评估表明，对于没有特权信息的系统，特权信息可以提高精度和召回率: 我们观察到快速通量机器人**检测**的**检测**误差相对下降了 7.7%，为 8.6%恶意软件流量**检测**, 7.3% 用于恶意软件分类, 16.9% 用于**人脸**识别。我们探讨了不同特权信息技术在**检测**系统中的局限性和应用。这种技术为**检测**系统提供了一种新的手段，以便从否则在运行时无法获得的数据中学习。少

2018 年 3 月 30 日提交;**v1** 于 2016 年 3 月 31 日提交;**最初宣布** 2016 年 3 月。

254. 高压：一种用于人脸检测、地标定位、姿势估计和性别识别的深度多任务学习框架

作者:rajeev ranjan, vishal m.patel , rama chellappa

文摘: 我们提出了一种利用深层卷积神经网络 (cnn) 同时进行人脸**检测**、地标定位、姿态估计和性别识别的算法。提出的名为 "超级脸" 的方法使用单独的 cnn 融合了深 cnn 的中间层，然后是在融合特征上运行的多任务学习算法。它利用任务之间的协同作用，提升他们的个人表现。此外，我们还提出了超脸的两个变体: (1) 基于 resnet-101 模型并显著提高性能的超面重触网，以及 (2) 使用高召回快速面检测器生成的快速**双面**区域建议，以提高算法的速度。大量实验表明，所提出的模型能够捕获**人**脸中的全局和局部信息，并且在这四项任务中的每一个任务中的许多竞争算法中的性能都明显优于许多竞争算法。少

2017 年 12 月 5 日提交;**v1** 于 2016 年 3 月 3 日提交;**最初宣布** 2016 年 3 月。