

人工智能在计算机视觉和网络安全的应用

杨 贺

(沈阳职业技术学院,辽宁 沈阳 110045)

摘 要:近些年来,人工智能技术已经出现,并在各个领域得到了广泛应用。人工智能技术,虽然并未全面普及,但是这种技术为社会发展所带来的促进作用,却已经被大众所熟知以及认可。目前,人工智能已经被应用到了计算机视觉以及网络安全中,不仅如此,还为上述两个领域的发展奠定了基础。基于此,本文主要以人工智能为出发点,针对其在上述两个领域的应用方法进行了研究。文章首先介绍了人工智能,指出了上述技术在各领域应用的重要性。同样,也指出了对上述技术进行应用是未来行业发展的主要趋势。其次,对人工智能应用于计算机视觉中的方法进行了总结,首先分析了应用方向,继而从医疗以及零售等众多角度出发,对具体的应用进行了阐述。最后,文章对人工智能在网络安全中的应用进行了分析。希望能够为有关人员提供参考。

关键词:人工智能;计算机视觉;网络安全

[DOI]10.12231/j.issn.1000-8772.2021.33.137

1 引言

近些年来,我国对人工智能这项技术所作出的研究不断深入,而在众多研究的影响下,人们的生活也发生了极大改变,不仅生活更加便利,同样物质享受也得到了改善。当前,我国市场上已经出现了多种以人工智能技术为衍生源头的产物。上述产物,不仅丰富了人们的生活,也展示了科技的发展。计算机视觉,本质上属于一个研究领域,在这一领域中,人们研究的是怎样才能充分应用机器,实现对图像以及视频的解析。简言之,该技术要求具有智能化分析的功能,应从图片或视频中,对信息进行提取。而这一功能的实现,务必要对人工智能技术进行使用。网络安全,是一项概念,指的是在互联网应用的过程中,人们能够保证自身信息安全的状态。这一状态的实现,同样需要借助人工智能来实现。由此可见,无论对于计算机视觉或网络安全而言,人工智能技术的应用都十分重要,因此,应当对这一技术的应用进行研究。

2 人工智能在计算机视觉中的应用

2.1 人工智能在计算机视觉中的应用方向

计算机视觉相关工作中更注重图像的识别与处理,在现实生活中图像有动态化、静态化的2种展现形式。静态化的图片往往是已经拍摄结束的画面和图片等。而动态化的图像,更注重实景拍摄或作品视频化地展现。计算机视觉技术,在静态图像识别阶段,技术应用机制相对较高,无须使用太复杂的技术手段;在进行动态化技术识别时,将人工智能技术应用其中,能保障最终的图像识别效果。

计算机视觉需要多个软件和设备配合应用,利用传感器将拍摄场景中的相关信息进行识别或采集。做好信息的分类、整理与计算,后期进行图片信息的处理,能够将信息的精准性提升,保障图像信息处理的有效性。

在实践中,只有在智能计算机有良好的处理能力,才能对产业发展起到积极影响。在人工智能技术的影响下,计算机的识别水平不断提升,已可对各种复杂图像,诸如肢体动作、眼球转动等动态化的图像信息进行识别处理。视觉识别能力有良好的发展空间与条件,因此计算机视觉的研究工作,需要以人工智能技术为基础,探索优化与创新的有效途径,保障技术应用效果。

2.2 人工智能在计算机视觉中的具体应用

2.2.1 安防领域

近些年来,人们对自身安全性的重视程度稳步提升,对于居住以及办公的重视度,同样明显提高。为了满足人们的需求,国家开发了摄像系统。在城市中,处处都存在摄像系统,而上述系统,则属于安防领域的重要组成部分。在安防领域中,有关人员主要需要通过对人物的图像以及视频进行识别,同时对其信息进行分析,这样才能够提取相关特征信息,从而实现对视频以及图像的分析。结合上文所述可知,计算机视觉便具备上述功能。将计算机视觉应用到安防领域中,能够取得显著效果。但是需要注意的是,为了保证计算机视觉的应用,可以取得更好的效果,还需要对人工智能技术进行使用,从而确保识别图像以及视频的过程具有一定智能性以及自动性,避免过多的应用人工,从而减轻人力劳动的强度,借助计算机以及人工智能技术,提高分析结果的准确性。为了达到上述目的,建议利用人工智能技术,实现对图像的实时监测,在此基础上,通过智能匹配的方式,将收集到的推向与数据库当中的图像进行对比。对比的过程中,需要分析两个图像之间的参数差异,在参数差异较小的情况下,便可得到两者相似的结论。差异越小,则相似度越高。分析完成后,系统将会给出分析结构,从而实现人物的匹配。上述流程,属于高精度搜索图片的流程,有利于帮助安防领域长远发展,促使计算机视觉的价值得到发挥。

2.2.2 零售领域

除了安防领域之外,将人工智能应用到计算机视觉领域中后,同样有利于促进了零售行业的长远发展。计算机视觉出,其本质上来说,属于获取信息的一种手段,而上述手段区别于其他手段的特点之一,便是其具有智能化的特征。上述特征,则来源于对人工智能技术的应用。在零售行业中,有关人员需要对用户的信息进行收集,此举的目的,在于实现对各项信息的整理以及分析,从而找到其中的规律。根据数据的规律,便可制定出更加具有针对性的销售策略,从而提高零售行业的整体发展水平。上述功能可借助计算机视觉而实现,而计算机视觉则需要依托于人工智能技术,充分发挥上述作用。除了上述应用方法之外,有关人员还可以将以人工智能技术为基础的计算机视觉应用到无人售货的过程中。当前,在部分超市中,已经实现了自主结账。而上述功能的实现,便于计算机视觉的应用存在一定联系。得益于人工智能技术的帮助,计算机视觉有利于实现对人脸的识别。除了人脸之外,还能够实现对人体的识别。而上述识别过程中,则是通过对人脸图像参数的收集而实现的。通

过上述分析可以看出,计算机视觉的应用,离不开人工智能技术的支持。

3 人工智能在网络安全方面中的应用

3.1 人工智能在网络安全方面中的应用方向

分析人们对互联网的了解状况,会发现现阶段的网络技术应用问题,主要是网络安全问题。人们在生产或实践工作中,网络技术手段能提供一定的便捷条件,但也存在安全隐患问题,甚至威胁人们的信息、财产安全。现如今计算机安全管理人员或用户,进行信息或数据的保护方式,主要是在计算机中安装杀毒软件,利用这种技术手段,能有效遏制病毒读取个人信息,保护计算机中的相关资料。在计算机系统中设置防火墙,也是安全管理的主要工作,能提升计算机文件安全管理水平。防火墙的核心工作,是完成文件安全性、有效性的判断,现如今人工智能技术不断发展,计算机防火墙识别文件的功能也显著增强,能够有效保护计算机的用户信息安全,提升计算机运行质量。

人工智能与网络管理工作有效结合,能使人工智能技术及电子信息技术得到进一步发展。工作人员在进行网络管理期间,要明确智能技术应用价值,在计算机系统中有针对性地制定管理计划。在计算机管理程序设置期间,依托人工智能技术,对历史的数据进行分析处理,实现管理措施的生成与完善,将自动化的计算机网络管理目标落实。如果在计算机运行阶段出现问题,计算机智能系统能够分析问题出现的频率,利用有效的管控措施与方法处理数据。在数据处理以及决策阶段,给决策人员提供可靠的数据信息的支持,有一定的辅助引导作用,这些都对发展计算机网络技术有积极作用。

3.2 人工智能在网络安全方面中的具体应用

在互联网应用的过程中,将会产生大量网络风险,而各项风险一般体现在网络入侵、网络钓鱼、垃圾信息等方面。将人工智能应用到网络安全的过程中,能够有效减少上述风险,从而建立一个绿色化的互联网环境。这对网络安全的保证,以及用户个人信息以及安全的保证,都能够起到重要作用。

3.2.1 支持向量机赋能网络安全

支持向量机,本质上属于一种学习方法。上述方法,来源于传统的统计学理论,是上述理论结合大量经验以及先进技术而发展起来的一种方法,同样属于人工智能技术的一种。将其应用到网络安全的过程中,能够实现对网络入侵以及钓鱼等风险的有效识别,并且能够有效避免风险,从而保证计算机网络安全。在这种学习方法应用的过程中,有关人员能够实现对少量样本的收集,而在收集之后,便可实现对样本规律的分析。例如:某台计算机在遭遇网络入侵风险后,人工智能技术会立刻发挥作用,而支持向量机则会实现对入侵时数据的收集。经过长时间对数据的收集,便可得到小样本量数据。此时,人工智能技术可实现对数据的自动化分析,并了解数据的规律。在掌握了规律之后,下次计算机再次遭遇网络入侵,系统便会立即发现异常,并且立即发出预警,提醒用户对风险进行规避。由此可见,将人工智能技术应用到网络安全中,对网络安全性的提升,具有重要价值。

3.2.2 卷积神经网络赋能网络安全

卷积神经,本身属于神经网络的一种,也是来源于传统的神经网络。神经网络需要依靠人工智能技术而实现,而其本质也属于人工智能技术。基于上述技术维护网络安全,对网络入侵等风险的减少,同样可起到重要作用。卷积神经,属于相对于

人工神经的一种概念,与后者相比,前者在结构层方面得到了优化,另外,有关人员还能够借助上述技术,实现对卷积核特征的提取。基于上述技术,有利于在减少训练的情况下,明确全局关系。由此可见,将人工智能中的卷积神经应用到网络安全中,能够有效提高网络安全维护的效率以及便利性。例如:在某台计算机出现网络风险后,卷积神经网络便可实现对风险的分析,首先提取风险数据,继而通过训练的方式,得到全局之间的关系。由于训练次数少,因此,计算机可在较短的时间内便发出预警,提醒用户小心计算机入侵。另外,同样可使计算机自动对入侵进行抵挡。

3.2.3 强化学习赋能网络安全

强化学习,指的是通过反复学习一个行为,从而对此项行为记忆深刻的一种学习方式。目前,强化学习已经成为了人工智能技术的典型特征。通过强化学习,有利于实现对事物规律的全面掌握,并且有利于通过多次错误的尝试,在找到最终最优的解决办法后,对错误的尝试也进行记录,从而获得更好的成长空间,避免再次出现错误情况。将人工智能技术中的强化学习应用到网络安全中,通过Q学习策略,对计算机出现的安全风险进行频繁学习,便能够掌握最佳的网络安全维护方法,同样也能够减少在网络安全维护中所出现的错误。

4 结束语

综上所述,本文针对人工智能在计算机视觉和网络安全的应用的,有利于促使人工智能技术得到进一步普及,从而为社会的发展做出更大贡献,为人民生活的进步发挥更大的推动作用。此外,本研究同样有利于促进计算机视觉的发展,有利于更大程度保证网络安全,减少网络用户的风险。当前,人工智能技术在上述两项领域中,已经有所应用,并且取得了效果。但是,未来随着技术发展速度的加快,当前的成果并不足以满足人们的长远需求。因此,在未来,有关领域应当进一步加强对人工智能技术的研究。通过对该技术的剖析,对其功能进行更加深入的了解以及挖掘,同时对技术进行进一步开发,从而将其更好的运用到计算机视觉、网络安全,乃至其他领域当中,充分发挥人工智能的作用,全面提高各个领域的发展水平。

参考文献

- [1]何娜,李涵.浅析人工智能在眼科疾病应用中带来的医学伦理学问题[J].中国医学伦理学,2021,34(10):1325-1328.
- [2]罗艳.“智能+”背景下金融专业应用型人才培养模式创新研究——以四川现代职业学院为例[J].中国商论,2021(20):175-177.
- [3]徐益,慈白山.基于人工智能技术的网络安全防护研究[J].科技创新与应用,2021,11(27):166-168.
- [4]王锋.基于大数据时代计算机网络安全防范的措施刍议[J].网络安全技术与应用,2021(09):71-72.