学科漫谈

验证码识别的研究永远是一个双赢的结果:或者有一种验证码不能被破解,网络安全依然有保障;或者验证码被识别,则人工智能和机器学习水平得到进一步的提高。

验证码防卫战

■本报见习记者 袁一雪

高海昌
西安电子科技大学软件学院副教授

全国火车票售卖网站12306日前再次更换了验证码，频繁地出招，却依然没有换来12306在“火车票保卫战”中的胜利。

因为很快,搜狗浏览器、智行火车票等第三方订票渠道已对外宣布成功实现了12306图形验证码的自动识别，用户借此可以实现全自动抢票的体验。

面对日新月异的验证码破解手段,西安电子科技大学软件学院的一只团队默默从事着提升验证码可靠性的工作。这个团队的带头人高海昌称自己的团队是“戴‘白帽’的黑客”。

寻找鲁棒性与可用性的平衡点

黑客(Hacker)一词,最初曾指热心于计算机技术、水平高超的电脑专家,尤其是程序设计人员,后来逐渐区分为白帽、灰帽、黑帽等。利用公共通讯网路，如互联网和电话系统,在未经许可的情况下,攻入对方系统的被称为黑帽黑客(black hat);调试和分析计算机安全系统的称为白帽黑客(white hat)。

“我们对于验证码的研究，概况起来主要关注两方面:鲁棒性和可用性。”高海昌告诉《中国科学报》记者。鲁棒是Robust的音译,即健壮和强壮的意思。它是在异常和危险情况下系统生存的关键。比如,计算机软件在输入错误、磁盘故障、网络过载或有意攻击情况下,能否不死机、不崩溃,就是该软件的鲁棒性。

在验证码的领域中，鲁棒性就是要求验证码机制防破解能力强，不会轻易被计算机程序自动识别。相对的,可用性就是要求验证码机制对于人类的使用交互友好，既不能识别困难,也不能让识别时间过长。

2013年，各大网站普遍推出了空心验证码。它打破了传统的实心字体的模式,用轮廓线的空心字体替代。这样当多个字符重叠粘连的时候,机器识别度较差,但是人类仍然可以很好的识别。

但这并非无法破解，高海昌发现只需先将空心填充成实心字符，使用颜色填充算法得到离散的笔画块。然后使用卷积神经网络和深度优先算法对笔画块进行组合识别,寻求最优解作为识别结果。“我们针对Yahoo、百度、新浪、腾讯、和中国移动在线支付网站的空心验证码分别取得了36%、51%、59%、89%和66%的成功率。国际公认的标准是只要成功率高于1%,就认为破解成功。所以我们的破解方法非常有效。”高海昌解释道。

这篇论文也被信息安全顶级旗舰会议CCS'2013录用发表,“这是中国大陆研究机构首次有论文在这个高档次会议上发表。”高海昌说。成功破解了这些机制后,在论文中提出了一系列改进建议。之后,高海昌提出的部分建议被Yahoo和腾讯网站所采纳，并使用在他们的后续改进版本里面。

随着技术的发展，一些公司也推出了新奇的验证码。在寻找鲁棒性和可用性平衡点的道路上，美国谷歌公司就觅到了一条新路——利用无法识别的门牌号图片。

谷歌公司为了充实“Google Earth(谷歌地图)”和“Google Street View(谷歌街景)”,让车辆沿街拍摄图片，并将这些图片与谷歌地图服务连接，人们便能从地球的此端近距离查看彼端的街景。“街景车扫描过程中,总会遇到一些无法识别的门牌号等，谷歌公司便将其作为验证码。”高海昌说。

具体做法是,设置两种验证码,其中之一作为验证程序，另外就用无法识别的门牌号照片替代,只要将第一种验证码输入正确,无论第二个输入什么都算成功。“他们再将人眼识别的结果进行统计，按照大部分人填写的数字,得出模糊的门牌号到底是什么。可谓一举两得。”高海昌解释道。

验证码:互联网安全的第一道护卫

验证码并非自互联网诞生之日起就存在。在互联网尚不普及的年代,黑客的数量屈指可数，也还没有人想到去占领有限的网络资源。

最先推出验证码的是雅虎公司。他们一边提供免费邮箱，一边还要解决用户们每天遇到的数以百计的垃圾邮件轰炸。

于是,验证码诞生了。“它就像是互联网前端的守护者。”高海昌说。

郭刚制图

目前，国际知名的验证码研究团队有三个，而在国内专注研究验证码的恐怕已知的只有高海昌团队。“像中国科学技术大学、南京理工大学、重庆大学、解放军电子工程学院等也有一些学者在关注和进行研究，并发表了一些相关的研究论文，但是他们并未把研究重心都放在验证码研究。”高海昌说。

计算机身份认证领域研究出身的高海昌，最终决定将重点放在验证码上,是因为“验证码作为一种能够防止网络资源被滥用的有效手段,其不易被破解的程度(也称鲁棒性)和可用性迫切需要提高,所以也促使我决定将近几年的研究重心放在验证码研究方面。”

现在，高海昌带领团队的验证码研究获得了国家自然科学基金的资助。在今年12306火车票售卖网站修改验证码事件中，高海昌也向有关部门提出了自己的建议。“不论图片还是字母的验证码,区别的都是人与计算机,这需要找到人工智能(AI)机制,让人容易通过,但是计算机程序则难以跨越。”高海昌说,“在这个过程中,最难的就是,如何保证验证码不易被破解,同时还要实现用户友好。”

安全无小事

研究、破解、提升、再破解、再弥补……在验证码此消彼长的拉锯战中，高海昌看到更多的是乐趣。“破解和防破解在某种程度上是互相促进,水平都在提高。但道高一尺,魔高一丈,验证码机制的设计者在明处,破解者在暗处,两者的较量本来就是不公平的。所以目前来说，还没有人敢说能提出一种永远无法被破解的验证码机制。事实上也是这样,现在99%的网站所使用的验证码机制其实已经都被成功破解了。”高海昌说。

在这个过程中，验证码识别的研究永远是一个双赢的结果：或者有一种验证码不能被破解,网络安全依然有保障;或者验证码被识别，则人工智能和机器学习水平得到进一步的提高。

“但是,现在我们羊圈的围栏很低,也有很多漏洞，而且很多不安全的验证码机制仍然在被大量使用。比如国内的一些银行。”高海昌说。尽管一些银行已经将验证码、U盾、短信等联系在一起，但是却依然存在一些购物网站不用U盾也能完成购物的情况。“这样就给用户带来很大的不安全性。”高海昌表示。

虽然验证码研究只是信息安全领域的一个很小的方面，但是斯诺登的棱镜门事件让人认识到整个计算机和网络空间的安全问题都不容大意。“网络安全无小事，棱镜门让我们认识到国家信息安全和个人信息安全都面临着严峻的形势,需要相关从业者不断努力,提升安全水平。”高海昌说,“验证码就要站好第一班岗。”

一问一答

《速7》中的『天眼系统』距现实有多远

当前火爆上映的电影《速度与激情7》(以下简称《速7》)中出现了一套很“酷炫”的系统被称为“天眼”的系统,这套能够调用地球上任何位置的摄像头和音频系统(如手机)，让你想要搜索的人或事物无所遁形。那么,这在现实中有可能实现吗?天眼系统中有哪些即将来临的高科技?

问:《速7》中的“天眼系统”距离现实有多遥远?有哪些即将实现的高科技?

答:其实,已经有不下数十部电影描绘过这个大数据应用前景。现实中要实现,代价可能很大,大到只能实现部分功能(比如实时监控),因为这需要系统具备高速的数据计算能力和大数据存储、挖掘和分析的能力,所以,这绝对不是电影中一个U盘大小的芯片能够实现的。不过,随着大数据和物联网时代的到来,建设“天眼系统”在技术上并不遥远。

影片《速7》中,天眼主要是依靠世界上互联的监控摄像头。这其中一项让人印象深刻的技术是“人脸识别”,电影中的敌对组织头目利用人脸识别来确认一行人的行踪。其实,人脸识别这项戴着高科技光环的技术已经在一些高级别的保密场合中得到应用，比如用于受安全保护的地区的门禁系统、考勤系统和智能手机上。

广义的人脸识别实际包括构建人脸识别系统的一系列相关技术，包括人脸图像采集、人脸定位、人脸识别预处理、身份确认以及身份查找等；而狭义的人脸识别特指通过人脸进行身份确认或者身份查找的技术或系统。电影《速7》中的人脸识别显然应归类为前者。

人脸识别的优势在于其自然性（进行个体识别时所利用的生物特征相同）和不被被测个体察觉的特点，不过要想在各种场合下使用它,也困难重重。不同个体之间的区别不大,所有的人脸的结构都相似,甚至人脸器官的结构外形都很相似。这样的特点对于利用人脸进行定位是有利的,但是对于利用人脸区分人类个体是不利的。此外,人脸的外形很不稳定,人可以通过脸部的变化产生很多表情，而在不同观察角度,人脸的视觉图像也相差很大,另外,人脸识别还受光照条件、人脸的很多遮盖物(如口罩、墨镜、胡须等)、年龄、拍摄的姿态角度等多方面因素的影响。迄今为止,人脸识别被认为是生物特征识别领域甚至人工智能领域最困难的研究课题之一。

值得一提的是,有不少观众指出,影片《速7》中的天眼系统类似于游戏“看门狗”中的“超信息化的中央操作系统”(ctOS)。系统的真实原型来自芝加哥2006年建立的虚拟防范计划(Operation Virtual Shield)。

在该游戏中,ctOS是由一台超级计算机控制城市的各种公共设施,同时管理和收集城市公民的所有数字信息。这个系统可以控制包括公共交通、城市电力、电子监控、银行系统、警察系统等各方面,同时将所有联网信息进行收集和整合,记录下公民的医保号、医疗记录、犯罪记录、甚至上网阅览内容、输入习惯等,结合以大数据分析时时更新后台资料。玩家可以利用这个系统了解一个人、找到一个人。

未来将是一个万物联网的时代，将会产生许多大数据的处理需求,从而倒逼技术不断升级。只要网络带宽足够大,影片中的天眼系统是有可能实现的。不过,信息安全也同样重要,在各国高度重视信息安全的形势下,天眼系统最初可能将以微型系统的方式登场。　(赵鲁)

趣味科学

舔完一根棒棒糖需要1000下

知道一根棒棒糖能舔多少次吗?谁会无聊到真的记录自己舔棒棒糖的次数。答案是,科学家。因为这项过程无聊结果又十分有趣的研究，纽约大学柯朗数学研究所的黄金紫团队获得了2015年“菠萝科学奖”数学奖。

科学家也不是专门为了搞清楚这个答案而做的实验。事实上,这项研究的初衷是为了解释溶解过程在自然界中的作用，却意外地用所推导出的数学公式计算出了这个“世界难题”的答案。

黄金紫介绍,在自然界中,有水流过的地方都会留下水特有的痕迹。一方面,水在流过固体表面时，通过侵蚀或溶解带走物质,从而改变固体的形状;另一方面，改变形状的物体又会干扰到水的流动，从而改变水流的速度并且影响物质被带走的速度。研究要观察的正是变边界固体——流体相互作用问题。

众多的水流侵蚀现象中,团队先选择了溶解作为研究方向，而球形是最简单的几何形状,均匀水流是最基本的水流。科研人员试图通过这种简单组合了解固体在水流中溶解的基本规律。

棒棒糖毫不意外地成为了一种最易获得的球形可溶固体。

他们把棒棒糖放在能产生均匀水流的实验用水洞中,让水从管道里流过。然后用延时摄影拍下棒棒糖的溶解过程。

研究人员发现，棒棒糖在溶解的过程中会形成一种独特的形状。根据黄金紫的描述，水流会将棒棒糖雕刻出圆而光滑的前部，在这之后由于水流从固体表面分离导致了球面上两道明显的分离线,再之后,由于水流在尾流区的混合,使棒棒糖的后部形成了平滑的表面。

> “这项研究的初衷是为了解释溶解过程在自然界中的作用,却意外地用所推导出的数学公式计算出了这个“世界难题”的答案。

图片来源:百度图片

这让研究人员很好奇。于是,他们又选择了其他几何形状的棒棒糖重复这个实验,结果发现,在快要溶解时,棒棒糖留下来的形状几乎总是一样的。

而在得到了这样一个形状后,他们又注意到，棒棒糖在溶解的过程中其溶解速率在不断增加。因此,研究人员希望通过理论求解棒棒糖的体积是如何随时间变化的。所得到的公式可以用来预测可溶解的固体在流动的液体中溶化所需要的时间。

不过,那时谁也没有意识到这项研究距离回答“一根棒棒糖能舔多少次”的“世界难题”只有一步之遥。

直到得到这个公式的几天之后,应用数学实验室的一位教授灵机一动，指出这个公式似乎可以解释那个困扰了很多人的问题。于是,大伙儿聚在一起,用新得到的公式算出了这个数字——直径1厘米左右的棒棒糖,大约需要舔1000次。

只是,谁也不能保证,理论推导得出的结论一定可靠，实践才是检验真理的唯一标准。

好在,推特上真的有“无厘头”的网友将自己亲自实验的结果摆了出来，一根棒棒糖舔到中心大约需要850次。

结果还算大体相近,可如果你非要知道到底是1000次还是850次更准确,除了自己花5毛钱重复一遍，似乎也没有别的办法了。事实上，在该研究公布之后,已经有不少实验党埋头苦舔啦!

(朱香综合整理自网络)

北京科普

(本栏目由北京市科委共办)

公众参与创新北京行动计划收获1000多项创意项目

由北京市科委联合新华网、北京发明协会等单位实施的公众参与创新北京行动计划(第一季)进入收获期,截至2014年底,相关合作单位共收到1000多项创意项目，彰显了公众参与创新北京行动计划的热情。

创新精神是一个国家和民族进步的灵魂。创新,不只是知识渊博的专家学者的事，只有激发起全民自主自发的创新意识，才能提高国家创新的广度和深度。那么,如何提高全民的创新积极性,释放我国人口数量蕴藏的巨大创新潜力?如何降低创新的门槛,打开创新大门的枷锁?如何让创新成果得到社会的广泛关注,并建立转化为生产力的通道或平台?

2014年5月,按照北京市委、市政府关于深入实施创新驱动发展战略的决策部署，立足首都城市战略定位，围绕北京建设国家科技创新中心对公众科学素质和创新环境的要求，北京市科委联合新华网、清华大学、北京发明协会等6家单位启动实施了公众参与创新北京行动计划(第一季),并开设了基于互联网的“北京网上科技创意坊”,将公众需求和创新主体供给进行对接,实现双方互动。希望有更多的人成为创新参与者和创新成果的受益者，使创新成为全社会共同的价值追求。

在去年的启动仪式上，北京市科委主任闫傲霜曾表示,对于参与的内容,公众、专家团队和专家机构将进行分类评价,依托市场机制,与创新创业的企业、孵化器或投资机构、大学生创意创新平台、民间发明创新活动以及市政府相关部门等进行对接,挑选出大家愿意支持的创意、设计等,把好的创新想法变成好的创新产品,提供给社会。

据了解，通过相关合作网站开展创意项目的征集,截至2014年底,共收到1000多项创意项目。经过筛选和专家评选,共选出60项创意项目进行网上展示，通过广大网友点赞投票的方式选出最受欢迎的创意项目、创意个人和团队。

据介绍,征集到的创意项目,体现了公众创新创意的智慧。例如由北京发明协会征集的“三轮活力板”项目,其核心技术是三个踏板由一个可以扭转的“Y”字型弹性钢板连接,每个踏板下有一个万向轮。而传统两轮活力板不易掌握平衡,初学者难学会,易摔伤,因而失去大量小孩及女性顾客群。三轮活力板同时具有灵活性和平稳性;既有灵活性,做各种花式动作,同时初学者易掌握平衡,易学会,适合广大儿童、年轻人玩,具有巨大的市场潜力。

而“2BL-280A型水稻盘育秧播种流水线”创意产品采用螺旋式排种专利技术，改传统直线排种为螺旋排种,实现了螺旋交替充、排种,大大提高了播种均匀性,具有播量调节方便,小播量精密播种均匀度高等优点,广泛应用于常规稻、杂交稻和超级稻的育秧播种。该产品现已通过部级科技成果鉴定。目前该水稻盘育秧播种流水线是移栽育苗的关键技术装备,解决了机械化育苗精准按粒对穴播种的难题;采用模块化组件,满足不同品种通用性的要求,适用于水稻、油菜、烟草、蔬菜及花卉等作物高效工厂化的精密盘育苗。通过产品的实施,对提升国产精密育苗装备竞争力,提高我国种植业机械化水平、保障粮食安全和有效供给具有重要的战略意义。

“希望有更多的人成为创新的参与者和创新成果的受益者，进一步推动创新精神成为全社会共同的价值追求。”闫傲霜表示,通过“创新参与平台”这个载体,将调动社会参与创新的积极性,共同推动创新创业环境的优化。

据悉，公众参与创新北京行动计划第一季的活动分为三个阶段。今年3月份到5月份,是商业模式对接和持续传播阶段，将对评价结果好的项目、成果,在今年5月的科技周现场进行集中展示。

(郑金武)