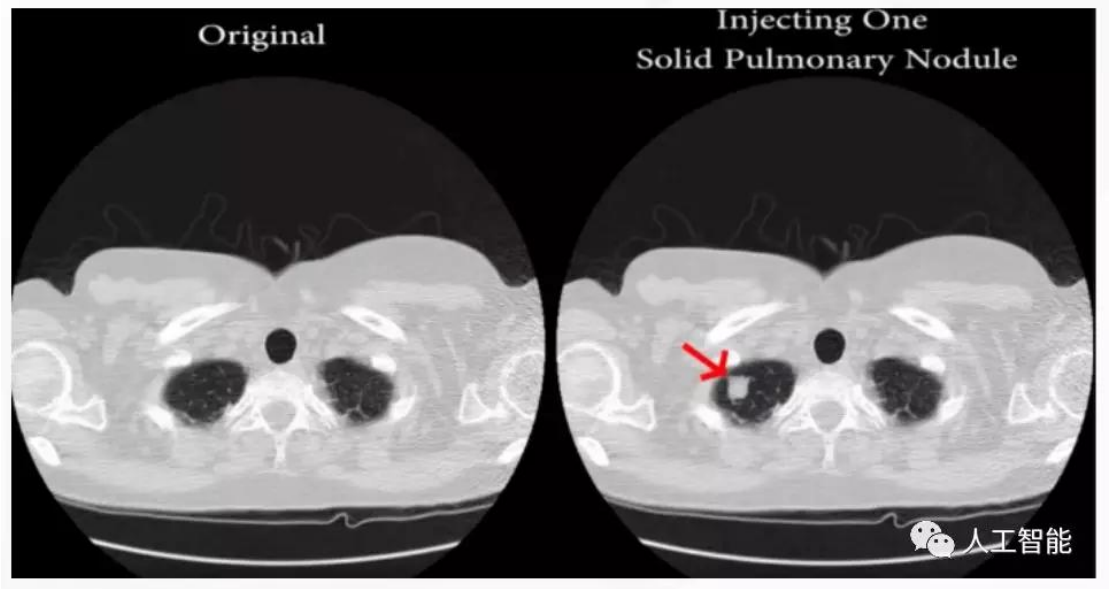
安全研究人员通过机器学习伪造 CT 扫描结果中的癌细胞节点

人工智能4 月 7 日

当我们获得 CT 或 MRI 扫描时，我们希望结果是准确无误的。毕竟我们正在谈论的是可能花费数百万美元的设备和经过多年培训或具有几十年经验的放射科医师。然而，医院安全性可能很宽松 ,研究人员现在已经证明他们可以使用生成性对抗网络(GAN ）伪造 CT 和 MRI 扫描结果。

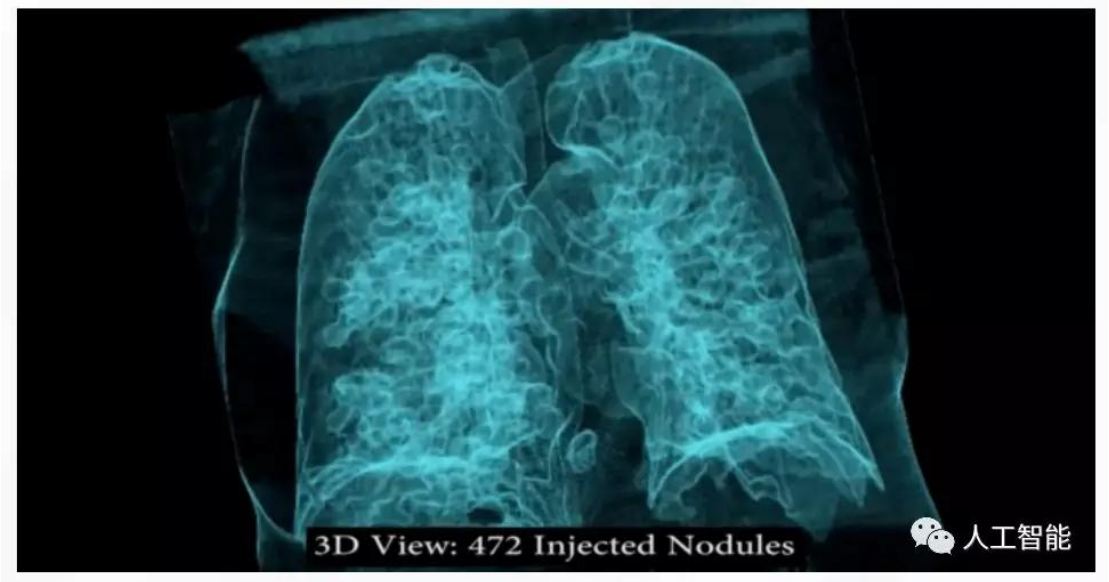


以色列研究人员制造的恶意软件可以很好地改变 CT 和 MRI 扫描结果，从而“愚弄”放射科医生。深度学习软件可以创建逼真的假冒恶性肿瘤，或者可以近乎实时地隐藏扫描结果的真实情况。

“我们使用 3D 条件 GAN 实施攻击，并展示框架（CT-GAN）如何实现自动化，”Yisroel Mirsky、Tom Mahler、Ilan Shelef 和 Yuval Elovici 在他们的研究中表示。“虽然身体很复杂，3D 医学扫描非常强大，但 CT-GAN 可以实现真实的结果，可以在几毫秒内完成。”

在盲法研究中，使用 70 次改变的肺部扫描结果，该软件几乎每次都会欺骗 3 名经验丰富的放射科医师。在他们看到假的癌细胞生长的情况下，他们认为存在癌细胞节点的几率为 99%。在恶意软件清除了实际肿瘤的扫描中，他们认为不存在肿瘤的几率为 94%。

然后，研究人员对用于检测图像中肺癌的软件进行了测试，放射科医生使用该软件确认自己的诊断。其百分之百地误诊了假结节。



“我感到非常震惊，” 参加这项研究的加拿大放射学家 Nancy Boniel 告诉《华盛顿邮报》。“我觉得地毯是从我身下拉出来的 ,而我却没有必要的工具向前移动。” Yisroel Mirsky、Yuval Elovici 和以色列 Ben-Gurion 大学网络安全研究中心的另外两人创建了恶意软件，以强调缺乏安全保护的诊断设备和其他医院系统。该软件专为本研究而设计，因此对医疗保健行业而言并非存在危险。然而，他们确实将其视为医院、医生和放射科医师未做好准备的风险的明确例证。

研究人员担心这种攻击可能会干扰政治对手或更糟。

“攻击者可能会采取这种行为，以阻止政治候选人，破坏研究，实施保险欺诈，实施恐怖主义行为，甚至谋杀，” Mirsky 等人的研究中写道。

他们表示，恶意方可以使用中间设备来解决攻击。他们使用 Raspberry Pi 3 在他们的视频中展示了这样的攻击 ,他们以大约 40 美元的价格购买了它。由于从 CT 或 MRI 扫描仪传输的数据未加密，攻击者可以轻易伪造扫描结果，然后将扫描结果发送回接收服务器。

解决问题看起来就像加密网络上的数据一样简单。然而，FDA 的科学与战略合作伙伴关系副主任 Suzanne Schwartz MD 表示，并非如此简单。

Schwartz 说道：“这需要的改变远远超出设备，而是需要改变网络基础设施。许多医院没有将资金用于投资更安全的设备，或者他们有 20 年历史的基础设施，不支持

更新的技术。这是吸引和参与其他当局并试图将整个社区团结在一起变得非常重要的地方。”

至于对这种攻击的受害者造成的后果是，虚假扫描结果可能导致患者接受手术或化疗。此外，有很多副作用可能会给患者带来麻烦。

“在我们接受某人接受手术[或管理化疗]之前，有几个步骤，” 加州大学圣地亚哥分校急诊室医师 Christian Dameff 说道。“但无论如何，患者仍然受到伤害。[从了解到你可能患有癌症]存在情绪困扰，并且存在各种各样的保险问题。”