论 见

向科技自立自强要战斗力

■裴 帅 石海明

9月3日，纪念中国人民抗日战争暨世界反法西斯战争胜利80周年大会在北京天安门广场隆重举行。

从坦克、舰载机、歼击机到无人智能和反无人装备，从网电作战等新型力量装备组团亮相到高超声速武器集体展示……阅兵场上，一系列国产化受阅装备令人振奋，反映出我军装备的迭代速度，也勾勒出一幅科技自立自强的时代画卷。

科技兴则民族兴，科技强则民族强。科技自立自强是国家强盛之基，安全之要。当前，世界各国军事实力的较量，从深层次看就是科技创新能力的较量，尤其是自主创新能力的较量。科技自立自强，始终是建设科技强国的必然要求，是打赢未来战争的必经之路。

——向科技自立自强要战斗力，要求我们必须“瞄准关键核心技术特别是‘卡脖子’问题，加快技术攻关”。曾经，面对帝国主义的武力威胁，我国科技工作者依靠自己的力量，仅用近10年时间就创造了原子弹爆炸的奇迹，增强了我国国防实力，振奋了民族精神，提高了国际地位。自力更生，成为科技强国、科技强军的有力支撑。如今，环顾阅兵场上的参阅武器装备，首次亮相的新型装备占比很大。从新一代陆战装备“100坦克”，到“20家族”领衔的国产全谱系航空装备受阅梯队，再到配装新型国产发动机的“运-20B”运输机，无不体现出我国对关键核心技术的持续突破。

——向科技自立自强要战斗力，离不开人才，特别是创新拔尖人才的支撑。“盖有非常之功，必待非常之人。”美国人曾经评价钱学森“一个人可以顶5个师”。今天，亮相阅兵场的装备背后，是一个个生机勃勃的年轻科研团队。据悉，中国兵器装备集团等军工企业中，35岁以下青年科研人员占比已超过50%，他们正在成为科技创新的主力军。“江山代有才人出”的生动局面启示我们，把科技的命脉牢牢掌握在自己的手中，就必须把人才作为支撑发展的第一资源。曾经，我国关键核心技术受制于人，本质上是高端人才供给不能完全适应建设世界科技强国的需要。实现高水平科技自立自强，一个重要的着力点就是围绕国家安全所需技术和大国竞争关键领域强化人才布局，培养一批高水平科技人才。

——向科技自立自强要战斗力，需要精准对接未来战场，紧盯颠覆性技术发展打造更多制胜“铁拳”。当前，新一轮科技革命和军事革命日新月异，科技从来没有像今天这样深刻影响国家安全和军队建设发展。阅兵场上接连亮相的“光之利刃”“闪击重锤”“点穴利器”“战略王牌”，让很多“军迷”惊呼自己已变“军盲”。由此可见，战场需要什么，自主创新的方向就对准哪里。面向未来战场，只要始终坚持高水平科技自立自强、自主创新，加强前瞻谋划设计和战略性、前沿性、颠覆性技术攻关，就能形成独特的军事科技优势，在新征程上赢得主动，保障军事发展主动权、未来战争制胜权。

唯创新者胜，唯自立者强。阅兵场上的装备方队渐行渐远，但科技强军的征程仍在继续。“历史的道路，不全是坦平的，有时走到艰难险阻的境界，这是全靠雄健的精神才能够冲过去的。”在强军新征程上，只要我们不畏艰险、奋勇攀登，就一定能抢占世界军事科技竞争战略制高点，以高水平科技自立自强为强军兴军提供坚实支撑。

打开手机，你是否有过这样的疑惑：眼前声情并茂的名人演讲视频、新闻事件的现场照片，是真的还是AI生成的？

随着技术发展，借助生成式AI技术制作的内容日益逼真，它就像一个超级“内容制造机”，能够根据用户输入的指令或条件，创造出文本、图像、视频等新内容。

其中，有些生成的内容几乎可以达到以假乱真的地步。比如，利用生成式AI技术实现换脸、拟声等，导致虚假信息泛滥、用户身份信息被冒充等乱象发生，严重破坏网络生态，对信息安全和公共信任构成严峻挑战。

为了解决这些难题，生成式AI水印技术应运而生。该技术在AI生成的内容中嵌入肉眼不可见的特殊标记，犹如为数字产品盖上一个隐形的“防伪印章”。

前不久，第十六届夏季达沃斯论坛在天津召开，论坛发布了2025年《十大新兴技术报告》。生成式AI水印技术正是位列其中的十大新兴技术之一。

此外，《人工智能生成合成内容标识办法》自2025年9月1日起正式施行，旨在规范人工智能生成合成内容的标识标注要求，标志着我国对生成式人工智能的治理从原则性规范迈向精细化规范的新阶段。

那么，什么是生成式AI水印技术？该技术目前发展程度如何？请看本期关注。

生成式AI水印——

人工智能产品的“防伪印章”

■秦 政 王艺霖 李旭东

高技术前沿

给数字内容做一个“秘密记号”

从本质上看，生成式AI水印技术是为了应对生成式AI技术，发展起来的一种安全机制，进而实现对AI生成内容的来源追溯与真实性验证。

该技术的核心原理是在AI生成的内容中，嵌入一种特殊的、不容易被人察觉到的标识信息，在不影响内容质量的前提下，让机器能够在后续检测中识别内容来源。

通俗地说，生成式AI水印技术就像给数字内容做一个“秘密记号”，这个记号平时不会干扰用户对内容的正常使用和浏览，但关键时刻能通过专用工具检测出来。

和传统数字水印技术相比，生成式AI水印技术显得更加“低调”。

传统数字水印标识，往往出现在用户肉眼可见的地方。例如，图片上的作者ID，或者视频角落的频道标识，都是人们能明显看到的。

相比之下，凭借独有的技术特点，生成式AI水印“藏”得很深，人们用肉眼很难发现水印标记。

——不可感知性。这意味着水印嵌入后，生成内容的视觉、听觉或者语义质量基本不会受到影响。例如，我们观看一张嵌入了生成式AI水印的图片，会发现这张图片无论是色彩还是细节，都和原图一模一样。

——鲁棒性。生成式AI水印技术的这个特性，保证了人工智能生成的产品在经历剪切、转码等操作后，水印依然不会“消失”，能被正确完整地提取出来。

——可验证性。这是指嵌入人工智能生成内容中的水印信息，能够始终通过专用算法或密钥被准确、可靠地提取和验证。可验证性与鲁棒性密切相关，只有当水印具有足够的鲁棒性，在人工智能生成的内容经过各种处理后仍然保持完整，才能为可验证性提供基础。

——可追溯性。生成式AI水印可以用于追踪生成内容的来源，确定其是由哪个AI模型生成的。例如，用户通过检测水印，可以判断生成的内容文本是由Deepseek生成，还是由其他模型生成。

可以说，生成式AI水印技术的出现，为数字内容的版权保护、安全管理和真实性验证提供了重要支持，是构建可信数字生态的关键技术之一。

在图像生成工具中，输入“天很蓝”指令后生成的图片。图片中嵌入了不可见水印，能通过特定技术手段检测出来。

不同模态数据的不同实现路径

目前，针对文本、图像、视频、音频等不同模态的数据，生成式AI水印的形态正在不断丰富，呈现出各具特色的实现路径。

文本类生成式AI水印，就像给文章打上了“只有机器才能看到的暗号”。

生成式AI在写作时，并不是直接“想好一句话”，而是逐字逐词，根据概率选择下一个词语。例如，写“今天心情很……”，生成式AI可能给出：“好”40%，“愉快”30%……

生成式AI水印技术的原理就是在生成过程中，对候选词的选择概率进行轻微调整，让整段文本的统计特征带有特定的“记号”。这种签名对人类阅读毫无影响，但该技术经过分析可以还原出这个“记号”，从而对AI生成内容进行身份识别。

对于上述的例子而言，水印组的词汇是“好”“愉快”；非水印组的词汇是“不错”“棒极了”等。

也就是说，在检测时，扫描整篇文本，生成式AI水印技术如果检测出文章中“水印组”的词频异常高，那就能够证明这篇文章是AI写的。

相比文本类生成式AI水印，图像类生成式AI水印技术则更加成熟。

本质上，图像是一种结构化的像素矩阵。图像类生成式AI水印，通过在高频像素数据中添加微小扰动或植入特定模式，从而实现水印的嵌入。

具体而言，在一幅图像中，每个像素包含3个数值，每个数值的范围是0~255。当这个数值在一个很小的范围内上下波动时，比如从127变成126或者128，人眼是很难观察到的，但机器则可以进行识别。

以著名图像生成工具Stable Diffusion为例。它能够在生成图像时自动调整像素值，从而嵌入只有检测工具才能读出的水印。

视频类生成式AI水印的难度更大，需要同时兼顾单帧画面的空间信息和多帧图像之间的连续性。

视频是由多帧图像组成的，其嵌入水印的常见方法，是在多个帧的像素亮度或颜色信息中重复嵌入相同的标识，并利用时间冗余来提高鲁棒性。

例如，某视频生成系统在生成视频内容时，每隔固定帧数就会在画面中嵌入极小幅度的变化像素值。当生成一段AI合成的视频时，这类水印会在每一秒钟的多帧画面里重复写入相同的编码，如此，即便视频被剪辑、转码或压缩，视频中依然有足够的帧画面保留水印信息。

音频类生成式AI水印，主要通过在声音信号中嵌入特定的频率或相位信息，实现标记。

声音本质上是一种振动波，人耳能够感知的声音振动频率范围为20Hz到20kHz，对区间内极高频和极低频部分很不敏感。

因此，音频类水印通常在高频段植入信号，这些信号在频谱分析中会显现出特定模式，但人耳察觉不到。

例如，一个AI配音系统在生成“欢迎收听”这句话时，会在高于18kHz的频率区域中嵌入一段特殊的声音，人耳听不到，但检测器却能“听到”并识别其中的内容。通过这种方式标记的水印，具有较好的抗压缩和抗干扰能力。即便音频被转成低码率或加入环境噪声，水印依然可以被识别。目前，该技术已被用于版权保护、虚拟主播身份验证、AI音乐溯源等领域，未来还可能与视频、文本结合，实现全链路的多模态水印。

可以看到，生成式AI水印的技术体系并非单一形式，而是伴随生成式AI技术的发展逐步演化。针对文本、视频、音频等不同模态设计的不同技术实现路径，帮助用户辨别生成式AI产品，为未来的标准制定与法律监管提供了技术支撑。

在多领域为内容安全护航

在人工智能生成内容爆发式增长的时代，生成式AI水印技术正应用于多个领域，成为构建数字信任体系的重要基础，为内容安全护航。

——版权保护与溯源。在内容创作领域，创作者可以借助生成式AI水印技术，在自己的作品中嵌入创作者身份等信息，确保自己的创意不被他人盗用。这将保护创作者版权，一旦发现侵权行为，水印就像是一张“证据牌”，在关键时刻帮助创作者维护自己的权益。

同时，版权登记机构也能通过深度整合水印检测技术，实现作品自动确权、侵权追踪和版税结算等。

——内容认证防篡改。生成式AI水印技术可以与内容认证平台结合，验证内容真伪及生成来源，防止信息被篡改。

以新闻机构发布新闻为例。利用生成式AI水印技术，新闻平台可针对深度伪造视频、虚假新闻稿等实施内容过滤、限流或标注警示，有效遏制虚假信息传播，提醒用户甄别筛选信息。

又如，在科研领域，生成式AI水印技术能够精准检测出学术论文和评审意见是否由AI生成，有效遏制学术不端行为。

——数据隐藏与秘密通信。在国家安全领域，生成式AI水印技术能被用于情报安全、信息攻防与认知对抗方面，成为维护国家安全的关键技术手段。生成式AI水印可以辅助政府部门确认信息的真实性，确保发布的政务信息经过官方审核，防止不法分子利用AI生成虚假的信息误导公众。

另外，通过在敏感文件、分析报告中嵌入高隐蔽性水印，可以快速溯源追踪文件的传播路径与责任人，有效防止失泄密行为的发生。

值得一提的是，未来战场上，指挥员利用生成式AI水印技术，还能快速检测敌方散播的伪造音视频、煽动性信息中的AI生成痕迹，及时进行反制和舆论澄清，瓦解其认知攻击。

不过，尽管生成式AI水印在各领域展现出广阔的应用前景，但正如很多刚刚诞生的技术创新一样，生成式AI水印技术在带来机遇的同时，也引发了一系列不容忽视的挑战。

首先，抵抗内容编辑和针对性攻击的能力是核心难题。对于有的生成式内容，用户通过改写即可破坏技术保护能力，抹除AI标记，科研人员只有进一步加强鲁棒性对抗才能够提高AI水印的应用价值。

其次，通用性与标准化还需完善。目前，行业内缺乏统一的水印标记技术标准，不同厂商的水印技术不兼容，检测工具也不通用，用户若想验证一段内容的来源，可能需要同时使用多个工具，效率较低。

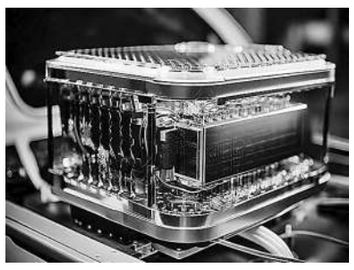
我们正生活在一个被数字内容包围的时代，如果虚假信息以假乱真，那么人们将逐渐丧失对数字世界的基本信任。从这个层面来说，合理运用生成式AI水印技术，将是数字时代内容保护与管理的关键一环，是我们通往可信数字未来的桥梁。

科 技 云

科技连着你我他

■本期观察：卢晨昊 李炜梁 曹兴旭

硅负极锂离子电池



据悉，复旦大学研究团队和中国科学院上海应用物理研究所团队共同开发了一款基于熔融盐电解质的硅负极锂离子电池，解决了锂离子电池的不稳定性和安全性问题，相关成果已在《能源与环境材料》期刊发表。

相较于传统以石墨作为负极的锂离子电池，硅负极锂离子电池的理论电容量远超其上。传统锂离子电池在充放电过程中会产生体积膨胀，导致电极颗粒粉碎、固体电解质界面不稳定和容量衰减。该电池有效地解决了这一问题，其熔融盐电解质能在硅负极表面形成结构均匀的无机界面，具有良好的机械韧性，从而大幅提高电池的机械稳定性、充放电效率和循环使用寿命。

随着全球向可再生能源系统和电动出行转型发展，基于熔融盐电解质的硅负极锂离子电池能够满足电网储能对安全、高能量电池系统的需求，将有力推动形成耐用性强、能量密度高的储能系统。

新型高能锂电池

近期，天津大学研究团队成功开发了一款基于离域电解液的新型高能锂电池。据悉，研究者提出了一种全新的离域电解液电池设计思路，相关成果已在《自然》杂志发表。

该电池的核心优势在于其摒弃了传统电解液设计对主导溶剂化结构的依赖，通过引入多样化的电解液微环境，增加溶剂化环境的无序性，从而优化整体电解液性能。这种设计理念能够有效平衡溶剂主导和阴离子主导的溶剂化结构，减少动力学障碍，稳定电极与电解液界面，大大提高了电池性能。

随着电动飞行器、无人机等新兴领域对高能量电池的需求不断增加，凭借长循环使用寿命和高能量密度等优异性能，新型高能锂电池有望在这些领域提供更加高效的能源解决方案。

新型钠离子电池

近日，温州大学研究团队开发了一种基于含硫添加剂的钠离子电池，该电池有效提升了电解液在钠离子电池中的抗氧化能力，大大增加了电池循环使用寿命，相关成果已在《先进功能材料》期刊发表。

钠离子电池因资源丰富、成本低、温度适应性强，被视为锂离子电池的有力替代品。不过，钠离子的实际应用受限于其电化学性能不足。研究人员发现，改变溶剂化鞘层结构、构建电极—电解液界面并抑制过度金属溶解，能显著提升电池电化学性能。经过实验测试，新型钠离子电池的电容量保持率约为传统电池的两倍，在不同温度和电流密度下均表现出优异的性能。

未来，该电池有望在电网储能系统、电动汽车和电动飞行器中广泛应用。