AI看图定位 超60%结果误差小于1.6公里

社交媒体照片可能被轻易“开盒”

当AI拥有了“视觉”，会展现出什么样的能力？日前，OpenAI发布了最新大模型ChatGPT o3和o4-mini，不仅能识别、理解画面内容，还能通过画面细节关联公开数据库，一步步推理出结论。记者实测发现，ChatGPT o3可根据一张普通街道照片，精准定位照片拍摄位置。在AI新“进化”出的强大图像理解与推理能力面前，如何兼顾个人信息保护成为亟待解决的新问题。

1 ChatGPT o3可分析照片 精准定位拍摄地

近日，OpenAI发布的最新大模型ChatGPT o3和o4-mini更新了视觉推理能力。不同于简单的图像识别，AI会像人类侦探般执行“观察-分析-验证”的完整思维链。网友发现，ChatGPT o3可根据一张照片中的种种细节，例如植被特征、标志性建筑、车牌甚至是一个特殊定制的餐盘，精准定位照片拍摄地点。

记者选取了3张照片进行实测，发现ChatGPT o3的确展现出较为精准的定位能力。对于第一张公交站附近随手拍摄的照片，AI准确捕捉到了栏杆横幅一角模糊的字体信息，将其裁切放大识别出“天河区石牌街道办事处”字样，并认为这是定位的关键信息。

对第二张俯瞰的风景照，AI通过裁切放大天际线处模糊的高楼轮廓，对比识别出广州市的地标建筑，再结合照片中出现的植被特征及拍摄视角，准确推理出照片拍摄地点位于广州白云山。

而对于第三张缺乏标志性建筑及提示性文字的普通街道照片，AI思考了10多分钟。它选择从街边店铺招牌下手，先是反复识别确认招牌上的文字信息，然后结合联网搜索能力，逐一查询店铺所在城市及具体位置，再对比百度地图街景显示的店铺排列顺序，排除掉所有其他可能后，最终定位出照片拍摄所在街道。

2 国产大模型 尚未展现出精准定位能力

AI这种“看图定位”的推理能力，已超越大多数普通用户。记者分别测试了国内具有视觉推理功能的豆包、夸克AI相机和通义千问，发现目前定位精准度普遍不高。

豆包认为，第一张照片仅根据图中元素（如公交站、街道、建筑、标语等），无法精确确定拍摄地点，第二张照片结合常见度和城市地貌，广州白云山是较可能的选项。而第三张照片，豆包推测是在广州的老社区，如天河、越秀的居民区附近，但无法给出更精细的地点。

夸克AI相机能根据城市天际线、山体植被特征及地理位置视角，推理出第二张照片在广州白云山拍摄，其余两张照片则只能根据图片中出现的中文字符、城市建筑及植被情况，推测照片于中国南方城市拍摄，无法进一步推理具体地点。

通义千问的视觉推理模型同样无法识别第一张照片中出现的文字信息，只能推测拍摄地为某华南城市。第二张照片则根据植被特征认为是在重庆、成都等西南城市。而对于第三张照片，通义千问也能识别出店铺招牌文字、植被与气候特征、建筑风格等信息，但无法将这些信息结合地图搜索进行进一步推理。

虽然国内大模型尚未展现出精准定位能力，但可以想见，随着未来大模型能力的不断提升，当卫星地图、街景影像等外部服务接入AI后，任何人都能用AI根据一张图片快速推测出精准的位置信息。而这也揭示出个人信息泄露的风险：社交媒体上随手发布的照片将可能被人用AI轻易“开盒”。

3 除位置信息AI还能根据桌面分析用户职业

AI推理图片地理位置带来的隐私泄露风险有多大？有研究人员用ChatGPT o3展开系统性受控实验，选取了50张包含人物和私人住宅背景的真实图片，模拟测试普通用户通过上传一张图片并与模型对话，获取图片中私人住宅的精确地理信息过程。测试发现，60%的模型预测结果与真实地理位置误差小于1英里（1.6公里），84%的预测结果误差小于5英里（8公里）。这意味着普通用户上传一张照片后，AI有很大概率将图上住宅位置锁定到具体街道或街区范围。

从AI思维链可看出，与传统依赖照片元数据（如Exif中的GPS信息）的方式不同，ChatGPT o3通过整合图像识别、逻辑推理和外部数据库调取能力实现定位。即使关闭手机定位、删除Exif信息，AI仍能通过分析照片中的地标建筑、植被特征甚至广告牌文字等视觉元素，结合公开地图数据和网络信息进行定位。

值得注意的是，AI能推理出的不只位置信息，还能从部分照片细节中分析用户喜好、性格特征及职业等更多个人信息。记者拍摄了一张办公桌面照片，尝试让AI推测职业。AI推测桌面主人的职业可能与记者、编辑、社交媒体运营相关。

针对新模型带来的个人信息泄露相关风险，OpenAI在ChatGPT o3/o4-mini的系统卡片中说明已采取限制措施，模型会拒绝基于图像的人物识别请求，以及无事实依据的推理请求。但这两项限制主要针对人脸识别，和无法通过图像本身的视觉元素得出可靠结论的推断（例如根据长相推断职业），并不包括地理位置信息推理、有根据的人物性格画像分析等。

4 用户在公开平台上传照片前要加强安全意识

当AI强大的推理能力被滥用时，恶意攻击者可通过AI分析公开照片，拼凑目标人物的身份特征、活动轨迹、家庭住址、社会关系。如何避免无意中发布在网络上的图片被人用AI“开盒”？研究人员发现，图片中出现的道路布局和房屋的前院设计，是AI在精准定位时最常利用，且对定位贡献度最高的线索，另一类高频线索则是带文字标识的招牌和路牌，而遮挡这些关键元素能显著降低AI定位精度。

记者测试时同样发现，当降低第一张照片清晰度后，ChatGPT o3无法通过裁切和放大细节准确识别出图片中横幅右下角的文字信息，仅根据公交车涂装等其他信息，将照片误认为在深圳某街道拍摄。同时，对于一些缺乏文字标识、标志性建筑的图片，AI也无法找到有效细节进行精准定位，只能根据植被等推测大致城市或区域。

但研究同样发现，即使遮挡主线索，若残留足够次要线索，模型仍能锁定城市或街区。对普通用户而言，将难以预判哪些画面细节会成为AI的关键“线索”而提高防范。此外，AI的多模态推理能力仍在不断提升，仅靠用户侧的谨慎自查不足以完全应对信息泄露风险。

对此，网络安全专家、汉华飞天信安科技有限公司总经理彭根在接受媒体采访时建议，普通用户在公开平台上传照片前，要加强基本的安全意识，AI厂商应像限制AI回答违规问题一样，也为图片分析能力设定安全边界，例如限制AI分析危险的请求。

（据《南方都市报》）