

# Nawet zanimizowane zdjęcia wskażą twoją lokalizację!

4 maja 2025

Nowe, zaawansowane narzędzia sztucznej inteligencji opracowane przez DeepAI, o nazwach „o3” i „o4-mini”, rewolucjonizują sposób, w jaki można ustalić lokalizację na podstawie zdjęć. W przeciwieństwie do dotychczasowych metod opierających się na metadanych, nowe modele analizują wyłącznie wizualne cechy obrazu, otwierając drzwi do nowej, potencjalnie niepokojącej formy nadzoru.



Dotychczasowe zalecenia dotyczące prywatności w sieci często skupiały się na usuwaniu metadanych EXIF ze zdjęć, które mogły zawierać poufne informacje, takie jak współrzędne GPS. Nowa technologia DeepAI czyni te środki ostrożności przestarzałymi. Modele „o3” i „o4-mini” potrafią identyfikować lokalizację na podstawie subtelnych szczegółów widocznych na zdjęciu, takich jak regionalne oznakowania, styl architektoniczny budynków, czcionki używane w menu czy nawet kształt latarni ulicznych.

Testy przeprowadzone przez użytkowników na platformie „X” potwierdzają zaskakującą precyzję tych narzędzi. Nawet zdjęcia, które zostały celowo przefiltrowane, rozmazane lub

pozbawione metadanych, były w stanie posłużyć do dokładnego zlokalizowania miejsca ich wykonania. W jednym z przykładów, zdjęcie słabo oświetlonego baru zostało prawidłowo zidentyfikowane jako lokal w Williamsburgu. Inny test na niepozornym zdjęciu z biblioteki również zakończył się szybkim i trafnym wskazaniem jej lokalizacji.

Choć dla niektórych użytkowników może to być tylko ciekawostka, eksperci podkreślają poważne konsekwencje dla prywatności. Nowa technologia umożliwia precyzyjne śledzenie lokalizacji bez konieczności posiadania specjalistycznej wiedzy technicznej czy interakcji z osobą, która opublikowała zdjęcie. Każdy, kto ma dostęp do publicznego narzędzia AI, może potencjalnie ustalić lokalizację dowolnej osoby na podstawie opublikowanego przez nią zdjęcia.

Wyobraźmy sobie sytuację, w której zdjęcie filiżanki kawy opublikowane na „Instagramie”, pozbawione widocznych znaków orientacyjnych czy metadanych, może natychmiast zdradzić innym użytkownikom dokładną lokalizację kawiarni, dzielnicy i miasta.

Przez lata usuwanie metadanych było podstawową zasadą dla osób dbających o prywatność, od dziennikarzy i aktywistów po zwykłych użytkowników. Założenie „brak metadanych = brak” przestało obowiązywać. Nawet osoby, które wyłączyły usługi geolokalizacyjne, usunęły metadane i korzystają z sieci VPN, nie są już w pełni bezpieczne. Sam obraz stał się teraz źródłem poufnych informacji, a to, co kiedyś wymagało aktywnego ujawnienia, jest teraz biernie „wydobywane” z pikseli.

Nadzór za pomocą analizy wizualnej przy użyciu sztucznej inteligencji budzi dodatkowe obawy ze względu na jego charakter. Nie jest on prowadzony wyłącznie przez służby państwowe, nie podlega nadzorowi sądowemu, nie wymaga nakazów przeszukania czy wezwań sądowych. Dzieje się to w sposób cichy, indywidualny, na skalę trudną do uchwycenia i

niemożliwą do całkowitego zablokowania. Użytkownicy nie otrzymują żadnych powiadomień o analizowaniu ich zdjęć, ani informacji o tym, kto to robi. Brakuje również procedur zgłaszania sprzeciwu dla wykorzystywania zdjęć do analizowania ich przez AI.

W obliczu tej nowej rzeczywistości pojawiają się pytania o to, jak te informacje mogą zostać wykorzystane przez stalkerów, przestępców, szpiegów, domorosłych detektywów czy służby specjalne. Nowa era nadzoru, w której sam obraz staje się narzędziem do szpiegowania, stawia przed nami poważne wyzwania dotyczące prywatności i bezpieczeństwa w cyfrowym świecie.

Autorstwo: Aurelia

Ilustracja: WolneMedia.net (CC0)

Na podstawie: [UncutNews.ch](https://uncutnews.ch)

Źródło: WolneMedia.net