

Przegląd znakowania wodnego obrazów we współczesnych zastosowaniach

Thursday 24 April 2025 11:30 (30 minutes)

Dynamiczny rozwój sztucznej inteligencji oraz mediów społecznościowych zwiększają potrzebę skutecznej ochrony przekazywanych danych. Znakowanie wodne jest jedną z możliwych technik modyfikujących m. in. obrazy w celu śledzenia przepływu informacji i pochodzenia. W niniejszej pracy przeanalizowano różne techniki znakowania wodnego, obejmujące zarówno tradycyjne algorytmy, jak i nowoczesne systemy oparte na głębokich sieciach neuronowych. Celem badań było porównanie odporności tych metod na różne aktualnie występujące ataki w mediach społecznościowych. Do eksperymentów wykorzystano rozbudowany zbiór danych zawierający zdjęcia o zróżnicowanych parametrach. Na każdy obraz został nałożony znak wodny, który w następnych etapach był atakowany. Największy wpływ na ekstrakcję znaku wodnego miały ataki takie jak kompresja stratna JPEG, rozmycie obrazu oraz dodanie szumu. Po każdym kroku były zbierane metryki takie jak BER, QualiCLIP, LPIPS, SSIM, na podstawie których oceniano skuteczność algorytmów. Eksperymenty wykazały, że ataki bazujące na kompresji stratnej oraz rozmywaniu obrazu miały największy wpływ na ekstrakcję znaku wodnego, utrudniając odzyskanie osadzonych znaków w przeciwieństwie do ataków opartych na szumie, które miały niewielki wpływ. Metoda naiwna, wykorzystująca obraz źródłowy przy dekodowaniu, wykazuje najlepszą przeżywalność ataków. Metody oparte na głębokich sieciach neuronowych również okazały się skuteczne, jednak ich czas działania był znacząco dłuższy.

Authors: PILEWSKI, Adam; Dr HRYNIÓW, Krzysztof (Warsaw University of Technology); KORDOWSKI, Mikołaj

Presenters: PILEWSKI, Adam; KORDOWSKI, Mikołaj

Session Classification: Session C (Poster)