Biometria

Projekt 1

Facial Recognition

Piotr Syga

Celem projektu grupowego jest wykorzystanie systemu autoryzacji użytkownika w oparciu o biometrię twarzy i przetestowanie odporności systemu na zakłócenia. W ramach projektu możesz wykorzystać (trenując lub finetunując) opublikowane modele, np. InsightFace, GhostFace, DeepFace lub ArcFace. Możesz również wykorzystać dowolną sieć klasyfikującą z wykorzystaniem funkcji straty z ArcFace.
Do trenowania (lub tuningu) modelu możesz wykorzystać zbiór FaceScrub lub CelebA.

Zarówno w ramach treningu modelu, wdrażania próbek do systemu jak i podczas autoryzacji dozwolone jest wykorzystywanie preprocessingu zdjęć. System powinien umożliwiać dodawanie nowych użytkowników oraz proces autoryzacji na podstawie zdjęcia.

Zadbaj o to by parami rozłączne były zbiory: treningowy, walidacyjny i testowy, ale również zbiór próbek, które zostały wdrożone do bazy danych użytkowników. W systemie powinny być wdrożone profile przynajmniej 80 osób (w tym wszystkich członków grupy, pamiętaj, że styl zdjęć dodawanych do bazy danych powinien być zgodny z wykorzystanym zbiorem danych). Czas autoryzacji, w tym preprocessingu, nie powinien być uciążliwy dla użytkownika.

Po wdrożeniu, korzystając z nie używanych dotąd zdjęć, przeprowadź testy, które uwzględniają:

1. przetestowanie skuteczności systemu (wyrażonej w omówionych metrykach) na nie mniej niż 500 zdjęciach wdrożonych użytkowników (zbalansuj prawidłowe autoryzacje i próby podszycia się pod innych użytkowników),

2. powtórz powyższy eksperyment, z dodatkiem przynajmniej 100 zdjęć osób, które nie były wdrożone (sprawdź czy taka operacja wpływa na FPR),

3. zbadaj odporność systemu poprzez dodawanie szumu (o dowolnej charakterystyce, np. Gaussa, Poissona, błędy kompresji lub reskalowania), przetestuj na nie mniej niż 300 zdjęciach dla każdego z poziomu PSNR: (50dB, 80dB), (40dB, 50dB), (30dB, 40dB), (20dB, 30dB), (10dB, 20dB)

4. w podobny sposób zbadaj odporność systemu na zmiany luminancji — przeskaluj luminancję w sposób kwadratowy, liniowy (z współczynnikiem $\frac{1}{2}$, $\frac{3}{5}$, $\frac{3}{4}$, $\frac{4}{3}$, $\frac{3}{2}$) oraz o stałą (-100, -20, -10, 30). Pamiętaj o zakresach wartości kanału Y.

Porównaj wyniki uzyskane w punkcie 1. z pozostałymi testami oraz wynikami raportowanymi przez autorów dla modelu bazowego (lub wybranego z listy proponowanych modeli w przypadku niebazowania na gotowej implementacji).

W ramach projektu przygotuj raport, w którym zostaną wskazane:

- dane autorów (imię, nazwisko, nr indeksu, termin laboratorium)
- opisana metoda autoryzacji, ze wskazaniem wszystkich wykorzystanych źródeł oraz zaznaczonymi elementami autorskimi (w tym modyfikacji funkcji straty, zmian w architekturze, preprocessingu)
- przedstawiony zbiór danych (oraz podział na odpowiednie podzbiory) – liczba osób oraz liczba zdjęć każdej z osób użyta na poszczególnych etapach, charakterystyka zdjęć
- opisana procedura wdrożenia oraz autoryzacji
- opis procedury testowania, wyniki oraz wnioski

Raport wyślij na adres mailowy prowadzącego laboranta najpóźniej 48 godzin przed terminem oddania projektu.