Biometria

Projekt 2

Biometria behawioralna

Piotr Syga

- Termin: 14.maja 2024 (grupa wtorkowa), 15. maja 2024 (grupy środowe)
- Raport: raport należy wysłać na skrzynkę mailową prowadzącego laboratorium przynajmniej 48 godzin przed oddaniem listy (wtorek, środa 15, środa 17)

Celem projektu grupowego jest wykorzystanie systemu autoryzacji użytkownika w oparciu o biometrię behawioralną (np. rozpoznawanie użytkowania na podstawie głosu, keystroke dynamics lub charakterystyki ruchów). W przypadku identyfikacji na podstawie głosu, w ramach projektu możesz wykorzystać, np. VGGVox, GE2E, SincNet, WeSpeaker lub wybraną metodę z 3D Speaker Toolkit. Alternatywnie wykorzystaj tylko elementy systemów weryfikacji (np. embeddingi lub funkcję celu) w połączeniu z dowoloną architekturą klasyfikacyjną (możesz zainspirować się pracą J. Peng et al.).

W celu wykonaniu listy możesz użyć podzbiorów wybranych z publicznych zbiorów VoxBlink, VoxCeleb1, VoxCeleb2 lub CNCeleb[1]. Możesz też wykorzystać youtube-dl w celu scrappowania materiałów z wypowiedziami i wyodrębnienia nagrania głosu.

Dozwolone jest dowolne prefiltowanie próbek danych, jak również dobór własnego ekstraktora cech sygnału lub embeddingu użytkownika. Możliwe jest wykorzystanie gotowych checkpointów modelu, trenowanie modelu od początku lub finetunowanie modelu na nowym (np. augmentowanym) zbiorze danych. Profil użytkownika może być tworzony na podstawie dowolnej liczby próbek, natomiast czas pobierania danych podczas rejestracji nie powinien przekraczać 20 minut i być odpowiednio krótszy dla uwierzytelniania na podstawie krótkich lub ustalonych fraz (jak fixed text speaker recognition, fixed text keystroke dynamics).

Podstawowym celem projektu jest implementacja, wdrożenie i przetestowanie systemu uwierzytelniania. System powinien pozwalać na dodawanie użytkowników do systemu, a następnie weryfikację lub identyfikację nowych próbek. W przypadku weryfikacji, wejściem do systemu jest identyfikator użytkownika oraz próbka sygnału, w przypadku identyfikacji jedynym wejściem jest próbka sygnału.

W przypadku trenowania lub douczania modelu zadbaj by żaden z użytkowników wdrożonych do bazy danych nie znajdował się w podzbiorach wykorzystanych podczas

[1] wymaga rejestracji i podpisania licencji

trenowania lub douczania. Dodatkowo zadbaj by wykorzystywane w procesie uwierzytelniania próbki danych nie były wcześniej widziane przez model na żadnym etapie.

W systemie powinny być wdrożone profile przynajmniej 100 osób (w tym wszystkich członków grupy, zadbaj by długość próbek oraz częstotliwość próbkowania były zgodne z oryginalnym zbiorem). Czas uwierzytelniania, w tym preprocessingu, nie powinien być uciążliwy dla użytkownika. Maksymalna długość wymaganej w celu uwierzytelnienia próbki sygnału nie powinna przekraczać 60s.

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

1. Przetestowanie skuteczności systemu (wyrażonej w omówionych metrykach) na nie mniej niż 500 próbkach wdrożonych użytkowników (zbalansuj prawidłowe próby uwierzytelnienia i próby podszycia się pod innych użytkowników).

2. Dla podzbioru przynajmniej 500 próbek wykonaj losowo (z prawdopodobieństwem jednostajnym) przemnożenia amplitudy próbki przez wartość ze zbioru $\{25, 1, 0.04\}$ a następnie porównaj skuteczność modelu z wynikami uzyskanymi w zadaniu 1.

3. Dla wybranych 200 próbek sygnału, zmniejsz częstotliwość próbkowania poprzez pozostawienie co 2, co 5 oraz co 10 wartości (pamiętaj o metadanych). Sprawdź jak subsampling wpływa na wymaganą długość próbki sygnału oraz na skuteczność uwierzytelniania.

4. Dodaj do 100 próbek zakłócenia o rozkładzie $\{\mathcal{N}(0, 1), \mathcal{N}(0, 10), \mathcal{N}(5, 1)\}$, a następnie zbadaj skuteczność systemu.

5. Utwórz lub pobierz plik z nieregularnymi zakłóceniami (np. odgłosy psów), zmniejsz jego amplitudę, tak by maksymalna amplituda zakłóceń była połową maksymalnej amplitudy oryginalnego sygnału, a następnie dodaj zakłócenia do próbek 100 próbek. Przetestuj system uwierzytelniania na tak zakłóconych próbkach.

W ramach projektu przygotuj raport, w którym zostaną wskazane:

- dane autorów (imię, nazwisko, nr indeksu, termin laboratorium)
- opisana metoda uwierzytelniania, ze wskazaniem wszystkich wykorzystanych źródeł (np. model bazowy) oraz zaznaczonymi elementami autorskimi
- przedstawiony zbiór danych (oraz podział na odpowiednie podzbiory i metoda subsamplingu) – istotne cechy to liczba osób, liczba próbek dla każdej z osób oraz czas trwania próbek, na poszczególnych etapach czasu życia systemu
- opisana procedura wdrożenia oraz uwierzytelniania

- opis procedury testowania, prac wykonanych w celu korekty wyników dla zaburzonych próbek, wyniki, porównanie z wynikami raportowanymi przez autorów modelu bazowego (lub innych zbliżonych funkcjonalnością modeli) oraz wnioski