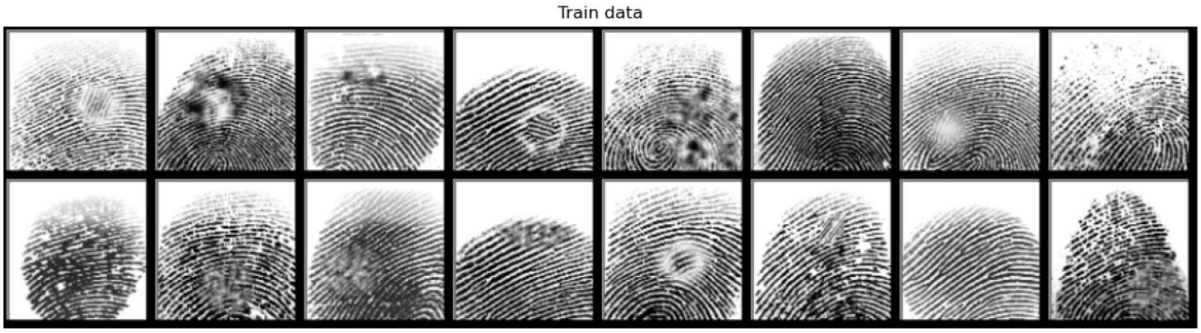
Anna Bielawska

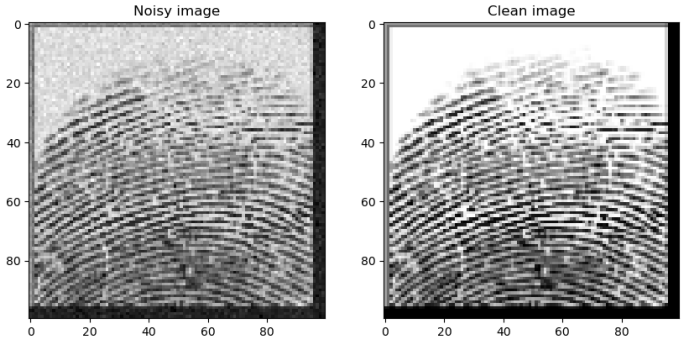
Biometryczny system autoryzacji i rozpoznawania użytkowników

Celem projektu było utworzenie systemu rozpoznawania / autoryzacji dostępu użytkowników na podstawie odcisku kciuka u lewej dłoni. W tym celu wykorzystany został zbiór odcisków palców, udostępniony do użytku niekomercyjnego, pod nazwą **Sokoto Coventry Fingerprint Dataset (SOCOFing)** (https://www.kaggle.com/datasets/ruizgara/socofing). Składał się on z 6 tysięcy oryginalnych zdjęć odcisków palców obu dłoni u 600 osób, a także dodatkowych ich zmodyfikowanych wersji (z-cut, obliteration, central rotation). W projekcie wybrano odciski kciuka lewej dłoni, po 100 użytkowników do zbioru treningowego i testowego. W zbiorze treningowym uwzględniono oryginalne i lekko zmodyfikowane zdjęcia („Easy-Altered"), uzyskując po 4 zdjęcia dla każdej osoby:



Zbiór walidujący składał się z zaszumionych szumem Gaussowskim(0, 0.05) oryginalnych zdjęć 100 użytkowników ze zbioru treningowego:

Szum dokładniej widać na powiększonej wersji obrazków:



Zbiór testowy składał się z oryginalnych (nieprzekształconych) zdjęć 100 innych użytkowników, traktowanych jako spoza bazy danych:

Po wybraniu interesujących podzbiorów dokonano losowego łączenia odcisków palców w pary (dopasowanie par już jest widoczne na powyższych rysunkach). Jeśli klasa była taka sama (to znaczy – jeśli sparowano odciski tego samego użytkownika), takiej parze przypisywano klasę 0, w przeciwnym przypadku klasę 1 (inni użytkownicy). Prawdopodobieństwo dopasowania obrazkowi innego z tej samej klasy ustalono jako 1/6, tak aby zrównoważyć zbiór par, ale uczyć model dobrze dyskryminować pod kątem autoryzacji, podczas której maksymalnie 1 element na 100 był z tej samej klasy, a pozostałe 99 z innej.

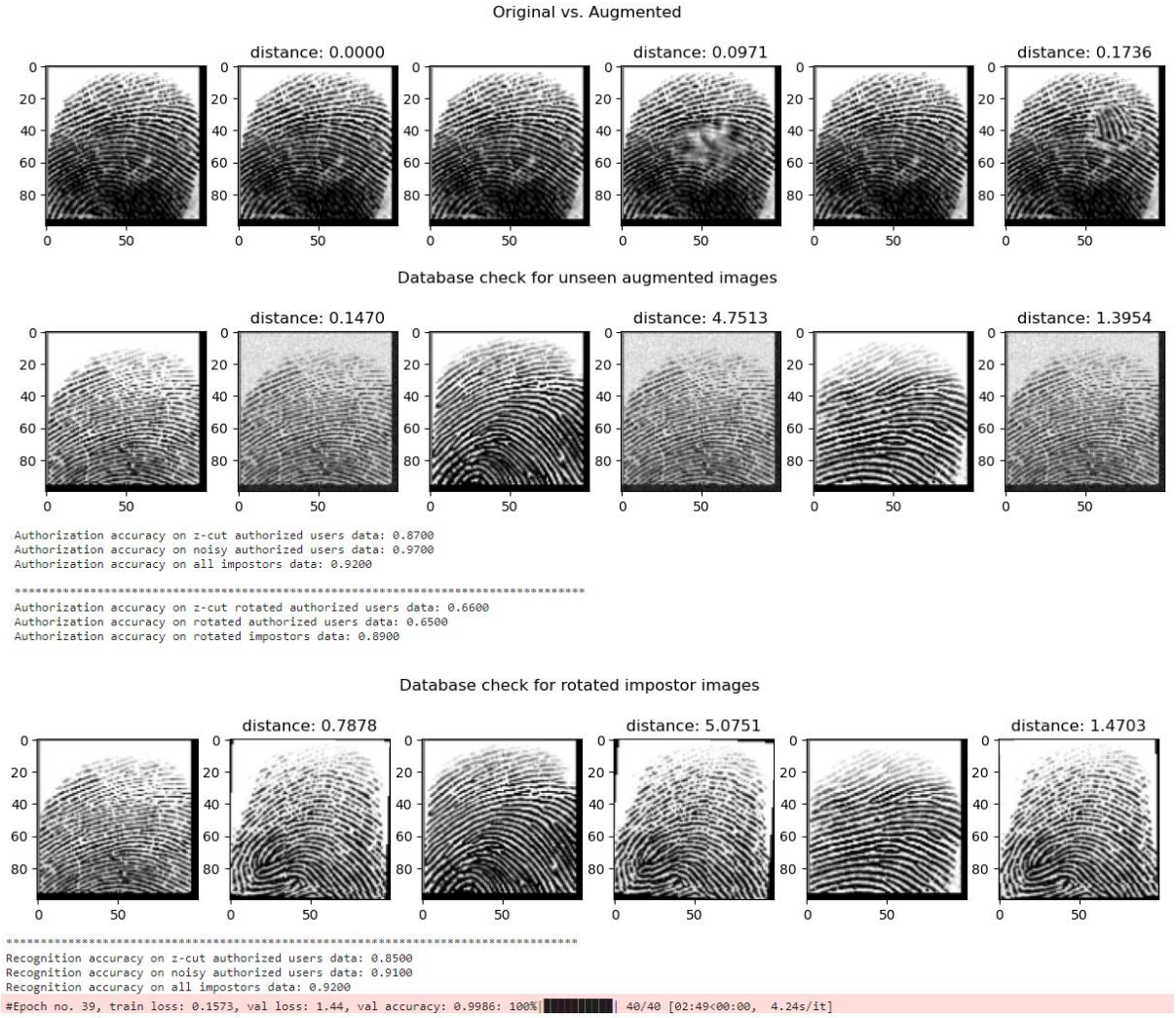
Aby model radził sobie z rozróżnianiem odcisków palców, potrzebował nauczyć się wyszukiwać charakterystyczne elementy, takie jak minucje. Następnie autoryzacja polegała na porównaniu odcisku danego użytkownika z każdym podstawowym odciskiem użytkowników z bazy danych (zbiór treningowy, obrazki oryginalne). Jeśli którykolwiek odcisk z bazy danych był wystarczająco podobny do odcisku użytkownika, użytkownik był wpuszczany do systemu (nawet jeśli użytkownik był w rzeczywistości spoza systemu lub użytkownikowi z bazy danych dopasowano inny niż jego własny odcisk). Dokładność autoryzacji była mierzona jako procent poprawnie rozpoznanych użytkowników z bazy danych lub poprawnie odrzuconych użytkowników nieznanych.

Skonstruowany model składał się z 4 warstw konwolucyjnych 2D z aktywacjami ReLU i dokonywanym MaxPoolingiem co warstwę oraz z 3 warstw liniowych (również z aktywacją ReLU), które sumarycznie tworzyły reprezentację w ukrytej, 128 wymiarowej przestrzeni. Każda para obrazków była przepuszczona przez model, dając łącznie 2 wektory, po 1 wektorze reprezentacji na obrazek. Te wektory były następnie porównywane przy pomocy funkcji kosztu kontrastu (Constrastive Loss) o marginesie 1.2, tak aby największy wpływ na błąd miały przypadki, w których obrazki z odmiennych klas miały podobną reprezentację (były trudne do odróżnienia):

$$Loss = \sum_{k=1}^{128} (1 - Y)\,\frac{1}{2}(D_k)^2 + Y\,\frac{1}{2}\{max(0, margin - D_k)\}^2$$

Za próg odróżniający wektory bliskie i dalekie przyjęto t=0.35, wyznaczone eksperymentalnie. Model był uczony przez 40 epok, przy użyciu optymalizatora Adam i stałej uczącej 1e-4. Dodatkowo wykorzystano metodę inicjalizacji wag dla warstw konwolucyjnych, która pomogła zmniejszyć nieregularność otrzymywanych wyników. Co 10. epokę nadzorowano wyniki autoryzacji dostępu dla augmentacji z-cut, zbioru walidującego oraz zbioru

nieautoryzowanych użytkowników. Po 40 epokach sprawdzono również wyniki dla zmodyfikowanych wersji tych zbiorów (dodano losową rotację o maksymalnie 4 stopnie). Udało się uzyskać następujące wyniki:



Zgodnie z oczekiwaniami, dokładność autoryzacji spadła dla użytkowników z dostępem przy dodatkowym zmodyfikowaniu danych. Z jakichś względów model wpuścił o 3 użytkowników więcej w przypadku obróconych danych spoza bazy.

W przypadku rozpoznawania użytkowników – tu sprawdzono, jak radzi sobie model bez dodatkowego modyfikowania danych. Dla przypadku z-cut u użytkowników z bazy danych model pomylił się w rozpoznaniu dwóch osób. Natomiast w przypadku zaszumionych danych oryginalnych, model źle rozpoznał aż 6 osób. Dla użytkowników spoza bazy danych, autoryzacja i rozpoznanie musiały dawać te same wyniki, gdyż użytkownik został wpuszczony do systemu wtedy i tylko wtedy, gdy został błędnie zweryfikowany jako dowolna osoba z bazy danych.

Przy dostosowywaniu modelu i treningu przetestowano różne funkcje aktywacji (Tanh, ReLU, LeakyReLU), a także warstwy Dropout, Average Pooling i 2 różne schedulery (StepLR, CosineAnnealingLR).

Bibliografia:

Shehu, Y.I., Ruiz-Garcia, A., Palade, V., James, A. (2018) “Detection of Fingerprint Alterations Using Deep Convolutional Neural Networks” in Proceedings of the International Conference on Artificial Neural Networks (ICANN 2018), Rhodes – Greece, 5 th - 7th October 2018. Springer-Verlag Lecture Notes in Computer Science.