**Sprawozdanie z przedmiotu**

**Inteligentne Systemy**

**Uwierzytelniania**

**Laboratorium nr. 5/6**

**Autor: Marek Sigmund**

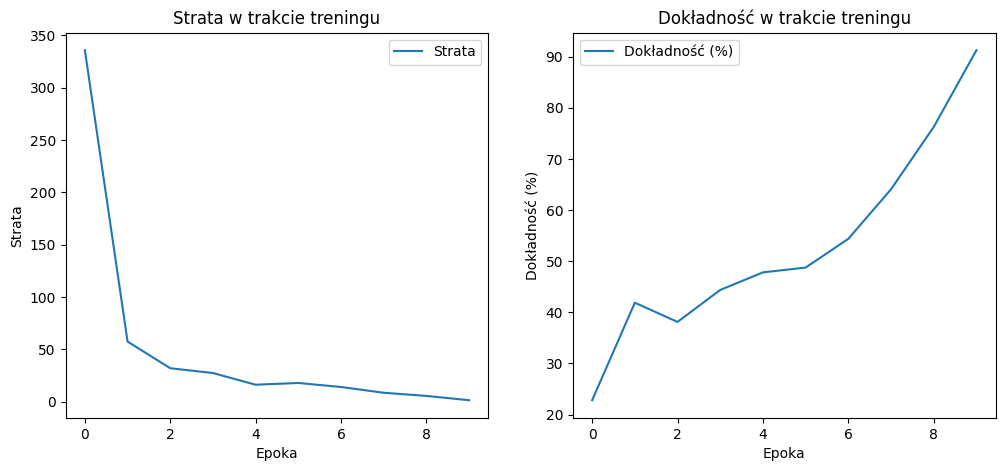
Celem niniejszego projektu było opracowanie systemu uwierzytelniania użytkowników z zastosowaniem dodatkowego mechanizmu autoryzacji. W ramach realizacji wybrano system rejestracji i logowania z wykorzystaniem odcisku palca jako kluczowego elementu biometrycznego. Aplikacja została zbudowana przy użyciu frameworka Flask, co umożliwiło stworzenie dynamicznej i responsywnej platformy webowej.

W projekcie zastosowano autorski model sieci neuronowej do ekstrakcji cech z odcisków palców, który łączy zaawansowane techniki analizy obrazu z danymi geometrycznymi i minucjami (charakterystycznymi punktami linii papilarnych). Takie podejście pozwoliło na precyzyjne odwzorowanie i weryfikację odcisków palców użytkowników, zwiększając bezpieczeństwo systemu. Dzięki temu powstał system zapewniający zarówno wygodę, jak i wysoki poziom ochrony danych użytkownika.

Zaprojektowany model do uwierzytelniania oparty na odciskach palców stanowi hybrydowe rozwiązanie, które łączy cechy wyodrębnione z obrazu odcisku palca z dodatkowymi cechami geometrycznymi i minucjami, czyli charakterystycznymi punktami linii papilarnych. Model składa się z trzech głównych komponentów. Pierwszym jest część CNN (Convolutional Neural Network), odpowiedzialna za analizę obrazu odcisku palca. CNN składa się z dwóch warstw splotowych wykorzystujących funkcje aktywacji ReLU, po których następują warstwy poolingowe redukujące wymiary danych wejściowych. Wyjściem tej części jest wektor cech o wymiarze 128, który, po spłaszczeniu i przejściu przez warstwę w pełni połączoną, zawiera istotne informacje o obrazie.

Drugim komponentem modelu są cechy geometryczne wyodrębniane z konturów odcisku palca. Obejmują one parametry takie jak powierzchnia, obwód, proporcje oraz tzw. "extent", czyli stosunek powierzchni odcisku do prostokątnego otoczenia danego obszaru. Dane te pozwalają na dodatkową analizę kształtu odcisku palca. Trzeci komponent stanowią cechy minucji, obliczane na podstawie szkieletu linii papilarnych. W ramach tej analizy zliczane są zakończenia oraz rozwidlenia linii, które są charakterystyczne dla każdego odcisku palca. Dane te są następnie normalizowane, co pozwala na efektywne połączenie ich z cechami wyodrębnionymi z obrazu i z cechami geometrycznymi. Ostatecznym etapem działania modelu jest połączenie wszystkich cech i przetworzenie ich przez warstwy w pełni połączone w celu dokonania klasyfikacji użytkownika.

Proces treningu modelu obejmował przygotowanie danych w postaci folderów, gdzie każdy folder reprezentował jednego użytkownika. Każdy folder zawierał obrazy odcisków palców konkretnej osoby. W ramach przygotowania danych zastosowano wstępne przetwarzanie obrazów, takie jak skalowanie do wymiarów 128x128 pikseli oraz normalizację. Wyciągnięto także cechy geometryczne z konturów oraz minucje na podstawie szkieletu linii papilarnych. Model był trenowany przez 10 epok z wykorzystaniem optymalizatora Adam oraz funkcji strat CrossEntropyLoss. Dane były ładowane w partiach (batch size = 16). Każda epoka obejmowała forward pass, czyli przejście danych przez model, obliczenie straty oraz backpropagację w celu optymalizacji wag. Dzięki wykorzystaniu GPU proces treningu był znacząco przyspieszony.



Rezultaty treningu wskazują na skuteczność zastosowanego podejścia. Strata modelu sukcesywnie zmniejszała się z każdą kolejną epoką, co świadczy o poprawnej optymalizacji. Dokładność modelu wzrosła z początkowych 22.81% w pierwszej epoce do 91.25% w epoce dziesiątej, co potwierdza, że model efektywnie nauczył się klasyfikować użytkowników na podstawie dostarczonych danych. Wizualizacje wyników treningu ilustrują zarówno redukcję straty, jak i wzrost dokładności modelu w trakcie kolejnych epok. Strata zmniejszyła się z 335.89 w pierwszej epoce do 1.28 w ostatniej, natomiast dokładność modelu wzrosła niemal czterokrotnie, co dowodzi skuteczności zaprojektowanego rozwiązania w zadaniu uwierzytelniania użytkowników.

W obecnej implementacji systemu dane użytkowników są przechowywane w plikach tekstowych, które pełnią rolę prostej „bazy danych”. Dla każdego użytkownika tworzone są oddzielne pliki, zawierające jego cechy wyekstrahowane z odcisku palca (wektor cech CNN, cechy geometryczne i minucje) oraz zahashowane hasło. Rozwiązanie to jest wystarczające dla prototypowego systemu, umożliwiając skuteczne przechowywanie i odczytywanie danych w niewielkiej skali.

Jednakże, w celu dalszego rozwoju projektu i skalowalności systemu, zasadne byłoby wykorzystanie tradycyjnej bazy danych. Takie podejście zapewniłoby lepsze zarządzanie danymi, większe bezpieczeństwo oraz możliwość łatwego przeszukiwania danych użytkowników. Dodatkowo baza danych umożliwiłaby przechowywanie większej liczby metadanych oraz obsługę bardziej złożonych zapytań, co w przypadku systemu uwierzytelniania może okazać się kluczowe. Implementacja z użyciem bazy danych stanowi naturalny kierunek rozwoju projektu, pozwalając na jego adaptację do realnych wymagań produkcyjnych.

