**Sprawozdanie z przedmiotu**

**Inteligentne Systemy**

**Uwierzytelniania**

**Laboratorium nr. 5/6**

**Autor: Marek Sigmund**

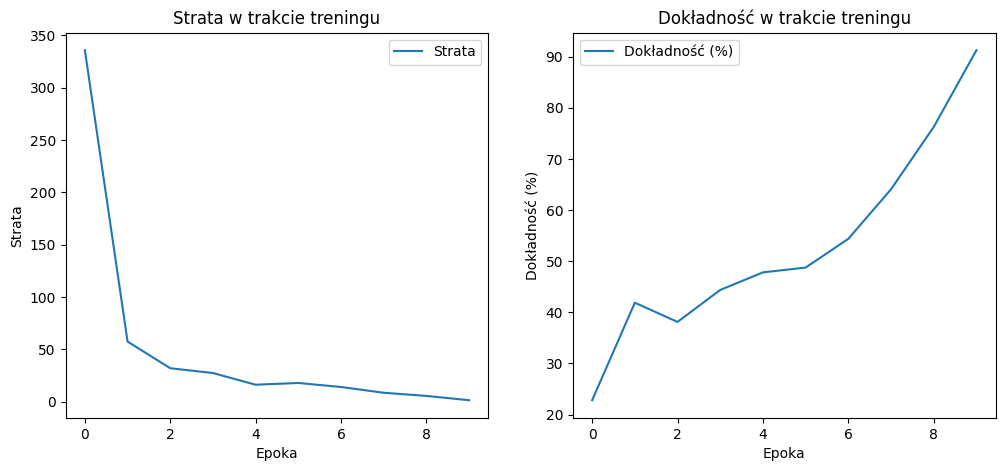
Celem niniejszego projektu było opracowanie systemu uwierzytelniania użytkowników z zastosowaniem dodatkowego mechanizmu autoryzacji. W ramach realizacji wybrano system rejestracji i logowania z wykorzystaniem odcisku palca jako kluczowego elementu biometrycznego. Aplikacja została zbudowana przy użyciu 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.

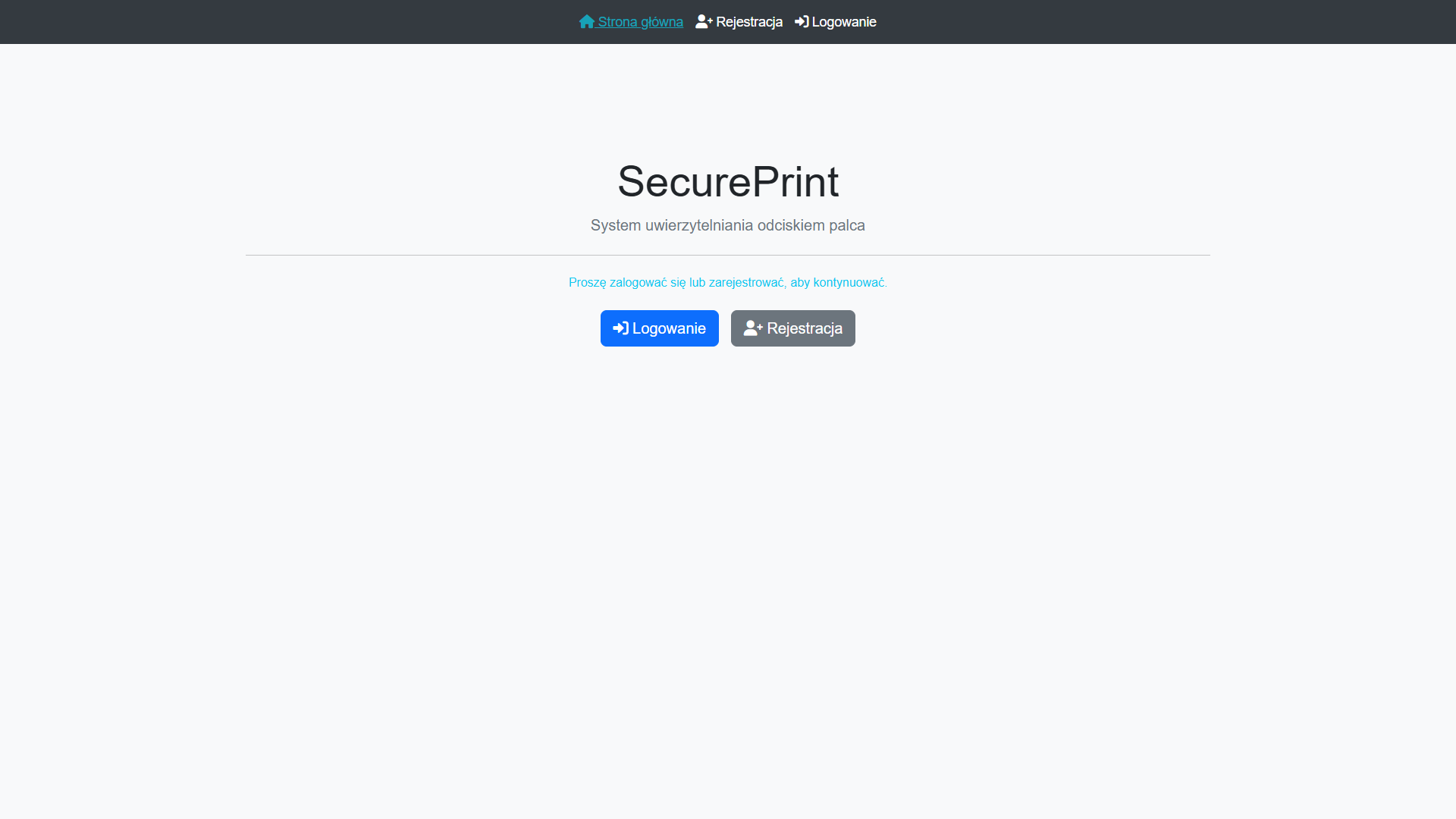
Proces treningu modelu obejmował przygotowanie danych w postaci folderów, gdzie każdy folder reprezentował jednego użytkownika. Każdy folder zawierał obrazy odcisków palców konkretnej osoby. W ramach przygotowania danych zastosowano wstępne przetwarzanie obrazów, takie jak skalowanie do wymiarów 128x128 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.

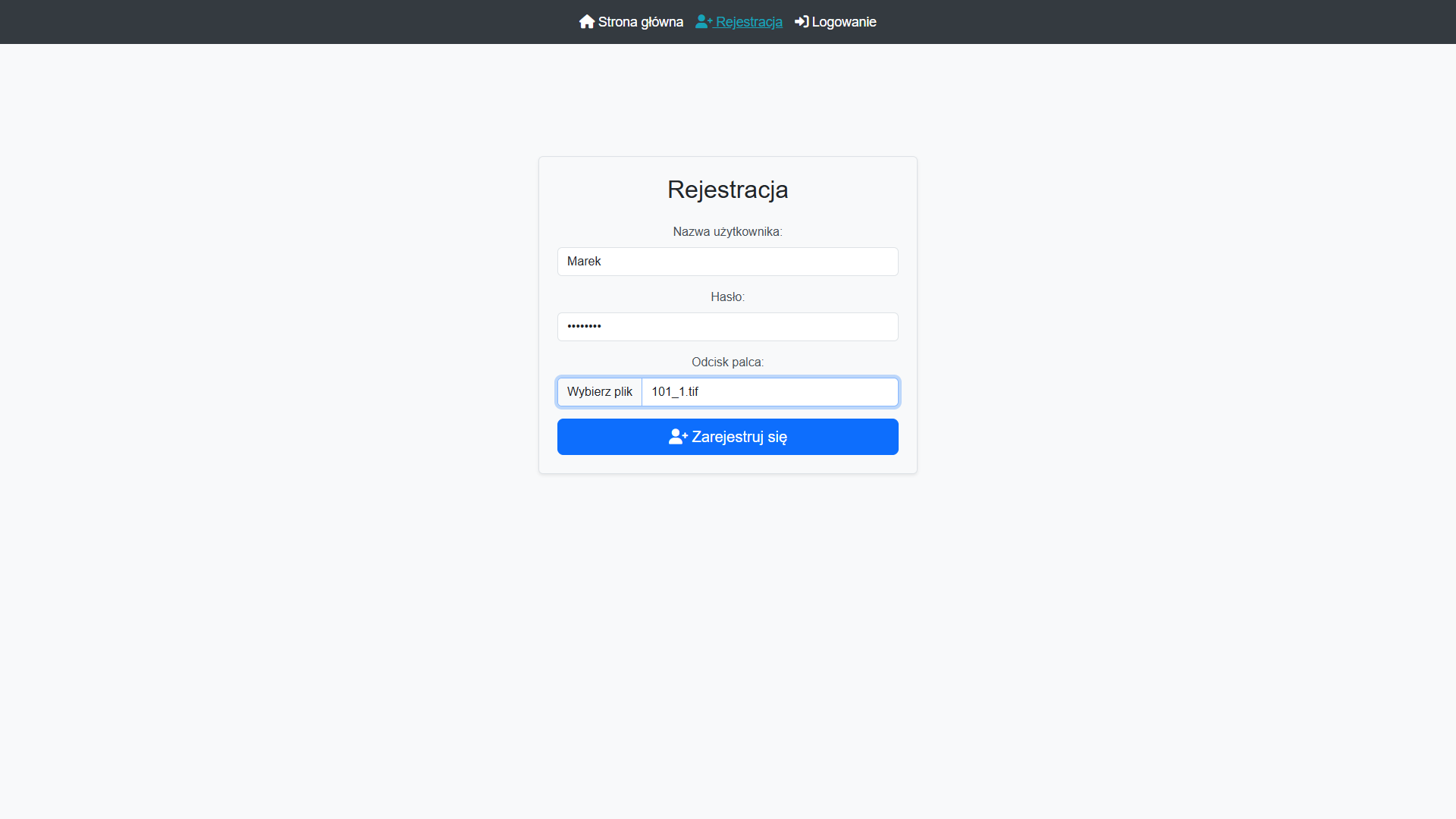
Jednakże, w celu dalszego rozwoju projektu i skalowalności systemu, zasadne byłoby wykorzystanie tradycyjnej bazy danych. Takie podejście zapewniłoby lepsze zarządzanie danymi, większe bezpieczeństwo oraz możliwość łatwego przeszukiwania danych użytkowników. Dodatkowo baza danych umożliwiłaby przechowywanie 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.

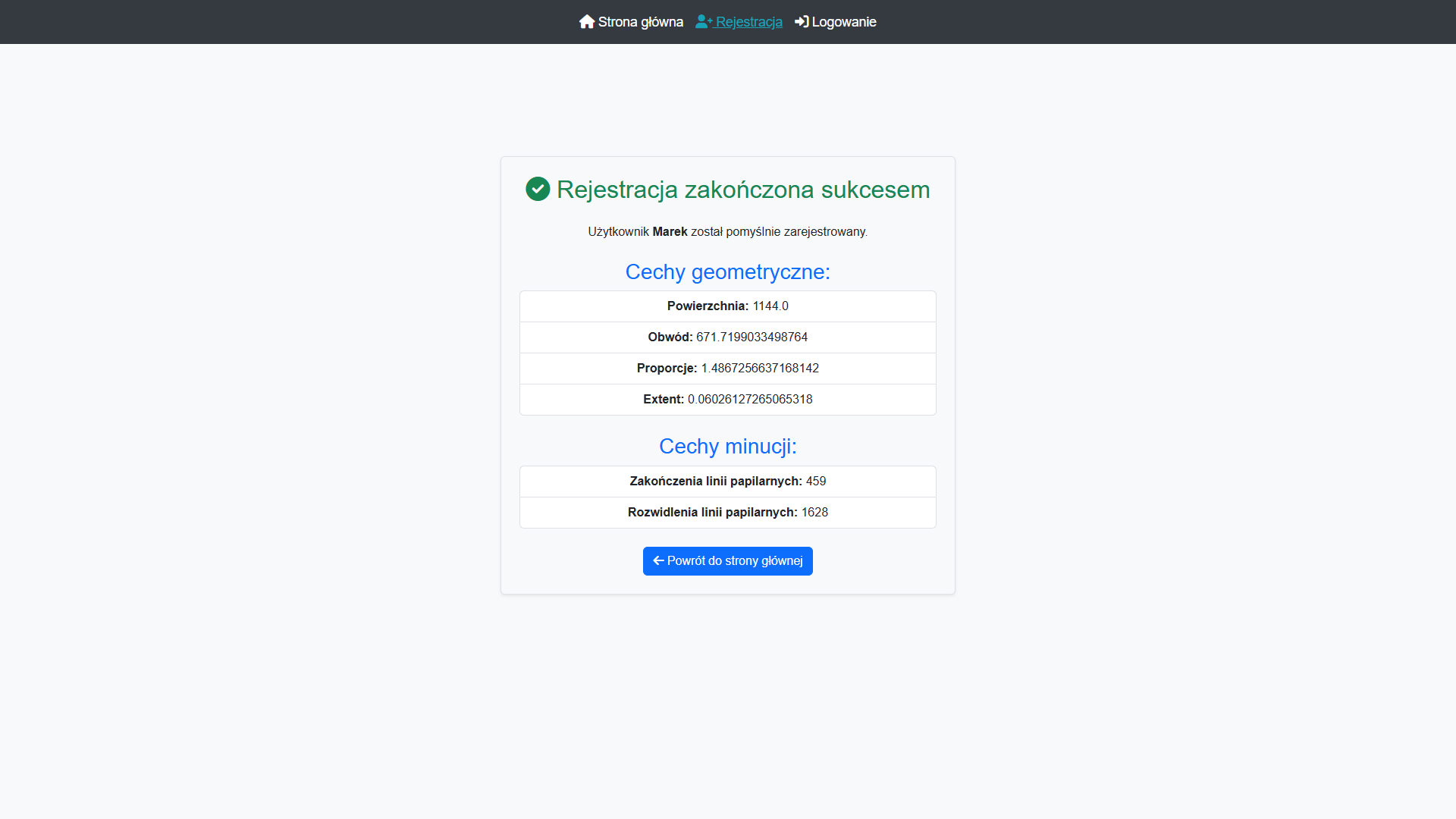


Ekran główny aplikacji „SecurePrint” to intuicyjne miejsce startowe, które wprowadza użytkownika do systemu uwierzytelniania za pomocą odcisku palca. Na samej górze widoczna jest estetyczna i minimalistyczna nawigacja, umożliwiająca przejście do najważniejszych funkcji aplikacji, takich jak rejestracja nowych użytkowników oraz logowanie.

W centralnej części strony znajduje się logo systemu oraz krótki opis celu aplikacji: „System uwierzytelniania odciskiem palca”. Poniżej użytkownik znajdzie zachętę do zalogowania się lub zarejestrowania, aby rozpocząć korzystanie z systemu. Przyciski nawigacyjne „Logowanie” i „Rejestracja” są wyraźnie oznaczone i łatwe do zauważenia, co podnosi komfort użytkowania.

Całość zaprojektowana jest w jasnej kolorystyce z wyraźnymi kontrastami, zapewniając nowoczesny i profesjonalny wygląd. Ekran główny stanowi doskonały punkt wyjścia do dalszej eksploracji funkcji aplikacji.





Powyższe zrzuty ekranu prezentują proces rejestracji użytkownika oraz komunikat o pomyślnym zakończeniu tego procesu. Na pierwszym ekranie użytkownik wprowadza swoją nazwę, hasło oraz przesyła obraz odcisku palca. Po kliknięciu przycisku „Zarejestruj się” dane są przetwarzane, a wyniki rejestracji są zapisywane w „bazie” projektu, która oparta jest na plikach tekstowych.

Drugi ekran przedstawia komunikat o pomyślnym zakończeniu rejestracji. System wyświetla kluczowe informacje wyekstrahowane z przesłanego obrazu odcisku palca:

**Cechy geometryczne:**

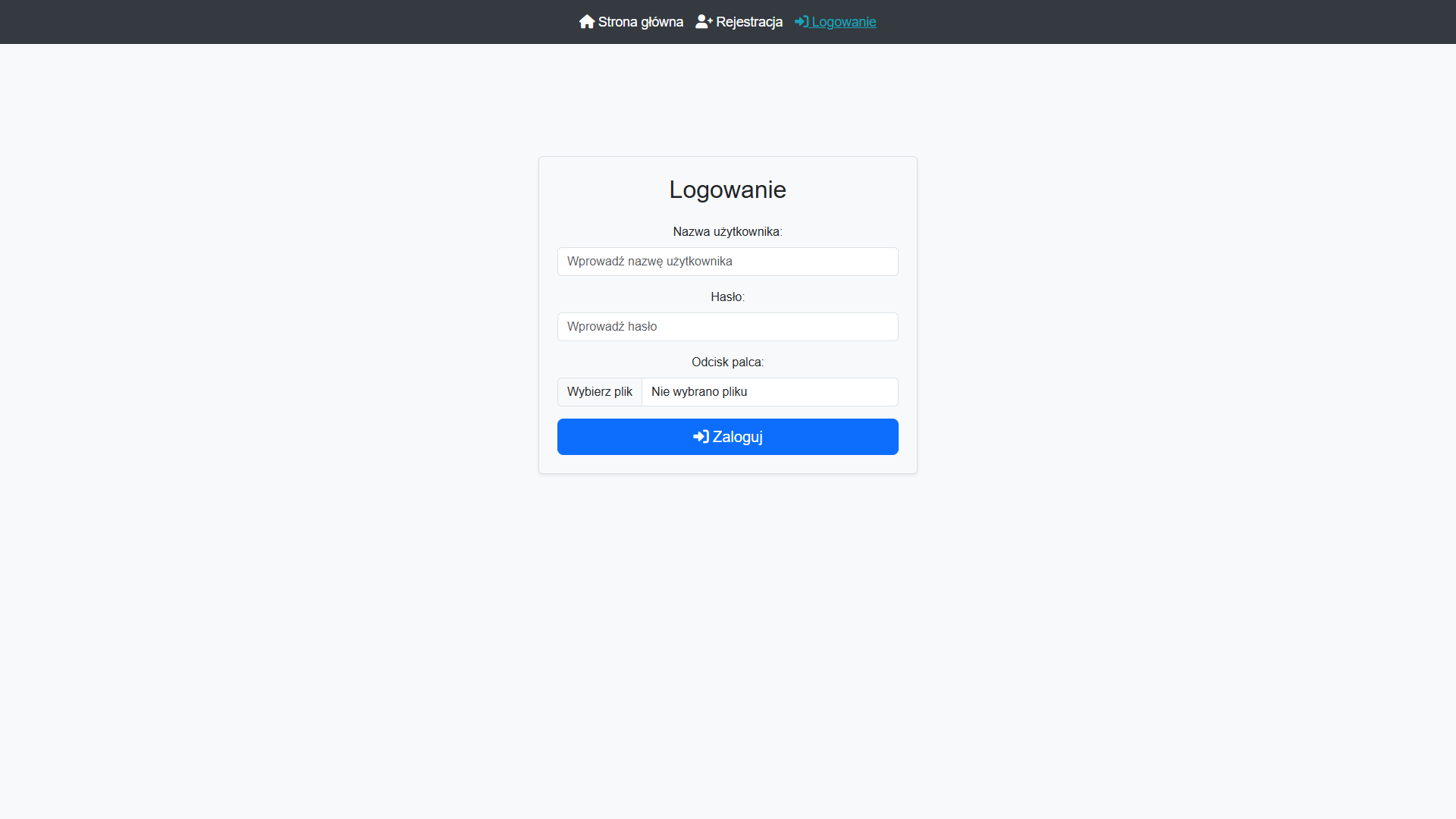
* Powierzchnia: obliczona na podstawie największego konturu odcisku palca.
* Obwód: długość obwodu konturu.
* Proporcje: stosunek szerokości do wysokości prostokąta otaczającego kontur.
* Extent: stosunek powierzchni odcisku do powierzchni prostokąta otaczającego.

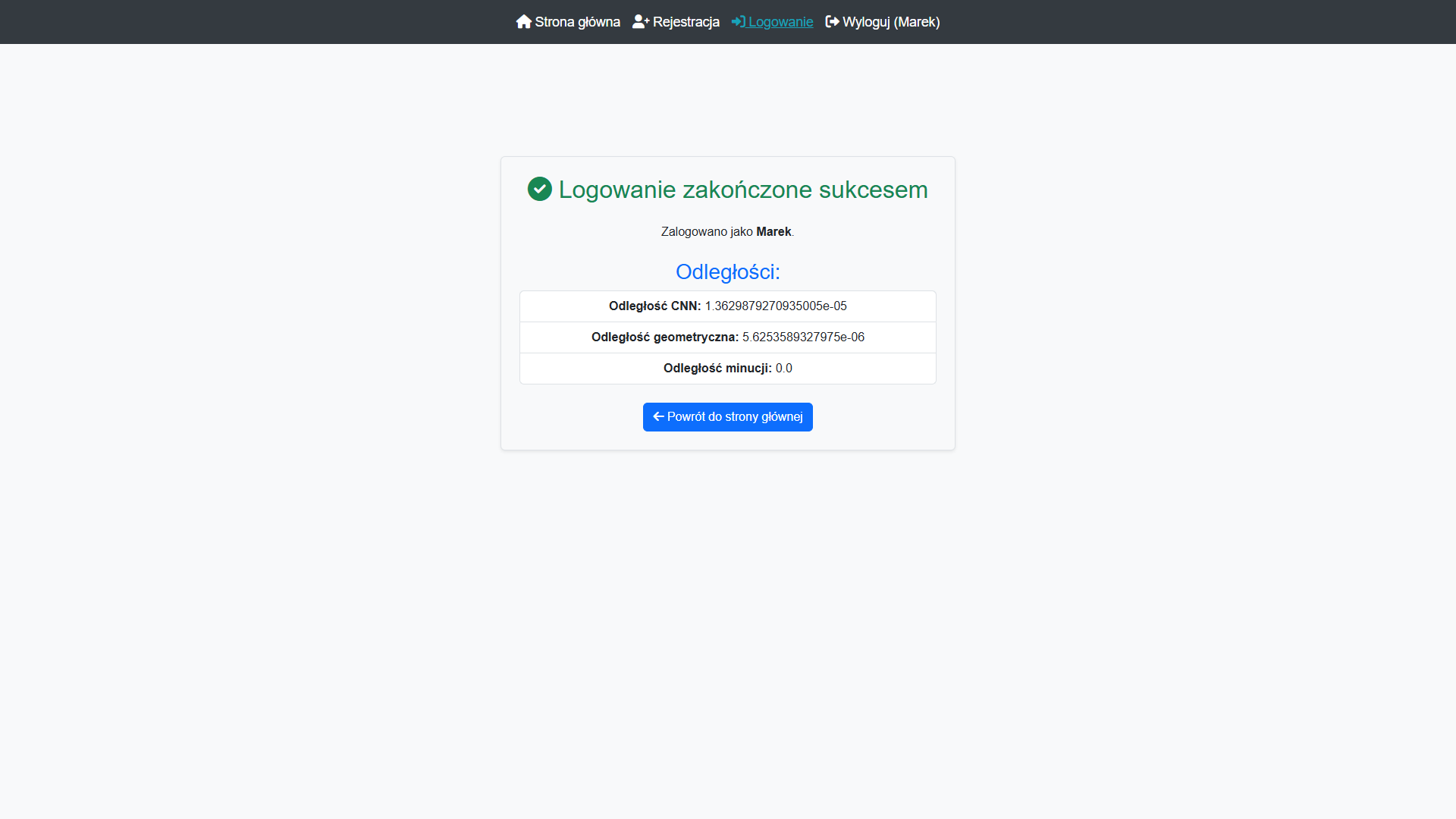
**Cechy minucji:**

* Zakończenia linii papilarnych: liczba miejsc, gdzie linie na obrazie kończą się.
* Rozwidlenia linii papilarnych: liczba punktów, gdzie linie rozwidlają się.

Dane te są zapisywane w dedykowanych plikach w „bazie” systemu. Hasło użytkownika jest haszowane w celu zabezpieczenia, a cechy geometryczne, minucji oraz wektor cech z modelu CNN są przechowywane w osobnych plikach tekstowych. Struktura „bazy” jest prosta, ale łatwo ją rozbudować do użycia profesjonalnego systemu zarządzania bazą danych w przyszłości.

Warto zaznaczyć, że wyświetlanie szczegółowych danych, takich jak cechy geometryczne i minucji, służy głównie celom deweloperskim, aby lepiej zilustrować działanie systemu. W finalnej wersji aplikacji te informacje mogłyby zostać usunięte lub ukryte, aby nie naruszać prywatności użytkowników oraz poprawić bezpieczeństwo aplikacji.





Logowanie do systemu SecurePrint to proces, w którym użytkownik podaje swoją nazwę użytkownika, hasło oraz przesyła plik z odciskiem palca. Na pierwszym ekranie logowania użytkownik wypełnia odpowiednie pola formularza, a następnie przesyła je do serwera za pomocą przycisku "Zaloguj". System weryfikuje poprawność danych na kilku etapach.

**Proces weryfikacji**

**Weryfikacja tożsamości użytkownika:**

* System sprawdza, czy istnieją pliki odpowiadające podanej nazwie użytkownika w „bazie”.
* Następnie wczytywane jest hasło zapisane w „bazie”, które zostało wcześniej zaszyfrowane algorytmem SHA-256. System porównuje hash tego hasła z wartością przesłaną przez użytkownika.

**Wyciąganie cech z przesłanego odcisku palca:**

* Z przesłanego obrazu odcisku palca system wyciąga:
* Cechy geometryczne, takie jak powierzchnia, obwód, proporcje i extent.
* Cechy minucji, czyli liczba zakończeń i rozwidleń linii papilarnych.
* Cechy CNN, które są wyliczane na podstawie analizy obrazu przez model konwolucyjnej sieci neuronowej.

**Porównywanie cech z zapisanymi danymi:**

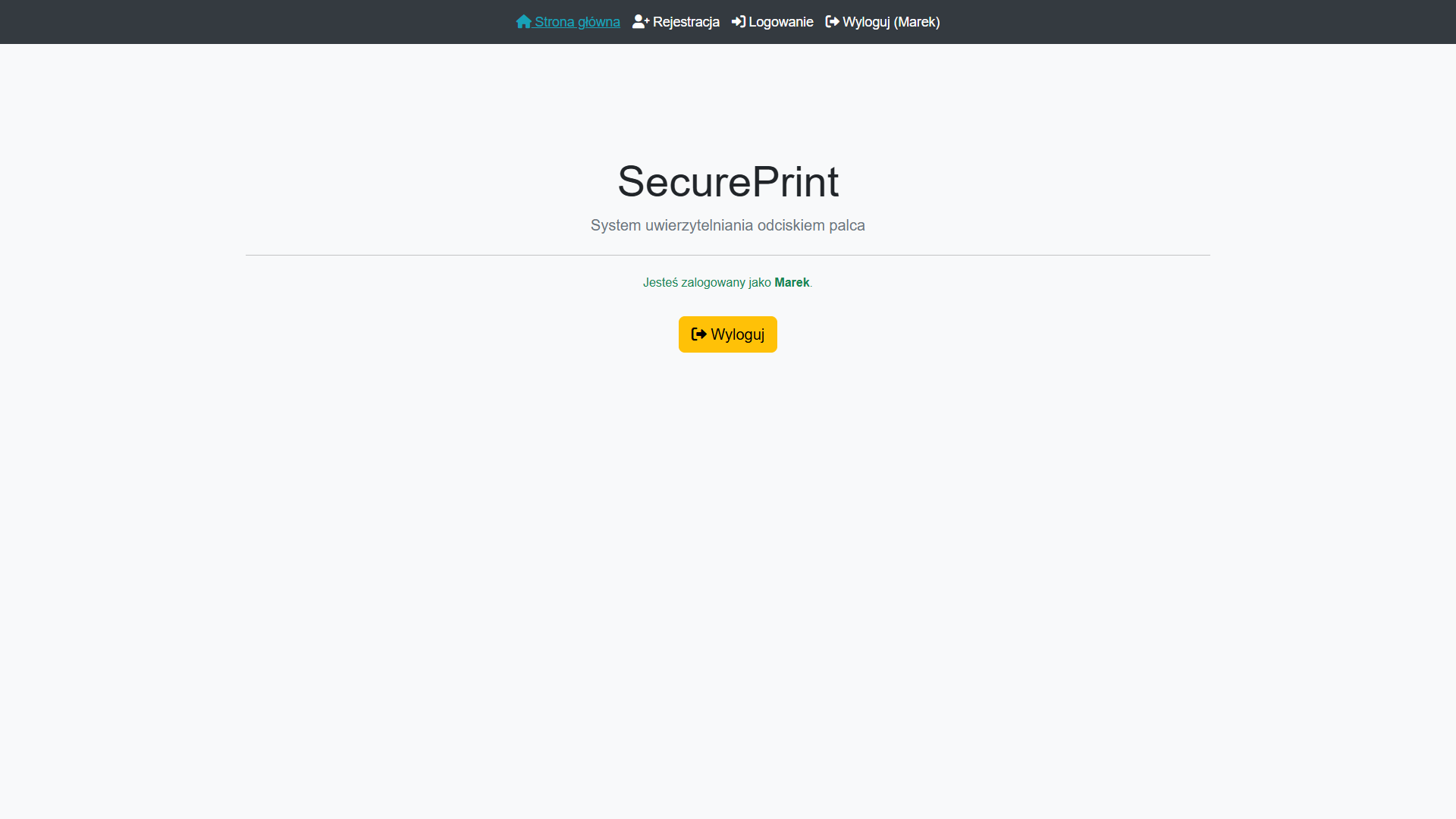
* Wyciągnięte cechy są porównywane z zapisanymi w „bazie” cechami odpowiadającymi podanemu użytkownikowi.
* Dla każdej grupy cech obliczana jest odległość:
* Odległość CNN – mierzona jako różnica wektorów wyjściowych modelu CNN.
* Odległość geometryczna – obliczana jako różnica wektorów cech geometrycznych.
* Odległość minucji – porównanie zakończeń i rozwidleń linii papilarnych.

**Podejmowanie decyzji:**

* System ocenia, czy wszystkie odległości mieszczą się w ustalonych progach. Jeśli tak, użytkownik zostaje zalogowany.
* W przeciwnym razie logowanie kończy się niepowodzeniem, a użytkownik otrzymuje odpowiedni komunikat.

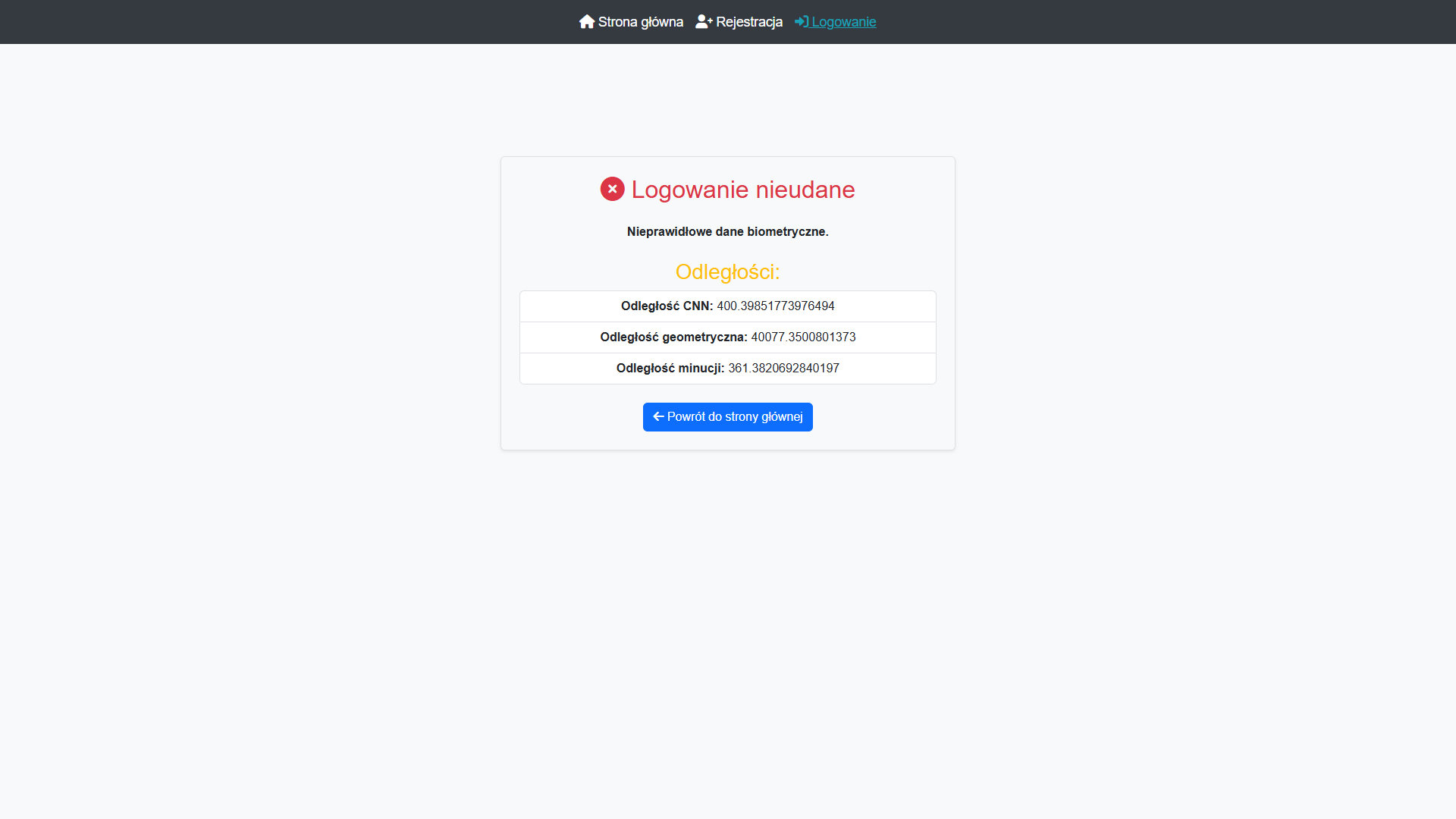
Informacje na ekranie sukcesu

Na ekranie sukcesu wyświetlane są obliczone odległości pomiędzy cechami zapisanymi w „bazie” a nowymi danymi. Prezentacja tych wartości ma na celu pomoc w analizie działania systemu w trakcie fazy rozwoju. W produkcyjnej wersji systemu te informacje mogą zostać ukryte.



Po pomyślnym zalogowaniu użytkownik trafia na stronę główną, która zmienia swój układ, aby odzwierciedlić stan zalogowania. Na górnym pasku nawigacyjnym widnieje teraz dodatkowy element „Wyloguj (Marek)”, umożliwiający szybkie wylogowanie z systemu. Dodatkowo na stronie głównej pojawia się wyraźny przycisk „Wyloguj” w kolorze żółtym, który również pełni tę funkcję.

Wprowadzenie widocznych opcji wylogowania zarówno w górnym menu, jak i na głównej stronie, ma na celu zwiększenie komfortu użytkownika oraz poprawę intuicyjności interfejsu. Te elementy pomagają użytkownikowi łatwo zakończyć sesję w systemie, zwiększając bezpieczeństwo oraz kontrolę nad dostępem.



W przypadku, gdy podane dane biometryczne (odcisk palca) nie spełniają kryteriów zgodności z zapisanymi w systemie, użytkownik zostaje poinformowany o niepowodzeniu logowania. Ekran prezentuje komunikat o błędzie oraz szczegóły dotyczące odległości obliczonych przez system:

Odległość CNN: różnica między cechami wyodrębnionymi przez model CNN.

Odległość geometryczna: różnica w cechach geometrycznych, takich jak powierzchnia, obwód itp.

Odległość minucji: różnica w liczbie zakończeń i rozwidleń linii papilarnych.

System działa na podstawie progów odległości, które określają dopuszczalne różnice dla każdego z wymienionych parametrów:

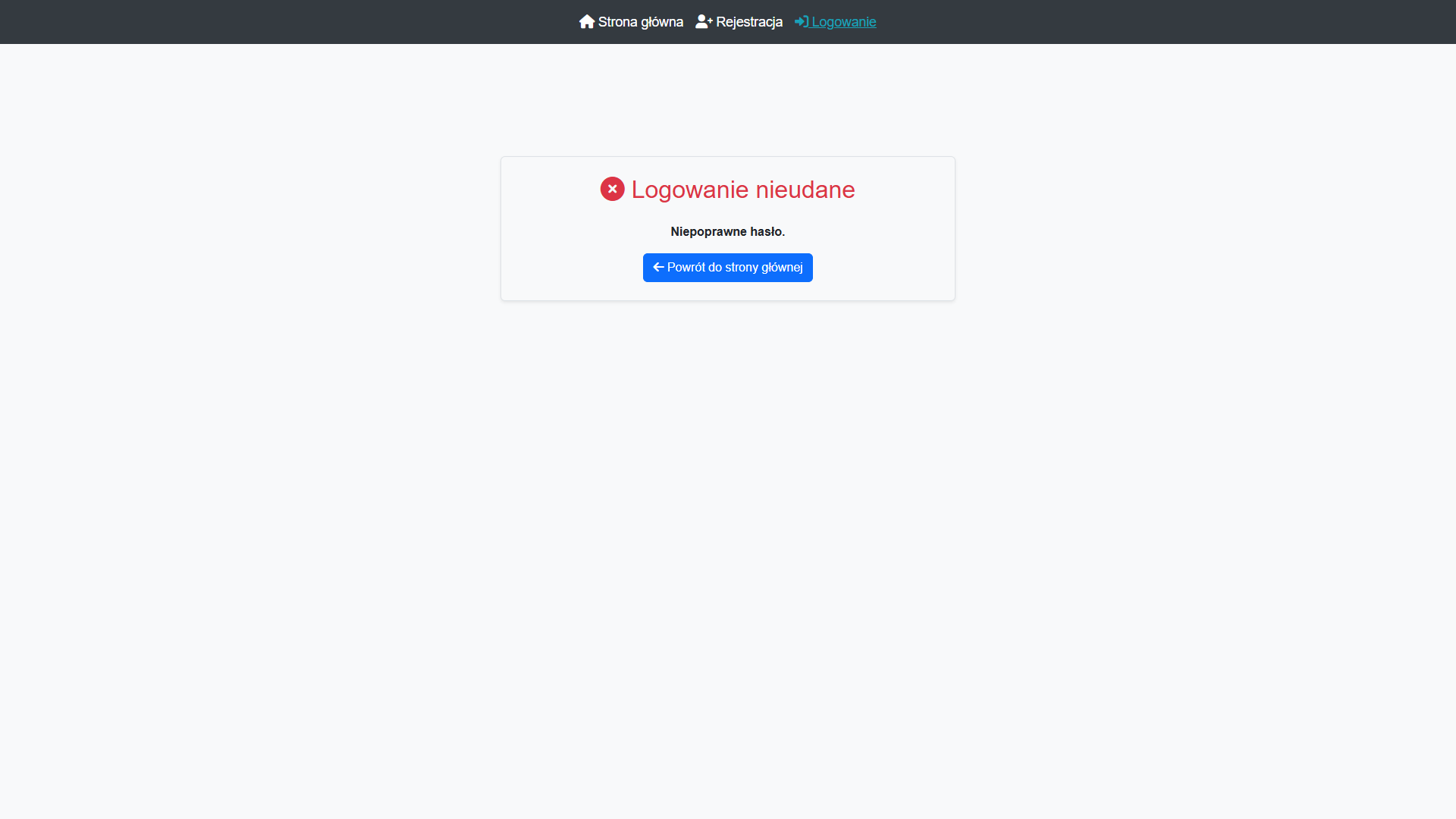
CNN: wartość graniczna wynosi 10.0.

Cechy geometryczne: wartość graniczna wynosi 5.0.

Cechy minucji: wartość graniczna wynosi 5.0.

Jeżeli którakolwiek z tych odległości przekroczy ustalone wartości progowe, logowanie zostaje odrzucone. Wartości progowe można dostosować podczas testowania systemu w celu dostosowania jego rygorystyczności. Mniejsze wartości progowe zwiększają bezpieczeństwo, ale mogą powodować większą liczbę błędnych odrzuceń (tzw. false negatives). Z kolei większe wartości mogą zwiększyć akceptację, ale kosztem potencjalnego obniżenia bezpieczeństwa systemu.

Ten ekran z informacjami ma również na celu ułatwienie testowania i doskonalenia systemu w fazie rozwoju. W docelowej wersji systemu wyświetlanie szczegółowych odległości można wyłączyć, aby zapewnić lepszą ochronę informacji biometrycznych.



W przypadku, gdy użytkownik poda nieprawidłowe hasło, system uniemożliwia zalogowanie i wyświetla stosowny komunikat o błędzie: "Niepoprawne hasło".

Hasło jest weryfikowane poprzez porównanie jego skrótu (hash) z zapisanym w systemie podczas rejestracji. W momencie rejestracji hasło użytkownika jest haszowane przy użyciu algorytmu SHA-256, co zapewnia jego bezpieczne przechowywanie w systemie. Przy logowaniu wprowadzone hasło również jest haszowane i wynik tego procesu jest porównywany z hashem zapisanym w „bazie”.

Taka metoda zabezpiecza dane użytkownika, ponieważ rzeczywiste hasło nigdy nie jest przechowywane w systemie, co minimalizuje ryzyko jego ujawnienia w przypadku naruszenia bezpieczeństwa.

Ten ekran ma na celu poinformowanie użytkownika o błędnym haśle bez podawania dodatkowych informacji, co jest dobrą praktyką w systemach uwierzytelniających, aby nie ujawniać potencjalnym atakującym, czy problem leży w haśle, czy w danych biometrycznych.

Wnioski i podsumowanie

Zaprojektowany i zrealizowany system uwierzytelniania oparty na odciskach palców spełnia założone cele, łącząc tradycyjne uwierzytelnianie oparte na haśle z nowoczesnym podejściem biometrycznym. System wykorzystuje model hybrydowy, który integruje różnorodne źródła informacji, takie jak cechy geometryczne, cechy minucji oraz wektor cech wygenerowany przez sieć neuronową (CNN). Takie podejście pozwala na skuteczną klasyfikację użytkowników i stanowi solidną podstawę do dalszego rozwoju.

Przeprowadzone testy wykazały, że model osiągnął znaczącą dokładność, osiągając 91,25% po 10 epokach treningu, co wskazuje na efektywność procesu uczenia oraz skuteczność wybranych cech w identyfikacji użytkowników. System działa w pełni poprawnie, przechowując dane użytkowników w lokalnej „bazie”, co umożliwia późniejsze porównania. Podczas rejestracji i logowania dokładne dane są wyświetlane w celach deweloperskich, ale w przyszłości mogą zostać ukryte, aby system był bardziej przyjazny dla użytkownika końcowego.

Projekt ten stanowi dowód, że możliwe jest zaprojektowanie intuicyjnego systemu uwierzytelniającego z wykorzystaniem technologii biometrycznych. Jednocześnie należy podkreślić, że system jest zbudowany w sposób umożliwiający dalszy rozwój. Możliwe ulepszenia obejmują:

Zastąpienie lokalnej „bazy” bardziej wydajnym systemem zarządzania bazą danych (np. MySQL, PostgreSQL).

Dalsze dostrajanie progów akceptacji danych biometrycznych w celu optymalizacji równowagi między bezpieczeństwem a użytecznością.

Dodanie bardziej zaawansowanych technik ekstrakcji cech, co może poprawić skuteczność systemu.

Rozszerzenie aplikacji o dodatkowe funkcje, takie jak resetowanie hasła lub wsparcie dla różnych typów danych biometrycznych.

Podsumowując, zrealizowany system to funkcjonalne rozwiązanie, które demonstruje możliwości nowoczesnych metod uwierzytelniania z wykorzystaniem odcisków palców. Projekt jest elastyczny i stanowi doskonałą bazę do dalszego rozwoju w kierunku bardziej zaawansowanych i skalowalnych systemów uwierzytelniania.