**Sprawozdanie z przedmiotu**

**Inteligentne Systemy**

**Uwierzytelniania**

**Laboratorium nr. 5/6**

**Autor: Marek Sigmund**

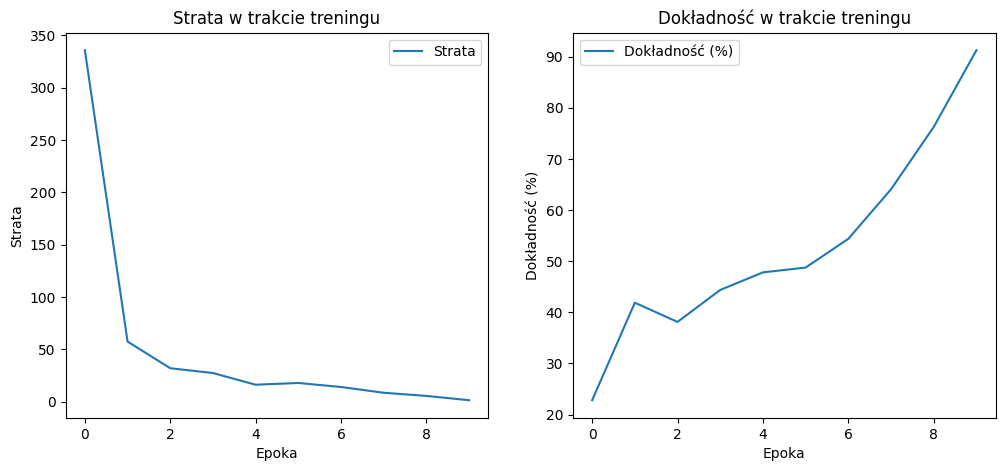
Celem projektu było zaprojektowanie systemu uwierzytelniania użytkowników, który wykorzystuje odciski palców jako główny element biometryczny. Wdrożenie obejmowało połączenie tradycyjnego mechanizmu rejestracji i logowania z dodatkowymi metodami autoryzacji, co zapewniło wyższy poziom bezpieczeństwa. Aplikacja została zbudowana w oparciu o framework Flask, który umożliwił stworzenie dynamicznej platformy webowej.

W projekcie zastosowano autorski model sieci neuronowej do ekstrakcji cech z odcisków palców. Model łączy zaawansowane techniki analizy obrazu z danymi geometrycznymi oraz cechami minucji, czyli charakterystycznych punktów linii papilarnych. Takie podejście pozwala na precyzyjną weryfikację odcisków palców użytkowników, zapewniając jednocześnie wysoki poziom ochrony danych i wygodę użytkowania.

Model hybrydowy oparty na odciskach palców został podzielony na trzy kluczowe komponenty:

1. **Część CNN (Convolutional Neural Network):** Analizuje obraz odcisku palca przy użyciu dwóch warstw splotowych z funkcjami aktywacji ReLU. Po nich następują warstwy poolingowe, które redukują wymiary danych. Wyjściem tej części jest wektor cech o wymiarze 128, który przechodzi przez w pełni połączoną warstwę, reprezentującą kluczowe informacje obrazu.
2. **Cechy geometryczne:** Wyodrębniane z konturów odcisku palca, obejmują parametry takie jak powierzchnia, obwód, proporcje oraz tzw. "extent" — stosunek powierzchni odcisku do prostokątnego otoczenia danego obszaru. Dane te dostarczają dodatkowych informacji o kształcie odcisku palca.
3. **Cechy minucji:** Wyznaczane na podstawie szkieletu linii papilarnych, obejmują zliczanie zakończeń oraz rozwidleń linii. Są to unikalne cechy każdego odcisku palca, które są normalizowane i integrowane z pozostałymi danymi wejściowymi.

Na końcowym etapie działania modelu wszystkie cechy są łączone i przetwarzane przez warstwy w pełni połączone, co umożliwia autoryzacje użytkownika.

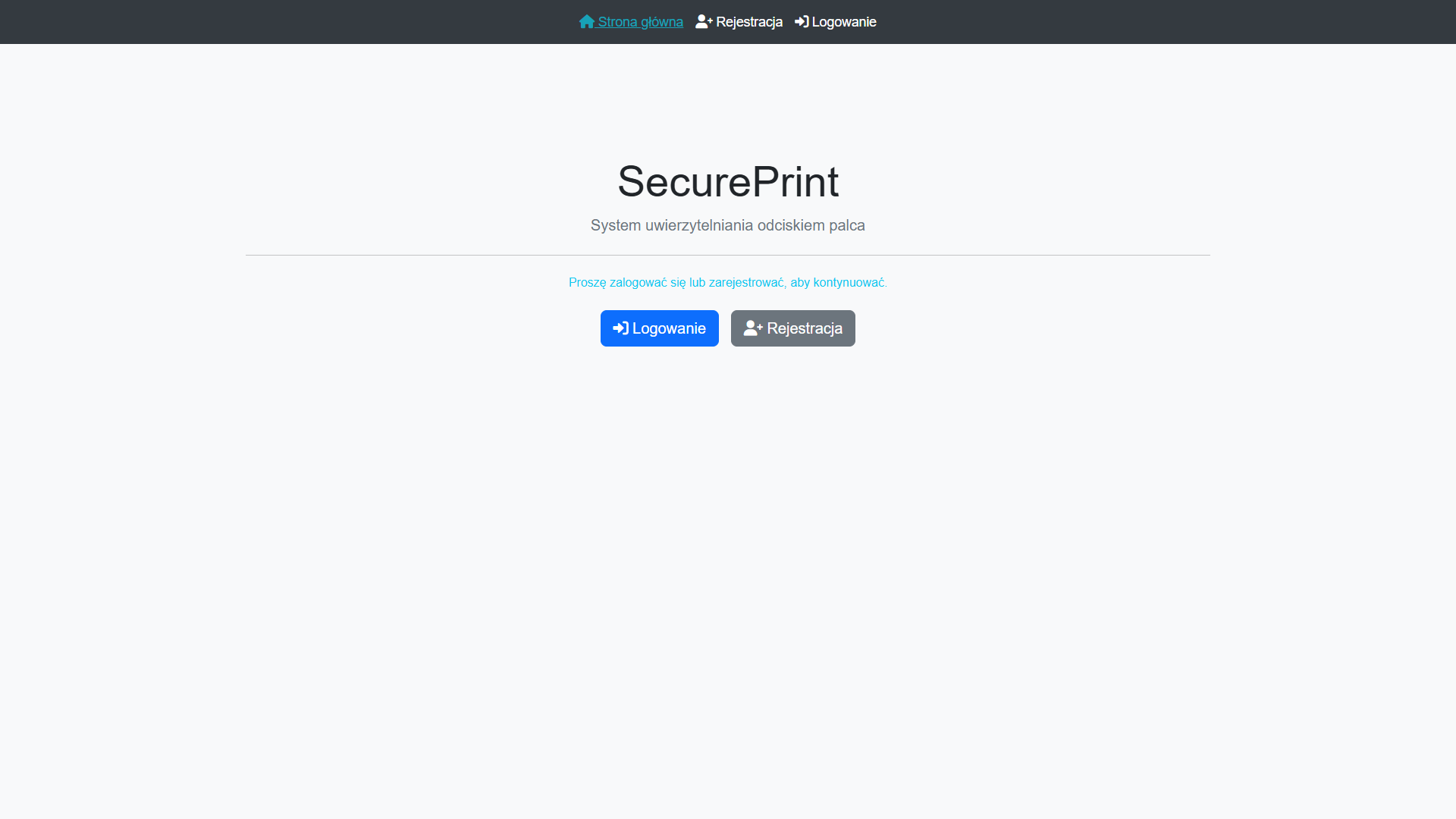


Model został przeszkolony na danych odcisków palców, które poddano wstępnemu przetwarzaniu, w tym skalowaniu i normalizacji. W procesie treningu uwzględniono cechy geometryczne i minucje jako dodatkowe dane wejściowe. Trening trwał 10 epok i wykorzystano optymalizator Adam oraz funkcję strat CrossEntropyLoss. Dzięki zastosowaniu GPU proces przebiegał szybko i efektywnie.

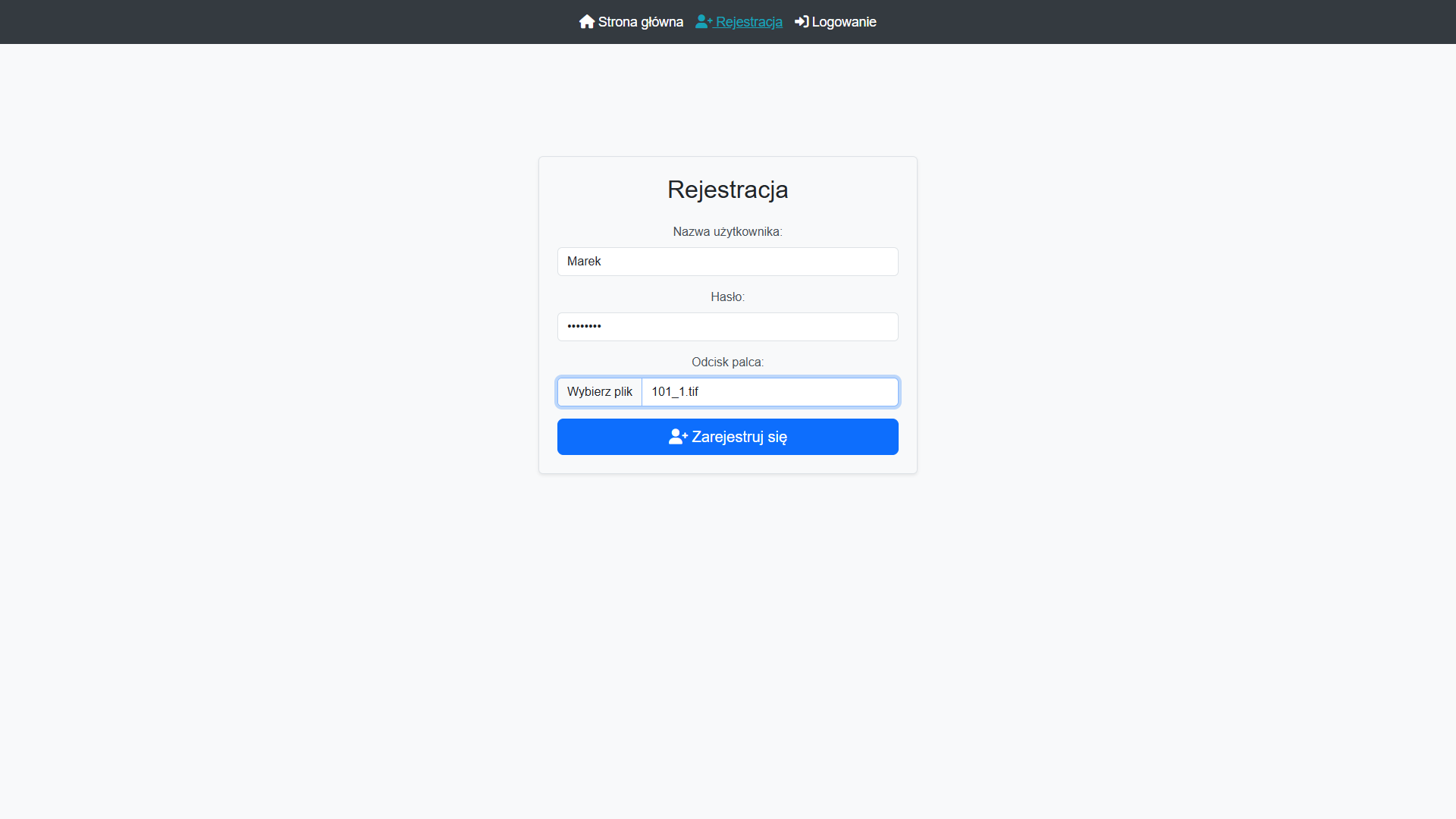
Wyniki treningu potwierdzają skuteczność zastosowanego podejścia. Strata modelu spadła z 335.89 do 1.28, a dokładność wzrosła z 22.81% do 91.25%. Wizualizacje wyników treningu ukazują sukcesywną poprawę wydajności modelu, co dowodzi jego zdolności do precyzyjnego uwierzytelniania użytkowników.

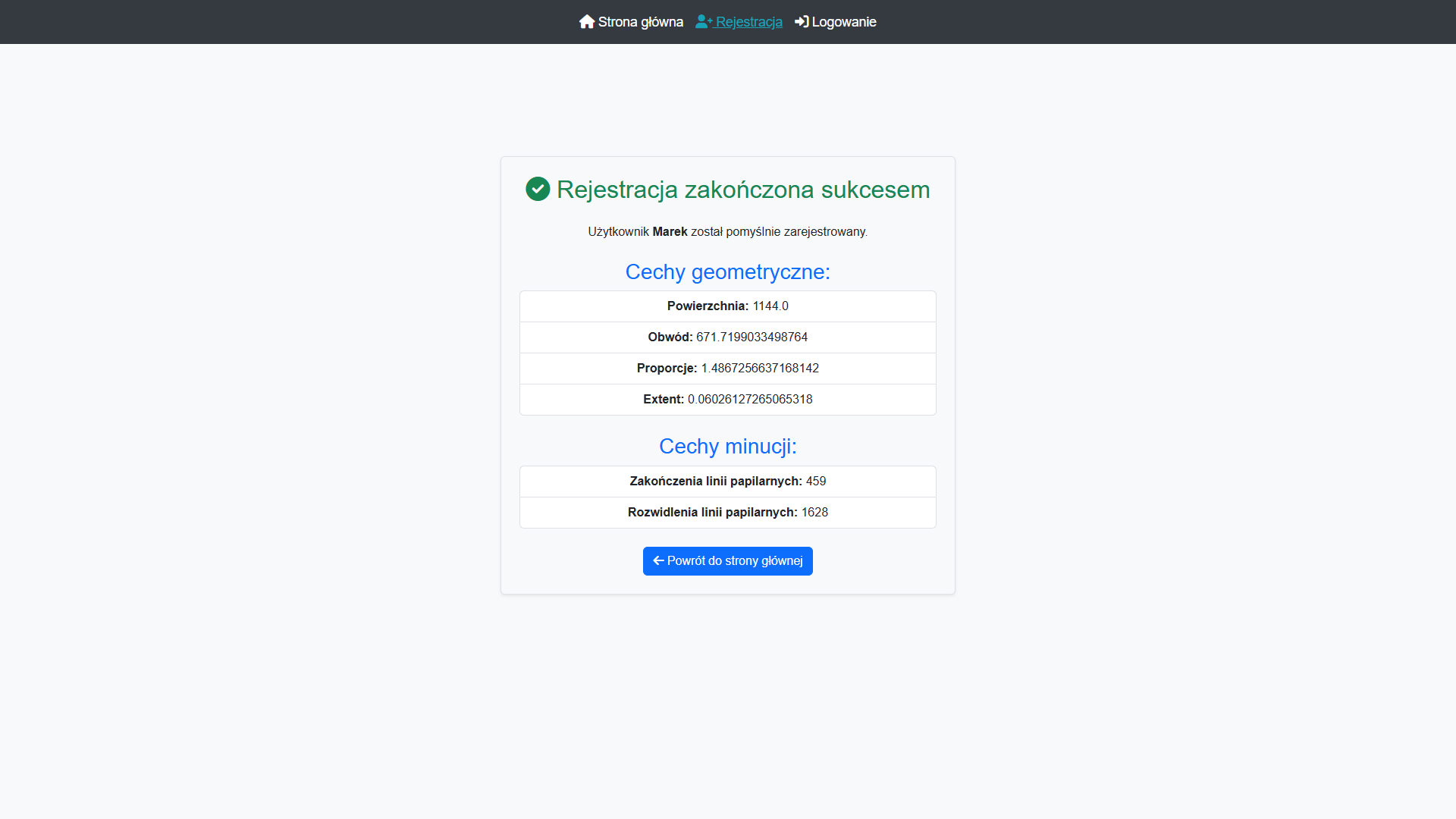
W obecnej implementacji dane użytkowników są przechowywane w plikach tekstowych, które pełnią funkcję prostej „bazy danych”. Dla każdego użytkownika generowane są oddzielne pliki zawierające cechy wyodrębnione z odcisku palca (wektor cech CNN, cechy geometryczne oraz minucje) oraz zahashowane hasło. Chociaż takie rozwiązanie jest wystarczające dla prototypowego systemu, sprawdza się jedynie w małej skali, umożliwiając podstawowe operacje przechowywania i odczytu danych.

W celu zwiększenia skalowalności i bezpieczeństwa systemu w przyszłości wskazane byłoby zastąpienie plików tekstowych tradycyjną bazą danych. Użycie bazy danych pozwoliłoby na efektywniejsze zarządzanie danymi, zapewniając łatwiejsze wyszukiwanie, przechowywanie metadanych oraz obsługę bardziej złożonych zapytań. Taka modernizacja byłaby kluczowa dla wdrożenia systemu w środowisku produkcyjnym, umożliwiając jego lepsze dostosowanie do rzeczywistych wymagań i większej liczby użytkowników.



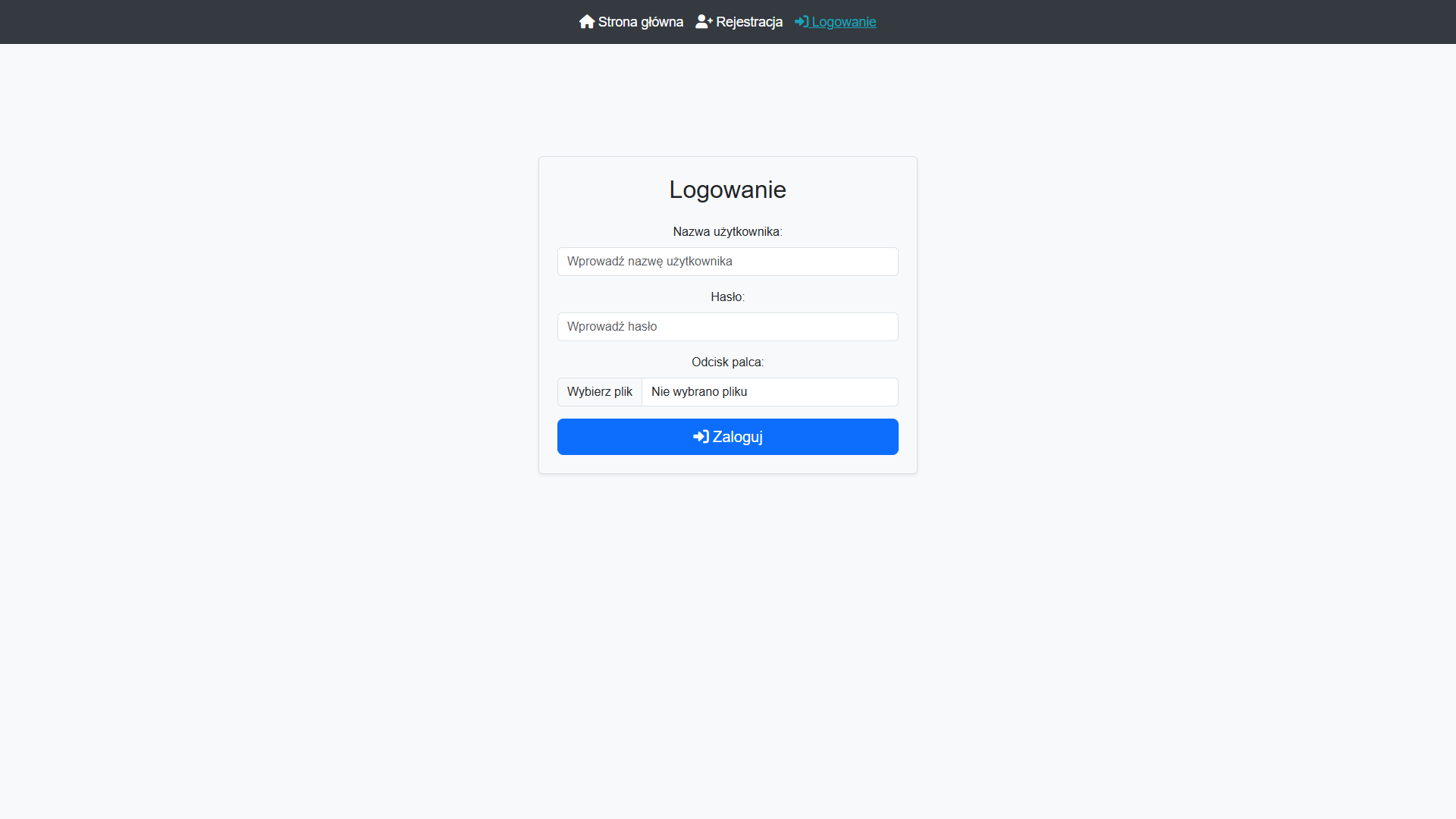
Ekran główny aplikacji „SecurePrint” cechuje się przejrzystością i intuicyjnością, co ułatwia użytkownikowi rozpoczęcie pracy z systemem. W górnej części strony znajduje się prosty pasek nawigacyjny, umożliwiający szybki dostęp do funkcji rejestracji oraz logowania. W centralnej części ekranu umieszczono wyraźnie oznaczone przyciski, które zachęcają do podjęcia kolejnych kroków. Minimalistyczny design i stonowana kolorystyka nadają aplikacji nowoczesny i profesjonalny charakter, wspierając pozytywne doświadczenie użytkownika.

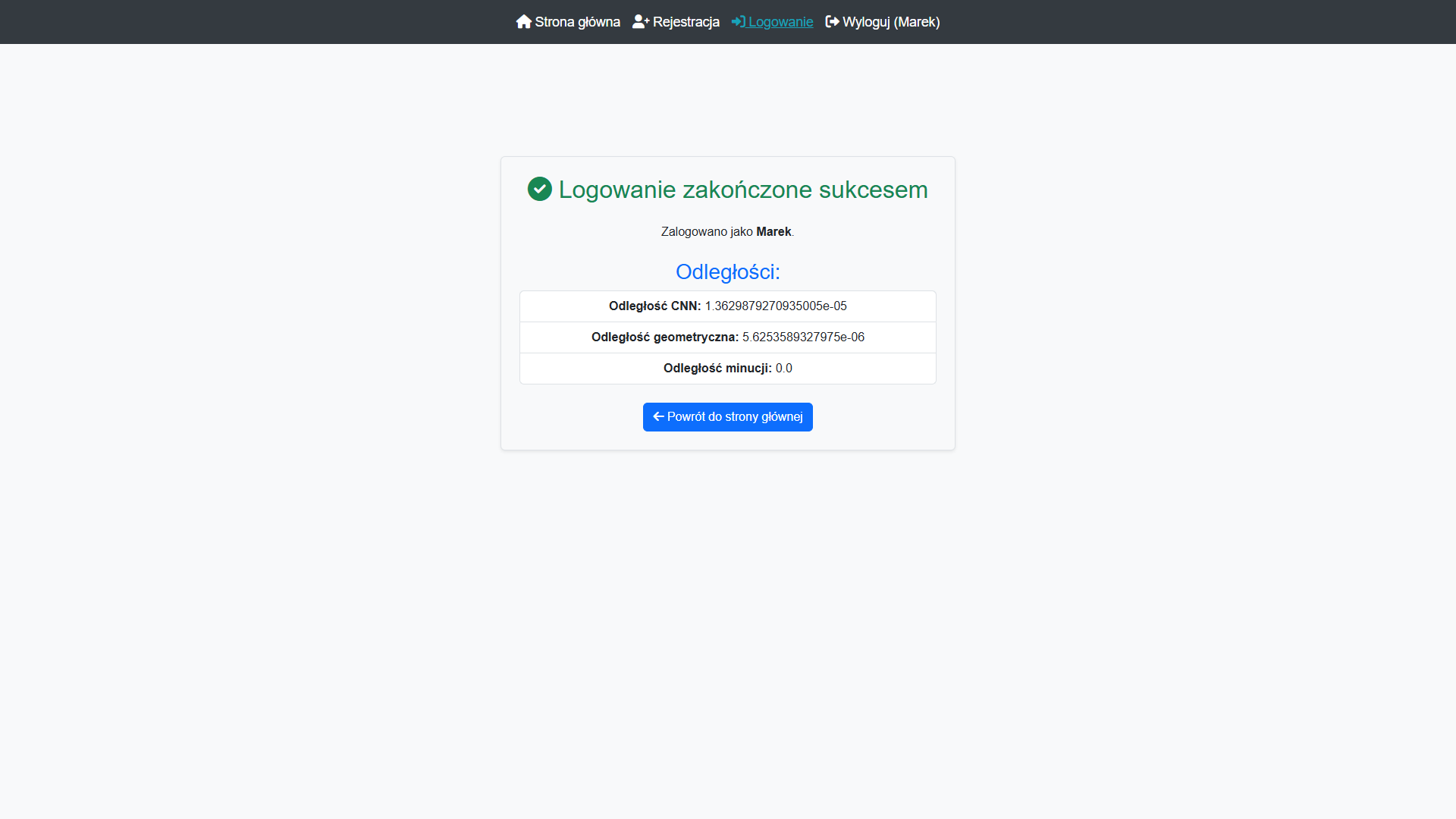




Powyższe zrzuty ekranu przedstawiają proces rejestracji użytkownika oraz potwierdzenie jej pomyślnego zakończenia. Na pierwszym ekranie użytkownik wprowadza nazwę, hasło oraz przesyła obraz odcisku palca, który następnie zostaje przetworzony przez system. Wyniki przetwarzania, takie jak cechy geometryczne, minucje oraz wektor cech uzyskany z modelu CNN, są zapisywane w plikach pełniących rolę bazy danych, a hasło użytkownika jest zabezpieczane w formie haszowanej.

Na drugim ekranie prezentowane jest potwierdzenie pomyślnej rejestracji, zawierające kluczowe informacje wyekstrahowane z obrazu odcisku palca: cechy geometryczne (powierzchnia, obwód, proporcje i extent) oraz cechy minucji (zakończenia i rozwidlenia linii papilarnych). Wyświetlanie szczegółowych danych ma charakter deweloperski i umożliwia wizualizację działania systemu. W przyszłych wersjach systemu te informacje mogłyby zostać ukryte, aby zapewnić większą prywatność i bezpieczeństwo użytkowników



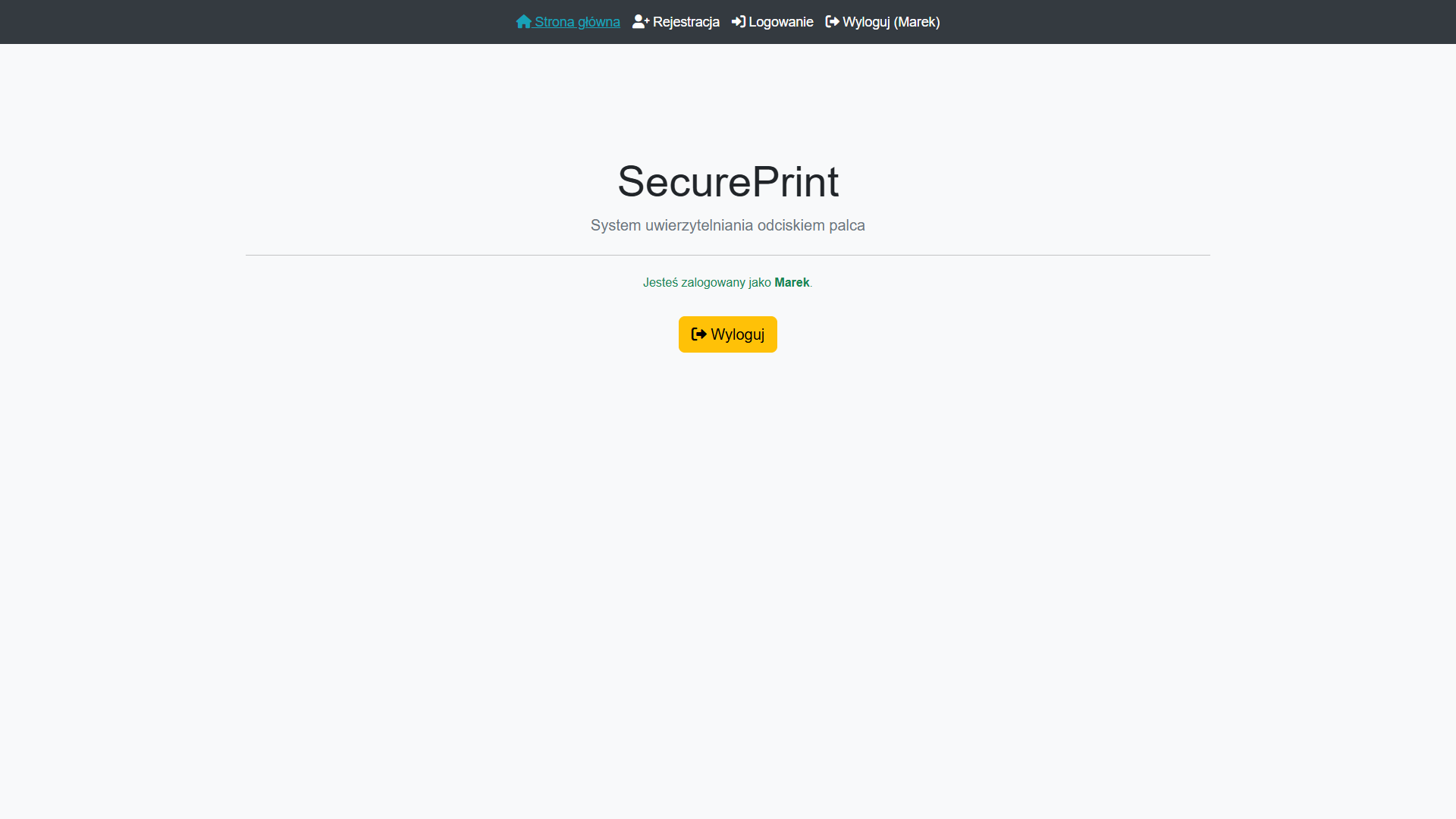


Proces logowania w systemie SecurePrint opiera się na weryfikacji nazwy użytkownika, hasła oraz analizy obrazu odcisku palca. Po wprowadzeniu danych przez użytkownika system sprawdza, czy w bazie istnieje odpowiadający użytkownik. Następnie hasło przesłane przez użytkownika jest porównywane z zahashowanym hasłem zapisanym w bazie przy użyciu algorytmu SHA-256. Po pomyślnej weryfikacji hasła system przechodzi do analizy biometrycznej odcisku palca.

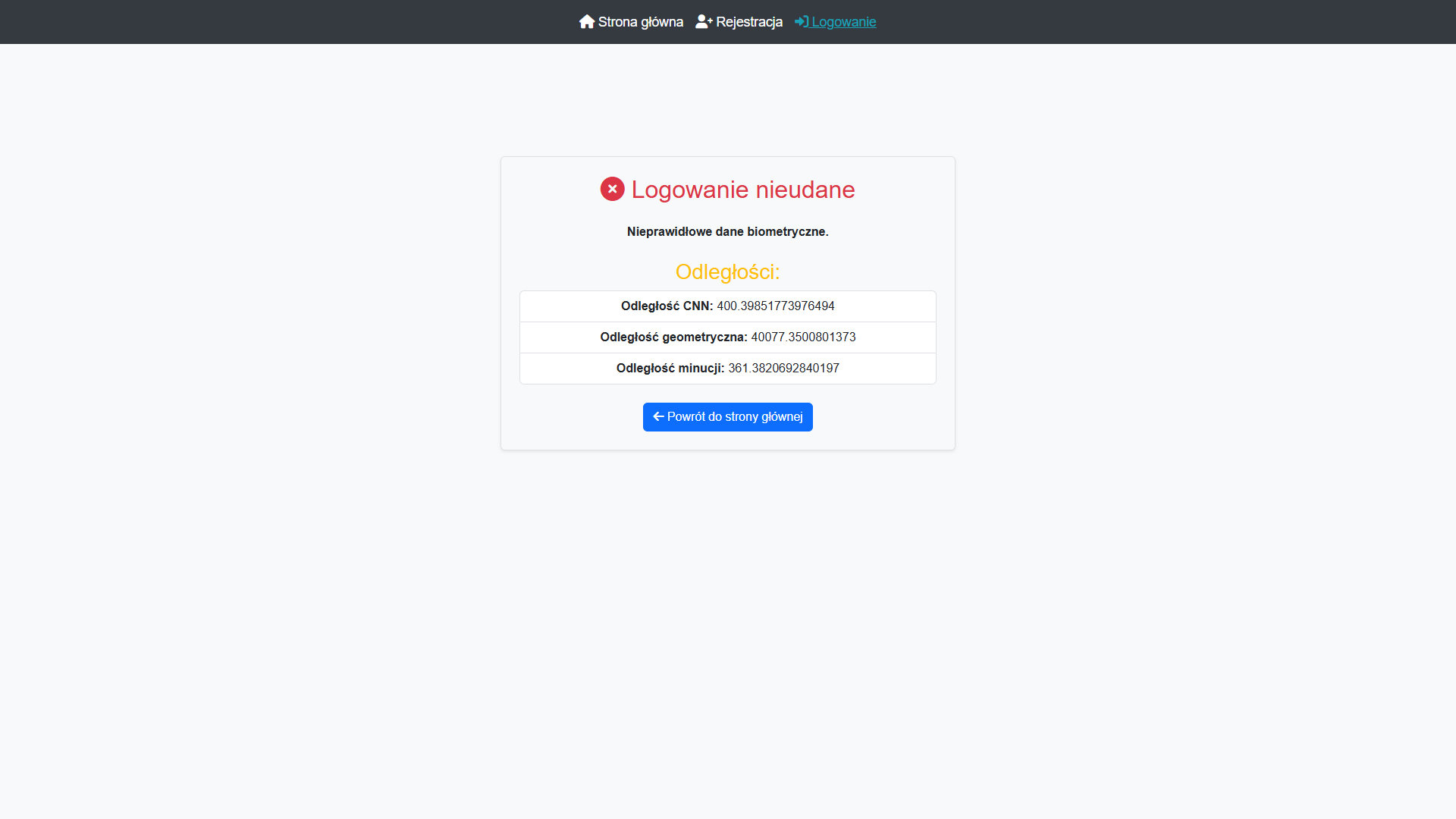
System wyodrębnia z przesłanego obrazu cechy geometryczne (powierzchnia, obwód, proporcje, extent), cechy minucji (zakończenia i rozwidlenia linii papilarnych) oraz cechy generowane przez model CNN. Nowo wyekstrahowane dane są następnie porównywane z zapisanymi cechami użytkownika za pomocą obliczania odległości euklidesowych. Trzy kluczowe metryki obejmują odległość wektorów cech CNN, odległość geometryczną oraz odległość minucji.

Aby proces logowania zakończył się sukcesem, wszystkie odległości muszą mieścić się w ustalonych progach. Progi te definiują poziom rygorystyczności systemu – niższe wartości zwiększają bezpieczeństwo, lecz mogą prowadzić do większej liczby błędnych odrzuceń, podczas gdy wyższe wartości mogą poprawić tolerancję kosztem bezpieczeństwa.

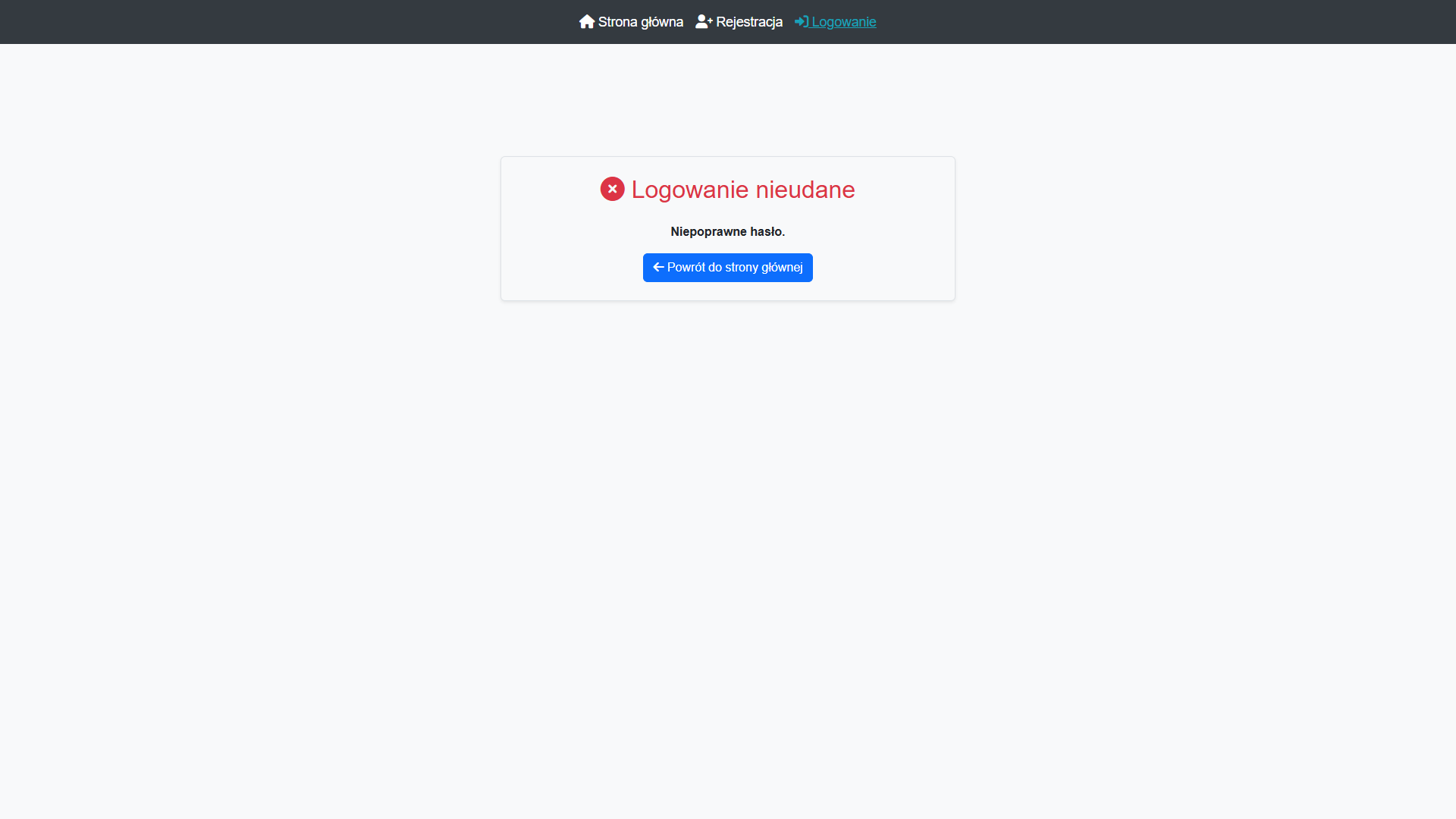
Po pomyślnym logowaniu system wyświetla wartości obliczonych odległości jako dane deweloperskie, co pozwala na analizę działania algorytmu. W wersji produkcyjnej te informacje mogą być ukryte, aby zwiększyć przejrzystość oraz bezpieczeństwo systemu. Dzięki możliwości regulacji progów SecurePrint może być łatwo dostosowany do różnych scenariuszy i wymagań bezpieczeństwa.



Po pomyślnym zalogowaniu interfejs systemu dostosowuje się do zalogowanego użytkownika. Na stronie głównej widoczna jest opcja wylogowania, dostępna zarówno w górnym pasku nawigacyjnym, jak i w centralnej części ekranu w formie przycisku. Taki układ zapewnia szybki i intuicyjny sposób zakończenia sesji, zwiększając wygodę obsługi systemu. Jednocześnie rozwiązanie to wspiera bezpieczeństwo, umożliwiając użytkownikowi pełną kontrolę nad dostępem do swojego konta.



Jeśli dane biometryczne użytkownika nie spełniają kryteriów zgodności z zapisanymi w systemie, logowanie zostaje odrzucone, a użytkownik otrzymuje odpowiedni komunikat. System porównuje nowo wyodrębnione cechy (modelu CNN, geometryczne i minucji) z zapisanymi danymi, obliczając odległości. Logowanie jest akceptowane, jeśli odległości mieszczą się w progach: 10.0 dla cech CNN, 5.0 dla geometrycznych i 5.0 dla minucji. Progi te można dostosowywać, aby znaleźć balans między bezpieczeństwem a tolerancją systemu — niższe wartości zwiększają bezpieczeństwo, ale mogą prowadzić do większej liczby odrzuceń, natomiast wyższe poprawiają tolerancję kosztem rygoru.



W przypadku nieprawidłowego hasła logowanie zostaje zablokowane, a użytkownik otrzymuje komunikat "Niepoprawne hasło". System weryfikuje hasło, porównując jego hash (SHA-256) z wartością zapisaną podczas rejestracji, co zwiększa bezpieczeństwo, ponieważ rzeczywiste hasło nie jest przechowywane. Taki sposób minimalizuje ujawnianie szczegółów dotyczących przyczyny błędu, zgodnie z zasadami bezpieczeństwa.

**Podsumowanie i wnioski**

Zaprojektowany system uwierzytelniania oparty na odciskach palców efektywnie łączy tradycyjne uwierzytelnianie hasłem z zaawansowanymi metodami biometrycznymi. Integracja cech geometrycznych, minucji oraz wektorów cech generowanych przez sieć neuronową (CNN) pozwoliła na osiągnięcie wysokiej skuteczności, co potwierdza dokładność na poziomie 91,25%. System nie tylko umożliwia rejestrację i logowanie użytkowników, ale także przechowywanie danych w lokalnej „bazie”, pozwalając na ich dokładne porównywanie podczas procesu uwierzytelniania.

Wyświetlanie szczegółowych danych w obecnej wersji pełni funkcję deweloperską, wspierając testowanie i optymalizację systemu. W przyszłości te informacje mogą zostać ukryte, co poprawi komfort użytkowania i zapewni większą ochronę prywatności użytkowników.

System cechuje się elastycznością i możliwością rozbudowy. Przyszłe usprawnienia mogą obejmować integrację z profesjonalną bazą danych, regulację progów akceptacji cech biometrycznych, a także implementację dodatkowych funkcji, takich jak obsługa wielu metod biometrycznych czy zaawansowane mechanizmy monitorowania bezpieczeństwa.

Podsumowując, projekt stanowi solidną podstawę dla budowy zaawansowanych systemów uwierzytelniania. Łączy intuicyjność obsługi z wysokim poziomem bezpieczeństwa, co czyni go atrakcyjnym rozwiązaniem zarówno w środowiskach edukacyjnych, jak i potencjalnych wdrożeniach komercyjnych.