**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.

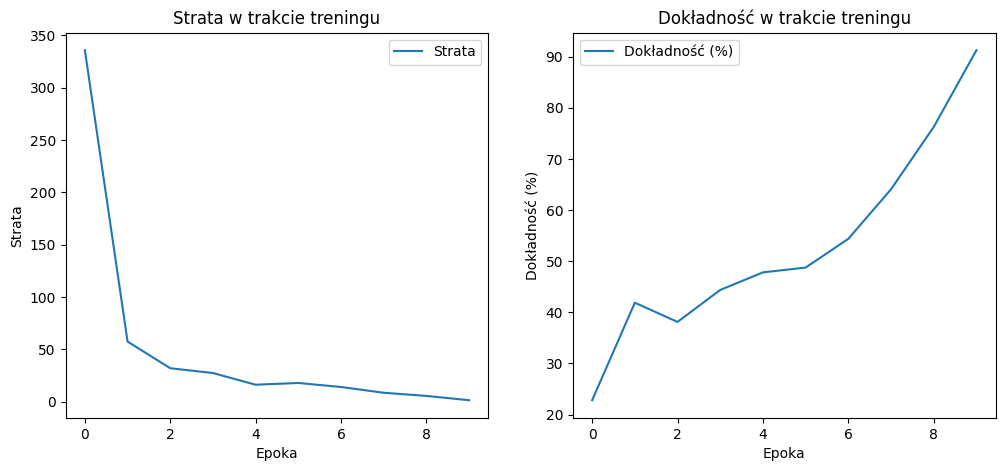
W projekcie zastosowano autorski model sieci neuronowej do ekstrakcji cech z odcisków palców, który łączy zaawansowane techniki analizy obrazu z danymi geometrycznymi i minucjami (charakterystycznymi punktami linii papilarnych). Takie podejście pozwoliło na precyzyjne odwzorowanie i weryfikację odcisków 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.

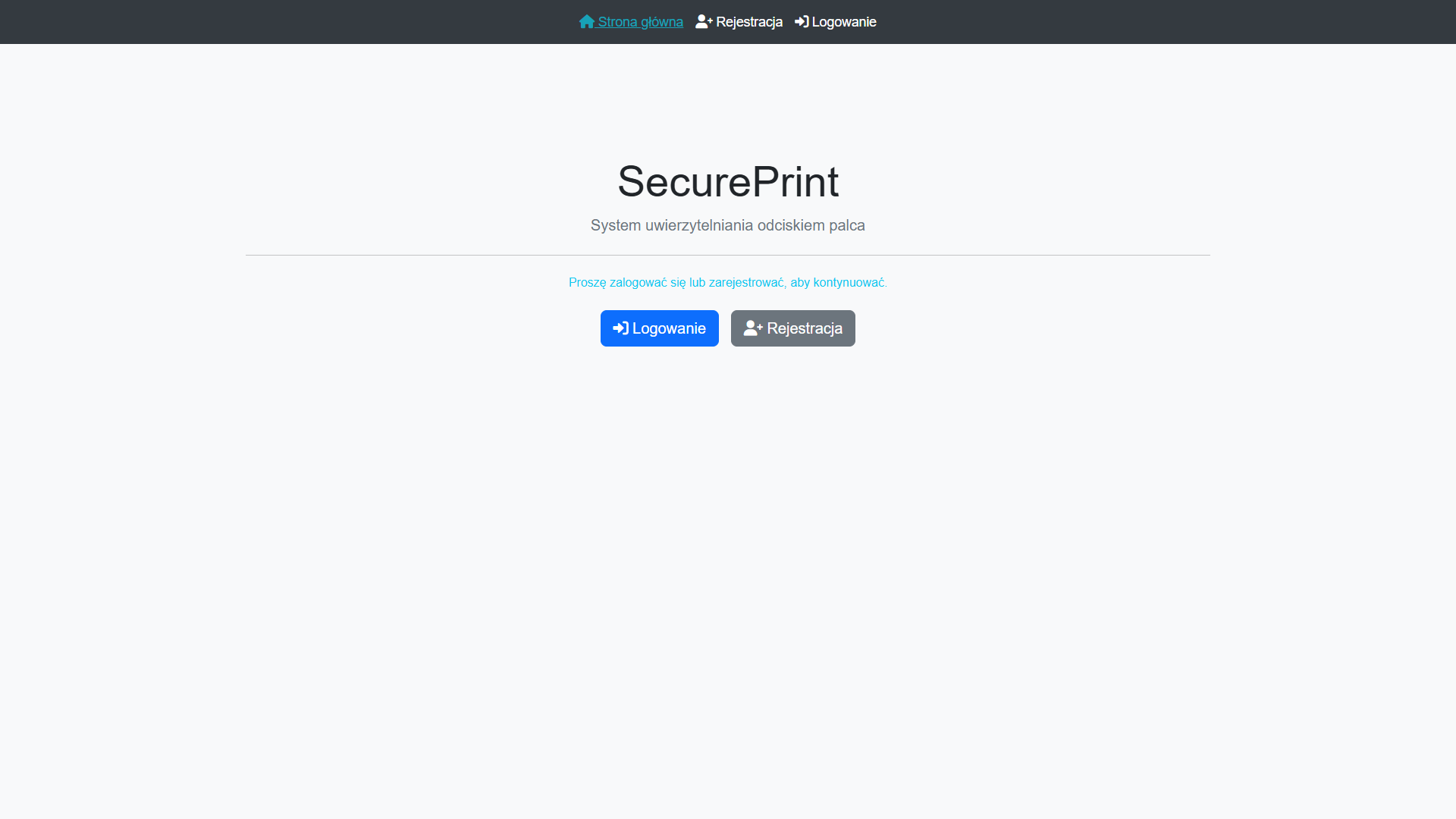
Proces treningu modelu polegał na przygotowaniu danych, gdzie każdy folder reprezentował użytkownika, zawierając obrazy jego odcisków palców. Dane wstępnie przetworzono, skalując obrazy do wymiarów 128x128 pikseli i normalizując je. Wyodrębniono cechy geometryczne oraz minucje, które posłużyły jako dodatkowe dane wejściowe. Model trenowano przez 10 epok, wykorzystując optymalizator Adam i funkcję strat CrossEntropyLoss. Proces obejmował forward pass, obliczanie straty i optymalizację wag za pomocą backpropagacji. Dzięki zastosowaniu GPU trening przebiegał szybko i efektywnie.



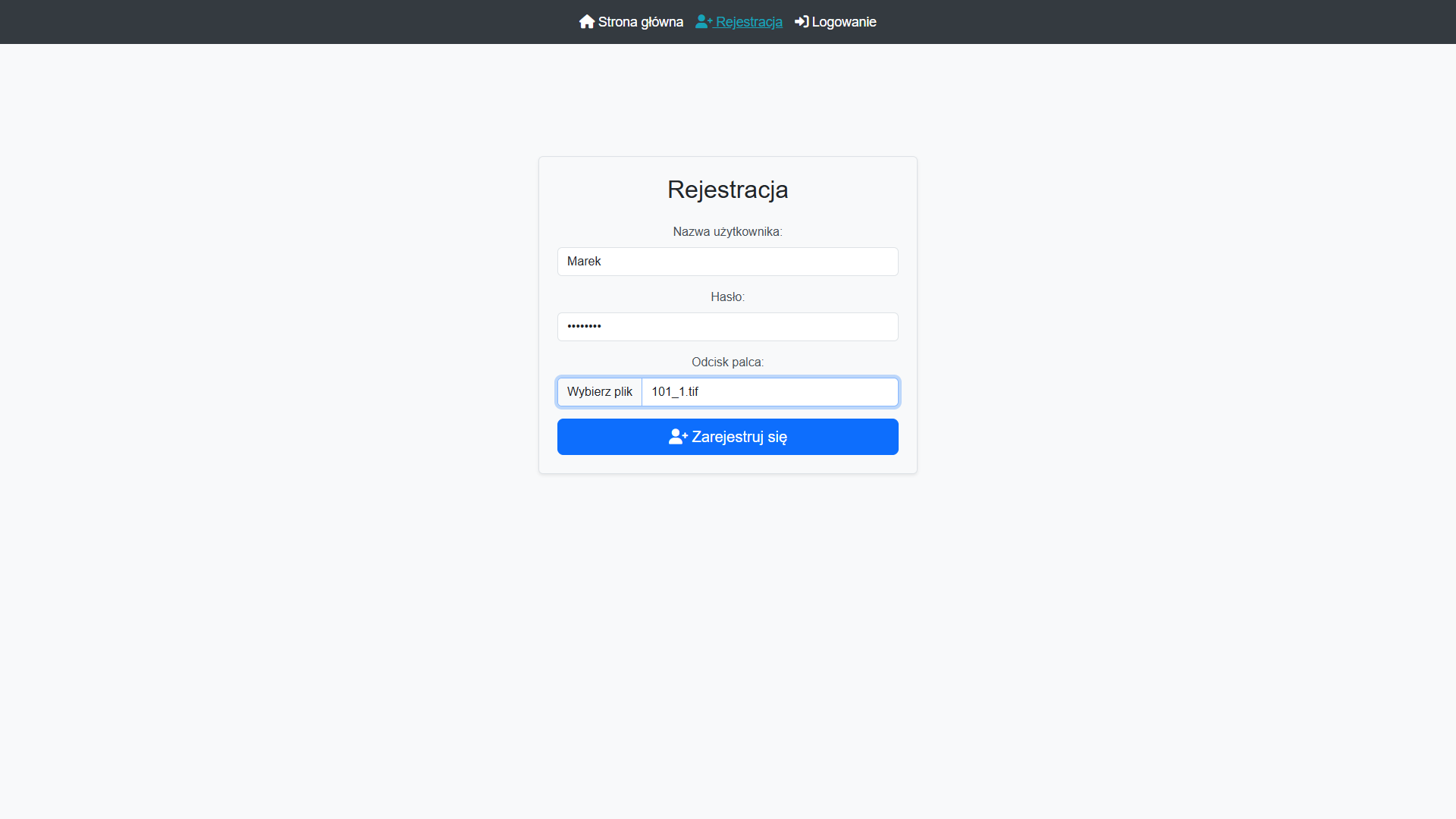
Rezultaty treningu potwierdzają skuteczność zastosowanego podejścia. Strata modelu zmniejszyła się z 335.89 do 1.28, a dokładność wzrosła z 22.81% do 91.25% w ciągu 10 epok, co dowodzi efektywnej optymalizacji i zdolności modelu do klasyfikacji użytkowników. Wizualizacje wyników treningu ukazują sukcesywną redukcję straty oraz wzrost dokładności, potwierdzając skuteczność rozwiązania w uwierzytelnianiu użytkowników.

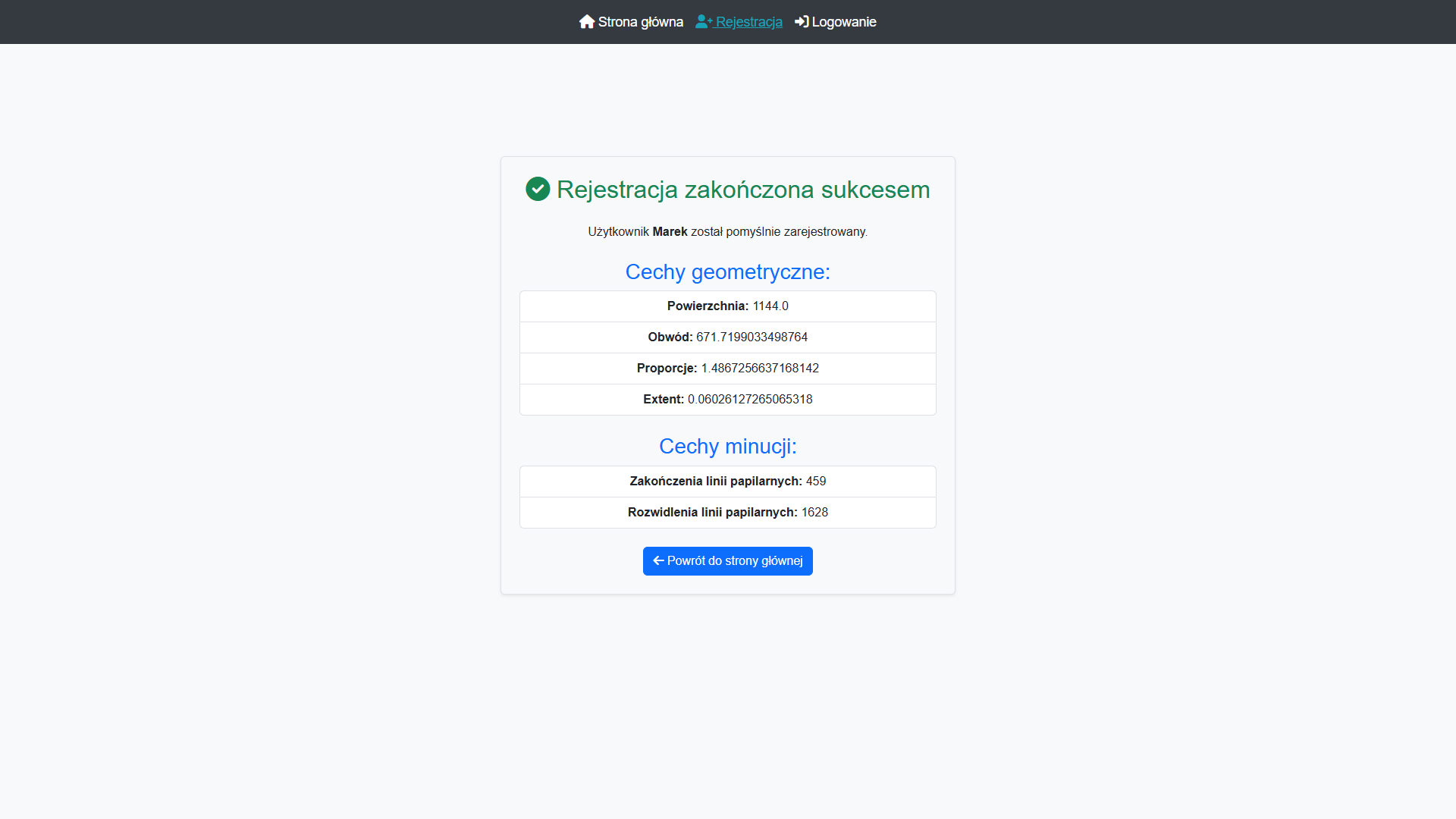
W obecnej implementacji systemu dane użytkowników są przechowywane w plikach tekstowych, które pełnią rolę prostej „bazy danych”. Dla każdego użytkownika tworzone są oddzielne pliki, zawierające jego cechy wyekstrahowane z odcisku palca (wektor cech CNN, cechy geometryczne i minucje) oraz zahashowane 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.



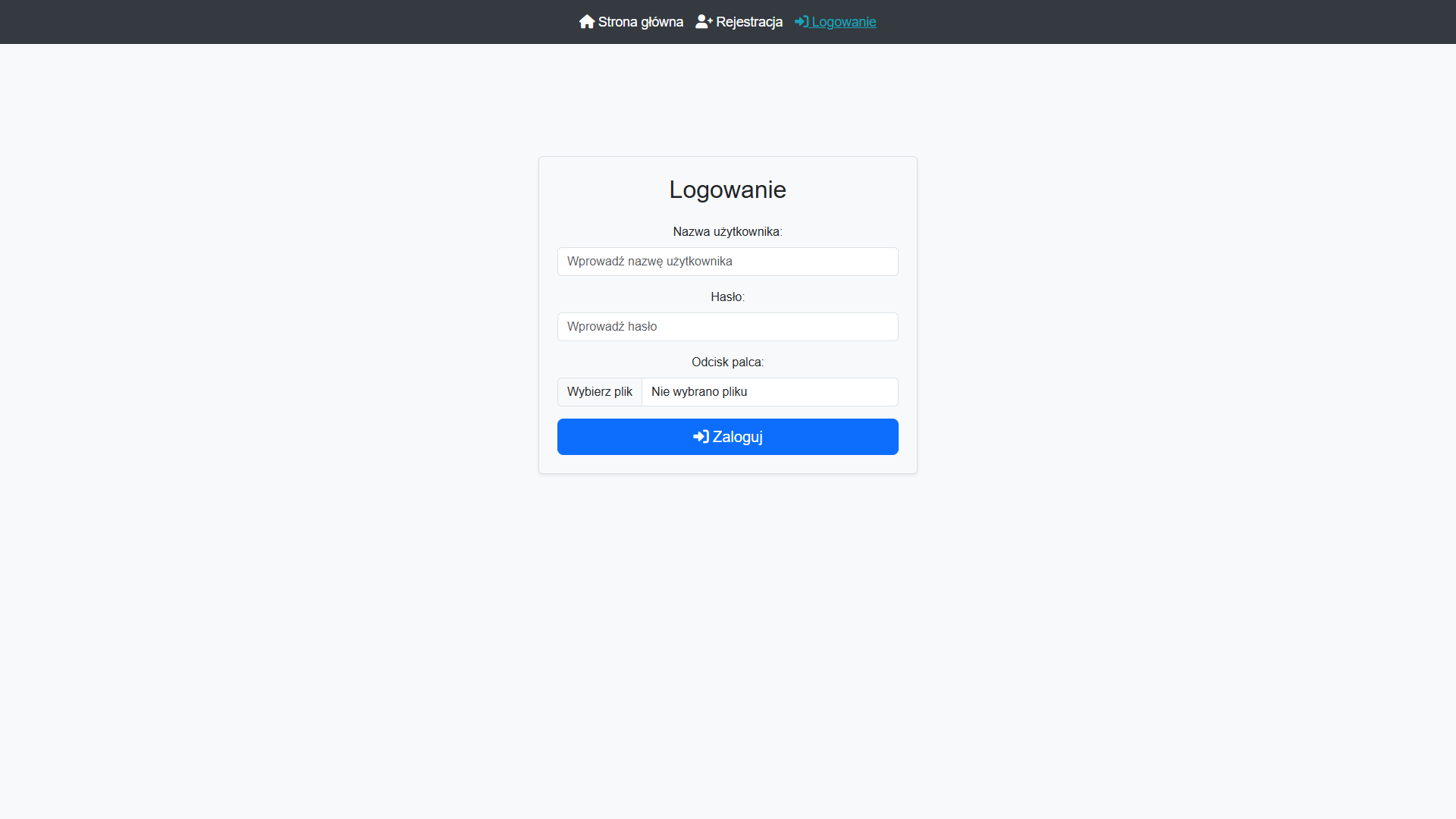
Ekran główny aplikacji „SecurePrint” to przejrzyste i intuicyjne miejsce startowe, które wprowadza użytkownika do systemu. Na górze strony znajduje się prosta nawigacja umożliwiająca dostęp do funkcji rejestracji i logowania. Centralna część ekranu zachęca do rozpoczęcia korzystania z aplikacji, oferując wyraźnie oznaczone przyciski. Jasna kolorystyka i minimalistyczny design zapewniają nowoczesny i profesjonalny wygląd, ułatwiając użytkownikowi pierwsze kroki w systemie.

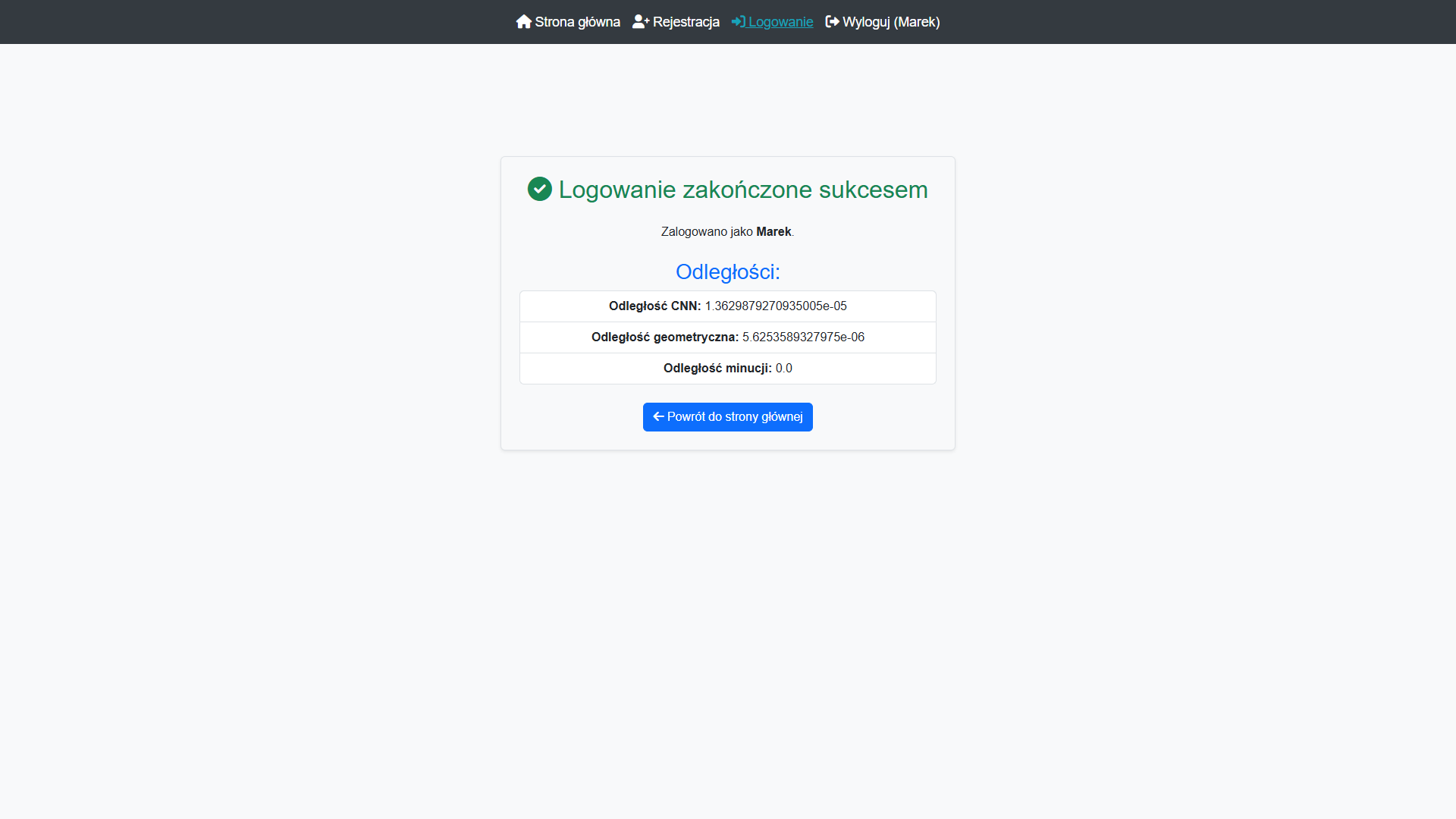




Powyższe zrzuty ekranu przedstawiają proces rejestracji użytkownika oraz potwierdzenie jej pomyślnego zakończenia. Na pierwszym ekranie użytkownik wprowadza swoją nazwę, hasło i przesyła obraz odcisku palca, który następnie jest przetwarzany. Wyniki rejestracji, takie jak cechy geometryczne i minucji oraz wektor cech z modelu CNN, są zapisywane w dedykowanych plikach „bazy” systemu, a hasło użytkownika jest zabezpieczane w postaci haszowanej.

Na drugim ekranie użytkownik widzi potwierdzenie rejestracji wraz z kluczowymi informacjami wyekstrahowanymi z obrazu, takimi jak cechy geometryczne (powierzchnia, obwód, proporcje, extent) i cechy minucji (zakończenia i rozwidlenia linii papilarnych). Wyświetlanie tych szczegółów ma charakter deweloperski i pomaga lepiej zilustrować działanie systemu. W przyszłości informacje te mogłyby zostać ukryte, aby zwiększyć prywatność i bezpieczeństwo użytkowników.





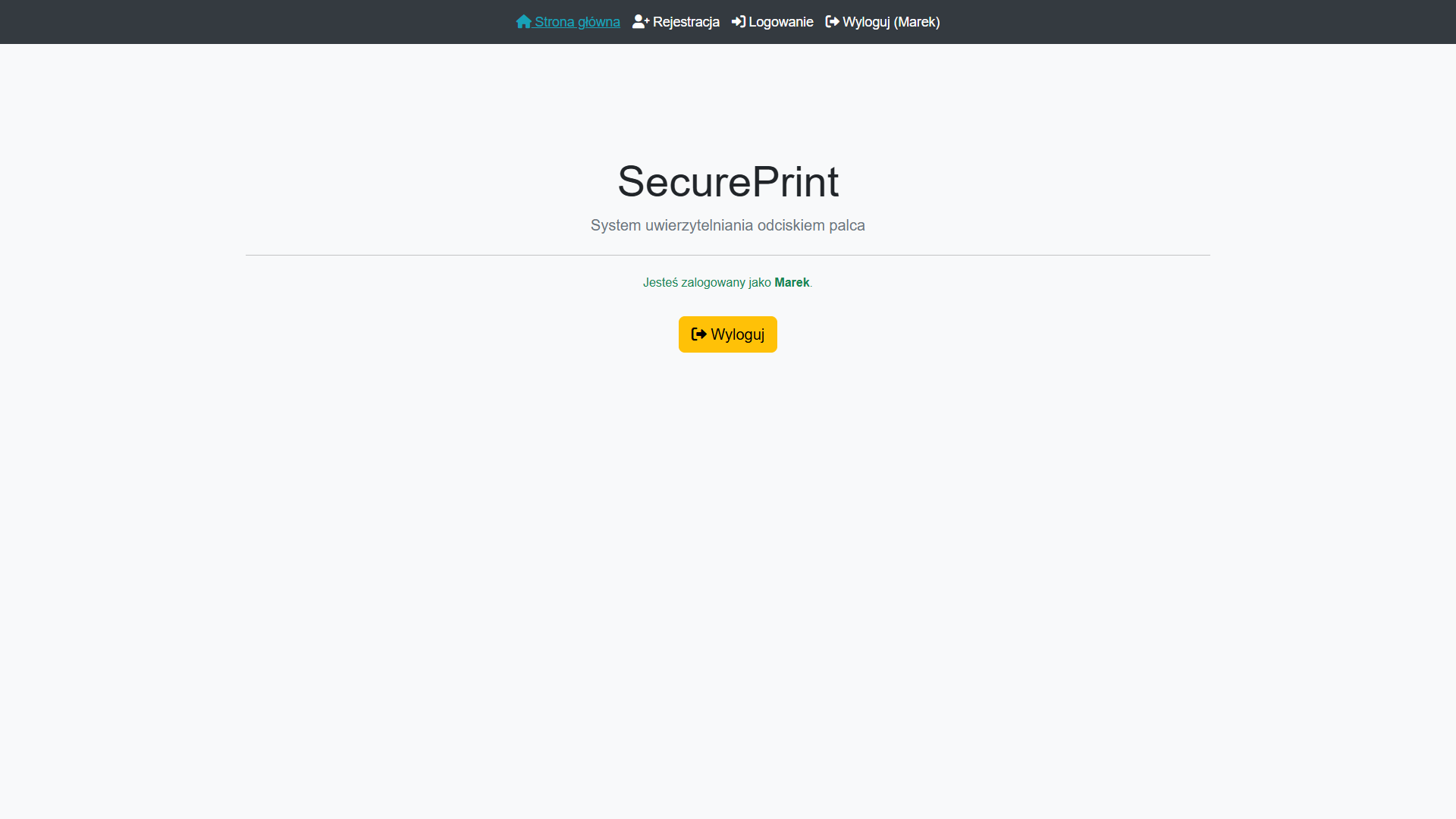
Logowanie w systemie SecurePrint opiera się na weryfikacji nazwy użytkownika, hasła oraz analizy obrazu odcisku palca. Po podaniu danych użytkownika system sprawdza czy istnieje odpowiadający użytkownik w bazie, a następnie porównuje hasło przesłane przez użytkownika z zapisanym w bazie, wykorzystując algorytm SHA-256 do weryfikacji zgodności hashy. Jeśli weryfikacja hasła powiedzie się, system przechodzi do analizy odcisku palca.

Z przesłanego obrazu odcisku palca system wyodrębnia cechy geometryczne (powierzchnia, obwód, proporcje, extent), cechy minucji (zakończenia i rozwidlenia linii papilarnych) oraz cechy generowane przez model CNN. Następnie nowo wyekstrahowane cechy są porównywane z odpowiadającymi im danymi zapisanymi w bazie użytkownika.

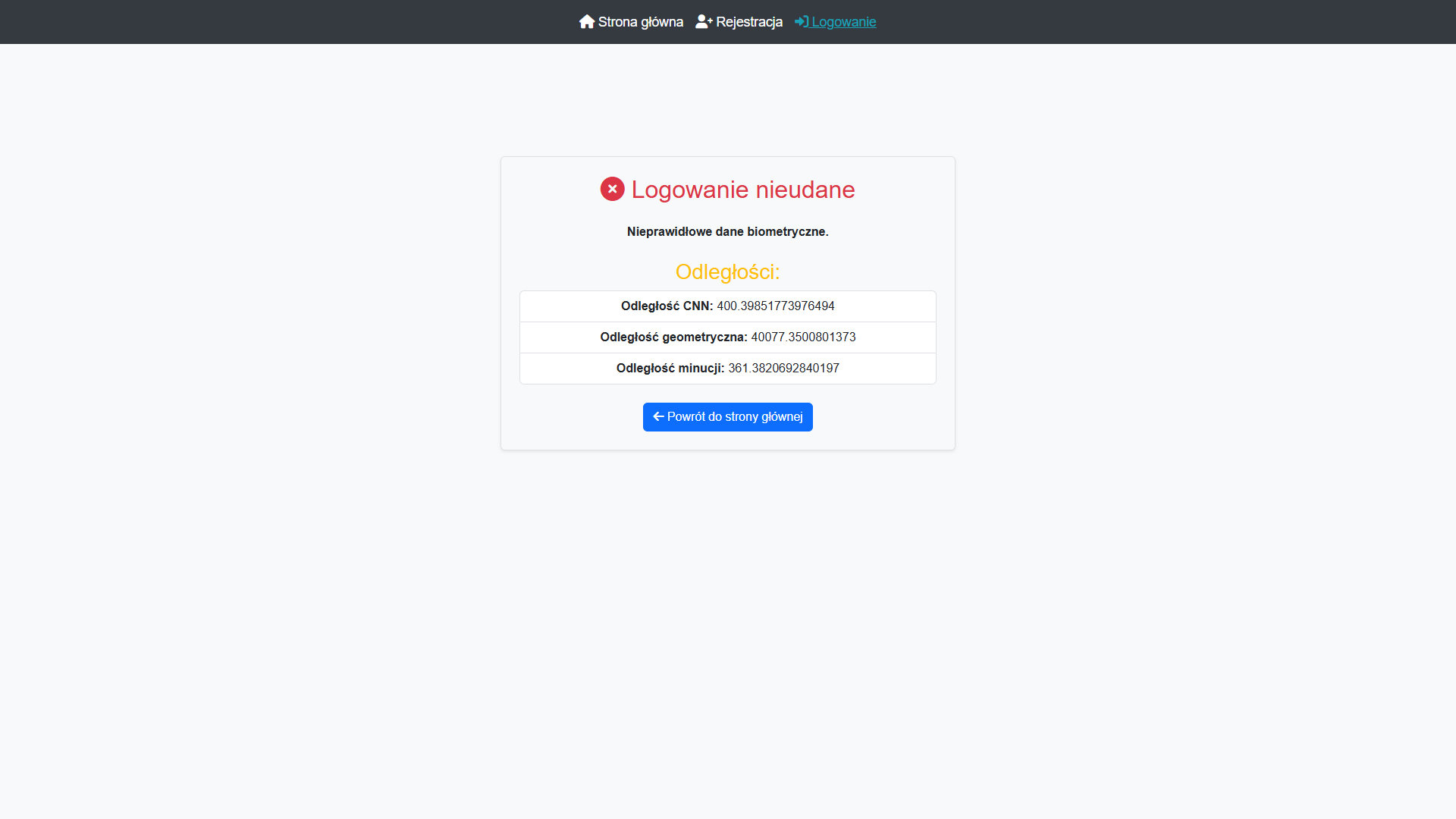
Porównanie cech odbywa się poprzez obliczanie odległości pomiędzy zapisanymi a nowymi danymi. Obliczane są trzy rodzaje odległości: odległość wektorów cech CNN, odległość geometryczna oraz odległość minucji. Aby użytkownik został zalogowany, wszystkie te odległości muszą mieścić się w ustalonych progach.

Progi te są kluczowe dla działania systemu i definiują, jak bardzo system ma być rygorystyczny. Wysokość progów można dostosować w zależności od wymagań – niższe wartości progów zwiększają bezpieczeństwo, ale mogą skutkować większą liczbą błędnych odrzuceń, podczas gdy wyższe wartości mogą być bardziej tolerancyjne, ale kosztem potencjalnego obniżenia bezpieczeństwa.

W przypadku pomyślnego logowania system wyświetla odległości pomiędzy nowymi a zapisanymi cechami jako informacje deweloperskie, które pozwalają na lepszą analizę działania systemu. Te informacje mogą być usunięte lub ukryte w produkcyjnej wersji aplikacji, aby poprawić przejrzystość oraz bezpieczeństwo systemu. Dzięki regulacji progów system może być dostosowywany do różnych scenariuszy i poziomów wymagań bezpieczeństwa.



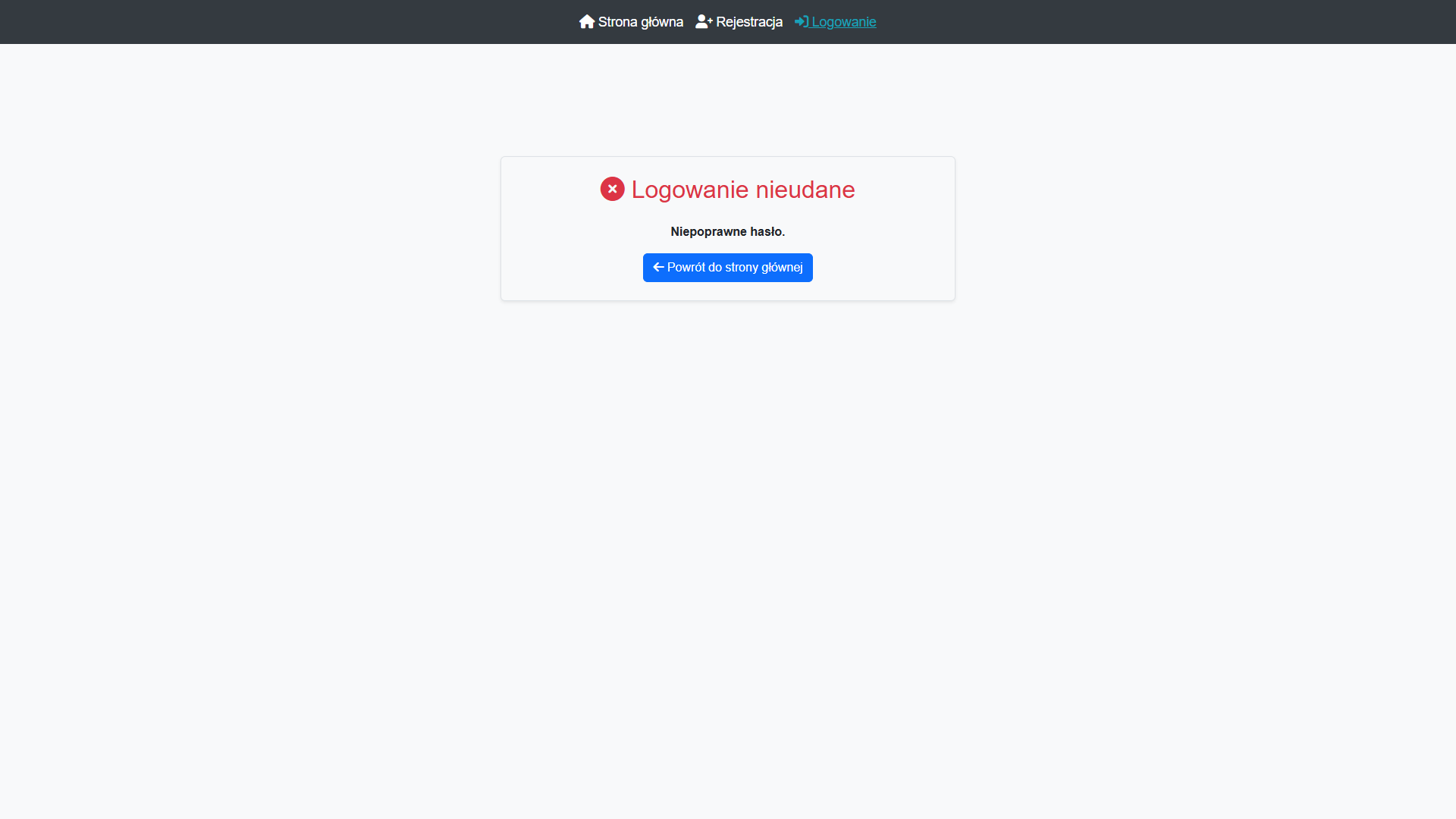
Po pomyślnym zalogowaniu interfejs systemu dostosowuje się do stanu zalogowania użytkownika. Na stronie głównej pojawia się wyraźna opcja wylogowania dostępna zarówno na górnym pasku nawigacyjnym, jak i na stronie w formie przycisku. Te elementy zostały wprowadzone, aby ułatwić użytkownikowi szybkie i intuicyjne zakończenie sesji w systemie. Dzięki takiemu rozwiązaniu zapewniona jest wygoda obsługi oraz bezpieczeństwo, dając użytkownikowi pełną kontrolę nad swoim dostępem do systemu.



Jeśli dane biometryczne użytkownika, nie spełniają kryteriów zgodności z zapisanymi w systemie, logowanie zostaje odrzucone, a użytkownik otrzymuje komunikat o niepowodzeniu. System oblicza i porównuje odległości dla cech wyodrębnionych przez model CNN, cech geometrycznych (np. powierzchnia, obwód) oraz cech minucji (zakończenia i rozwidlenia linii papilarnych).

Logowanie jest akceptowane tylko wtedy, gdy odległości te mieszczą się w ustalonych progach: 10.0 dla cech CNN, 5.0 dla cech geometrycznych i 5.0 dla cech minucji. Te wartości progowe można dostosować w trakcie testowania systemu, aby zwiększyć jego rygorystyczność lub dopasować do wymagań bezpieczeństwa. Niższe progi zwiększają bezpieczeństwo, ale mogą prowadzić do większej liczby błędnych odrzuceń, podczas gdy wyższe wartości mogą zmniejszyć ich liczbę kosztem dokładności.

Wyświetlanie szczegółowych odległości ma na celu wspieranie procesu testowania i optymalizacji systemu. W finalnej wersji aplikacji te dane mogą zostać ukryte w celu zwiększenia ochrony prywatności użytkowników.



W przypadku podania nieprawidłowego hasła system blokuje logowanie i wyświetla komunikat "Niepoprawne hasło". Hasło użytkownika jest weryfikowane poprzez porównanie jego hashu (SHA-256) z wartością zapisaną w systemie podczas rejestracji. Dzięki temu rzeczywiste hasło nie jest przechowywane, co zwiększa bezpieczeństwo danych.

Taki sposób informowania użytkownika eliminuje ujawnianie szczegółów, czy problem dotyczy hasła, czy danych biometrycznych, co jest zgodne z dobrymi praktykami zabezpieczeń.

Zaprojektowany system uwierzytelniania oparty na odciskach palców skutecznie łączy tradycyjne uwierzytelnianie hasłem z nowoczesnymi metodami biometrycznymi. Dzięki integracji cech geometrycznych, minucji oraz danych z sieci neuronowej (CNN), system osiąga wysoką skuteczność, co potwierdza dokładność 91,25%.

System umożliwia rejestrację i logowanie użytkowników, przechowując dane w lokalnej „bazie”, co zapewnia możliwość ich porównywania. Aktualnie wyświetlane szczegóły danych służą celom deweloperskim, ale w przyszłości mogą zostać ukryte dla lepszego komfortu użytkownika.

Projekt jest elastyczny i łatwo go rozbudować, na przykład poprzez integrację z profesjonalną bazą danych, dostosowanie progów akceptacji dla cech biometrycznych lub dodanie nowych funkcji. Stanowi solidną podstawę dla zaawansowanych systemów uwierzytelniania, łącząc intuicyjność użytkowania z wysokim poziomem bezpieczeństwa.