POLITECHNIKA ŚLĄSKA

WYDZIAŁ INŻYNIERII BIOMEDYCZNEJ

Projekt z Biometrii

Czytnik lini papilarnych

Autor: Dawid Barański, Dawid Nyderek, Kamil Kozieł

Prowadzący: dr inż. Marta Danch-Wierzchowska

Zabrze, czerwiec, 2019

Spis treści

Spis rysunków

Spis tabel

1. Wstęp

1.1 Cel projektu

Celem pracy była analiza biometrycznych systemów zabezpieczeń opartych na odczycie linii papilarnych w urządzeniach użytku codziennego oraz implemetacja autoryzacji dostępu do aplikacji mobilnej przy pomocy czytnika linii papilarnych.

1.2 Zakres pracy

Zakres pracy:

1. Analiza wykorzystywanych systemów biometrycznych.
2. Analiza dostępnych czytników linii papilarnych.
3. Analiza metod implementacji czytników linii papilarnych w aplikacjach.
4. Implementacja obsługi autoryzacji dostępu do aplikacji poprzez czytnik linii papilarnych:
   (a) przygotowanie widoków,
   (b) opracowanie API,
   (c) połączenie widoków i API z istniejącą aplikacją.
5. Opracowanie podsumowania i wniosków.

1.3 Wstęp teoretyczny

1.3.1 Systemy biometryczne

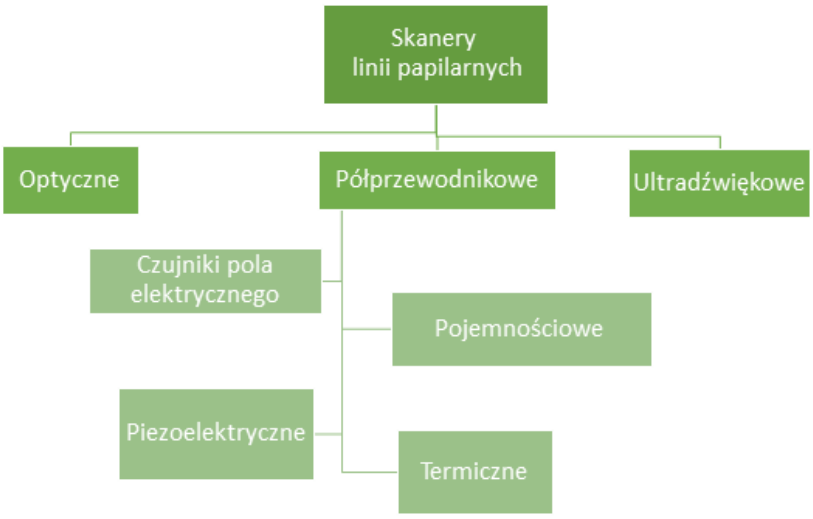
Biometria jest nauką zajmującą się pomiarami i analizą cech fizycznych i behawioralnych organizmów żywych. Dane te wykorzystywane są w wielu innych dziedzinach nauki kryminologii, antropologii, fizjologii, medycynie[1, 2]. Najczęściej spotykanym zastosowaniem metod biometrycznych jest kontrola dostępu w systemach zabezpieczeń. Systemy takie mogą za pomocą danych biometrycznych udzielać dostępu do systemu bądź określonych danych jedynie osobom do tego uprawnionym. Mocną stroną tego rozwiązania jest indywidualność cech, które są wykorzystywane. Cechami biometrycznymi

nazywamy indywidualne atrybuty, które charakteryzują się znikomą powtarzalnością w obrębie populacji. Do cech takich zaliczamy między innymi:

- odcisk palca,
- wzór tęczówki oka,
- głos,
- zapach,
- chód,
- podpis.

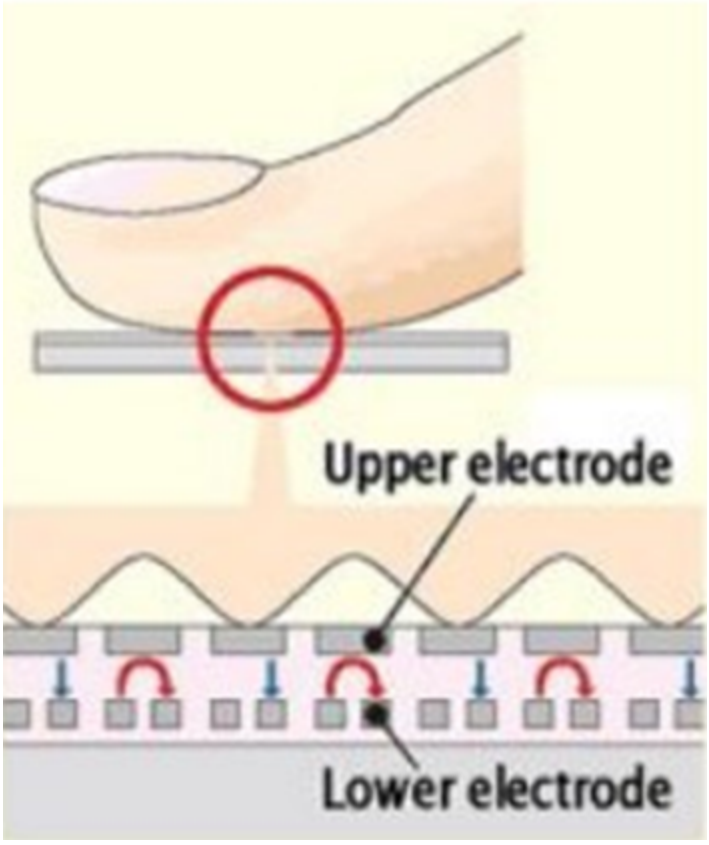
Najbradziej rozpowszechnioną cechą wykorzystywaną do autoryzacji dostępu jest analiza linii papilarnych. Czytniki linii papilarnych motowane są w większości współczesnych smartphonów, mogą zasępować klucz do drzwi lub być alternatywnym sposobem logowania się do komputera. Cechy biometryczne mierzone kilkukrotnie u tego samego człowieka, charakteryzują się zmiennością dla poszczególnych pomiarów. Wiąże się to z zależnością tych cech od stanu psychofizycznego człowieka, warunków otoczenia czy interakcji użytkownika z czujnikiem[3]. Wynikiem tego jest brak możliwości określenia stuprocentowej zgodności wzorca z innym pomiarem danej cechy.

1.3.2 Czytniki linii papilarnych



Rys. 1.1: Skanery linii papilarnych.

Praktyka wykorzytywania cech biometrycznych do identyfikacji, weryfikacji oraz autoryzacji osób za pomocą cech biometrycznych wiąże się z behawioralnym przystosowaniem człowieka. Ma to miejsce za każdym razem kiedy rozpoznajemy ludzi na podstawie twarzy. Umiejętność ta wykorzystywana jest przez ludzi często nie świadomie. Świadome wykorzytywanie cech biometrycznych miało jednak miejsce już 500 p.n.e. kiedy to zaczęto wykorzystywać odcisk palca do rejestracji transakcji. W poźniejszym okresie, za sprawą M. Malpighi'ego oraz J. C. A. Mayer'a, odcisk palca a właściwie jego cechy zostały opisane oraz stwierdzono ich unikatowość. Dzięki pracy tych osób na końcu XIX w. stworzony został pierwszy kompletny system klasyfikacji osób na podstawie odcisków palca. Autorem prac był Sir E. Henry [4]. Pomiarów dokonywano na odbitych na papierze palców wcześniej zamoczonych w tuszu. Dziś do pomiarów odcisków palców wykorzystuje się czytniki odcisków palców. Skanery linii papilarnych, ze względu na ykorzystywaną metodę pomiaru możemy podzielić na optyczne, półprzewodnikowe oraz ultradźwiękowe. Skanery optyczne będące, jednymi z pierwszych stosowanych, wykorzystują zjawisko odbicia światła. Najczęściej obraz zbierany jest z serii jednowymiarowych zestawów danych, których wychwycenie następuje na skutek przeciągnięcia palcem po czujniku. Tworzony przez takie czujniki dwuwymiarowy obraz jest złożeniem tych kawałków, przy wykorzystaniu algorytów rekonstrukcyjnych [5]. Podział skanerów został przedstawiony na rysunku (Rys. 1.1).



Rys. 1.2: Schemat działania czujnika pojemnościowego.

W przypadku budowy macierzowej, które jednocześnie pozwala zebrać całość obrazu, rejestracja sygnału odbywa się przy wykorzystaniu kamer CMOS. Wykorzystanie zjawiska odbicia światła pozwala, na stosunkowo proste, podrobienie odcisku palca. Metoda ta, w wersji podstawowej, nie pozwala wkryć człowieczeństwa badanego obiektu. Nowocześniejsze, droższe wersje czytników pozwalają określić człowieczeństwo dzięki, na przykład pomiaowi natlenowania krwi w naczyniach wieńcowych. Najnowszymi pod względem wykorzystania technologi są czytniki ultradźwiękowe. Wykorzystują one to samo falowe zjawisko co czujniki optyczne. Ich przewagą jest możliwość ukrycia ich pod osłonami. Wykorzystywane jest to w telefonach komórkowych, w których czytniki takie umieszczane są pod ekranem. Dzięki temu są nie widoczne dla oczu, dając możliwość autoryzacji użytkownikowi. Najczęściej stosowanymi z czujników są czujniki półprzewodnikowe. Ich budowa najczęściej sprowadza się do dwuwarstwowej macierzy półprzewodników tworzącymi pewien rodzaj kondensatora. Mierzona jest pojemność tych kondensatorów, która zmienia się jeżeli do wierzchniej strony przyłożony zostanie palec. Do zmiany pojemności konieczny jest żywy palec, lub kopia z odpowiedniego materiału, jest on zatem bezpieczniejszy od czujnika optycznego [5,6]. Schemat działania czujnika linii papilarnych został przedstawiony na rysunku (Rys. 1.2).

2. Projekt

2.1 Rozwiązanie problemu

2.1.1 Wykorzystane technologie

Do stworzenia implementacji modułu autoryzacji dostępu do aplikacji wykorzystano różne technologie. Zostały one wymienione w tabeli (Tab. 2.1).

2.1.2 Widoki modułu

Przygotowany moduł obsługiwany jest przy pomocy trzech widocznych na rysunkach widoków (Rys. 2.2, 2.1, 2.3). Widoki zaprojektowane zostały w Adobe XD, a następnie przygotowane w programie Android Studio.

2.1.3 Utworzone API

2.1.4 Połączenie aplikacji

Moduł logowania połączony został aplikacją *Audiometria*, która umożliwia przeprowadzanie badań audiometrii tonalnej oraz zapisie wyników w pamięci telefonu.
W pierwszej kolejności owy moduł pozwala na zalogowanie do aplikacji przy pomocy odcisku palca. Korzysta on z wewnętrznego magazynu odcisków palca, które dostarcza system Android od wersji API 23. Wersja dostępu do aplikacji poprzez zalogowanie się tradycyjną metodą (login i hasło) zrealizowana jest poprzez połączenie z zewnętrznym dzięki bibliotece *Volley*. Aplikacja może połączyć się z API wystawionym w serwisie *Azure*.

Tab. 2.1: Szczegóły wykorzystanych technologii.

Zakres	**Wykorzystana technologia**
System operacyjny	Android (wersja >= 7.1)
Środowisko programistyczne	Android Studio
Język programowania	Java
Baza danych	SQLite
Technologia autoryzacji	Android Fingerprint API, Biblioteki: Volley, Gson

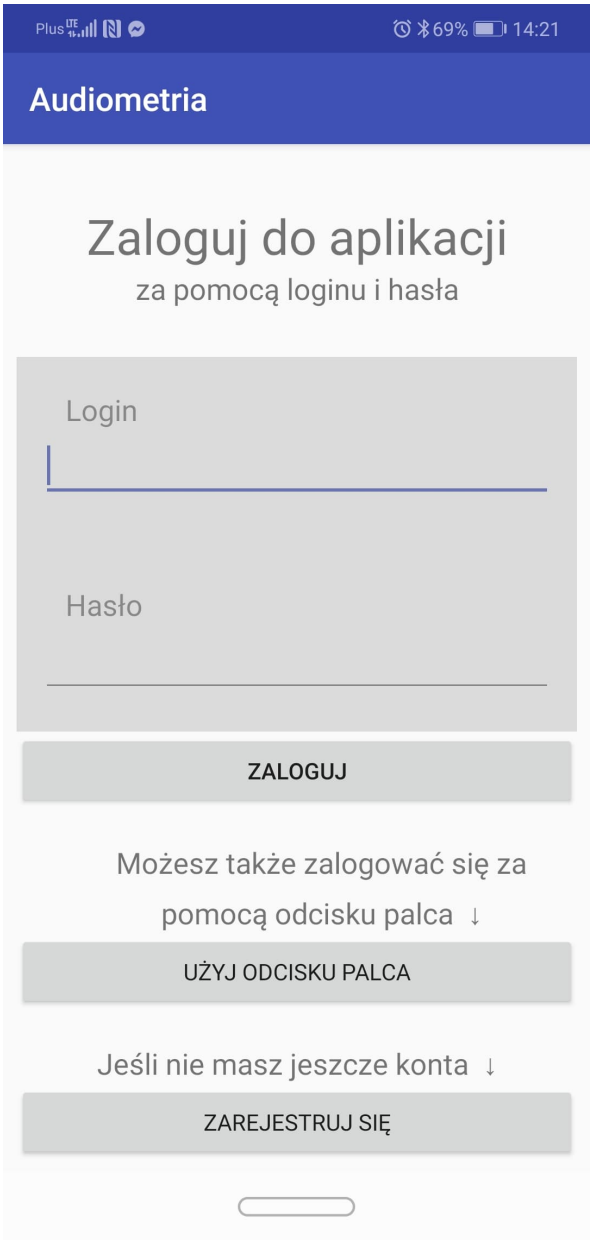
Rys. 2.1: Powitalny widok logowania odciskiem palca.

2.1.5 Użytkowanie

Przygotowany moduł pozwala na logowanie się do zasobów aplikacji za pomocą dwóch metod. Pierwszą z metod jest wykorzystanie do tego celu loginu i hasła. Drugą metodą jest wykorzystanie odcisku palca, który jest zarejestrowany w specjalnie przeznaczonej do tego części pamięci telefonu. O ile logowanie wyłącznie przy pomocy pierwszej metody może funkcjonować samodzielnie, jednak autoryzacja biometryczna wymaga dodatkowego niezależnego rodzaju logowania. Wiąże się to z różnicami cech biometrycznych tej samej osoby w zależności na przykład od otaczającego środowi-

Rys. 2.2: Widok rejestracji.

ska. Ponadto moduł posiada formularz umożliwiający rejestrację nowego użytkownika, wymagającą określenia tylko danych do pierwszego rodzaju autoryzacji. Poszczególne części posiadają osobne, spójne stylistyczne widoki, pomiędzy którymi można się przełączać za pomocą przycisków.



Rys. 2.3: Widok tradycyjnego logowania.

3. Podsumowanie

3.1 Zastosowanie

Przygotowany moduł podłączony został do aplikacji *Audiometria*, która w pełni nie pozwala na wykorzystanie jego potencjału. Autoryzacja przy pomocy dwóch metod może być wykorzystywana przy różnych intencjach. Wiele osób uważa, że wykorzystywanie autoryzacji odciskiem palca jest metodą szybszą i wygodniejszą niż standardowe wpisanie loginu i hasła. Oznacza to, że taki element z powodzeniem sprawdził by się w aplikacjach często włanczanych na krótki okres czasu. Drugą opcją są programy obsługujące dane wrażliwe, które wymagają autoryzacji wykonania pewnych zadań. To takich zaliczamy na przykład aplikacje bankowe. Wykorzystanie do tego odcisku palca utrudnia przechwyt danych autoryzacyjnych przez osoby postronne. Aplikacje takie wymagają zazwyczaj autoryzacji na kilku poziomach (np. Otwarcie aplikacji, dostęp do danych konta, autoryzacja przelewu). Kilkukrotna konieczność wpisania tych samych danych logowania pozwala osobie postronnej zapamiętać dane logowania. Wykorzystanie do tego celu odcisku palca jest szybsze i trudniejsze do odtworzenia. Ponadto odcisk palca działa tylko w przypadku jednego, konkretnego urządzenia, z którym jest sparowany wraz z aplikacją.

3.2 Ograniczenia

Ograniczeniem w korzystaniu przez użytkownika w stworzonym module są wymagania odnośnie hasła. Implementacja nie pozwala na wykorzystanie hasła krótszego niż sześcioznakowe. Ta redukcja elastyczności przy wyborze hasła kierowana jest dbałością o bezpieczeństwo użytkowników. Wykorzystanie platformy Android nie pozwala na użycie innych bibliotek do autoryzacji odciskiem palca niż oficjalne API od Google. Wiąże się to z koniecznością wydobycia danych, z odrębnej części pamięci telefonu, przechowującej dane wrażliwe. Jest to część systemu zabezpieczeń systemu operacyjnego, zatem jest to ograniczenie nałożone dla bezpieczeństwa.

3.3 Wnioski

Stworzony moduł działa poprawni i stanowi warstwę bezpieczeństwa dla aplikacji *Audiometria*. Z powodzeniem mógłby również byc zastosowany w innych rozwiązaniach, np. aplikacjach bankowych lub pracowniczych.

3.4 Literatura

1. www.biometria.pl (dostęp: 1.06.2017)
2. www.wikipedia.pl (dostęp: 1.06.2017)
3. E. Dziuban „Metrologiczne aspekty biometrycznego rozpoznawania osób" PAK 12/2008
4. M. Danch-Wierzchowska „Wykład z przedmiotu Biometria: Odcisk palca" Zabrze 2019
5. X. Xia, L. O'Gorman „ Innovations in fingerprint capture devices" Pergamon 2001
6. M. Sandstrom „Liveness Detection in Fingerprint Recognition Systems" Linkoping 2004