UNIWERSYTET RZESZOWSKI

WYDZIAŁ NAUK ŚCISŁYCH I TECHNICZNYCH

INSTYTUT INFORMATYKI

Oleksii Nawrocki, Tomasz Nowak

oa131400, tn131478

Informatyka

Projekt - BiometricSafe

Sprawozdania

Grupa: 02

Prowadzący

dr Zbigniew Gomółka

Rzeszów 2025

1. Dokumentacja

Streszczenie

Niniejszy dokument opisuje aplikację desktopową stworzoną w języku Python z użyciem biblioteki Tkinter, której celem jest zabezpieczanie plików za pomocą unikalnych cech biometrycznych – odcisku palca użytkownika. System wykorzystuje ekstrakcję punktów charakterystycznych (minucji) i przekształca je na klucz kryptograficzny, umożliwiając szyfrowanie i deszyfrowanie plików.

1.1. Technologie i biblioteki

Projekt został zaimplementowany z użyciem następujących technologii i bibliotek:

- **Python 3.x**
- **Tkinter** – GUI (graficzny interfejs użytkownika)
- **OpenCV** – przetwarzanie obrazu
- **scikit-image** – szkieletowanie obrazu (skeletonization)
- **cryptography (Fernet)** – symetryczne szyfrowanie danych
- **NumPy** – obliczenia numeryczne
- **PIL (Pillow)** – manipulacja obrazami w GUI

1.2. Opis działania

1.2.1. 1. Przetwarzanie obrazu odcisku palca

Obraz wejściowy zostaje przekształcony do skali szarości i przefiltrowany przy użyciu filtra Gaussa. Następnie obraz zostaje zbinarnizowany metodą Otsu i poddany procesowi *skeletonization*, by uprościć strukturę odcisku.

1.2.2. 2. Ekstrakcja punktów minucji

Minucje to punkty charakterystyczne, takie jak zakończenia linii lub bifurkacje. System analizuje sąsiedztwo każdego punktu szkieletu, aby znaleźć potencjalne minucje.

1.2.3. 3. Generowanie klucza szyfrującego

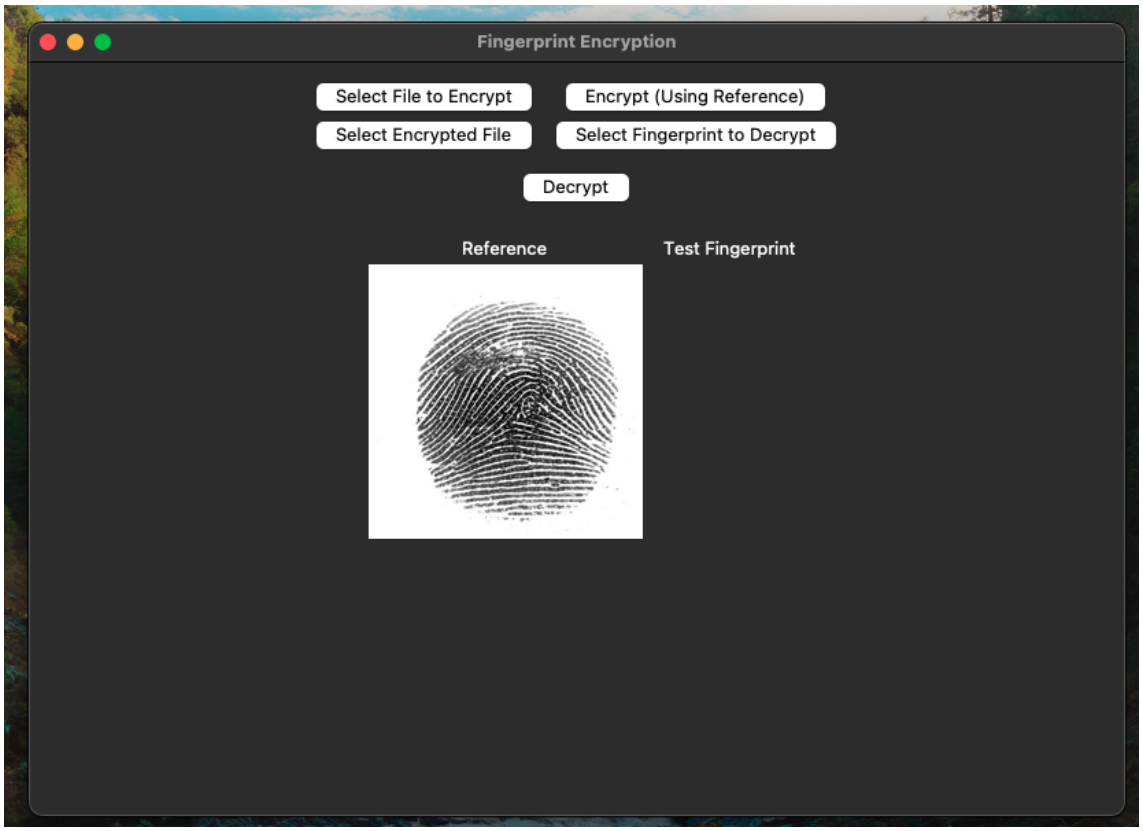
Zestaw punktów minucji jest konwertowany na łańcuch tekstowy i haszowany przy użyciu SHA-256. Na podstawie tego hasza tworzony jest klucz szyfrujący (Fernet), który jest następnie używany do szyfrowania lub odszyfrowywania pliku.

1.2.4. 4. Porównanie odcisków palców

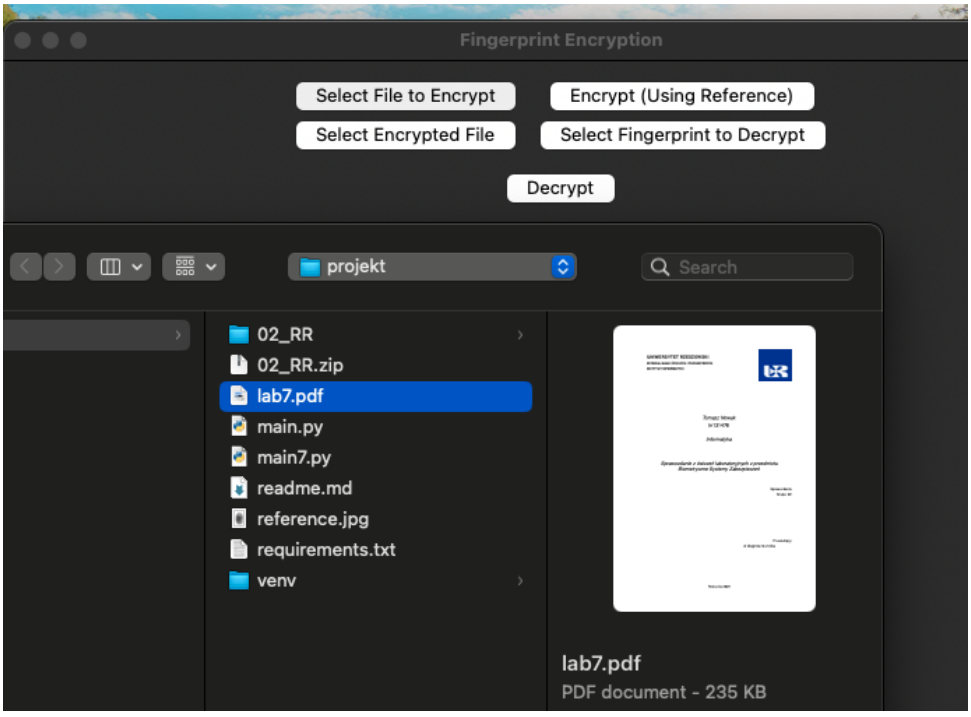
Podczas deszyfrowania system porównuje odcisk referencyjny (z użycia przy szyfrowaniu) z nowym odciskiem dostarczonym przez użytkownika. Miara podobieństwa jest oparta na średniej odległości euklidesowej między punktami.

1.3. Interfejs użytkownika

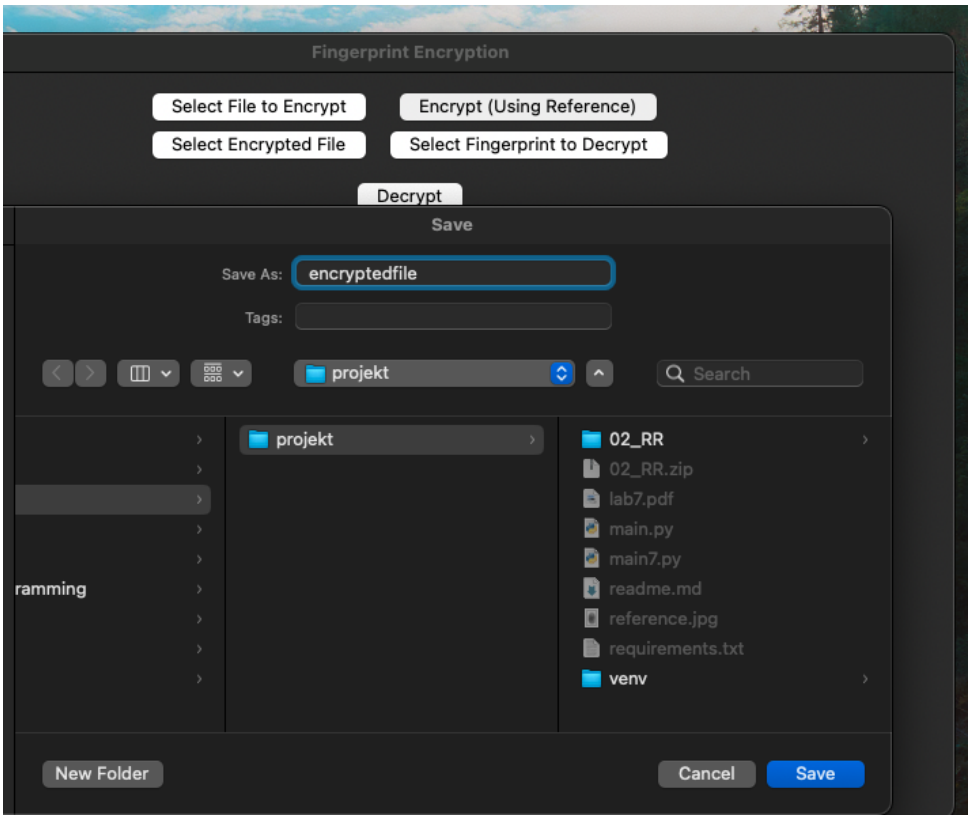
Poniżej przedstawiono główne etapy działania aplikacji w formie zrzutów ekranu:



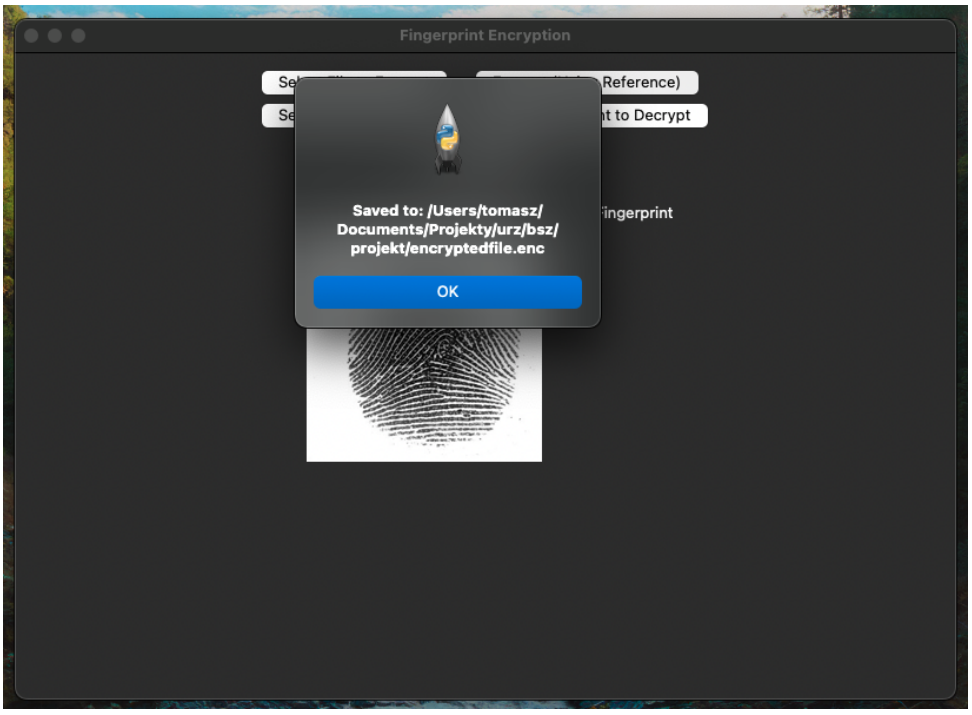
Widok głównego okna aplikacji



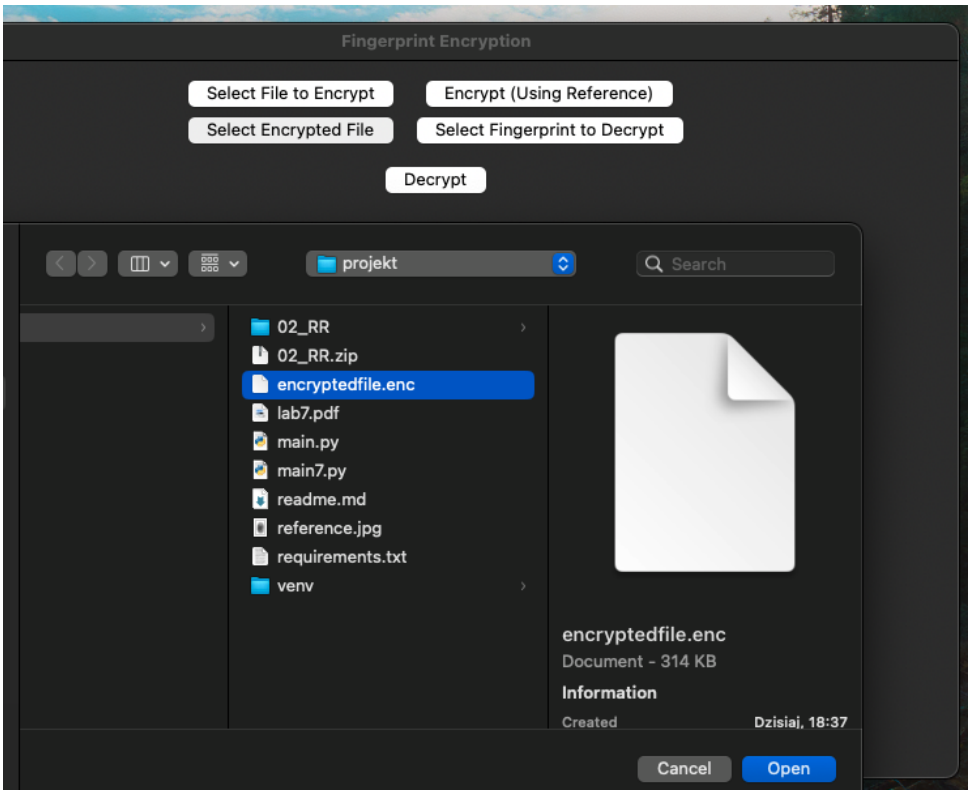
Wybór pliku do zaszyfrowania



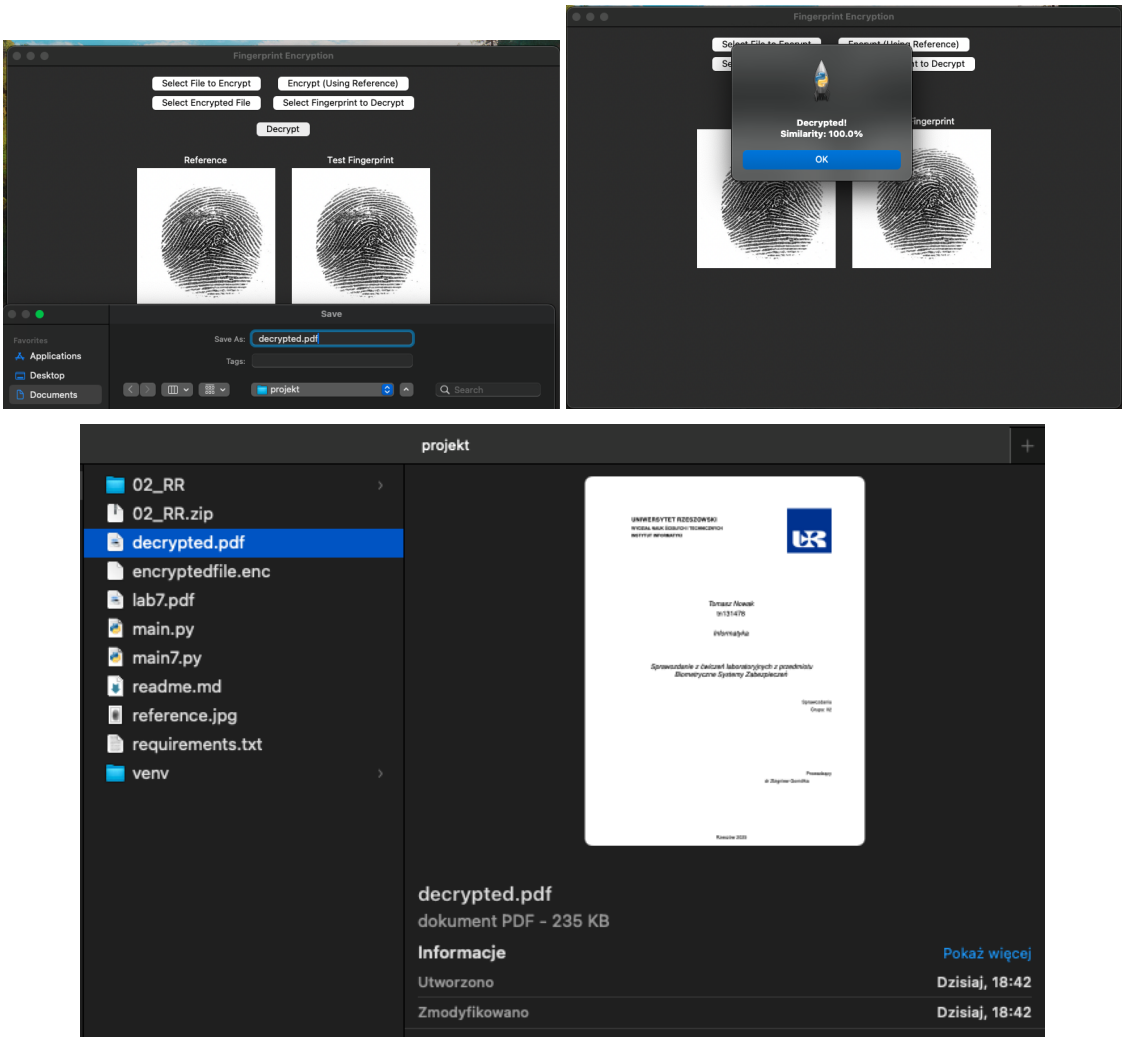
Zapis zaszyfrowanego pliku



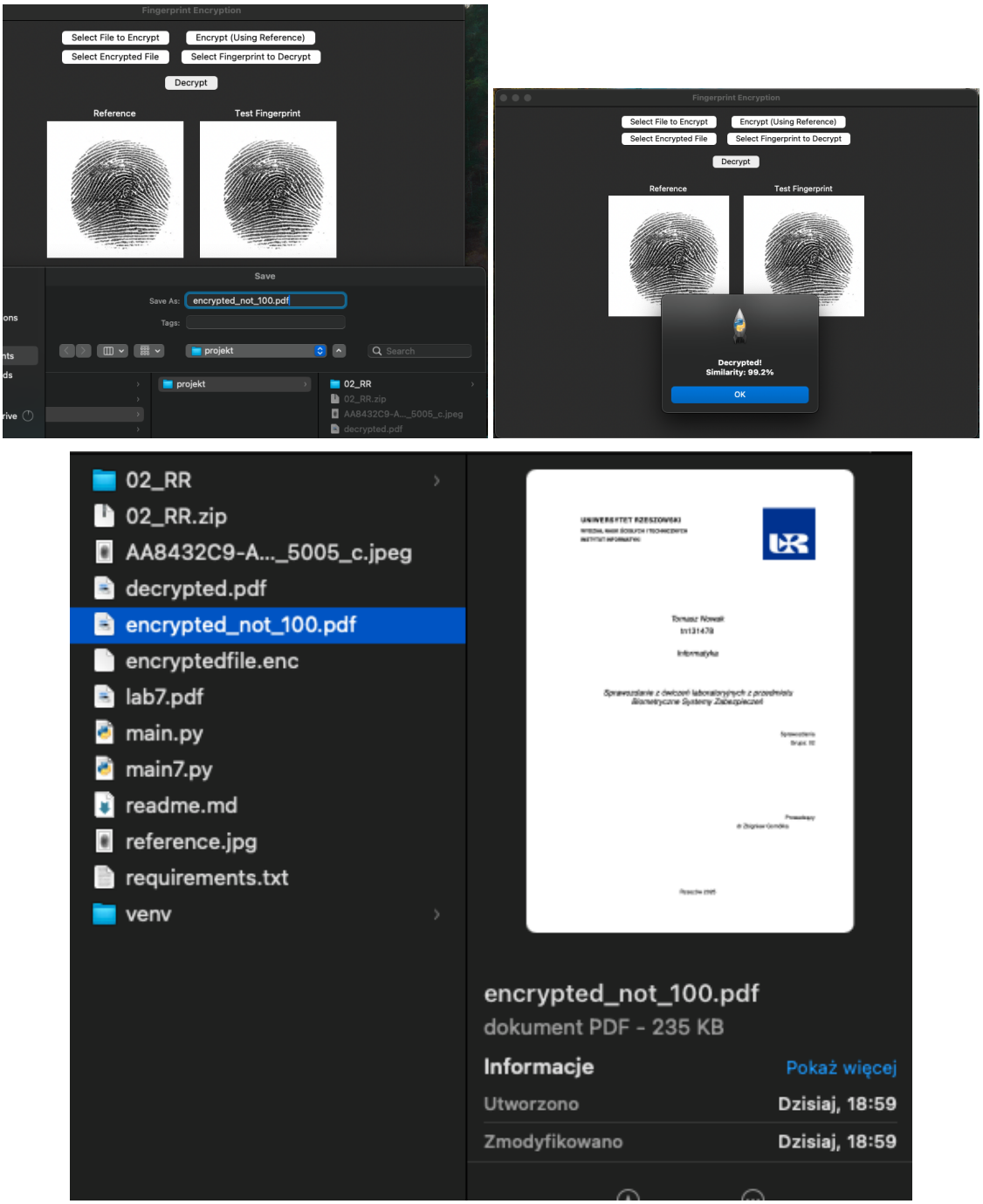
Potwierdzenie zapisu zaszyfrowanego pliku



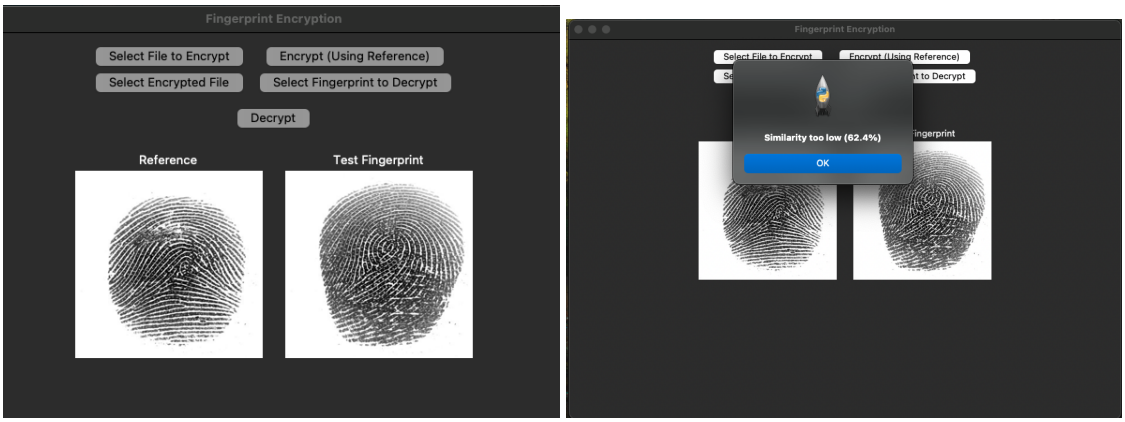
Wybór pliku zaszyfrowanego do deszyfrowania



Deszyfrowanie z poprawnym odciskiem palca



Deszyfrowanie z lekko zmienionym, ale poprawnym obrazem



Próba deszyfrowania z błędnym odciskiem palca

1.4. Instrukcja obsługi

1. Uruchom aplikację.
2. Kliknij „Wybierz plik do zaszyfrowania” i wybierz plik.
3. Kliknij „Szyfruj (używając referencji)” – zostanie użyty obraz `reference.jpg`.
4. Aby odszyfrować, wybierz zaszyfrowany plik oraz nowy obraz odcisku palca.
5. Kliknij „Deszyfruj”. Jeśli odcisk jest zgodny, plik zostanie odszyfrowany.

1.5. Bezpieczeństwo

Bezpieczeństwo aplikacji bazuje na dwóch poziomach:

- Unikalność klucza – generowany z danych biometrycznych.
- Szyfrowanie symetryczne – za pomocą Fernet (AES w trybie CBC z HMAC).

1.6. Zastosowania

- Bezpieczne przechowywanie danych lokalnych.
- Systemy kontroli dostępu.
- Przykład zastosowania biometrii w kryptografii.

Podsumowanie

Aplikacja stanowi prosty, ale skuteczny przykład integracji biometrii i kryptografii w celu ochrony danych. Poprzez użycie cech odcisków palców jako źródła kluczy szyfrujących, system zapewnia wysoki poziom personalizacji i bezpieczeństwa.