Raport z laboratorium 1 – Steganografia

1. **Wstęp**

Celem laboratorium było poznanie metod ukrywania danych w różnych nośnikach multimedialnych oraz analiza skuteczności poszczególnych technik steganograficznych. W ramach ćwiczenia wykorzystano dostępne narzędzia online oraz program S-Tools, aby sprawdzić, jak różne formaty plików wpływają na możliwość ukrywania informacji.

2. **Pobieranie i przygotowanie plików**

Do eksperymentów wybrano pliki multimedialne w następujących formatach:

- **Obrazy:** TIFF, PNG, JPG
- **Dźwięk:** FLAC, WAV, MP3
- **Wideo:** MKV, MP4

Każdy z tych formatów został poddany testom steganograficznym w celu sprawdzenia, jak dobrze ukrywają informacje oraz czy ukryte dane są podatne na zniekształcenia w wyniku kompresji.

3. **Ukrywanie informacji w plikach**

a) Steganografia w plikach graficznych

TIFF

- **Charakterystyka:** Format bezstratny, zachowujący pełne dane obrazu.
- **Zalety:** Możliwość precyzyjnej manipulacji pikselami bez ryzyka kompresji stratnej.
- **Wady:** Duży rozmiar plików.
- **Analiza wyników:** Po ukryciu danych jakość obrazu pozostała bez zmian. TIFF okazał się bardzo skuteczny do steganografii.

PNG

- **Charakterystyka:** Format bezstratnej kompresji, zachowujący wysoką jakość obrazu.
- **Zalety:** Brak strat danych sprawia, że ukryta informacja pozostaje nienaruszona.
- **Wady:** Większy rozmiar niż formaty stratne.
- **Analiza wyników:** Plik PNG dobrze zachowywał ukrytą informację, bez widocznych zmian w obrazie.

JPG

- **Charakterystyka:** Format stratnej kompresji.
- **Zalety:** Mniejszy rozmiar pliku.
- **Wady:** Standardowe metody LSB mogą nie działać poprawnie z powodu kompresji.
- **Analiza wyników:** Nieznaczne artefakty pojawiły się po ukryciu danych, a intensywniejsza kompresja mogła prowadzić do utraty ukrytych informacji.

b) Steganografia w plikach dźwiękowych

FLAC

- **Charakterystyka:** Bezstratny format dźwiękowy.
- **Zalety:** Możliwość ukrywania danych bez pogorszenia jakości dźwięku.
- **Wady:** Większy rozmiar niż MP3.
- **Analiza wyników:** Ukryte dane pozostały nienaruszone, a jakość dźwięku nie uległa zmianie.

WAV

- **Charakterystyka:** Format nieskompresowany.
- **Zalety:** Wysoka skuteczność ukrywania danych.
- **Wady:** Duży rozmiar plików.
- **Analiza wyników:** Metoda LSB była skuteczna, ukryte informacje nie wpływały na jakość dźwięku.

MP3

- **Charakterystyka:** Format stratnej kompresji.
- **Zalety:** Mniejszy rozmiar plików.
- **Wady:** Kompresja może uszkodzić ukryte dane.
- **Analiza wyników:** Ukryte dane mogły ulec degradacji, skuteczność steganografii była niższa niż w plikach bezstratnych.

c) Steganografia w plikach wideo

MKV

- **Charakterystyka:** Kontener obsługujący wiele formatów kodowania.
- **Zalety:** Możliwość ukrywania danych w wielu warstwach (np. napisy, dźwięk, obraz).
- **Wady:** Duży rozmiar plików.
- **Analiza wyników:** Ukrywanie informacji w klatkach wideo było skuteczne, a zmiany niewidoczne dla ludzkiego oka.

MP4

- **Charakterystyka:** Format stratnej kompresji.
- **Zalety:** Powszechne stosowanie, mniejsze rozmiary plików.
- **Wady:** Kompresja może wpływać na ukryte informacje.
- **Analiza wyników:** Po ukryciu danych mogły pojawić się niewielkie artefakty w obszarach o niskiej szczegółowości.

d) Odzyskiwanie ukrytych informacji

Po utworzeniu steganogramów przeprowadzono ich ekstrakcję przy użyciu tych samych narzędzi. W formatach bezstratnych odzyskiwanie było w 100% skuteczne. W formatach stratnych (MP3, JPG, MP4) część informacji mogła ulec uszkodzeniu w wyniku kompresji.

Wnioski

1. **Bezstratne formaty** (TIFF, PNG, FLAC, WAV) są najlepsze do steganografii, ponieważ nie zmieniają ukrytych danych.
2. **Stratne formaty** (JPG, MP3, MP4) mogą powodować utratę informacji, co wpływa na skuteczność steganografii.
3. **Pliki wideo** oferują dużą pojemność do ukrywania danych, ale wymagają zaawansowanych technik, aby uniknąć degradacji informacji.
4. **Platformy online** ułatwiają steganografię, ale wybór odpowiedniego formatu jest kluczowy dla sukcesu.

4. Porównanie obrazów

Przed ukryciem

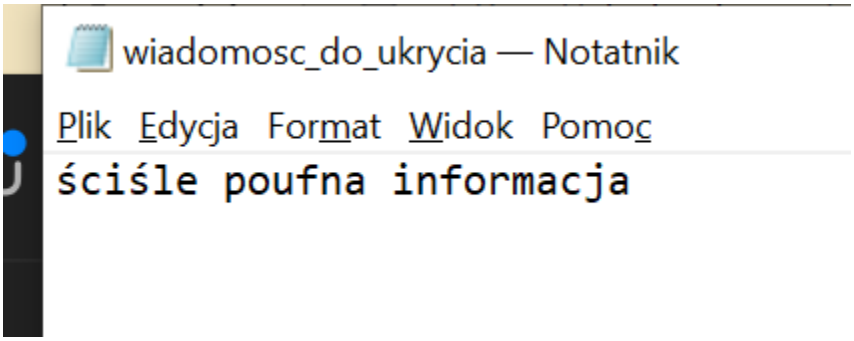
Po ukryciu teskt png:: "Widok piękny, ale sekrety jeszcze piękniejsze".

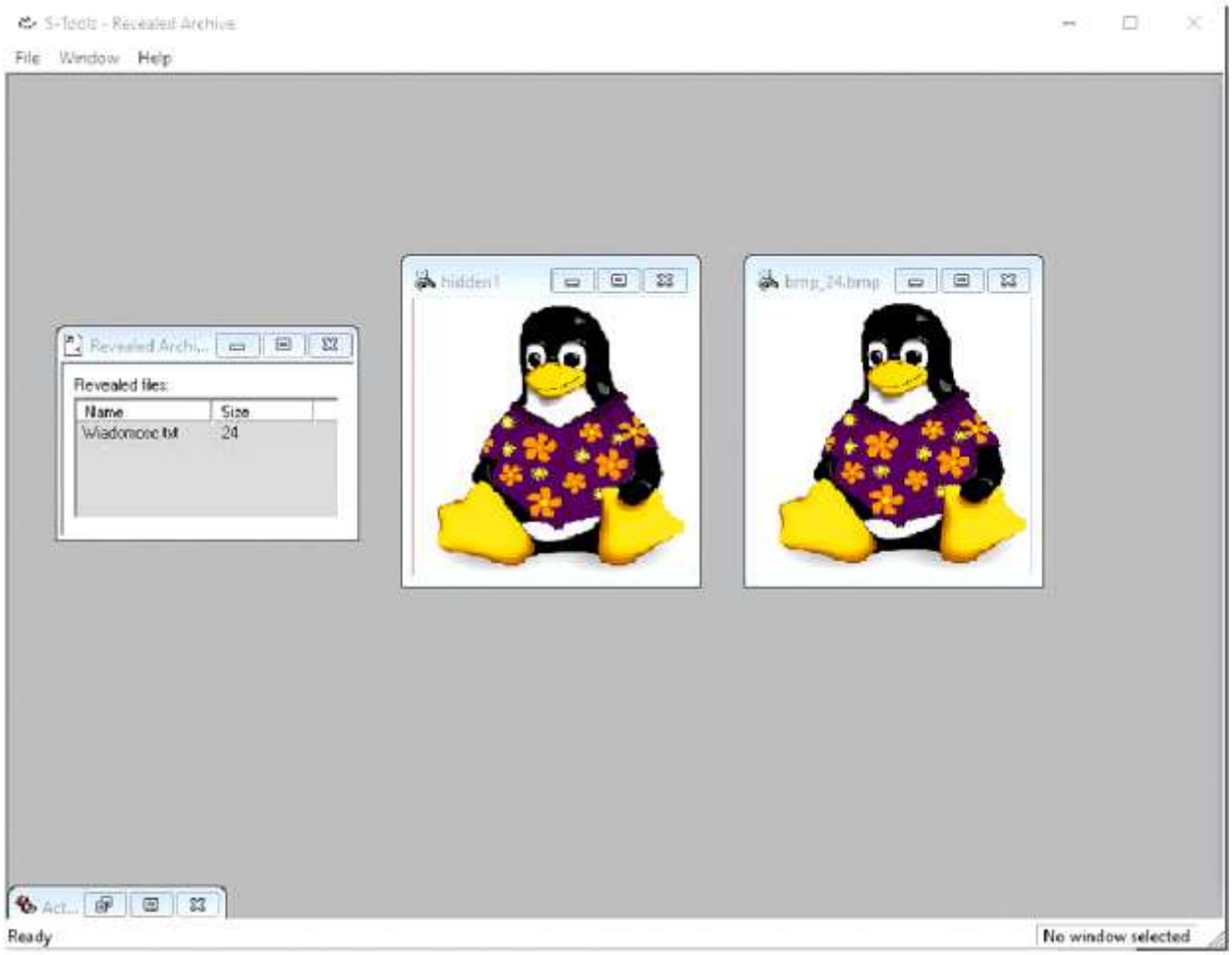
Przed jpg

Jpg po ukryciu wiadomości „Chmury kryją więcej, niż myślisz.”

S-Tools

S-Tools Korzystając z narzędzia S-Tools, zgodnie z instrukcją w zadaniu, osadziłem plik tekstowy o nazwie sekret.txt w obrazie BMP. Po zakończeniu procesu steganograficznego, obraz nie wykazywał żadnych widocznych zmian. Następnie, używając tego samego narzędzia, pomyślnie odszyfrowałem ukrytą wiadomość, której treść brzmiała: "ściśle poufna informacja".





5. **Odzyskiwanie ukrytych danych Po wygenerowaniu plików steganograficznych przeprowadzono proces odzyskiwania zaszyfrowanych informacji. Do ekstrakcji danych użyto tych samych narzędzi, które posłużyły do ich ukrycia:**

• Dźwięk (WAV, MP3):

Pliki WAV, jako formaty nieskompresowane, umożliwiały łatwe i dokładne odzyskanie ukrytej informacji. W plikach MP3 proces ten był bardziej wymagający – choć dane udało się odczytać, kompresja wpłynęła na ich integralność, co mogło osłabić skuteczność steganografii.

• Wideo (MP4):

W przypadku plików MP4 odzyskanie ukrytych treści było możliwe, ale ze względu na ich dużą objętość oraz złożony sposób kodowania wymagało więcej czasu i precyzji.

• Obrazy (JPEG, PNG):

Proces wydobywania informacji był szybki i bezproblemowy. Pliki PNG, dzięki swojej bezstratnej kompresji, pozwalały na precyzyjne odzyskanie ukrytych danych bez utraty jakości. W przypadku JPEG, ze względu na kompresję stratną, konieczna była dokładniejsza analiza, ponieważ część danych mogła ulec zniekształceniu.

6. **Wybór najlepszych nośników Podczas analizy różnych formatów stosowanych w steganografii najskuteczniejsze okazały się:**

• Obrazy PNG i BMP:

Dzięki bezstratnej kompresji ukryte dane pozostawały nienaruszone i trudne do wykrycia. W przeciwieństwie do nich, format JPEG, choć powszechnie stosowany, powodował drobne artefakty wynikające z kompresji stratnej, co mogło wpłynąć na czytelność ukrytych informacji.

• Pliki WAV:

Z uwagi na brak kompresji, format WAV zapewniał najwyższą skuteczność w ukrywaniu informacji w plikach dźwiękowych. MP3, mimo swojej popularności, nie był tak niezawodny, ponieważ algorytmy kompresji mogły usuwać lub modyfikować ukryte dane.

• Pliki wideo MP4:

Mimo że formaty wideo oferowały dużą pojemność na ukryte informacje, proces kompresji mógł prowadzić do powstawania artefaktów, co utrudniało skuteczne

przechowywanie danych. Dlatego MP4 okazał się mniej efektywny w porównaniu do formatów graficznych i dźwiękowych.

7. **Wnioski**

   • Format PNG, WAV oraz BMP najlepiej sprawdzają się w steganografii, gdyż ich struktura umożliwia ukrycie danych bez widocznych zmian jakościowych.

   • Format JPEG, MP3 i MP4, ze względu na stosowaną kompresję stratną, mogą prowadzić do degradacji zaszyfrowanych informacji, co zwiększa ryzyko ich wykrycia.

   • Platformy online ułatwiają proces steganografii, jednak należy zwracać uwagę na wybór odpowiedniego formatu, by zapewnić jak największą skuteczność ukrywania informacji.

8. **Podsumowanie analizy:**

   Każdy z testowanych formatów plików wykazał różny poziom skuteczności w zakresie steganografii. Pliki BMP, PNG oraz WAV wyróżniały się wysoką jakością i dużą odpornością na utratę danych, co czyniło je najbardziej niezawodnymi nośnikami. Natomiast formaty JPG, MP3 oraz MP4 były bardziej podatne na zniekształcenia wynikające z procesu kompresji, co mogło negatywnie wpłynąć na skuteczność przechowywania ukrytych informacji.