Cel ćwiczenia laboratoryjnego: ukrywanie informacji w plikach graficznych - implementacja wybranego prostego algorytmu steganograficznego – algorytmu najmniej znaczącego bitu lub algorytmu patchwork.
Materiały do laboratorium: materiały z wykładu oraz materiały dodatkowe podane przez prowadzącego.

Zadanie: Zaimplementować jeden z wybranych algorytmów (lub jego modyfikacji).

Algorytm najmniej znaczącego bitu polega na zmianie najmniej znaczącego bitu słowa opisującego dany piksel, przy czym wynik zależy ściśle od liczby bitów przeznaczonych do opisu pojedynczego piksela.

Przykład:

Litera C może zostać ukryta w 3 pikselach. Oryginalny zapis danych dla trzech pikseli w 24-bitowym kolorze mógłby wyglądać następująco:

PIKSEL	KOLORY		
	R	G	B
1	00101011	11001101	00011000
2	10101011	10001100	00101001
3	00011100	11100111	01011010

Niech $C = 43_H = 01000011_2$

Chcąc osadzić literę C w obrazie, przeznaczając po jednym bicie każdego koloru, otrzymamy następujące wartości oryginalnych pikseli:

PIKSEL	KOLORY		
	R	G	B
1	0010101**0**	1100110**1**	0001100**0**
2	1010101**0**	1000110**0**	0010100**0**
3	0001110**1**	1110011**1**	0101101**0**

Pytania:

1. Czy taki sposób ukrywania informacji w obrazie jest odporny na ataki i próby zniszczenia osadzonej wiadomości.
2. Zaproponuj ataki na osadzoną wiadomość.
3. Jaki jest rozmiar wiadomości którą możemy ukryć w obrazie/pliku graficznym?

Algorytm Patchwork:

- Polega na osadzeniu w chronionym obrazie informacji pseudolosowej
- Wymaga stosowania generatora liczb pseudolosowych uruchamianego za pomocą tajnego klucza

Jeśli:
a_i – to jasność obrazu w punkcie A_i
b_i – to jasność obrazu w punkcie B_i

To niech: $S_n = \sum_{i=1}^{n}(a_i - b_i)$

1. **Algorytm osadzania znaku wodnego**

Wejście: obraz, tajny klucz generatora pseudolosowego, liczba naturalna n
Wyjście: obraz z osadzonym znakiem wodnym
Metoda:
Dla i=1 do n wykonaj:

- Za pomocą generatora wybierz dwa obszary (piksele) obrazu A_i i B_i
- Zwiększ jasność punktów/u obszaru A_i o zadaną wartość δ
- Zmniejsz jasność punktów/u obszaru B_i o zadaną wartość δ

Wartość δ zależy od głębi kolorów obrazu.
Po osadzeniu znaku wodnego obliczamy:

$$S'_n = \sum_{i=1}^{n}\big((a_i + \delta) - (b_i - \delta)\big) = 2\delta n + \sum_{i=1}^{n}(a_i - b_i)$$

2. **Algorytm detekcji znaku wodnego**

Wejście: obraz, tajny klucz generatora pseudolosowego, liczba naturalna n
Wyjście: wynik detekcji pozytywny/negatywny
Metoda:
Dla i=1 do n wykonaj:

- Za pomocą generatora wybierz dwa obszary (piksele) obrazu A_i i B_i
- **Zmniejsz** jasność punktów/u obszaru A_i o zadaną wartość δ
- **Zwiększ** jasność punktów/u obszaru B_i o zadaną wartość δ

Dekodując zmodyfikowany obraz otrzymamy:

$$S'_n = \sum_{i=1}^{n}\big((a_i + \delta - \delta) - (b_i - \delta + \delta)\big) = \sum_{i=1}^{n}(a_i - b_i)$$

Jeśli na skutek modyfikacji obrazu otrzymamy przesunięcie zmiennej S_n to oznacza, że obraz został zmodyfikowany w sposób nieuprawniony (znak wodny się nie zgadza).

Zadanie:
Przeanalizuj skuteczność i odporność na ataki tej metody osadzania znaku wodnego.