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 obrazu dla trzech pikseli w 24bitowym kolorze mógłby wyglądać następująco:

Piksel	Kolory		
	R	G	B
1	0010 1011	1100 1101	0001 1000
2	1010 1011	1000 1100	0010 1001
3	0001 1100	1110 0111	0101 1010

Zakodujmy C jako $43_H = 0100\ 0011_2$

Po osadzeniu litery w danych obrazu, przeznaczając po jednym bicie w kodzie każdego koloru poszczególnych pikseli na osadzenie informacji o literze, otrzymuje się następujące wartości kolorów poszczególnych pikseli.

Piksel	Kolory		
	R	G	B
1	0010 1010	1100 1101	0001 1000
2	1010 1010	1000 1100	0010 1000
3	0001 1101	1110 0111	0101 1010

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 osadzaniu w chronionym obrazie informacji pseudolosowej
- wymaga stosowania generatora liczb pseudolosowych uruchamianego za pomocą tajnego klucza

Niech:
a_i –jasność obrazu w punkcie A_i
b_i – jasność obrazu w punkcie B_i

Przyjmujemy, że: $S_n = \sum_{i=1}^{n}(a_i - b_i)$

Algorytm osadzania znaku wodnego

Wejście: obraz, tajny klucz k generatora pseudolosowego, liczba naturalna n

Wyjście: obraz z osadzonym znakiem wodnym

Metoda:

Dla i = 1 do n wykonaj:

- za pomocą generatora pseudolosowego z kluczem k wybierz dwa obszary obrazu A_i oraz B_i
- **zwiększ** jasność punktów obszaru A_i o zadaną wartość δ
- **zmniejsz** jasność punktów obszaru B_i o zadaną wartość δ

Wartość δ zależy od głębi kolorów obrazu, tj. od liczby bitów przeznaczonych do opisu pojedynczego piksela.

Po osadzeniu znaku wodnego obliczamy:

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

Algorytm detekcji znaku wodnego

Wejście: obraz, tajny klucz k generatora pseudolosowego, liczba naturalna n

Wyjście: wynik detekcji pozytywny/negatywny

Metoda:

Dla $i = 1$ do n wykonaj:

- za pomocą generatora pseudolosowego z kluczem k wybierz dwa obszary obrazu A_i oraz B_i
- **zmniejsz** jasność punktów obszaru A_i o zadaną wartość δ
- **zwiększ** jasność punktów obszaru B_i o zadaną wartość δ

Dekodując zmodyfikowany obraz obliczamy:

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

Jeżeli w skutek modyfikacji obrazu uzyskalibyśmy przesunięcie zmiennej S_n to oznaczałoby, że obraz został zmodyfikowany w sposób nieuprawniony.

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