Laboratorium nr 2: *Algorytm LSB dla plików BMP – część 1*

Zalecany język programowania: C#

Zadanie:

Należy napisać program implementujący algorytm LSB dla zdjęć BMP. Program ma ukrywać informacje w następujący sposób:

Dane do ukrycia -> **szyfrowanie -> kodowanie za pomocą parzystości -> zakodowanie w subpikselach** -> Dane ukryte

Szczegółowe wymagania są następujące:

- Interfejs:
  - Program ma posiadać graficzny interfejs użytkownika;
  - Interfejs ma składać się minimalnie z:
    - 2 „*picture box*" , w których będą wyświetlane zdjęcie przed i po modyfikacji;
    - 4 przycisków (wczytaj plik, wstaw, odczytaj ukrytą informacje, zapisz zmodyfikowany plik);
    - pola tekstowego umożliwiającego wpisywanie tekstu do osadzenia;
    - 2 pól do wprowadzania haseł (1 do szyfrowania i 1 do klucza steganograficznego –do użycia w następnym zadaniu).
- Ukrywany tekst należy osadzić w najmniej znaczących bitach pierwszych *n* pikseli (tj. wiersz po wierszu, od lewej do prawej, od góry do dołu). Proszę pamiętać, że każdy piksel składa się z trzech subpikseli, a więc każdy piksel posiada 3 najmniej znaczące bity w każdym z trzech subpikseli.
- W pierwszych kilku bitach ukrywanego tekstu umieszczamy informacje o długości osadzanego tekstu, a w następnych sam tekst.
- Szyfrowanie (oraz deszyfrowanie):
  - Należy zaszyfrować ukrywany tekst za pomocą algorytmu AES, hasło w postaci ciągu tekstowego należy zamienić na tablicę bajtów służącą jako klucz z użyciem funkcji skrótu SHA512. Operacja szyfrowania ma na celu ukrycie struktury ukrywanego tekstu i upodobnienie go do białego szumu.
- Kodowanie (oraz dekodowanie) za pomocą parzystości:
  - Zamiast prostej podmiany najmniej znaczącego bita w każdym subpikselu, informację ukrywamy z wykorzystaniem mechanizmu parzystości w następujący sposób: chcemy osadzić bity x_1 i x_2 w lokalizacjach LSB a_1, a_2 i a_3, to postępujemy w następujący sposób:

$$x_1 = a_1 \oplus a_3,\ x_2 = a_2 \oplus a_3 \Rightarrow \text{change nothing}$$
$$x_1 \neq a_1 \oplus a_3,\ x_2 = a_2 \oplus a_3 \Rightarrow \text{change } a_1$$
$$x_1 = a_1 \oplus a_3,\ x_2 \neq a_2 \oplus a_3 \Rightarrow \text{change } a_2$$
$$x_1 \neq a_1 \oplus a_3,\ x_2 \neq a_2 \oplus a_3 \Rightarrow \text{change } a_3.$$