НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Інститут прикладного системного аналізу  
Кафедра системного проектування

Лабораторна робота №5  
з дисципліни “**Безпека інформаційних систем**”  
на тему: “Дослідження стеганографічних методів приховування даних”

Виконав:  
студент групи ДА-82  
факультету “ІПСА”  
Муравльов А. Д.  
Варіант 18

Київ — 2021

# **Мета роботи**

Дослідити стеганографічні методи приховування даних та їх реалізація.

# **Завдання роботи**

1. Обрати варіант текстового файлу (див. Додаток до лабораторної роботи № 1) згідно з порядковим номером студента в списку академічної групи.
2. Вибрати підходящий контейнер у вигляді файлу зображення в форматі bmp для приховування текстового файлу і за допомогою програми S-Tools 4.0 виконати приховування файлу, використовуючи один з доступних алгоритмів шифрування. Вилучити файли з контейнера і порівняти їх з оригіналом. Зберегти отримані результати.
3. За допомогою засобів пакету CrypTool виконати статистичний аналіз порожнього контейнера і контейнера з прихованими даними. Для цього знайти ентропії контейнерів і гістограми контейнерів. Порівняти отримані дані, результати зберегти.
4. Для обраного при виконанні п. 2 контейнера розрахувати допустимий обсяг приховуваних даних за методом LSB і порівняти його з можливостями програми S-Tools 4.0.
5. Обрати підходящий контейнер у вигляді звукового файлу. Виконати приховування файлу, використовуючи один з доступних алгоритмів шифрування. Вилучити файли з контейнера і порівняти їх з оригіналом. Виконати статистичний аналіз порожнього контейнера і контейнера з прихованими даними. Для цього знайти ентропії контейнерів і гістограми контейнерів.
6. Написати програму для приховування (і вилучення) даних в файлах напівтонових (у відтінках сірого) зображень за методом LSB (без шифрування) з вісьма біт на один піксель, налагодити її і перевірити працездатність на заданому текстовому файлі.
7. За допомогою засобів пакету CrypTool виконати статистичний аналіз порожнього контейнера і контейнера з прихованими даними, отриманого за допомогою розробленої програми. Для цього знайти ентропії контейнерів і гістограми контейнерів. Порівняти отримані дані, результати зберегти. Зробити висновки про можливість використання гістограмного аналізу для виявлення прихованих даних.
8. Оформити звіт по роботі.

# **Хід роботи**

# **1. Приховування файлу за допомогою програмного забезпечення**

Вибрати підходящий контейнер у вигляді файлу зображення в форматі bmp для приховування текстового файлу і за допомогою програми S-Tools 4.0 виконати приховування файлу, використовуючи один з доступних алгоритмів шифрування. Вилучити файли з контейнера і порівняти їх з оригіналом. Зберегти отримані результати.

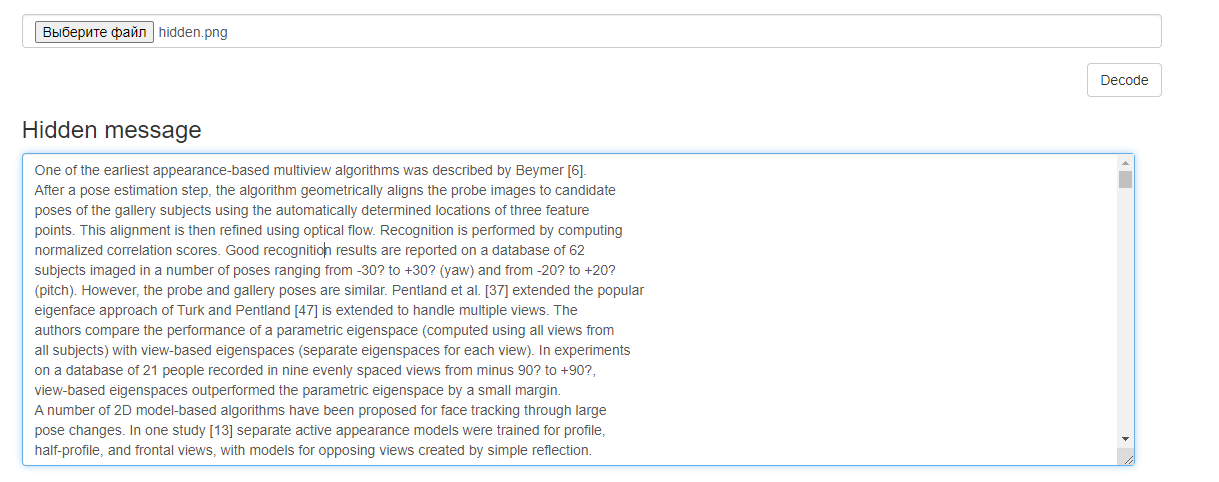
Скористатись програмою S-Tools не вдалося – програма видавала повідомлення Out of memory при спробі приховати текст в картинці, тому скористаємось [сайтом](https://stylesuxx.github.io/steganography), який надає схожий функціонал.



Оригінал (порожній контейнер)



Контейнер з прихованим текстом



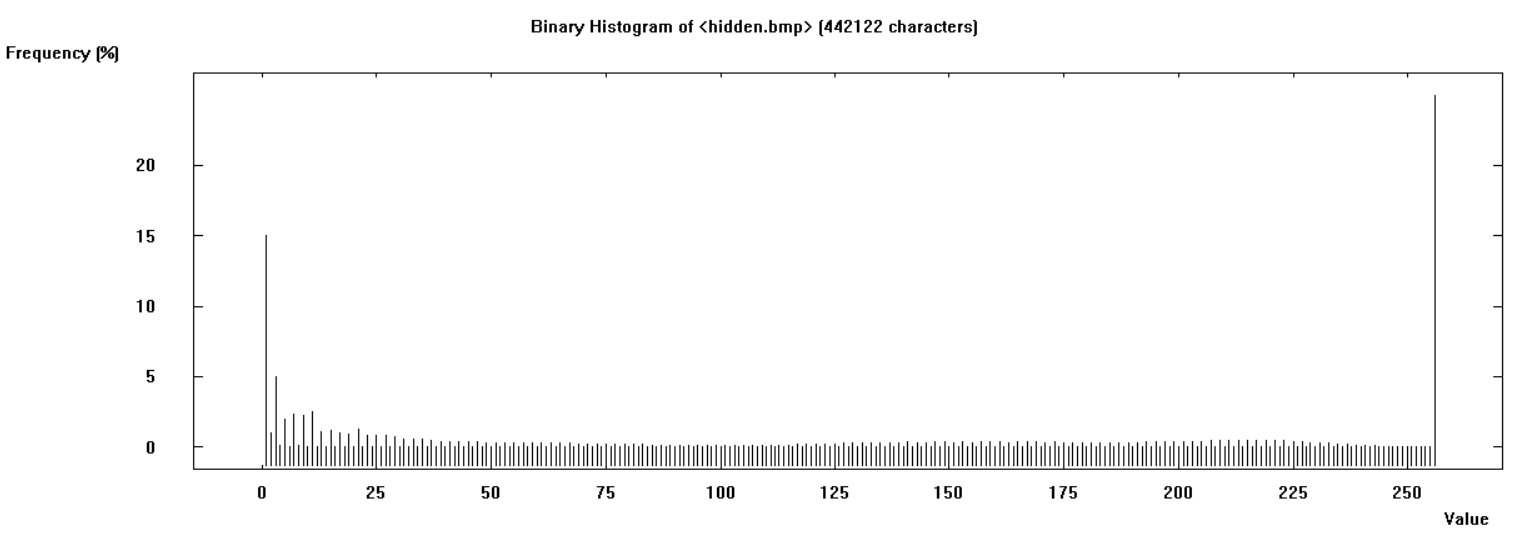
Результат декодування

# **2. Статистичний аналіз у CrypTool**

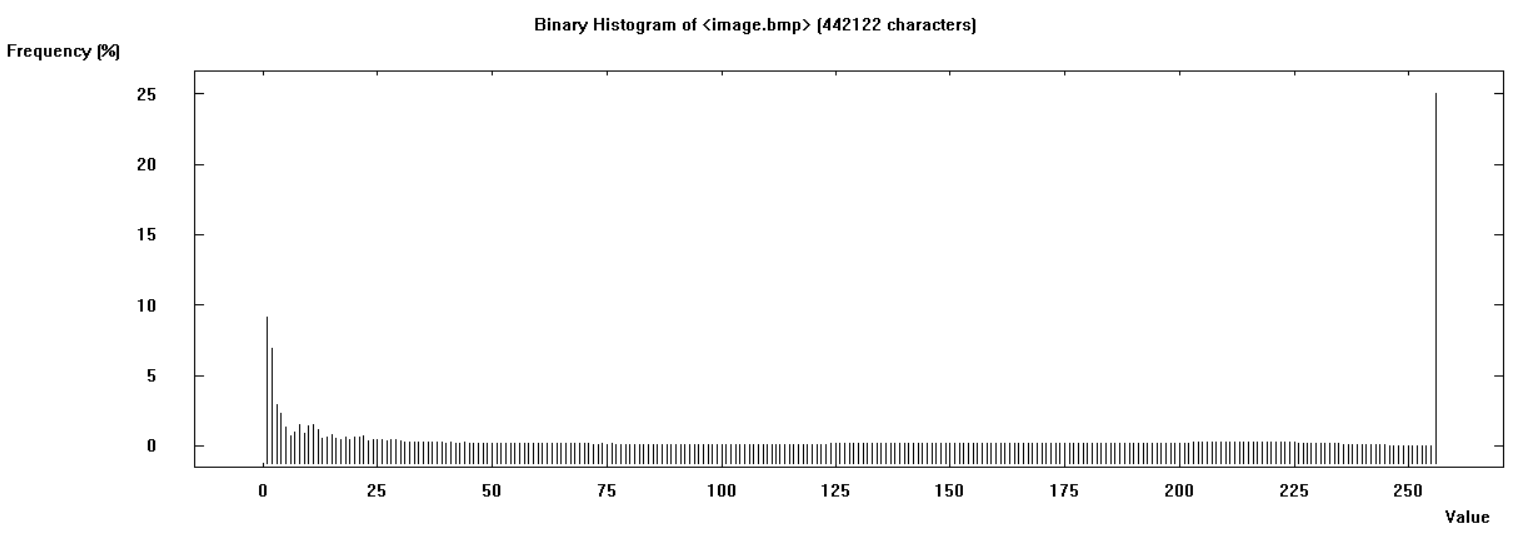
За допомогою засобів пакету CrypTool виконати статистичний аналіз порожнього контейнера і контейнера з прихованими даними. Для цього знайти ентропії контейнерів і гістограми контейнерів. Порівняти отримані дані, результати зберегти.

Ентропія

|  |  |
| --- | --- |
| Порожній контейнер | Контейнер з прихованим текстом |
| 5.23 | 3.86 |



Гістограма контейнера з прихованим текстом



Гістограма порожнього контейнера

# **3. Підрахунок допустимого обсягу приховуваних даних**

Для обраного при виконанні п. 2 контейнера розрахувати допустимий обсяг приховуваних даних за методом LSB і порівняти його з можливостями програми S-Tools 4.0.

Обрали контейнер розміром 325 х 340 пікселів. Зображення кольорове, тому кількість байт в зображенні 325 x 340 x 3 = 331500.

В залежності від того, яку кількість молодших бітів будемо змінювати, буде змінюватись розмір інформації, яку хочемо зашифрувати.

Так, якщо вирішуємо змінювати лише один молодший біт, то максимальний розмір приховуваних даних буде становити 975360 / 8 = 41438 байт.

Аналогічним чином розраховується обсяг для випадків, коли кількість змінюваних молодших бітів зростає.