

ВСТУП ДО СТИГОНОГРАФІЇ

Лабораторна робота

Мета: Дослідити можливість «приховування» даних у зображеннях

Індивідуальне завдання:

- Навести реалізацію технології Rar-Jpeg, та продемонструвати її роботу.
- Виконати скриття даних у зображення за допомогою методу найменш значимих бітів (Less Significant Bits)
- Виконати аналіз скриття даних за допомогою методу стегоаналізу "атака хі квадрат"

ХІД РОБОТИ

RARJPEG - особливий вид файлового контейнера: ілюстрація JPEG, до якої встик (в той же файл) дописаний архів RAR. Залежно від розширення такий файл може сприйматися різними програмами і як ілюстрація JPEG, і як архів RAR. Ця обставина дозволяє, наприклад, використовувати іміджборди (що приймають тільки ілюстрації) в якості анонімних файлових хостингів для архівів.

Лістинг функції, що демонструє rar-jpeg технологію:

```
public void RarJpeg(string containerFilePath, string archivePath, string
outputFilePath){
    byte[] containerBytes = File.ReadAllBytes(Paths.get(containerFilePath));
    byte[] archiveBytes = File.ReadAllBytes(Paths.get(archivePath));
    byte[] outputBytes = new byte[containerBytes.Length + archiveBytes.Length];
    System.arraycopy(containerBytes, 0, outputBytes, 0,
containerBytes.Length);
    System.arraycopy(archiveBytes, 0, outputBytes, containerBytes.Length,
archiveBytes.Length);

    FileUtils.writeByteArrayToFile(new File(outputFilePath), outputBytes);
}
```

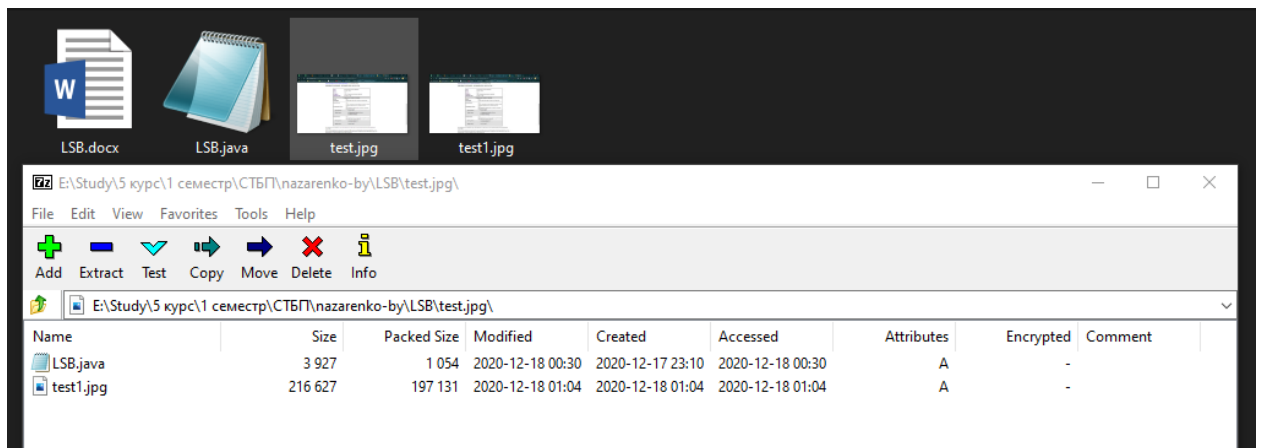


Рисунок 1 – Результат технології rar-jpeg

Суть методу полягає в наступному: ми замінюємо молодші біти в байтах, які відповідають за кодування кольору. Припустимо, якщо черговий байт нашого секретного повідомлення - 11001011, а байти в зображенні - ... 11101100 01001110 01111100 0101100111 ..., то кодування буде виглядати так. Ми розіб'ємо байт секретного повідомлення на 4 двохбітові частини: 11, 00, 10, 11, і замінимо отриманими фрагментами молодші біти зображення: ... 11101111 01001100 01111110 0101100111 Така заміна в загальному випадку не помітна для людського ока. Більш того, багато старі пристрої виведення, навіть не зможуть відобразити такі незначні зміни.

Лістинг функції, що демонструє скриття даних методом lsb:

```
public static void Encode(String mess, String srcname) throws IOException {
    String bin = messtobin(mess) + "00000000";
    File f = new File(srcname + ".png");
    BufferedImage bufferedImage = ImageIO.read(f);

    ByteArrayOutputStream bos = new ByteArrayOutputStream();
    ImageIO.write(bufferedImage, "png", bos);
    byte[] arr = bos.toByteArray();

    int data = HEADER_SIZE;
    char temp;
    int x = 0;
    if (bin.length() > (arr.length - HEADER_SIZE)) {
        System.out.println("message too large for image to hide!");
    }
}
```

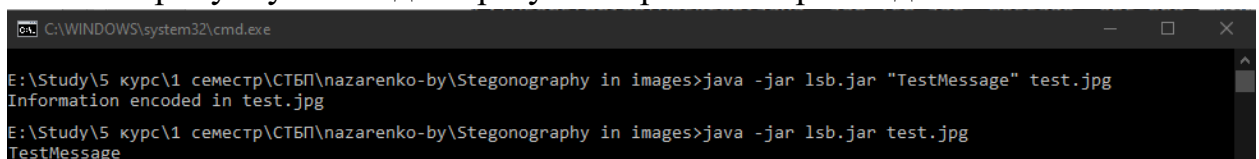
```

    } else {
        for (int i = 0; i < bin.length(); i++) {
            arr[data] >>= 1;
            arr[data] <<= 1;
            arr[data] += (bin.charAt(i) - 48); //
            data++;
        }
    }

    File output = new File(srcname + ".png");
    bufferedImage = ImageIO.read(new ByteArrayInputStream(arr));
    if (ImageIO.write(bufferedImage, "png", output)) {
        System.out.println("Information encoded in" + srcname);
    }
}

```

На рисунку 2 наведено результат роботи скриття даних.



```

C:\WINDOWS\system32\cmd.exe
E:\Study\5 курс\1 семестр\СТБП\nazarenko-by\Stegonography in images>java -jar lsb.jar "TestMessage" test.jpg
Information encoded in test.jpg
E:\Study\5 курс\1 семестр\СТБП\nazarenko-by\Stegonography in images>java -jar lsb.jar test.jpg
TestMessage

```

Рисунок 2 – Результат скриття даних за допомогою метода lsb

Для аналізу скриття даних може використовуватися атака «Хі-квадрат». Атака «Хі-квадрат» ґрунтується на тому припущенні, що ймовірність одночасної появи сусідніх (відмінних на найменш значущий біт) кольорів (pair of values) в незаповненому стегоконтейнері вкрай мала. Це дійсно так, можеш перевірити. Якщо говорити іншими словами, то кількість пікселів двох сусідніх кольорів істотно відрізняється для порожнього контейнера. Все, що нам потрібно зробити, це порахувати кількість пікселів кожного кольору і застосувати пару формул. Насправді, це проста задача на перевірку гіпотези з використанням критерію хі-квадрат.

Висновки: в ході лабораторної роботи було досліджено приховування даних у зображеннях.