Петров Д.М. КІТ-М120б

Лабораторна робота № 1

Вступ до стігонографії

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 найменьш значимих бітів (Less Significant Bits)
- Виконати аналіз скриття даних за допомогою методу стегоаналізу "атака хі квадрат"
- Додаткове завдання (опціональне, на додаткові бали)

Виконати аналіз скриття даних за допомогою RS методу стегоаналізу

RarJpeg

Rarjpeg - картинка, склеєна з RAR-архівом (JPEG with embedded RAR-file). Рарджепегі мають найбільшого поширення, хоча операція з'єднання графічного файлу та архіву можлива також для інших графічних форматів (PNG, оно, до речі, і так має вбудований беспотерьний архіватор, GIF, навіть BMP, і т. д.) І архівів (ZIP, 7Z, в тому числі і JAR-додатків на платформі Java, але не з TAR), Алсо аудіо- та відеофайлів в форматі Ogg.

Для склеювання файлів використовується консольна команда copy (для віндузятнікі) або cat (для юніксоід):

(Win): copy / b image1.jpg + something.rar image2.jpg
(Ще win): type image1.jpg something.rar> image2.jpg
(Nix): cat image1.jpg something.rar> image2.jpg
(Ще nix): cat something.rar >> image1.jpg

Комп'ютерна стеганографія — напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи. Приклади — стеганографічна файлова система StegFS для Linux, приховування даних в невикористовуваних областях форматів файлів, підміна символів в назвах файлів, текстова стеганографія і т. д. Наведемо деякі приклади:

- Використання зарезервованих полів комп'ютерних форматів файлів — суть методу полягає в тому, що частина поля розширень, не заповнена інформацією про розширення, за замовчуванням заповнюється нулями. Відповідно ми можемо використовувати цю

«нульову» частину для запису своїх даних. Недоліком цього методу є низький ступінь скритності і малий обсяг переданої інформації.

- Метод приховування інформації в невикористовуваних місцях гнучких дисків — при використанні цього методу інформація записується в невживані частини диска, наприклад, на нульову доріжку. Недоліки: маленька продуктивність, передача невеликих за обсягом повідомлень.
- Метод використання особливих властивостей полів форматів, які не відображаються на екрані — цей метод ґрунтується на спеціальних «невидимих» полях для отримання виносок, покажчиків. До прикладу, написання чорним шрифтом на чорному тлі. Недоліки: маленька продуктивність, невеликий обсяг переданої інформації.
- Використання особливостей файлових систем — при зберіганні на жорсткому диску файл завжди (не рахуючи деяких ФС, наприклад, ReiserFS) займає ціле число кластерів (мінімальних адресуються обсягів інформації). До прикладу, в раніше широко використовуваної файлової системи FAT32 (використовувалася в Windows98/Me/2000) стандартний розмір кластера — 4 Кб. Відповідно для зберігання 1 Кб інформації на диску виділяється 4 Кб інформації, з яких 1Кб потрібен для зберігання файлу,, а інші 3 ні на що не використовуються — відповідно їх можна використовувати для зберігання інформації. Недолік даного методу: легкість виявлення.

Хід роботи

1. Реалізація технології Rar-Jpeg

```
[danilpetrov@MacBook-Pro lab01]$ cat testrar.jpg rartest.rar > image2.jpg
[danilpetrov@MacBook-Pro lab01]$ ll
total 11440
-rw-r--r--@ 1 danilpetrov  staff   291911 Nov 16 20:38 ChiSquare.png
-rw-r--r--@ 1 danilpetrov  staff     9173 Nov 16 20:17 README.md
-rw-r--r--  1 danilpetrov  staff        0 Nov 14 15:07 README.md~
-rw-r--r--@ 1 danilpetrov  staff   293370 Nov 15 11:25 image1.png
-rw-r--r--  1 danilpetrov  staff   994755 Nov 16 20:46 image2.jpg
-rw-r--r--@ 1 danilpetrov  staff   295384 Nov 16 20:38 imageAfterEncoder.png
-rw-r--r--@ 1 danilpetrov  staff   125519 Nov 16 20:38 imageColorAfterEncoder.png
-rw-r--r--@ 1 danilpetrov  staff   125518 Nov 16 20:38 imageColorBeforeEncoder.png
-rw-r--r--@ 1 danilpetrov  staff     1205 Nov 16 20:44 lab01.pro
-rw-r--r--  1 danilpetrov  staff    24048 Nov 16 20:44 lab01.pro.user
-rw-------@ 1 danilpetrov  staff   592825 Oct  5 14:34 rartest.rar
drwxr-xr-x  4 danilpetrov  staff      128 Nov 16 20:44 src
-rw-r--r--@ 1 danilpetrov  staff   401930 Mar 13  2020 testrar.jpg
-rw-r--r--  1 danilpetrov  staff     3400 Nov 15 18:54 text.txt
-rw-r--r--@ 1 danilpetrov  staff      162 Nov 16 20:15 ~$лаб01.docx
-rw-r--r--@ 1 danilpetrov  staff  2469739 Nov 16 20:41 лаб01.docx
```

Розмір image1.jpg = 402к
Розмір rartest.rar = 593к
Розмір кінцевого зображення image2.jpg = 995к

2. Скриття даних у зображення за допомогою методу найменьш значимих бітів (Less Significant Bits)

Рис. 2

На рис. 2 знаходиться зображення до скриття даних.

Рис. 3

На рис.3 знаходиться зображення з кольорами пікселей. Кожний колір змінюється якщо молодший біт червоного, або зеленого, або синього кольору має одиницю. Наприклад, якщо в червоному кольору молодший біт встановлений в «1», значення змінюється на 255, аналогічно з усіма іншими кольорами. Потім R, G, B складає колір пікселя.

Текст, що зберігається у фото:

```
19:34:01: Starting /Users/danilpetrov/build-testrgb-Desktop_Qt_5_12_0_clang_64bi
"The United States of America (USA), commonly known as the United States (US or
America, between Canada and Mexico. It consists of 50 states, a federal district
possessions.[h] At 3.8 million square miles (9.8 million square kilometers), it
With a population of over 328 million, it is the third most populous country in
populous city is New York City.\n\nPaleo-Indians migrated from Siberia to the No
colonization began in the 16th century. The United States emerged from the thirt
over taxation and political representation with Great Britain led to the Americo
independence. In the late 18th century, the U.S. began vigorously expanding acro
and displacing Native Americans, and admitting new states; by 1848, the United S
United States until the second half of the 19th century when the American Civil
War I established the U.S. as a world power, a status confirmed by the outcome o
Soviet Union engaged in various proxy wars but avoided direct military conflict.
spaceflight that first landed humans on the Moon. The Soviet Union's collapse in
world's sole superpower, with immense power in global geopolitics.\n\nThe United
three separate branches of government, including a bicameral legislature. It is
International Monetary Fund, Organization of American States (OAS), NATO, and ot
United Nations Security Council. The U.S. ranks high in international measures o
quality of life, and quality of higher education. Despite income and wealth disp
```

Рис. 4

На рис. 4 зображено результат програми. Програма зберігає текст в фотографію у форматі png, а потім це зображення декодує та отримує з нього текст.

Рис. 5

На рис. 5 зображено картину після зберігання текста. Як можно бачити декілька перших ліній картини змінились після зберігання тексту. Це один із способів перевірити зберігається текст в картині чи ні. Можна побачити систематичне зміннення кольорів.

В байт з червоним кольором збережено 2 біти, в байт з зеленим 3 біти, з синім 3 біти. Як можна побачити, шум по середині картини відрізняється шуму з текстом.

3. Дослідження зображення за допомогою хі квадрата.

Атака «Хі-квадрат» грунтується на тому припущенні, що ймовірність одночасної появи сусідніх (відмінних на найменш значущий біт) кольорів (pair of values) в незаповненому стегоконтейнер вкрай мала.

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(n_k - n_k^*)^2}{n_k^*};$$

Рис. 6

На рис. 6 зображена формула за допомогою якої можна зрозуміти зберігається текст в зображенні чи ні. Х - це критерій зі степенями свободи. Якщо практичне значення занадто відрізняється від теоретичного, можна зробити висновок, що з цими пікселями щось не так.

Так за допомогою хі-квадрата можна дослідити зображення з текстом.

Рис. 7

За допомогою хі-квадрата, червоним кольором помічено де зберігається текст.

Висновок

Дослідив можливість «приховування» даних у зображеннях. Навчився зберігати текст в картинках, та користуватися алгоритмом хі-квадрат для знаходження прихованих даних.