ИССЛЕДОВАТЕЛЬСКИЙ УЧЕБНО-НАУЧНЫЙ СТЕГАНОГРАФИЧЕСКИЙ КОМПЛЕКС

Студент 4 курса группы 6 КБ Кукса В.И.

Научный руководитель – кандидат технических наук Садов В.С.

Белорусский Государственный Университет

Минск, Беларусь

Введение

Информационная безопасность и методы её реализации являются крайне важными понятиями в эпоху интернета и цифровых технологий. Стеганография, как наука о незаметном и устойчивом скрытии данных, находит широкое применение в различных областях как средства скрытых коммуникаций, защита авторского права, хранение конфиденциальной информации [1].

В отличие от криптографии, целью которой является скрытие данных за счёт их шифрования, стеганография направлена на скрытие самого факта передачи конфиденциального сообщения. В рамках стеганографии есть несколько направлений, одним из самых популярных является цифровая стеганография, где для хранения информации используются файлы, обычно они являются изображением, видео и аудио.

В работе будет рассмотрен один из востребованных методов цифровой стеганографии, метод LSB, а также структура разработанного на основе данного метода программного комплекса с исследованием изображений разных классов.

Стеганографический LSB метод

LSB (Least Significant Bit) метод подразумевает, что информация об контейнере хранится в определённо сформированном виде байт, в нашем случае в виде 3-х матриц, каждая из которых отвечает за 1 цвет: красный, зелёный или синий [2]. Каждый элемент такой матрицы представляет из себя байт, т.е. диапазон всех возможных значений можно представить в виде множества целых чисел [0; 255]. Изменив младший бит, максимальное отклонение значения интенсивности цветовой компоненты пикселя составит всего 1, что не принесёт изменений,

видимых человеческим глазом, в то время как изменение старшего бита может увеличить либо уменьшить действительную интенсивность на 128, что сильно бросается в глаза.

Рисунок 2. Слева зануление младшей битовой плоскости 3-х цветовых компонент, справа – старшей

Таким образом суть метода LSB заключается в записи информации в младшие битовые плоскости изображения, будь то это младшая битовая плоскость, вторая, обе и т.д. Далее же можно встретить различные вариации данного метода в зависимости от порядка записи в цветовые компоненты и выбора битовых плоскостей.

Структура программного комплекса

Программный комплекс представляет из себя программу, написанную на языке C++ с использованием фреймворка Qt 6.8.0. Программа последовательно записывает биты цветовых компонент bmp-сообщения в промежуточный файл в порядке: красная компонента (R), зелёная компонента (G), синяя компонента (B), в итоге получается файл, состоящий из последовательности бит. После происходит запись последовательности бит из промежуточного файла в bmp-контейнер: в младшие битовые плоскости его цветовых компонент в порядке B, R, G, т.е. сначала идёт запись бит в младшую битовую плоскость B, если остаются биты, то и в младшую битовую плоскость R, если после этого ещё остались биты, то и в G. Изменение в последнюю очередь зелёной компоненты выбрано не случайно, т.к. считается, что человеческий глаз более восприимчив к зелёным оттенкам.

Интерфейс программы состоит из 2-ух вкладок:

•*Creating stegocontainer* для создания стегоконтейнера.

•*Comparing low-bit images* для сравнения изображений младшей битовой плоскости контейнера и стегоконтейнера.

Первая вкладка содержит в себе 3 кнопки:

•*Open container (.bmp)* для выбора контейнера.

•*Open message (.bmp)* для выбора сообщения.

•*Insert message* для создания стегоконтейнера (активна только после выбора контейнера и сообщения).

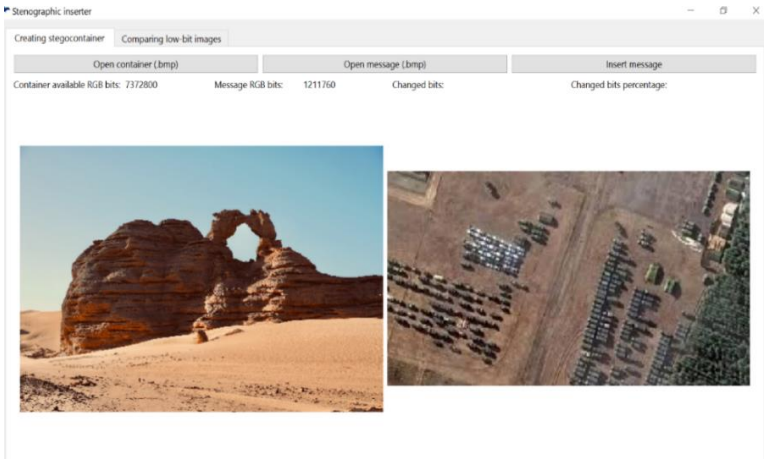

Рисунок 2. Выбраны контейнер и сообщение

Также первая вкладка содержит в себе 4 поля с данными:

•*Container available RGB bits* показывает количество битов младших битовых плоскостей RGB контейнера

•*Message RGB bits* показывает количество битов RGB сообщения.

•*Changed bits* показывает количество изменённых битов контейнера.

•*Changed bits percentage* показывает процентное отношение изменённых битов к количеству младших битов контейнера.

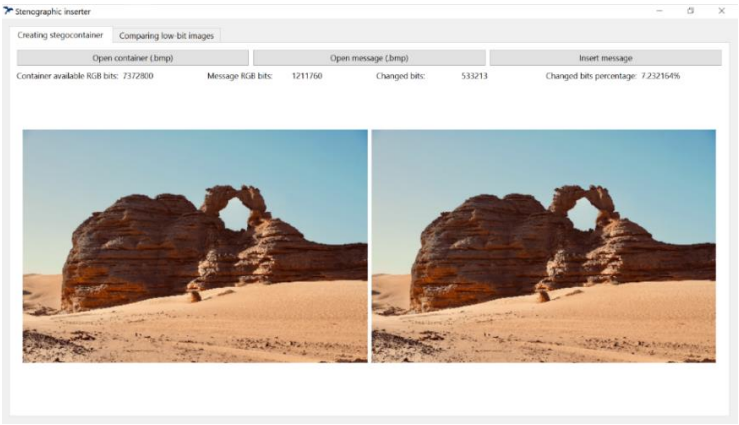

Рисунок 3. Контейнер и стеганоконтейнер

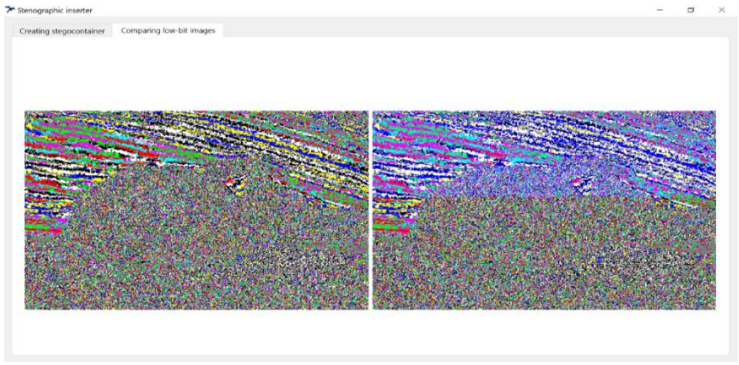

Рисунок 4. Изображения младшей битовой плоскости контейнера (слева) и стегоконтейнера (справа)

Исследование

В качестве исследования было предложено сравнить количество изменённых бит при встраивании в естественный и синтезированный контейнеры изображений такого же происхождения. Естественное изображение, т.е. фото, имеет в себе много шумов в младшей битовой плоскости, в то время как синтезированные имеют более однородную структуру младшей области, т.к. зачастую это изображения, созданные с помощью различных графических редакторов, т.е. рисунки.

Эксперимент будет заключаться в том, что будет выбран контейнер, представляющий из себя естественное и синтезированное изображение, а также по 10 изображений естественного и синтезированного происхождения, при этом встраиваемые изображения будут подобраны таким образом, чтобы они заполняли практически весь контейнер. После чего будет проведена серия встраиваний и подсчитан средний процент изменённых бит для каждого класса изображения.

В качестве контейнеров выбраны изображения размером 5300 × 3533 пикселя, встраиваемые изображения имеют размер 1920 × 1200 пикселей. На рис.5 представлены их младшие битовые плоскости.

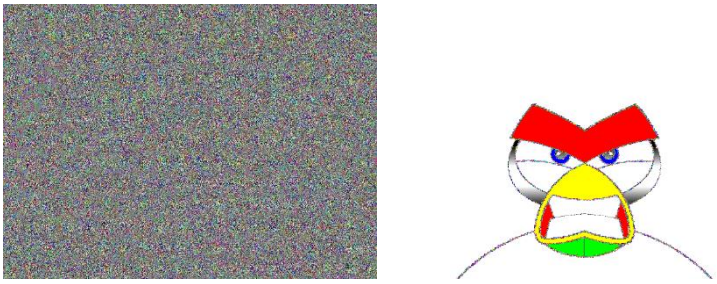

Рисунок 5. Изображения младшей битовой плоскости выбранного естественного контейнера (слева) и синтезированного контейнера (справа)

Таблица 1. Процентное соотношение изменённых бит младшей битовой плоскости естественного контейнера к её размеру (%)

Естественное изображение	Синтетическое изображение
44,69	46,01
52,79	41,95
40,14	34,38
42,13	52,64
43,41	37,15
48,41	52,00
44,96	34,85
24,92	48,73
45,88	41,46
44,25	36,91
43,15	***42,60***

Таблица 2. Процентное соотношение изменённых бит младшей битовой плоскости синтезированного контейнера к её размеру (%)

Естественное изображение	Синтетическое изображение
40,65	47,75
35,00	42,79

42,63	44,00
39,68	33,32
43,00	44,30
37,96	35,49
41,84	49,69
51,28	41,08
41,40	43,77
41,22	45,28
41,47	***42,75***

Как видно из эксперимента средние значения практически не различимы для всех четырёх серий встраиваний, что означает, что класс изображения в среднем не влияет на количество изменённых пикселей, схожие расхождения в количестве изменённых пикселей наблюдаются в обоих классах изображения.

Заключение

В работе была дана базовая информация о стеганографии и её применении. Был разобран и программно реализован метод LSB, также программно была реализована возможность просмотра младшей битовой плоскости контейнера и стегоконтейнера, подсчёта доступных и изменённых бит при встраивании. Было произведено сравнение количества изменённых бит при встраивании изображений естественного и синтетического происхождения в контейнеры таких же классов, сделан вывод о равенстве количества изменённых бит.

В случае же с распознаванием факта встраивания информации в контейнер необходимо сказать, что естественный контейнер зачастую имеет случайный характер расположения единиц и нулей в младшей битовой плоскости, в то время как синтезированный контейнер имеет намного более структурированное расположение значений бит. Для скрытия факта встраивания информации в случае с естественным контейнером используется ее кодирование, во-первых, в таком случае встроенная информация будет защищена от прямого считывания, если

удастся разгадать стенографический метод, во-вторых, при таких преобразованиях сообщение начинает носить случайный характер, что при встраивании сообщения не приведёт к изменению распределения значений битов. В синтезированном же контейнере, наблюдаются однородные участки, в таком случае для встраивания сообщения, которое носит случайный характер распределения значений его битов, для скрытия факта передачи скрытой информации в таком контейнере находят участки, которые носят случайный характер. В них и происходит встраивание информации.

Литература

1. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев — М.: СОЛОН-ПРЕСС, 2009 — 272 с. (Серия «Аспекты защиты»)

2. Kaspersky [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-steganography – Дата доступа: 24.02.2025