# ВЛИЯНИЕ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ НА ГИСТОГРАММЫ ЯРКОСТЕЙ ИХ ПИКСЕЛЕЙ

студент гр. 4КБ Новоженина А. В.
Кафедра информатики и компьютерных систем
***Научный руководитель – профессор Садов В. С.***
Белорусский государственный университет
Минск, Беларусь

*Введение*

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. В настоящее время выделяется два основных направления решения этой задачи: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. Криптография опирается на свойства информации, а не на свойства материальных носителей, особенности узлов ее обработки, передачи и хранения. При стеганографии скрывается сам факт существования тайного сообщения. Сообщение – это любая информация, подлежащая скрытой передаче. В качестве сообщения может использоваться любой вид информации: текст, изображение, аудиосигнал. Контейнер – некоторые цифровые данные, используемые для сокрытия сообщения. Например, изображения, аудиофайлы, видеофайлы, текстовые документы и прочие мультимедиа файлы. [1]

Чтобы обеспечить максимальную скрытность передаваемого сообщения, можно применить сразу два метода. Однако, надо также следить, чтобы сообщение было достаточно зашифрованным и при этом не наблюдалось значительных искажений в контейнере.

*Цель работы*: согласовать параметры незаполненного стеганографического контейнера с параметрами сообщений, что должно привести к незаметности встраивания сообщения.

Задачи работы:

- Обзор различных контейнеров;
- Минимизировать связь между битами сообщения, при помощи шифрования.

*Типы шифрования*

Существует два основных метода шифрования: симметричное и ассиметричное.

Метод симметричного шифрования, как и следует из названия, использует один криптографический ключ для шифрования и дешифрования данных. Использование одного ключа для обеих операций делает процесс простым. Когда требуется зашифровать большой кусок данных, симметричное шифрование оказывается отличным вариантом.

Существуют сотни алгоритмов симметричного типа. Наиболее распространенные из них — AES, RC4, DES, 3DES, RC5, RC6, “Шифр Цезаря”, гаммирование и т. д.

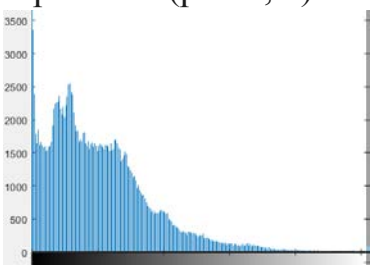
Асимметричное шифрование, в отличие от симметричного, включает в себя несколько различных ключей для шифрования и дешифрования данных, которые математически связаны друг с другом. Один из этих ключей известен как «открытый ключ», а другой — как «закрытый ключ». [2]

*Шифрование изображений*

В данной работе будут рассмотрены и проанализированы два вида изображений. Одно из них будем называть контейнером, а другое - сообщением.

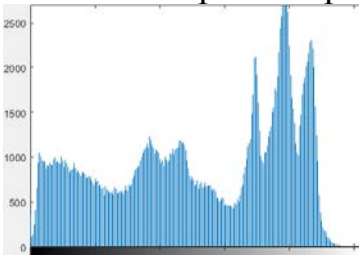
При помощи программных средств Matlab было проведено исследование этих изображений. Для исследования сообщений были построены гистограммы яркости изображения. Каждый пиксель изображения состоит из трех компонентов цвета — RGB. Значение яркости RGB варьируется от 0 до 255. Гистограмма яркостей показывает количество значений RGB, соответствующих определенной яркости (0-255). Для исследования контейнеров были рассмотрены три младших битовых плоскости. Значение пикселя изображения лежит в диапазоне от 0 до 255 для каждого RGB, поэтому его информация содержится в 8-битном формате. Таким образом, мы можем разделить это изображение на 8 плоскостей. Младшие плоскости несут в себе мало информации, поэтому их можно использовать для передачи информации.

Ниже представлены два различных изображения и их совокупные по всем цветам гистограммы распределения яркостей (рис.1, 2).


а)


б)

Рис 1. Исходное изображение (а) и его гистограмма яркостей (б).


а)


б)

Рис 2. Исходное изображение (а) и его гистограмма яркостей (б).

Как видно, гистограммы распределения яркостей приведенных сообщений соответствуют визуальному восприятию изображений.

Для шифрования изображений был использован метод гаммирования. Принцип шифрования гаммированием заключается в генерации гаммы (последовательности случайных чисел) и наложения этой гаммы на данные. Гамма представляет собой матрицу размером, соответствующим размеру исходного изображения. Далее эта гамма добавляется к матрицам значений RGB изображения. Также, видоизменять можно не все три матрицы цвета. В результате мы получили изображения такого вида (рис.3, 4):

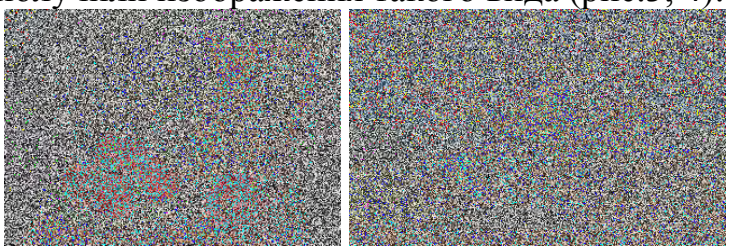


Рис 3. Зашифрованные изображения.

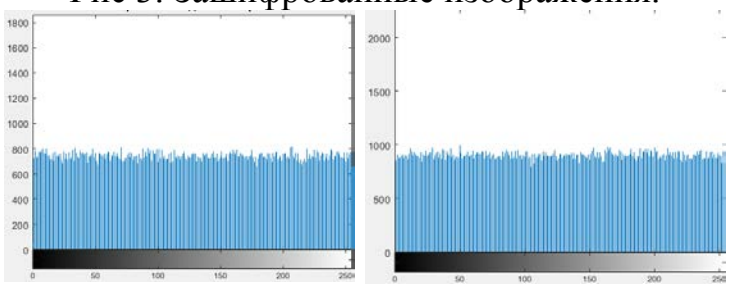


Рис 4. Гистограммы зашифрованных изображений.

Проанализировав полученные зашифрованные изображения и их гистограммы распределения яркостей, можно сделать вывод, что они выглядят как шум.

*Исследование стеганографических контейнеров*

Для исследования контейнеров были рассмотрены их три младших битовых плоскости Рис. 5 - 8).

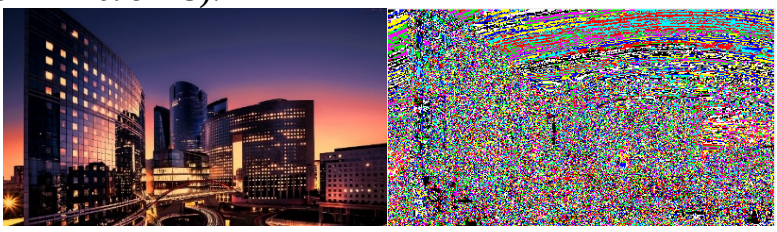


Рис 5. Контейнер и его первая битовая плоскость.

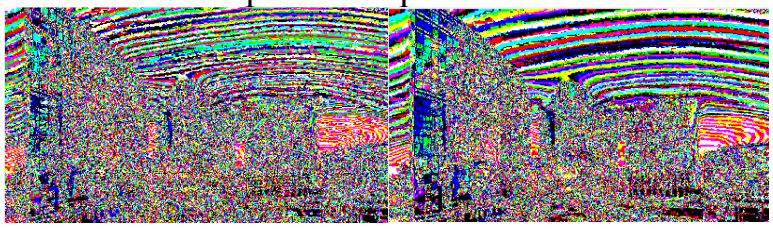


Рис 6. Вторая и третья битовая плоскость.

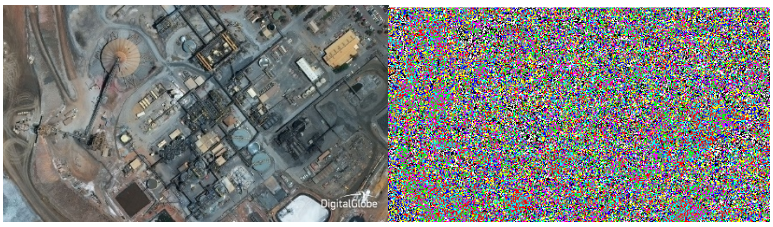


Рис 7. Контейнер и его первая битовая плоскость.

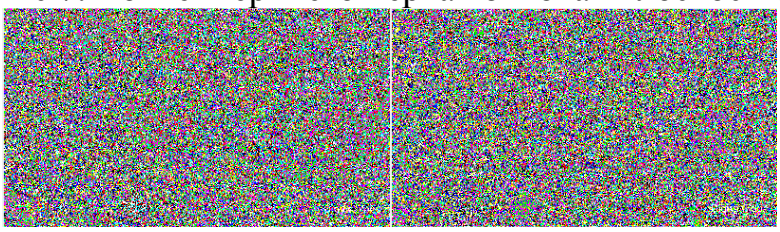


Рис 8. Вторая и третья битовая плоскость.

Видно, как битовые плоскости разных контейнеров отличаются друг от друга. Есть контейнеры, где биты случайно распределены только на некоторых участках битовой плоскости, а есть такие, что биты случайно распределены на всей первой битовой плоскости. Это значит, что изображение некачественное.

Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек обычно не способен заметить изменение в этом бите. Фактически, он является шумом. Поэтому его можно использовать для встраивания информации [3].

Теперь рассмотрим, как меняется первая битовая плоскость при встраивании изображений в контейнер (рис. 9 – 12).

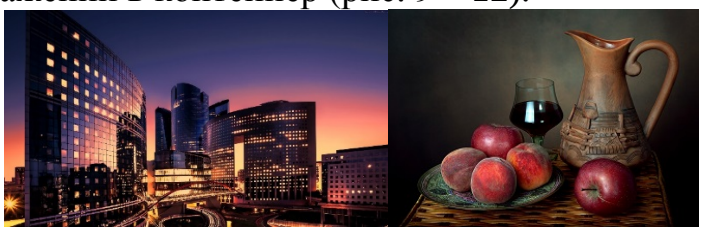


Рис 9. Контейнер и встраиваемое изображение.

Рис 10. Первая битовая плоскость после встраивания исходного и зашифрованного изображения.

Рис 11. Контейнер и встраиваемое изображение.

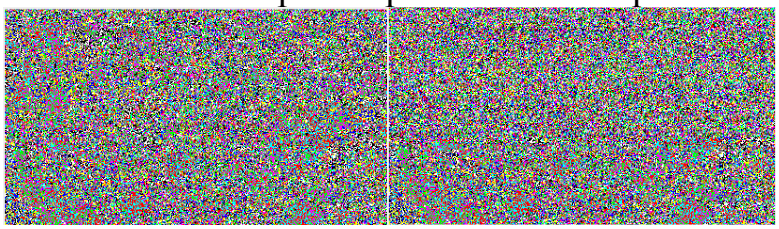


Рис 12. Первая битовая плоскость после встраивания исходного и зашифрованного изображения.

Можно заметить, что при встраивании зашифрованного изображения в те области, где биты имеют случайное распределение, характер связей в этих областях не меняется.

*Результаты анализа*

Так как после криптографического шифрования сообщений они превращаются в поток случайных битов, то и встраивать их следует в те области контейнера, где биты также случайно распределены. Есть контейнеры, где младшая битовая плоскость носит случайный характер полностью, что дает нам возможность незаметного встраивания изображения. Так как связи между битами не нарушаются, обнаружить сообщение становится трудно, но при обнаружении зашифрованного сообщения злоумышленник получит не исходное изображение, а шум. И в дальнейшем ему придется подбирать алгоритмы и ключи для дешифрования сообщения.

*Заключение*

Встраивание сообщений производится в незначащие битовые плоскости контейнера, то есть в младшие незначащие биты. В большинстве случаев младшие биты носят случайный характер, но также могут быть взаимосвязанными. При стеганографической модификации младших битов контейнера эти связи разрушаются. Тогда наша главная задача – согласование параметров контейнера с параметрами сообщения. Что мы и сделали благодаря шифрованию.

Для шифрования изображений был использован метод гаммирования, то есть к матрицам значений RGB изображения была добавлена матрица случайных чисел.

В ходе проведенного эксперимента удалось установить, что для человеческого глаза незаметны изображения, встраиваемые в такие контейнеры, где первая битовая плоскость сильно зашумлена. Также возможен вариант встраивания только в участки с шумами, что делает количество встраиваемой информации значительно меньше. Шифрование сообщений позволяет нам не нарушать связи между битами в первой

битовой плоскости. Но уже точно можно сказать, что шифрование сообщений добавляет дополнительную защиту.

*Литература*

1. Грибунин В.Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. СПб.:ВУС, 2009.

2. Шифрование: типы и алгоритмы. [Электронный ресурс]. – Режим доступа: https://wiki.hostpro.ua/knowledgebase/shifrovanie-tipy-i-algoritmy/ –Дата доступа: 17.12.2021

3. Бородин Г.А., Чиркова С.В., «Классификация критериев выбора контейнера для LSB-метода», «Радиоэлектроника, электротехника и энергетика 13-ая межд. науч.-техн. конф. студ. и асп. Тезисы докладов в 3-ех томах». Т.1. –М.: МЭИ, 2007