МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

Дисциплина стеганография

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К КУРСОВОМУ ПРОЕКТУ

Обнаружение стегосистем СГ-НЗБ

*(тема курсового проекта)*

11.03.02 Инфокоммуникационные технологии и системы связи

*(код и наименование направления/специальности)*

Студент:

Громов Артем Андреевич, ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Преподаватель:

К.т.н., доцент кафедры ЗСС, Ахрамеева Ксения Андреевна

(ученая степень, ученое звание, ФИО)

(дата, подпись)

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 3](#_Toc98354941)

[Визуальная атака 3](#_Toc98354942)

[Атака на основе статистики 1 порядка 4](#_Toc98354943)

[Атака на основе статистики 2 порядка 4](#_Toc98354944)

[ОСНОВНАЯ ЧАСТЬ 5](#_Toc98354945)

[Исследование изображений 5](#_Toc98354946)

[Ход работы с изображениями 5](#_Toc98354947)

[Первичные результаты исследований 9](#_Toc98354948)

[Изменение порогов обнаружения 12](#_Toc98354949)

[ЗАКЛЮЧЕНИЕ 15](#_Toc98354950)

# ВВЕДЕНИЕ

СГ-НЗБ изменяет наименее значащие биты покрывающего сообщения, вкладывая в них скрываемое сообщение. В качестве покрывающего объекта можно использовать неподвижные изображения. Скрываемым сообщением может быть текст или изображение.

Разберем замещение на примере:

112 = 01110000+1 = 01110001 = 113

253 = 11111101+1 = 11111101 = 253

255 = 11111111+0 = 11111110 = 254

Как видно из примера выше происходит замещение наименьшего бита на подставляемый бит.

В данной курсовой работе мы используем 3 метода атаки:

- Визуальная атака

- Атака на основе статистики 1 порядка

- Атака на основе статистики 2 порядка

Кратко разберем каждую атаку.

## Визуальная атака

Исследуемое изображение приводится к черно-белому виду. Это происходит по следующему принципу: если наименьший значащий бит равен 0, то данный пиксель закрашивается черным, иначе – белым. Если в исследуемом изображении нет вложения, то на полученном черно-белом изображении будут видны очертания первоначального рисунка. Если же в исследуемое изображение вложили сообщение, то полученное черно-белое изображение может иметь очертания первоначального рисунка, но с шумом. Чем большое доля вложения, тем более явно проявляется шум.

Использование данной атаки возможно только в присутствии человека. Это связано с тем, что наличие или отсутствие вложения скрытой информации в исследуемом изображении определятся непосредственно человеком.

## Атака на основе статистики 1 порядка

Атака на основе статистики 1 порядка сводится к сравнению двух показателей: экспериментально полученного значения *χ*2 и нами заданного порогового значения . Если полученное значение больше заданного, то считаем, что вложения нет, иначе – присутствует.

## Атака на основе статистики 2 порядка

Данный метод называется sample pair analysis – парно-выборочный анализ. В этой атаке вычисляются корни квадратного уравнения, состоящего из некоторых параметров. Суть этих параметров в количестве последовательных пар яркостей пикселей в различных комбинациях. Наименьший корень данного уравнения сравнивается с заданным нами пороговым значением. Если полученное значение меньше заданного, то считаем, что вложения нет, иначе – присутствует.

Парно-выборочный анализ интересен тем, что позволяет определить не только наличие вложенного сообщения, но и оценить долю этого вложения.

# ОСНОВНАЯ ЧАСТЬ

Вариант – 4

Исследуемые изображения: 4, 18, 33, 38, 43

## Исследование изображений

По заданию необходимо исследовать 3 метода стегоанализа для СГ-НЗБ. Для исследования было выбрано 5 изображений в которые будет погружаться следующее сообщение – 83GromovAA. Для каждого изображения будет проведен цикл погружений сообщения со следующими долями вложения – 1; 0,5; 0,1; 0,01.

## Ход работы с изображениями

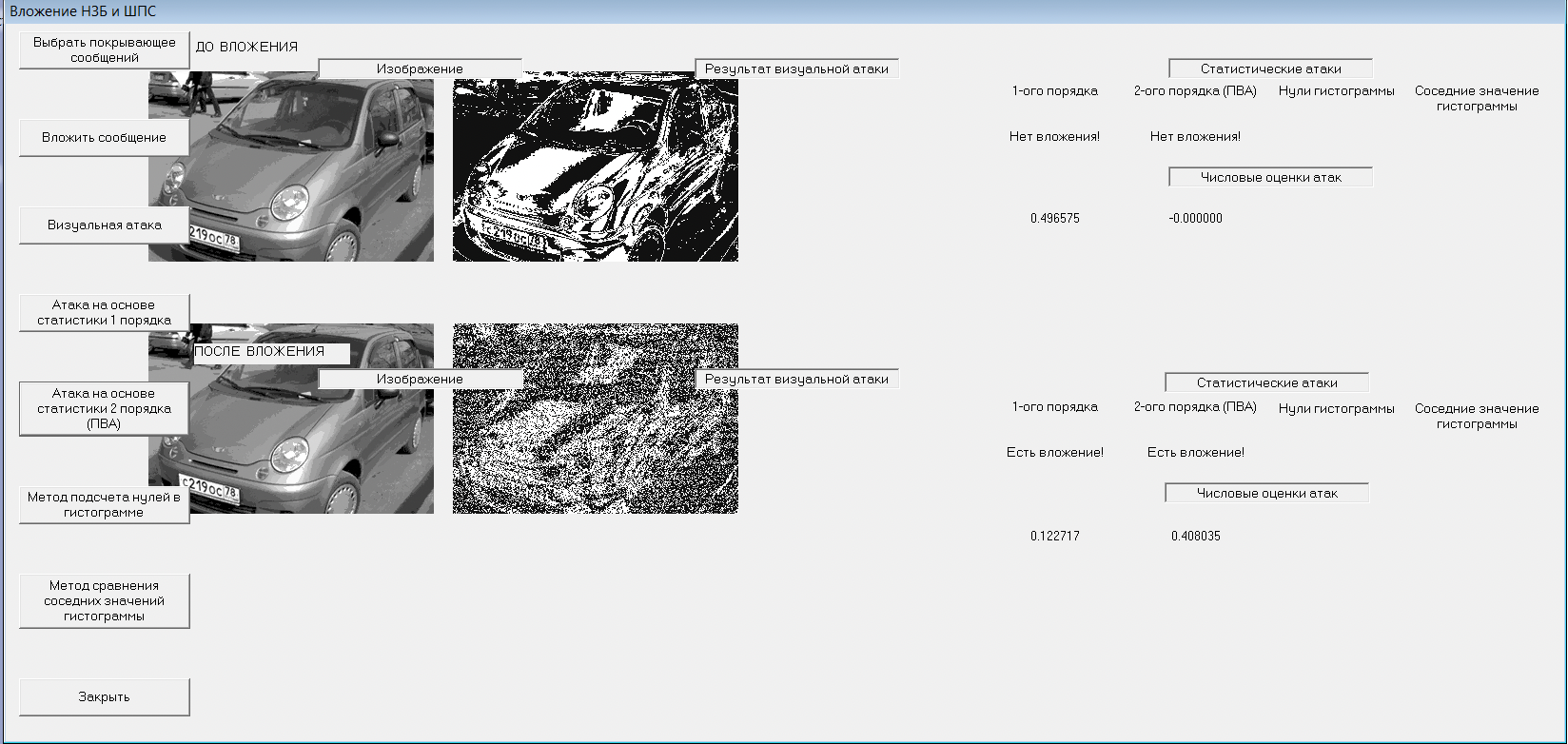


Рис. 1 – Интерфейс приложения

Алгоритм работы с приложением:

1. Выбираем изображение
2. Вкладываем сообщение
3. Проводи визуальную атаку
4. Проводим атаку на основе статистики 1 порядка
5. Проводим атаку на основе статистики 2 порядка

Пример изображений, получаемых при разной доле вложения сообщения:

Таблица 1 – Изображения с долей погружения сообщения 100%

|  |  |
| --- | --- |
| Изображение до погружения | Изображение после погружения сообщения с долей 100% |
|  |  |
| Атака на изображение до погружения | Атака на изображение после погружения сообщения с долей 100% |
|  |  |

Таблица 2 – Изображения с долей погружения сообщения 50%

|  |  |
| --- | --- |
| Изображение до погружения | Изображение после погружения сообщения с долей 50% |
|  |  |
| Атака на изображение до погружения | Атака на изображение после погружения сообщения с долей 50% |
|  |  |

Таблица 3 – Изображения с долей погружения сообщения 10%

|  |  |
| --- | --- |
| Изображение до погружения | Изображение после погружения сообщения с долей 10% |
|  |  |
| Атака на изображение до погружения | Атака на изображение после погружения сообщения с долей 10% |
|  |  |

Таблица 4 – Изображения с долей погружения сообщения 1%

|  |  |
| --- | --- |
| Изображение до погружения | Изображение после погружения сообщения с долей 1% |
|  |  |
| Атака на изображение до погружения | Атака на изображение после погружения сообщения с долей 1% |
|  |  |

По мере выполнения работы необходимо записывать полученные расчеты.

Перейдем к первичным результатам исследования.

## Первичные результаты исследования

По результатам исследования, можно сделать вывод: визуальная атака хорошо себя проявляет вплоть до 10%. При доле вложения 1% анализ визуальной атаки может занимать достаточно большое количество времени. Также стоит учитывать, что данный метод требует присутствие человека. Работать 8 часов, внимательно изучая изображения, требует невероятной концентрации. Использовать данный метод, по моему мнению необходимо для решения спорных ситуаций. По этой причине обратимся к двум другим методам стегоанализа.

Ниже представлены таблицы с результатами анализа изображений с помощью второго и третьего метода. Пороговое значение для анализа первого порядка – 0,48; для анализа второго порядка – 0,0001.

Таблица 5 – Анализ изображения №4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 4 | | 4 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,000708 | 0,587837 | Есть | Есть |
| 0,50 | 0,123892 | 0,409616 | Есть | Есть |
| 0,10 | 0,400933 | 0,098157 | Есть | Есть |
| 0,01 | 0,487425 | 0,009301 | Нет | Есть |
| 0,00 | 0,496575 | 0 | Нет | Нет |

Таблица 6 – Анализ изображения №18

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 18 | | 18 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,001125 | 0,557797 | Есть | Есть |
| 0,50 | 0,112875 | 0,364716 | Есть | Есть |
| 0,10 | 0,3763 | 0,000471 | Есть | Есть |
| 0,01 | 0,45565 | 0 | Есть | Нет |
| 0,00 | 0,464058 | 0 | Есть | Нет |

Таблица 7 – Анализ изображения №33

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 33 | | 33 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,000958 | 0,564383 | Есть | Есть |
| 0,50 | 0,125425 | 0,401321 | Есть | Есть |
| 0,10 | 0,408108 | 0,092608 | Есть | Есть |
| 0,01 | 0,489567 | 0,009009 | Нет | Есть |
| 0,00 | 0,5 | 0 | Нет | Нет |

Таблица 8 – Анализ изображения №38

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 38 | | 38 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,0009 | 0,572037 | Есть | Есть |
| 0,50 | 0,1131 | 0,389351 | Есть | Есть |
| 0,10 | 0,370167 | 0,058423 | Есть | Есть |
| 0,01 | 0,448017 | 0 | Есть | Нет |
| 0,00 | 0,456917 | 0 | Есть | Нет |

Таблица 9 – Анализ изображения №43

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 43 | | 43 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,0008 | 0,579444 | Есть | Есть |
| 0,50 | 0,1241 | 0,406107 | Есть | Есть |
| 0,10 | 0,402233 | 0,099751 | Есть | Есть |
| 0,01 | 0,49035 | 0,009323 | Нет | Есть |
| 0,00 | 0,5 | 0 | Нет | Нет |

Изучая полученные результаты, можно заметить, что программа в некоторых случаях совершает ошибки. Предлагаю посчитать количество ложноположительных и ложноотрицательных обнаружений для каждого из методов.

Таблица 10 – Количество ложных обнаружений

|  |  |
| --- | --- |
| Количество ложноположительных обнаружений анализа первого порядка | 2 |
| Количество ложноотрицательных  обнаружений анализа первого порядка | 3 |
| Количество ложноположительных обнаружений анализа второго порядка | 0 |
| Количество ложноотрицательных  обнаружений анализа второго порядка | 2 |

А теперь рассчитаем вероятность ложноположительных и ложноотрицательных обнаружений. Каждый метод был использован 20 раз. Соответственно для получения вероятности надо разделить количество ложных обнаружений на количество попыток.

Таблица 11 – Вероятность ложных обнаружений

|  |  |
| --- | --- |
| Вероятность ложноположительных обнаружений анализа первого порядка | 2/5=0,4=40% |
| Вероятность ложноотрицательных  обнаружений анализа первого порядка | 3/20=0,15=15% |
| Вероятность ложноположительных обнаружений анализа второго порядка | 0 |
| Вероятность ложноотрицательных  обнаружений анализа второго порядка | 2/20=0,1=10% |

Из пяти ложноотрицательных обнаружений, три приходятся на анализ первого порядка. Следует увеличить пороговое значение для данного метода. Таким образом удастся уменьшить количество ошибок.

Ложноотрицательные обнаружения при анализе второго порядка, к сожалению, убрать не удастся, так как результатом расчетов является 0.

## Изменение порогов обнаружения

Опираясь, на значения из прошлого раздела, пороговое значение для анализа первого порядка было изменено на 0,4904. Таким образом удалось сократить количество ложноотрицательных обнаружений в 2,5 раза.

Таблица 12 – Анализ изображения №4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 4 | | 4 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,000708 | 0,587837 | Есть | Есть |
| 0,50 | 0,123892 | 0,409616 | Есть | Есть |
| 0,10 | 0,400933 | 0,098157 | Есть | Есть |
| 0,01 | 0,487425 | 0,009301 | Есть | Есть |
| 0,00 | 0,496575 | 0 | Нет | Нет |

Таблица 13 – Анализ изображения №18

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 18 | | 18 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,001125 | 0,557797 | Есть | Есть |
| 0,50 | 0,112875 | 0,364716 | Есть | Есть |
| 0,10 | 0,3763 | 0,000471 | Есть | Есть |
| 0,01 | 0,45565 | 0 | Есть | Нет |
| 0,00 | 0,464058 | 0 | Есть | Нет |

Таблица 14 – Анализ изображения №33

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 33 | | 33 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,000958 | 0,564383 | Есть | Есть |
| 0,50 | 0,125425 | 0,401321 | Есть | Есть |
| 0,10 | 0,408108 | 0,092608 | Есть | Есть |
| 0,01 | 0,489567 | 0,009009 | Есть | Есть |
| 0,00 | 0,5 | 0 | Нет | Нет |

Таблица 15 – Анализ изображения №38

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 38 | | 38 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,0009 | 0,572037 | Есть | Есть |
| 0,50 | 0,1131 | 0,389351 | Есть | Есть |
| 0,10 | 0,370167 | 0,058423 | Есть | Есть |
| 0,01 | 0,448017 | 0 | Есть | Нет |
| 0,00 | 0,456917 | 0 | Есть | Нет |

Таблица 16 – Анализ изображения №43

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 43 | | 43 | |
|  | 1 порядок | 2 порядок | 1 порядок | 2 порядок |
| 1,00 | 0,0008 | 0,579444 | Есть | Есть |
| 0,50 | 0,1241 | 0,406107 | Есть | Есть |
| 0,10 | 0,402233 | 0,099751 | Есть | Есть |
| 0,01 | 0,49035 | 0,009323 | Есть | Есть |
| 0,00 | 0,5 | 0 | Нет | Нет |

Рассчитаем количество ложноположительных и ложноотрицательных обнаружений для каждого из методов.

Таблица 17 – Количество ложных обнаружений

|  |  |
| --- | --- |
| Количество ложноположительных обнаружений анализа первого порядка | 2 |
| Количество ложноотрицательных  обнаружений анализа первого порядка | 0 |
| Количество ложноположительных обнаружений анализа второго порядка | 0 |
| Количество ложноотрицательных  обнаружений анализа второго порядка | 2 |

А теперь рассчитаем вероятность ложноположительных и ложноотрицательных обнаружений.

Таблица 18 – Вероятность ложных обнаружений

|  |  |
| --- | --- |
| Вероятность ложноположительных обнаружений анализа первого порядка | 2/5=0,4=40% |
| Вероятность ложноотрицательных  обнаружений анализа первого порядка | 0 |
| Вероятность ложноположительных обнаружений анализа второго порядка | 0 |
| Вероятность ложноотрицательных  обнаружений анализа второго порядка | 2/20=0,1=10% |

Ложноположительные обнаружения менее важны в данной задаче, так как не обнаружить стеганограмму хуже, чем повторно перепроверить ложную тревогу.

# ЗАКЛЮЧЕНИЕ

В заключении исследования методов стегоанализа, я пришел к следующим выводам: метод визуальной атаки точный и быстрый до 10% вложения. Ниже этого значения, определить наличие скрытого сообщения, становится значительно сложнее. По этой причине эффективнее использовать статистические методы для автоматического стегоанализа. Если сравнивать первый и второй методы, то исходя из моих изображений, после корректировки порогового значения, анализ первого порядка оказался более точным на любых долях вложения.

Однако, в связи с ростом вычислительных мощностей современных компьютеров, по моему мнению желательно использовать оба метода статистического анализа. А любые конфликтные результаты статистических методов, или решения, принятые близко к пороговым значениям, необходимо перепроверять с помощью визуальной атаки.