**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**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 Основы стеганографии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

СГ с вложением в наименьшие значащие биты

*(тема отчета)*

11.03.02 Инфокоммуникационные технологии и системы связи / ЗСС

*(код и наименование направления/специальности)*

Студенты:

Мазеин Д.С., ИКТЗ-83

*(Ф.И.О.,№группы) (подпись)*

Громов А.А., ИКТЗ-83

*(Ф.И.О.,№группы) (подпись)*

Микколаени М.С, ИКТЗ-83

*(Ф.И.О.,№группы) (подпись)*

Жиляков Г.В., ИКТЗ-83

*(Ф.И.О.,№группы) (подпись)*

Принял:

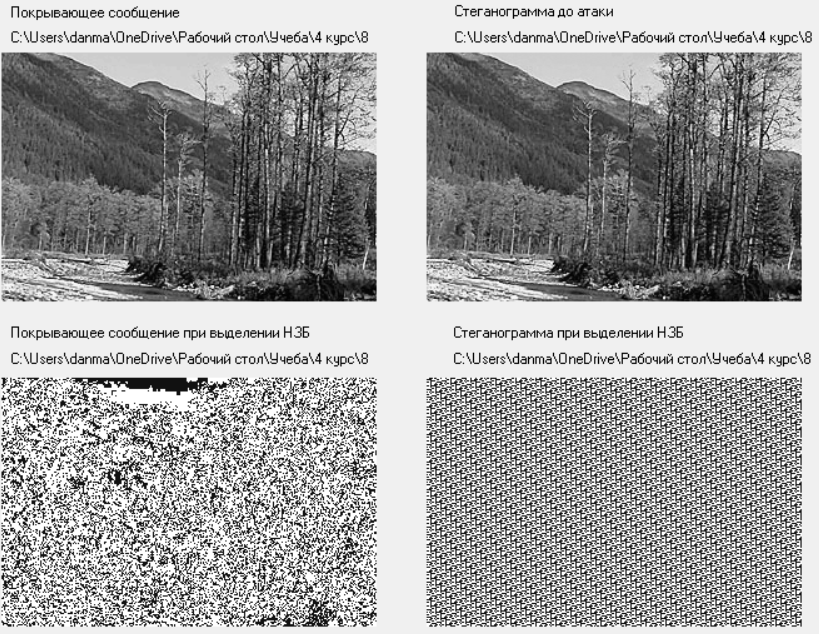
доц. Герлинг Е.Ю.

*(Ф.И.О.) (подпись)*

Цель работы: Понять технику вложения и извлечения информации методом наименьших значащих бит. Проанализировать эффективность различных атак по выявлению вложения.

**Ход работы.**

Вкладываемый текст с вероятностью вложения 100%.



Статистические атаки.

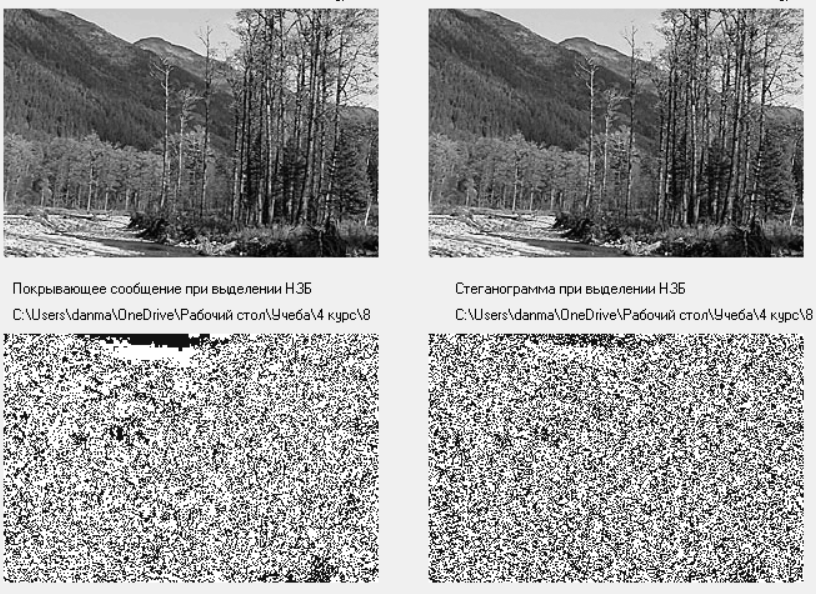
С помощью таблицы можно сравнить эффективность статистической атаки, основанной на гистограммах изображений, и статистической атаки с учетом корреляции пикселей.

Извлечение сообщения



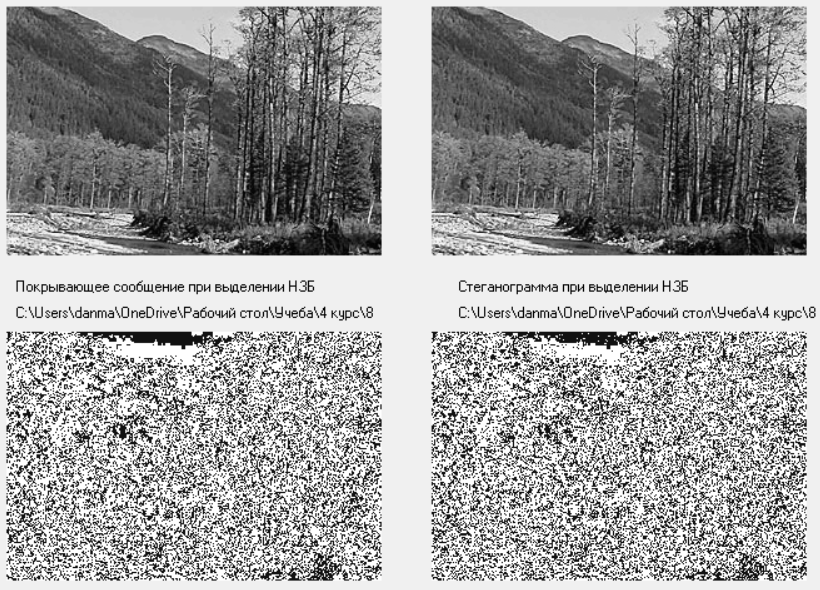
Т.к. количество символов в извлеченном тексте более пятидесяти, то появится только пятьдесят первых символов (чтобы не загружать экран), и будет указан путь к файлу, в котором можно прочитать полное извлеченное сообщение.

Вероятность вложения сообщения 50%

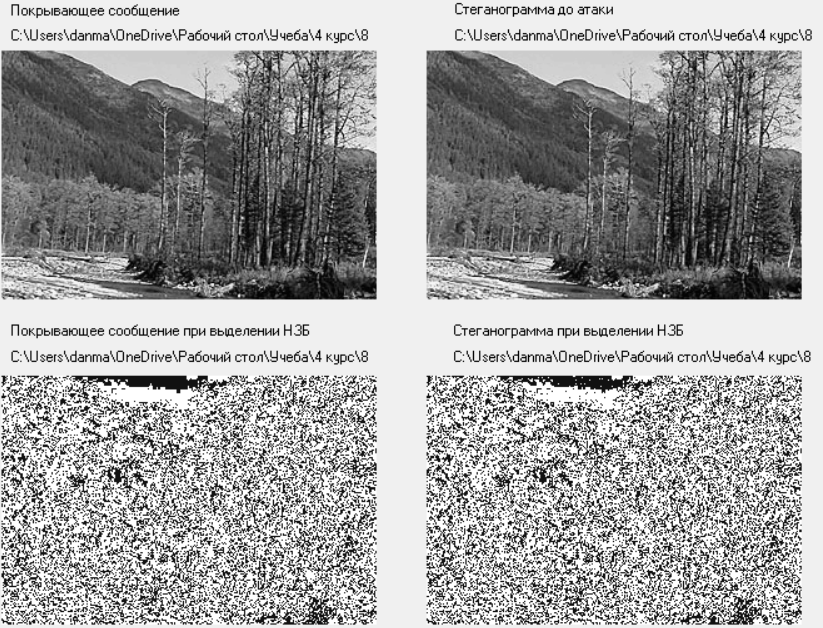


Если сравнить полученный результат с предыдущим, можно заметить, что количество шумов на картинке значительно уменьшилось и само изображение проглядывается значительно чётче.

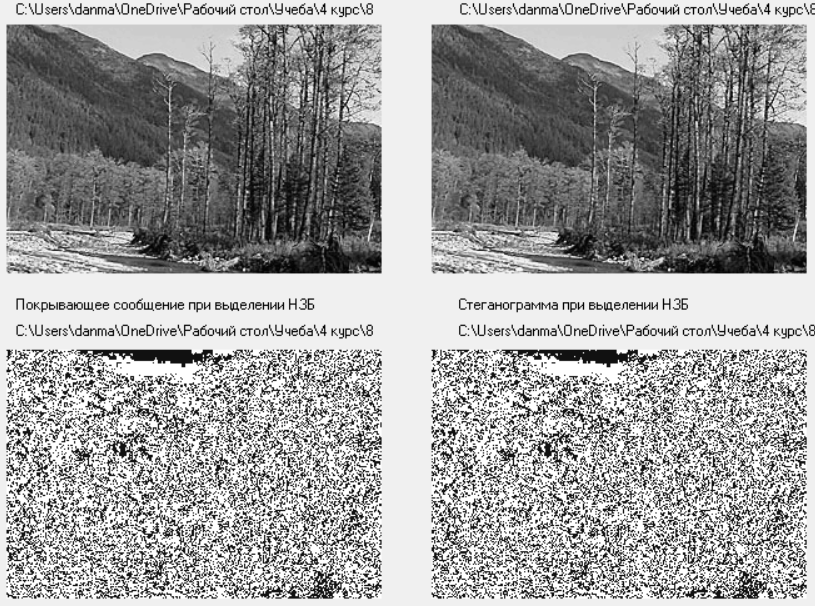
Вероятность вложения 10%



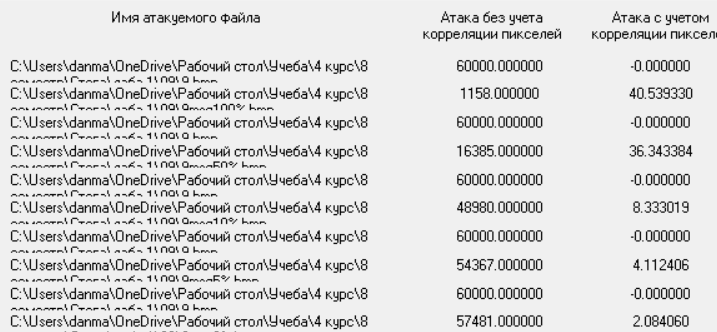
Вероятность вложения 5%



Вероятность вложения 2%



Статистическая атака при вероятностях вложения: 1%, 0.1%, 0.05%, 0.01%, 1 двоичный символ.

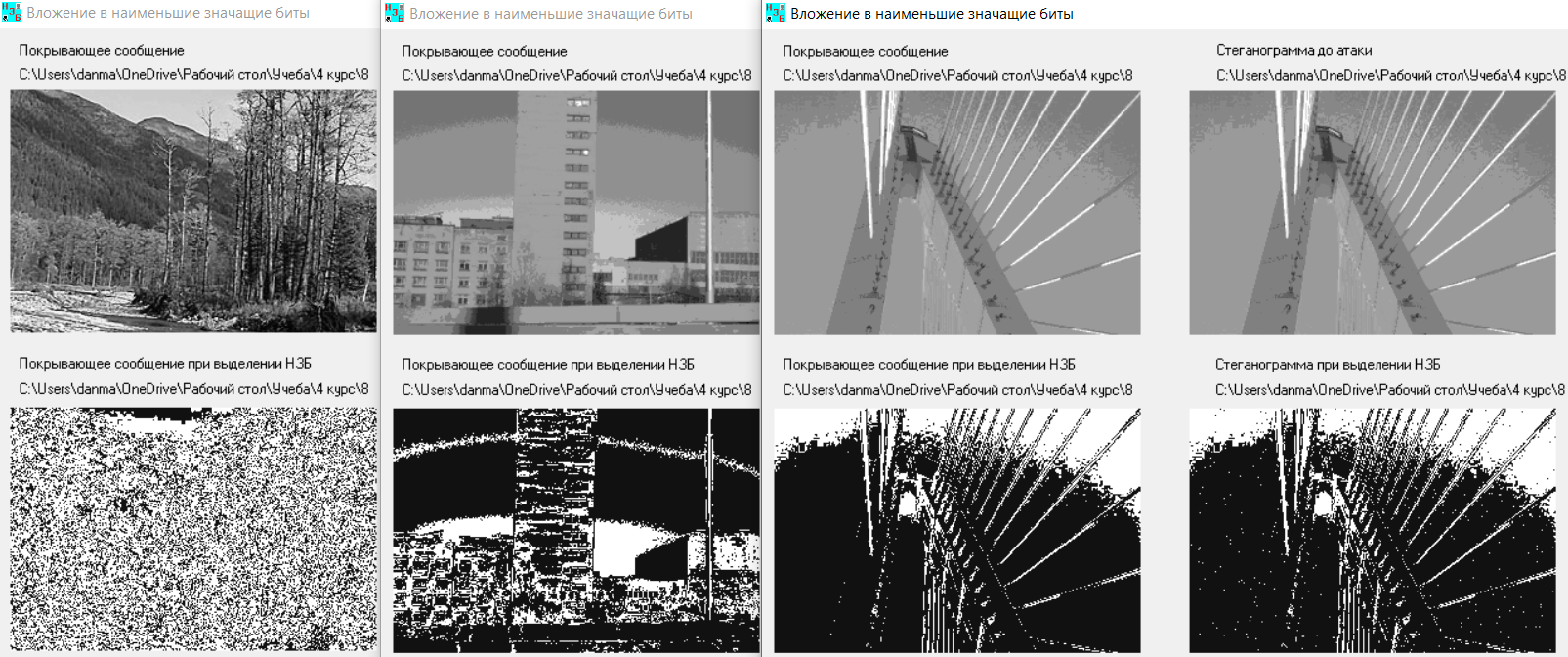


|  |  |  |
| --- | --- | --- |
| Вероятность вложения | Атака без учета корреляции пикселей | Атака с учетом корреляции пикселей |
| Без вложения | 60000 | -0,0 |
| 100% | 1158 | 40.539330 |
| 50% | 16385 | 36.343384 |
| 10% | 48980 | 8.333019 |
| 5% | 54367 | 4.112406 |
| 2% | 57481 | 2.084060 |

Таблица данных статистических атак

В качестве примера рассмотрим три различных изображения при тех же вероятностях вложения.

Вероятность вложения 1%



Статистическая атака при вероятностях вложения: 1%, 0.1%, 0.05%, 0.01%, 1 двоичный символ.

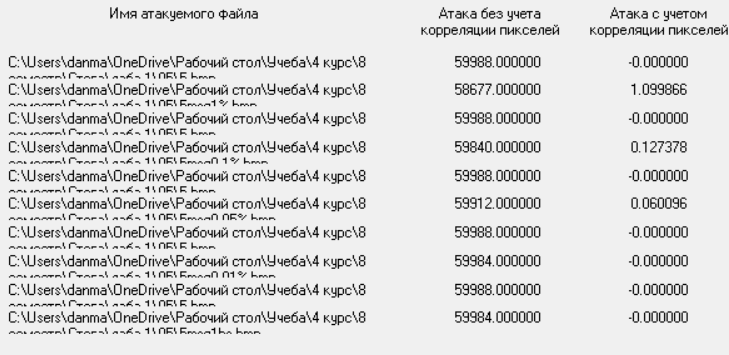
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Изображение 1 | | Изображение 2 | | Изображение 3 | |
| Вероятность вложения | Атака без учета корреляции пикселей | Атака с учетом корреляции пикселей | Атака без учета корреляции пикселей | Атака с учетом корреляции пикселей | Атака без учета корреляции пикселей | Атака с учетом корреляции пикселей |
| Без вложения | 60000 | -0.0 | 59998 | -0.0 | 60000 | -0.0 |
| 1% | 58384 | 1.040699 | 58677 | 1.099866 | 58766 | 0.985819 |
| 0,1% | 59880 | 0.046304 | 59840 | 0.127378 | 59868 | 0.111607 |
| 0,05% | 59940 | 0.115727 | 59912 | 0.060096 | 59940 | 0.039063 |
| 0,01% | 60000 | -0.0 | 59984 | -0.0 | 59992 | 0.0 |
| 1 двоичный символ | 60000 | -0.0 | 59984 | -0.0 | 59996 | 0.0 |

Таблица данных статистических атак

Изображение 1



Изображение 2



Изображение 3



Выводы: разобрали механизм вложения и извлечения информации методом наименьших значащих бит. Проанализировали эффективность различных атак по выявлению вложения, и на основе проделанной работы можно сделать вывод о том, что статистические атаки при малой вероятности вложения намного эффективнее, чем визуальные.

**Преимущества СГ-НЗБ:**  
- Просто реализуется.  
- Дает небольшие искажения ПС.  
- Выглядит секретно, поскольку НЗБ кажутся в ПС равновероятными и не зависящими от других бит и других пикселей, а w(n) тоже равновероятна и независима вследствие шифрования.  
- Дает большую скорость вложения (1 бит/пиксель).  
- Допускает обобщение, когда секретная информация вкладывается не во все, а лишь в определенные пиксели, задаваемые секретным стегоключом (правда, это понижает скорость вложения).  
  
**Недостатки СГ-НЗБ:**  
- Она не является в действительности секретной (т.е. легко обнаруживается с использованием существующих методов).  
- Секретная информация легко удаляется без искажения ПС при помощи “рандомизации” ПС.