

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

ПРАКТИЧЕСКАЯ РАБОТА №1

Стегосистема с вложением информации в наименьшие
значащие биты (СГ-НЗБ)
(тема практической работы)

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи
(код и наименование направления/специальности)

Студенты:

Громов А. А., ИКТЗ-83

(Ф.И.О., № группы)

(подпись)

Жиляков Г. В., ИКТЗ-83

(Ф.И.О., № группы)

(подпись)

Мазеин Д. С., ИКТЗ-83

(Ф.И.О., № группы)

(подпись)

Миколаени М. С., ИКТЗ-83

(Ф.И.О., № группы)

(подпись)

Научный руководитель:

К.т.н., доцент каф. ЗСС, Герлинг Е. Ю.

(учетная степень, учетное звание, ФИО)

(подпись)

Санкт-Петербург
2022

ОГЛАВЛЕНИЕ

| | |
|-----------------------------------|---|
| ЦЕЛЬ РАБОТЫ | 3 |
| ЗАДАЧА 1..... | 3 |
| ЗАДАЧА 2..... | 4 |
| ЗАДАЧА 3..... | 4 |
| ЗАДАЧА 4..... | 4 |
| ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ | 6 |
| ВЫВОДЫ..... | 9 |

ЦЕЛЬ РАБОТЫ

Целью данного практического занятия является закрепление на практике, материала, пройденного на лекции. В данном практическом занятии будут даны примеры, для практического решения задач по теме СГ-НЗБ и ± 1 НЗБ.

ЗАДАЧА 1

Предположим, что для 8-битового в каждом пикселе цифрового изображения значение яркости некоторых пикселей будут равны: 1, 7, 112, 253, 255. Какие значения яркостей этих пикселей получатся после погружения в эти пиксели двоичной информации 10110 для методов НЗБ-замены и ± 1 НЗБ?

Ответ:

10110

$$1 = 00000001 + 1 = 00000001 = 1$$

$$7 = 00000111 + 0 = 00000110 = 6$$

$$112 = 01110000 + 1 = 01110001 = 113$$

$$253 = 11111101 + 1 = 11111101 = 253$$

$$255 = 11111111 + 0 = 11111110 = 254$$

10110

$$1 = 00000001 + 1 = 00000001 = 1$$

$$7 = 00000111 + 0 = 00001000 = 8$$

$$112 = 01110000 + 1 = 01101111 = 111$$

$$253 = 11111101 + 1 = 11111101 = 253$$

$$255 = 11111111 + 0 = 11111110 = 254$$

ЗАДАЧА 2

Сколько (в среднем) бит информации можно погрузить по методу СГ-НЗБ в цифровое изображение размером 200×300 пикселей при вероятностях погружения P в каждый пиксель: 1; 0.5; 0.1; 0.01?

Ответ:

Кол-во пикселей – $200 \times 300 = 60000$

При $P = 1$ можно вложить 60000 бит информации

При $P = 0,5$ можно вложить 30000 бит информации

При $P = 0,1$ можно вложить 6000 бит информации

При $P = 0,01$ можно вложить 600 бит информации

ЗАДАЧА 3

Предположим, что на части цифрового изображения имеется прямой вертикальный контур, для которого значение яркости слева равна 16, а справа 153. Каковы будут значения яркости на этом контуре после его преобразования к двоичному виду с вложением, соответствующем НЗБ случайной (зашифрованной) двоичной последовательностью без вложения? В каком случае сохраняется контур?

Ответ:

После проведения атаки, изображение слева будет черным (так как $16 = 10000$), а справа будет белым (так как $153 = 101010011$).

В левую часть надо вложить 0, а в правую часть – 1.

ЗАДАЧА 4

Предположим, что часть гистограммы цифрового изображения имеет следующий вид:

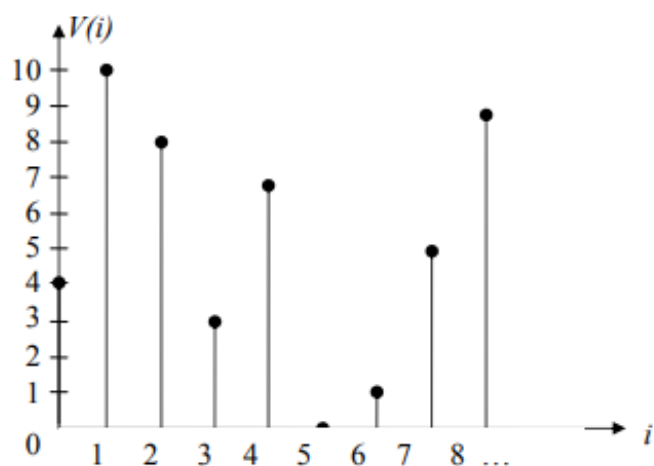


Рисунок 1 – Данная гистограмма

Какой вид будет иметь гистограмма после вложения по методу СГ-НЗБ (замещения) равновероятной и взаимонезависимой последовательности информационных бит?

Ответ:

Там надо складывать по парам начиная с 0:

0+1 их сумму делить на 2

1+2 их сумму делить на 2

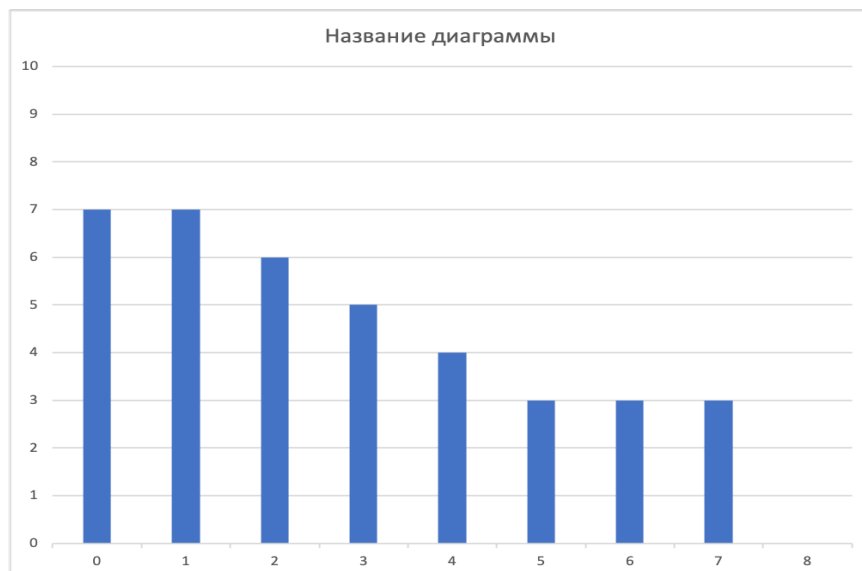


Рисунок 2 - Полученная гистограмма

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

1. Какую задачу решают стегосистемы (СГ)? - Погрузить дополнительное сообщение в ПО так, чтобы сам факт его присутствия в нем нельзя было бы обнаружить нелегитимным пользователям;
2. В какие покрывающие объекты (ПО) может вкладываться дополнительная информация? – Изображение, текстовые сообщения и данные, речевые сообщения;
3. Какими параметрами можно оценить эффективность заданий СГ? - вероятность пропуска стегосигнала, вероятность ложного обнаружения стегосигнала, вероятность ошибки бита при извлечении легитимными пользователями вложенного сообщения, качество ПО после вложения (отношение сигнал/шум или более сложные, в том числе экспертные, оценки), скорость вложения (число бит вложенного сообщения на один отсчет ПО).
4. Чем стеганография отличается от криптографии? - КР делает невозможным понимание содержание сообщения, сохраняя при этом возможность обнаружить факт ее использования (шумоподобные сигналы), а СГ утаивает сам факт погружения дополнительной информации в "невинное" сообщение.
5. Как формулируется предположение Кирхгофа для стеганографии? - нелегитимным пользователям известно о ИС-системе все, кроме стегоключа;
6. Как реализуется вложение и извлечение информации для СГ-НЗБ (НЗБ-замена, ± 1 НЗБ)? – Процедура вложения для СГ-НЗБ происходит методом псевдослучайного вложения 0 и 1 в НЗБ, а процедура извлечения происходит методом изменения четных чисел НЗБ на 0, а нечетных на 1.
7. Преимущества и недостатки СГ-НЗБ?

ПРЕИМУЩЕСТВА:

- - Просто реализуется;

- Дает небольшие искажения ПО;
- Выглядит секретно, поскольку НЗБ кажутся в ПО 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:

- Она не является в действительности секретной (т.е. легко обнаруживается с использованием существующих методов);
- Секретная информация легко удаляется без искажения ПО при помощи “рандомизации” ПО.

8. Визуальный метод обнаружения СГ-НЗБ –

Преобразовать полутоновое изображение в черно-белое по правилу:

$$C(n) = \begin{cases} \text{белое, если } c_0(n) = 1; \\ \text{черное, если } c_0(n) = 0; \end{cases}$$

Тогда, если вложения не было, то будут просматриваться некоторые контуры изображения; если было, то получим чисто шумовое поле.

9. Обнаружение СГ-НЗБ по критерию χ^2 - Критерий χ^2 – обнаружения СГ-НЗБ.

Если $\chi^2 < \alpha$, то СГ-НЗБ присутствует,

если $\chi^2 \geq \alpha$, то СГ-НЗБ отсутствует.

Вероятность пропуска СГ можно рассчитать, как

$$P_m \leq \int_{\alpha}^{\infty} \frac{1}{2^{\frac{k-1}{2}} \cdot \Gamma(\frac{k-1}{2})} x^{-\frac{k-1}{2}} e^{-\frac{x}{2}} dx$$

10. Обнаружение СГ-НЗБ по методу парно-выборочного стегоанализа. –

Атака с использованием статистики 2-го порядка, если ввести особые обозначения, тогда оценка вероятности p вложения бита в СГ-НЗБ

может быть найдена как наименьший вещественный корень квадратного уравнения:

$$\frac{(2C_0 - C_1)P^2}{4} - \frac{(2D_0 - D_2 + 2Y - 2X)P}{2} + Y - X = 0$$

при условии, что $2C_0 > C_1$.

ВЫВОДЫ

В данной практической работе, результаты которой представлены выше, мы закрепили материал, пройденный по теме СГ-НЗБ и ± 1 НЗБ. Научились погружать двоичную информацию в НЗБ, научились рассчитывать количество вкладываемой информации в зависимости от вероятности вложения P , а также при помощи параметра яркости и при помощи гистограмм научились понимать, где была вложена информация.