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 №6

Стегосистема для каналов с шумом (СГ-Ш)
(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.
(ученая степень, ученое звание, ФИО)

_____
(подпись)

Санкт-Петербург
2022

ОГЛАВЛЕНИЕ

ЦЕЛЬ РАБОТЫ

Целью данного практического занятия является закрепление на практике, материала, пройденного на лекции. В данном практическом занятии будут даны примеры,

ЗАДАЧА 1

Пусть максимальное количество допустимых для вложения бит m обеспечения необнаруживаемости СГ, соответствующей относительной энтропии D=0,1 и вероятности ошибки извлечения бита $P_e = 10^{-3}$ при количестве отсчетов $N = 10^7$ и вероятности ошибки юита в ДСК $P_0 = 0{,}01$

Указание. Можно воспользоваться следующими соотношениями [7]:

$$P_e \le \left[(2\sqrt{P_0(1-P_0)} - 1)P_w + 1 \right]^{N/m},$$

где P_w – вероятность единицы в псевдослучайной вкладываемой последовательности.

Ответ:

Рассчитываем P_1

$$D = N\left(P_0 \log \frac{P_0}{P_1} + (1-P_0)\log \frac{1-P_0}{1-P_1} \right),$$

$$0{,}1 = 10^7 \left(0{,}01 \log\left(\frac{0{,}01}{P_1}\right) + 0{,}99 \log\left(\frac{0{,}99}{1 - P_1}\right)\right)$$

$$P_1 = 0{,}010021$$

$$P_1 = P_0(1-P_w) + P_w(1-P_0).$$

$$0{,}010021 = 0{,}01(1 - P_w) + P_w(1 - 0{,}01)$$

$$P_w = \frac{3}{140000} = 2{,}14286 \times 10^{-5}$$

$$10^{-3} = \left[\left(2\sqrt{0{,}01(1 - 0{,}01)} - 1\right) \times 2{,}14286 \times 10^{-5} + 1\right]^{10^7/m}$$

m=24,35117

ЗАДАЧА 2

Найти максимальное количество допустимых для вложения бит m для обеспечения необнаруживаемости СГ, соответствующей относительной энтропии D=0,1 при количестве отсчетов $N = 10^7$ и требованием к вероятности ошибки при извлечении бита $P_e \leq 10^{-4}$.

Указание. Можно воспользоваться следующим соотношением [1]:

$$P_e \leq Q\left(1{,}29\sqrt{\frac{(ND)^{1/2}}{m}}\right)$$

Ответ:

$$10^{-4} = e^{\frac{\left(1{,}29\sqrt{\frac{(10^7 \times 0{,}1)^{\frac{1}{2}}}{m}}\right)^2}{2}},$$

отсюда – m = 90,33868

Какое отношение мощностей ПО и вложение требуется в этом случае? Допустимо ли оно при цифровой реализации процедуры вложения?

$$\eta_w = 0{,}6\sqrt{\frac{N}{D}}. \qquad 0{,}6\sqrt{\frac{10^7}{0{,}1}} = 6000$$

Нет, такое соотношение мощности к вложению не допустимо для цифровой реализации.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

1. Что означает понятие СГ в каналах с шумом?

СГ в каналах с шумом – это задача маскировки скрытого сообщения под шум канала.

2. В чем состоит задача обнаружения в каналах с шумом?

Отличить, присутствует ли только наложение шума канала, или суммы шума канала и стегосигнала.

3. Может ли быть известен стегоаналитику покрывающий объект в случае сценария канала с шумом?

Да, может. При этом секретность СГС не пострадает.

4. Описать две основные модели каналов с шумом, использующих для оценки эффективности СГ-Ш.

- Двоичный симметричный канал без памяти (BSC) – в данную модель калана с шумом можно надежно и секретно погружать ограниченное количество бит.
- Гауссовский канал с белым шумом – в данную модель канала с шумом можно погрузить надежно и секретно любое количество бит, однако, скорость передачи будет стремиться к нулю при стремлении к бесконечности количества отсчетов.

5. Почему целесообразно использовать СГ с распределенным вложением (с вложением, рассредоточенны м во времени)

Основное преимущество данной стегосистемы, заключается в том, что вложенное сообщение не удается обнаружить визуальными, аудиальными и статистическими методам и стегоанализа.

6. Скорость вложения информации для СГ-Ш.

Скорость вложения для BSC прямо пропорциональн о количеству отсчетов. Для Гауссовского канала с белым шумом обратно пропорционально количеству отсчетов.

ВЫВОДЫ

В данной практической работе, результаты которой представлены выше, мы закрепили материал, пройденный по теме стегосистема для каналов с шумом.