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 №3

Стегосистема, использующая широкополосные сигналы, формируемые по секретному стегоключу (СГ-ШПС)   
*(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)*

ОГЛАВЛЕНИЕ

[ЦЕЛЬ РАБОТЫ 3](#_Toc99006715)

[ЗАДАЧА 1 3](#_Toc99006716)

[ЗАДАЧА 2 4](#_Toc99006717)

[ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ 6](#_Toc99006718)

[ВЫВОДЫ 7](#_Toc99006719)

# 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-ШПС.

# ЗАДАЧА 1

Рассчитать вероятность ошибки извлечения биты информации информированным и слепым декодером, если СГ-ШПС имеет следующие параметры: дисперсия (ПО-изображение) , глубина погружения , дисперсия шума при атаке , количество пикселей, в которые погружается один бит информации . Во сколько раз нужно увеличить количество пикселей *N*, в которые погружается 1 бит информации, чтобы для слепого декодера получить при извлечении такую же вероятность ошибки, как и для информированного декодера? Указание. При расчетах можно использовать следующую верхнюю границу для функции

Ответ:

Возьмём формулу отношение сигнал/шум после погружения WM:

Возьмём формулу отношение сигнал/шум после атаки:

Подставим эти значения в данную формулу:

но, типичным является случай, когда

Тогда для предыдущей формулы получаем:

Для информированного декодера расчет происходит по следующей формуле:

,

где

Рассчитаем количество пикселей, необходимое для выполнения :

Ответ: кол-во пикселей нужно увеличить в 14 раз.

# ЗАДАЧА 2

Предположим, что, для, обнаружение СГ-ШПС, используется статистика [1]:

,

где N – общее количество пикселей изображения,

Причем при вложении информации используется модифицированный метод СГ-ШПС:

*,*

где .

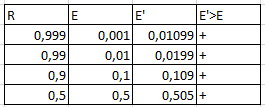
Требуется рассчитать среднее значение этой статистики при отсутствии вложения информации [1]:

и при наличии вложения

где – коэффициент корреляции между смежными пикселями покрывающего изображения.

Расчет производить при выборе следующих параметров = 0,999; 0,99; 0,9; 0,5, . Сделать вывод о возможности (или нет) обнаружения СГ-ШПС по данной статистике.

Ответ:



Следовательно, условие выполняется, обнаружение возможно.

# ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

1. Почему СГ-НЗБ не устойчива к атаке удаления вложений информации даже при невозможности обнаружения вложения?

Легко удаляется без искажения ПО, при помощи “рандомизации” ПО.

1. Как выполняется вложение информации в СГ-ШПС?

Вложение происходит в два прохода: первый – по псевдослучайному пути, определяемому стегоключом (паролем), как в Jsteg, а второй – с изменением коэффициентов, не затронутых первым проходом, с целью приближения гистограммы СГ-изображения к гистограмме ПО, что затрудняет *χ2*-атаку.

1. Что такое информированный и слепой декодер?

Информированный знает о ПС, а слепой нет.

1. Как выполняется извлечение информации информированным и слепым декодером?

Информированный декодер принимает решение о наличии бита, выполняя сравнение ПО и стеганограммы. Слепой декодер выполняет сравнение стеганограммы со средним значением ПО.

1. Как зависит вероятности ошибки при извлечении информации в случае информированного и слепого декодера от параметров СГШПС и атаки?

Вероятность ошибки уменьшается при увеличении количества пикселей N и при увеличении глубины погружения. При увеличении остальных параметров она увеличивается.

1. Каким образом осуществляется обнаружение СГ-ШПС?

Одномерная статистика, статистика второго порядка, использование критерия , ПВА, подсчет нулей в гистограмме, статистика суммы квадратов разностей яркостей соседних пикселей

# ВЫВОДЫ

В данной практической работе, результаты которой представлены выше, мы закрепили материал, пройденный по теме стегосистемы, используемые метод широкополосных сигналы. Научились рассчитывать вероятность ошибки при извлечении информации информированным и слепым декодером, а также вручную обнаруживать стегосистемы используемые широкополосные сигналы.