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)

Санкт-Петербург
2022

ОГЛАВЛЕНИЕ

ЦЕЛЬ РАБОТЫ 3

ЗАДАЧА 1 3

ЗАДАЧА 2 4

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ 6

ВЫВОДЫ 7

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) $\sigma_c^2 = 350$, глубина погружения $\alpha = 5$, дисперсия шума при атаке $\sigma_\varepsilon^2 = 25$, количество пикселей, в которые погружается один бит информации $N = 5$. 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 $Q(x) \leq e^{-\frac{x^2}{2}}$

Ответ:

Возьмём формулу отношение сигнал/шум после погружения WM:

$$\eta_w = \frac{\sigma_c^2}{\alpha^2} = 14$$

Возьмём формулу отношение сигнал/шум после атаки:

$$\eta_\alpha = \frac{\sigma_c^2}{\alpha^2 + \sigma_\varepsilon^2} = 7$$

Подставим эти значения в данную формулу:

$$p = Q(\sqrt{N \cdot \eta_\alpha / (\eta_\alpha \eta_w + \eta_w - \eta_\alpha)})$$

но, типичным является случай, когда $\eta_w \geq \eta_\alpha >> 1$

Тогда для предыдущей формулы получаем:

$$p = Q\left(\sqrt{\frac{N}{\eta_w}}\right) = 0{,}8367 - \text{слепой декодер}$$

Для информированного декодера расчет происходит по следующей формуле:

$$p' = Q\left(\frac{\alpha\sqrt{N'}}{\sigma_\varepsilon}\right) = Q\left(\sqrt{\frac{N'}{(\eta-1)}}\right),$$

где $\eta = \eta_w/\eta_\alpha$

$$\text{p}' = 0{,}082 - \text{информированный декодер}$$

Рассчитаем количество пикселей, необходимое для выполнения $p = p'$:

$$\frac{N}{\eta_w} = \frac{N'}{(\eta-1)} => \frac{N}{N'} = \frac{\eta_w}{(\eta-1)} => \frac{N}{N'} = 14$$

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

ЗАДАЧА 2

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

$$\Gamma = \frac{1}{2N\sigma_c^2}\sum_{n=1}^{N}(C(n+1) - C(n))^2,$$

где N – общее количество пикселей изображения,

$$\sigma_c^2 = Var\{C(n)\}$$

Причем при вложении информации используется модифицированный метод СГ-ШПС:

$$C_w(n) = \beta C(n) + \alpha(-1)^b\pi(n), n = 1,2,\dots,N,$$

где $\beta = \sqrt{1 - \frac{\alpha^2}{\sigma_c^2}}$.

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

$$E\{\Gamma\} = 1 - R_c(n, n+1)$$

и при наличии вложения

$$E\{\Gamma\} = 1 - \beta^2 R(n, n+1)$$

где $R(n, n+1)$ – коэффициент корреляции между смежными пикселями покрывающего изображения.

Расчет производить при выборе следующих параметров $R(n, n+1)$ = 0,999; 0,99; 0,9; 0,5, $\alpha = 5, \sigma_c^2 = 2500$. Сделать вывод о возможности (или нет) обнаружения СГ-ШПС по данной статистике.

Ответ:

R	E	E'	E'>E
0,999	0,001	0,01099	+
0,99	0,01	0,0199	+
0,9	0,1	0,109	+
0,5	0,5	0,505	+

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.

2. 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 χ^2-атаку.

3. Что такое информированный и слепой декодер?

Информированный знает о ПС, а слепой нет.

4. 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.

5. 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.

6. Каким образом осуществляется обнаружение СГ-ШПС?

Одномерная статистика, статистика второго порядка, использование критерия χ^2, 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.