МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МЕТОДИЧНІ ВКАЗІВКИ

до контрольних завдань з дисципліни

“СТЕГАНОГРАФІЧНІ СИСТЕМИ”

для студентів усіх форм навчання
спеціальності 125 «Кібербезпека»,
спеціалізації «Безпека інформаційних і комунікаційних систем»

Електронне видання

ЗАТВЕРДЖЕНО
кафедрою БІТ
Протокол № 1 від 29.08.2017

ХАРКІВ 2017

Методичні вказівки до контрольних завдань з дисципліни “Програмування”. Для студентів усіх форм навчання спеціальності 125 «Кібербезпека», спеціалізація «Безпека інформаційних і комунікаційних систем»[Електронне видання] /Упорядник О.І. Федюшин. - Харків: ХНУРЕ, 2017. - 15 с.

Упорядник О.І. Федюшин

Рецензент О.Качко, професор каф. ПЗЕОМ

ЗМІСТ

ВИМОГИ ДО ВИКОНАННЯ ТА ОФОРМЛЕННЯ КОНТРОЛЬНОЇ РОБОТИ

Контрольна робота є засобом перевірки правильності засвоєння студентами основних положень дисципліни, що вивчається, при самостійній підготовці.

На титульному аркуші контрольної роботи необхідно вказати: наіменування кафедри, назву дисципліни, курс, номер контрольної роботи, свій шифр, шифр групи, прізвище, ім'я та по батькові (повністю).

Контрольна робота виконується на комп'ютері та роздруковується на принтері на аркушах формату А4..

Номера завдань контрольної роботи вибираються відповідно до двох останніх цифр в журналі групи.

КОНТРОЛЬНА РОБОТА №1. Приховування даних в області зображень

Практичне завдання № 1

Виконайте приховування одного біту повідомлення у канал синього кольору зображення за допомогою методу Куттера-Джордана-Боссена (методу «хреста»). Вихідні данні: піксель, в який відбувається приховування інформації, задано значеннями яскравості кольорів R = 100, G =120, B = 194. Відносна кількість енергії приховування дорівнює 0,1. На скільки збільшиться рівень внесеної похибки при підвищенні цього показника в двічі?

Практичне завдання № 2

Виконайте двовимірне пряме перетворення Фур'є (пряме дискретно-косинусне перетворення) над блоком:

$$\begin{pmatrix} 189 & 186 & 175 \\ 195 & 195 & 183 \\ 203 & 197 & 194 \end{pmatrix}.$$

Виконайте загрублення із порогом P = 10. Поясніть фізичний смисл низькочастотних, середньочастотних та високочастотних областей масиву компонентів дискретно-косинусного перетворення. В яку область найбільш доцільно вбудовувати дані для стеганографічного приховування повідомлення?

Практичне завдання № 3

Виконайте декодування одного біту повідомлення у фрагменті контейнеру за допомогою методу Коха-Жао. Позиції компонент дискретно-косинусного перетворення, що модифіковані при вбудовуванні, мають координати (0, 4) та (1, 3). Фрагмент контейнера:

$$\begin{pmatrix} -2048 & 1866 & -34 & 181 & 78 \\ 795 & 195 & -83 & -55 & 15 \\ -95 & 97 & 75 & 18 & 0 \\ 21 & -20 & -11 & 9 & 3 \\ 34 & 17 & 0 & -2 & 0 \end{pmatrix}.$$

Яким чином можна покращити цей метод з точки зору зменшення

перешкод, що уносяться при модифікації?

Практичне завдання № 4

Виконайте приховування одного біту m = 1 повідомлення у фрагменті контейнеру за допомогою методу Коха-Жао при значенні порогу P = 10. Як зміняться коефіцієнти дискретно-косинусного перетворення, якщо значення інформаційного біту буде іншим, тобто при m = 1? Позиції компонент дискретно-косинусного перетворення, що потрібно модифікувати при вбудовуванні мають координати (0, 4) та (1, 3). Фрагмент контейнера:

$$\begin{pmatrix} -2048 & 1866 & -34 & 181 & 78 \\ 795 & 195 & -83 & -55 & 15 \\ -95 & 97 & 75 & 18 & 0 \\ 21 & -20 & -11 & 9 & 3 \\ 34 & 17 & 0 & -2 & 0 \end{pmatrix}.$$

Яким чином можна покращити цей метод з точки зору збільшення ймовірності правильного вилучення повідомлення на приймальній стороні?

Практичне завдання № 5

Виконайте приховування трьох бітів m = 1, 0, 1 повідомлення у фрагменті контейнеру за допомогою методу Хсу-Ву при значенні порогу P = 10. Позиції компонент дискретно-косинусного перетворення, що потрібно модифікувати при вбудовуванні мають координати (0, 4), (4,0) та (1, 3). Базовий коефіцієнт має координати (2, 2). Фрагмент контейнера:

$$\begin{pmatrix} -2048 & 1866 & -34 & 181 & 78 \\ 795 & 195 & -83 & -55 & 15 \\ -95 & 97 & 75 & 18 & 0 \\ 21 & -20 & -11 & 9 & 3 \\ 34 & 17 & 0 & -2 & 0 \end{pmatrix}.$$

До чого призведе підвищення порогу P вдвічі?

Практичне завдання № 6

Виконайте вилучення трьох бітів повідомлення із фрагмента контейнеру

за допомогою методу Хсу-Ву при значенні порогу P = 10. Позиції компонент дискретно-косинусного перетворення, що були модифіковані при вбудовуванні, мають координати (0, 4), (4,0) та (1, 3). Базовий коефіцієнт має координати (2, 2). Фрагмент контейнера:

$$\begin{pmatrix} -2048 & 1866 & -34 & 181 & 78 \\ 795 & 195 & -83 & -55 & 15 \\ -95 & 97 & 75 & 18 & 0 \\ 21 & -20 & -11 & 9 & 3 \\ 34 & 17 & 0 & -2 & 0 \end{pmatrix}.$$

Які біти повідомлення будуть вилучені із цього ж фрагменту контейнера, якщо базовий коефіцієнт буде мати координати (3, 1)?

Практичне завдання № 7

Виконайте декодування п’яти бітів повідомлення з фрагменту контейнеру за допомогою методу блочного приховування. Вихідні данні: блоки відповідають строкам матриці контейнера:

$$\begin{pmatrix} 189 & 186 & 180 & 181 & 178 \\ 195 & 195 & 183 & 180 & 175 \\ 203 & 197 & 215 & 186 & 182 \\ 210 & 203 & 201 & 191 & 193 \\ 221 & 217 & 211 & 205 & 202 \end{pmatrix}.$$

До яких атак найбільш вразливий метод блочного приховування? Вкажіть, до якого методу спроститься метод блочного приховування при розмірі блоку в один символ. Поясніть фізичний смисл цього спрощення.

Практичне завдання № 8

Виконайте приховування п’яти бітів повідомлення m = {1, 0, 1, 1, 0} у фрагмент контейнеру за допомогою методу блочного приховування. Вихідні данні: блоки відповідають стовпцям матриці контейнера:

$$\begin{pmatrix} 189 & 186 & 180 & 181 & 178 \\ 195 & 195 & 183 & 180 & 175 \\ 203 & 197 & 215 & 186 & 182 \\ 210 & 203 & 201 & 191 & 193 \\ 221 & 217 & 211 & 205 & 202 \end{pmatrix}.$$

На які показники ефективності стеганостистеми впливає розмір блоків контейнеру?

Практичне завдання № 9

Виконайте декодування одного символу у форматі ASCII за допомогою методу квантування. Модифікація виконувалася почергово із значеннями першого і другого та третього і четвертого стовпців контейнеру:

$$\begin{pmatrix} 189 & 186 & 180 & 181 \\ 195 & 195 & 183 & 180 \\ 203 & 197 & 191 & 186 \\ 210 & 203 & 201 & 197 \end{pmatrix}.$$

Таємний ключ (таблиця квантування) має вигляд:

	7	6	5	4	3	2	1								
i															

Яку властивість зорової системи людини використовує цей метод? До яких атак зловмисника він має стійкість?

Практичне завдання № 10

Виконайте приховування чотирьох бітів повідомлення m = {1, 0, 1, 1} за допомогою методу квантування. Модифікацію контейнеру проведіть шляхом кодування міжпіксельної різниці третього і четвертого стовпців контейнеру:

$$\begin{pmatrix} 189 & 186 & 180 & 181 \\ 195 & 195 & 183 & 180 \\ 203 & 197 & 191 & 186 \\ 210 & 203 & 201 & 197 \end{pmatrix}.$$

Таємний ключ (таблиця квантування) має вигляд:

	7	6	5	4	3	2	1								
i															

Яка атака найбільш ефективна проти методу квантування? Як позбавитися цієї вразливості?

Практичне завдання № 11

Масив компонент дискретно-косинусного перетворення має вигляд:

$$\begin{pmatrix} 2785 & -251 & 24 \\ 334 & -15 & -3 \\ -16 & 4 & 1 \end{pmatrix}.$$

Обґрунтуйте параметри стеганографічного методу Коха-Жао при врахуванні можливого використання зловмисником атаки стиском у форматі jpeg із показником загрублення P = 10. Виконайте вбудовування одного біту повідомлення методом Коха-Жао у середньочастотній області масиву компонент. Що відбудеться, якщо зловмисник збільшить втричі показник P?

Практичне завдання № 12

Розрахуйте максимальну та мінімальну довжину повідомлення, яке можна приховати методом псевдовипадкового інтервалу, якщо контейнер має розміри 100x200 пікселей у форматі *.bmp (24 біта на піксель) а інтервал приховування лежить в межах 1..128. Поясніть основні переваги цього методу у порівнянні із методом модифікації найменш значущого біту. Яка максимальна абсолютна різниця значень яскравості пустого та заповненого контейнерів для цих методів?

Практичне завдання № 13

За допомогою методу модифікації найменш значущого біту приховайте повідомлення m = {1, 0, 0, 1, 0, 1, 1, 0, 1} у фрагмент контейнеру:

$$\begin{pmatrix} 207 & 221 & 224 \\ 195 & 223 & 225 \\ 199 & 223 & 221 \end{pmatrix}.$$

Розрахуйте максимальну абсолютну різницю та середню абсолютну різницю пустого та заповненого контейнерів.

Практичне завдання № 14

За допомогою методу модифікації найменш значущого біту вилучите інформаційне повідомлення довжиною дев'ять бітів з фрагменту контейнеру:

$$\begin{pmatrix} 207 & 221 & 224 \\ 195 & 223 & 225 \\ 199 & 223 & 221 \end{pmatrix}.$$

Розрахуйте максимальну абсолютну різницю та середню абсолютну різницю пустого та заповненого контейнерів.

Практичне завдання № 15

За допомогою методу псевдовипадкової перестановки приховайте повідомлення m = {1, 0, 0, 1} у фрагмент контейнеру:

$$\begin{pmatrix} 207 & 221 \\ 195 & 223 \end{pmatrix}.$$

Таємний ключ задано перестановочною матрицею:

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Скільки варіантів таємного ключа для цього розміру матриці перестановок? Чи відрізняється пропускна здатність стеганографічних каналів, які організовано цим методом та методом LSB?

Практичне завдання № 16

За допомогою методу псевдовипадкової перестановки вилучити чотири біти інформаційного повідомлення з фрагменту контейнера:

$$\begin{pmatrix} 207 & 221 \\ 195 & 223 \end{pmatrix}.$$

Таємний ключ задано перестановочною матрицею:

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Як залежить стійкість методу від розміру перестановочної матриці? Чим можна замінити перестановочне перетворення?

Практичне завдання № 17

Виконайте двовимірне пряме перетворення Фур'є (пряме дискретно-косинусне перетворення) над блоком:

$$\begin{pmatrix} 189 & 186 & 189 \\ 195 & 195 & 183 \\ 210 & 183 & 186 \end{pmatrix}.$$

Змініть значення одного із компонентів у середньочастотній області компонент та виконайте зворотне перетворення Фур'є. З урахуванням отриманого результату поясніть вразливість методів приховування у просторовій області зображення до атаки стиском зображення стиском у форматі jpeg.

Практичне завдання № 18

Виконайте декодування одного біту повідомлення у фрагмент контейнеру за допомогою методу Куттера-Джордана-Боссена (методу «хреста»). Вихідні данні: розмір «хреста» - 2 значення зверху, справа, зліва та знизу від значення (інтенсивність дорівнює 215), що модифікується. Фрагмент контейнера:

$$\begin{pmatrix} 189 & 186 & 180 & 181 & 178 \\ 195 & 195 & 183 & 180 & 175 \\ 203 & 197 & 215 & 186 & 182 \\ 210 & 203 & 201 & 191 & 193 \\ 221 & 217 & 211 & 205 & 202 \end{pmatrix}.$$

Вкажіть основні недоліки методу «хреста». Яким чином їх можна

позбутися?

Практичне завдання № 19

За результатами дискретного перетворення Фур'є фрагменту аудіоконтейнеру отримано набір комплексних амплітуд:

(-35+60i), (15-20i), (-25-45i), (60+15i).

Застосовуючи ці значення вилучите чотири біти інформаційного повідомлення методом фазового кодування.

Практичне завдання № 20

За результатами дискретного перетворення Фур'є фрагменту аудіоконтейнеру отримано набір комплексних амплітуд:

(-65+10i), (5-25i), (-15-15i), (6+15i).

Застосовуючи ці значення вилучите чотири біти інформаційного повідомлення методом фазового кодування.

Практичне завдання № 21

Фрагмент дискретних відліків моно аудіосигналу має вигляд:

(33, 115, 245, 145, 64, 32, 78, 111).

Застосовуючи метод кодування луна сигналів приховайте два біти (1, 0) у цей фрагмент (кожен біт у чотири послідовні відліки). Перший луна сигнал (для кодування «1») має затримку 1 відлік та затухання у 2 рази, другий луна сигнал (для кодування «0») має затримку 2 відліки і затухання у 3 рази. Які значення будуть мати дискретні відлікі заповненого аудіоконтейнеру?

Практичне завдання № 22

Фрагмент дискретних відліків моно аудіосигналу має вигляд:

(134, 115, 45, 45, 64, 132, 178, 111).

Застосовуючи метод кодування луна сигналів приховайте два біти (0, 1) у цей фрагмент (кожен біт у чотири послідовні відліки). Перший луна сигнал (для кодування «1») має затримку 1 відлік та затухання у 2 рази, другий луна сигнал (для кодування «0») має затримку 2 відліки і затухання у 3 рази. Які значення будуть мати дискретні відлікі заповненого аудіоконтейнеру?

Практичне завдання № 23

Виконайте вилучення інформаційних бітів з наступного прикладу лінгвістичної стеганограми:

«П'ять підземних поштовхів зареєстровано за добу на півдні Республіки Алтай. Сила землетрусів складала від 2,2 до 3,1 балів за шпалою Ріхтера, повідомили на Акташській сейсмічній станції сьогодні пополудні.»

Інформацію приховано семантичним методом, групи відносних синонімів в тексті подано наступним правилом:

0. за 24 години 1 за добу
0. Алтай 1. Республіка Алтай
0. землетруси 1. підземних поштовхів
0. дорівнювати 1. складати
0. проінформувати 1. повідомити
0. сейсмічна станція 1 сейсмостанстанція
0. у другу половину дня 1. Пополудні

Практичне завдання № 24

Приховайте інформаційну послідовність (10110010) із використанням лінгвістичного стеганоперетворення у наступне речення:

«П'ять підземних поштовхів зареєстровано за добу на півдні Республіки Алтай. Сила землетрусів складала від 2,2 до 3,1 балів за шкалою Ріхтера, повідомили на Акташській сейсмічній станції сьогодні пополудні.»

Інформацію треба приховати семантичним методом, групи відносних синонімів в тексті подано наступним правилом:

0. за 24 години 1 за добу
0. Алтай 1. Республіка Алтай
0. землетруси 1. підземних поштовхів
0. дорівнювати 1. складати
0. проінформувати 1. повідомити
0. сейсмічна станція 1 сейсмостанстанція
0. у другу половину дня 1. пополудні

Практичне завдання № 25

Виконайте вилучення одного байту інформаційного повідомлення з наступного фрагменту лінгвістичної стеганограми:

«Сьогодні в мене свято, мій День Народження! Прийшли родичі, друзі і знайомі. Ми пили вино, їли торт, жартували. Було все: і танці, і конкурси, і навіть феєрверк! В вечорі, коли вже було темно і гості пішли, ми ще довго були під враженнями і сиділи разом. Потім ми ще пили чай, мріяли про майбутнє. Я люблю такі дні, коли свято, гості, подарунки!».

Стеганограму сформовано за допомогою синтаксичного методу, таємним ключем є правило перерахування:

«1» - при перерахуванні застосовуються лише коми;

«0» - при перерахуванні можуть застосовуватися союзи «і».

Як можна збільшити пропускну здатність такої стеганосистеми? Чи можна синтаксичні методи комбінувати із іншими, наприклад з семантичними?

Електронний навчальний документ

МЕТОДИЧНІ ВКАЗІВКИ
до контрольних завдань

з дисципліни
СТЕГАНОГРАФІЧНІ СИСТЕМИ

для студентів усіх форм навчання
спеціальності 125 Кібербезпека
Освітня програма
"Безпека інформаційних та комунікаційних систем”

Упорядник Федюшин Олександр Іванович

Відповідальний випусковий Г.З. Халімов

Авторська редакція