

Міністерство освіти і науки України
Вінницький національний технічний університет

В. В. Лукічов, В. А. Лужецький, А. С. Васюра

**МЕТОДИ ТА ЗАСОБИ
СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
НА ОСНОВІ ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ**

Монографія

Вінниця
ВНТУ
2014

УДК 004.056.55
ББК 32.97-018.2
Л84

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 9 від 24.04.2014 р.)

Рецензенти:

В. М. Дубовой, доктор технічних наук, професор

О. Г. Корченко, доктор технічних наук, професор

Лукічов, В. В.

Л84 Методи та засоби стеганографічного захисту інформації на основі вейвлет-перетворень : монографія / В. В. Лукічов, В. А. Лужецький, А. С. Васюра. – Вінниця : ВНТУ, 2014. – 160 с.
ISBN 978-966-641-572-4

В монографії розглянуто моделі і методи стеганографічного захисту інформації і визначено якості, що впливають на стійкість вбудованих даних. Наведено узагальнені моделі та методи неадаптивного й адаптивного вбудовування даних у зображення, які враховують взаємозв'язки між стеганографічними перетвореннями. На основі неадаптивної моделі вбудовування даних розроблено метод шаблонного вбудовування даних у вейвлет-коефіцієнти зображень на основі таблиці відповідності між таємними даними та значеннями шаблону, який дозволив збільшити пропускну здатність стегаканалу та забезпечити високу швидкість вбудовування.

УДК 004.056.55
ББК 32.97-018.2

ISBN 978-966-641-572-4

© В. В. Лукічов, В. А. Лужецький, А. С. Васюра, 2014

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	6
ВСТУП	7
1 МОДЕЛІ ТА МЕТОДИ СТЕГANOГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ.....	9
1.1 Види загроз безпеці інформації в комп'ютерних системах і мережах	9
1.2 Моделі стеганографічних перетворень.....	12
1.2.1 Теоретико-множинна та структурна моделі стеганографічних перетворень	12
1.2.2 Теоретико-ігрова модель стеганографічних перетворень з врахуванням активної протидії	14
1.2.3 Теоретико-ігрова модель вбудовування даних в область зображень.....	15
1.3 Методи цифрової стеганографії зображень.....	19
1.3.1 Задачі цифрової стеганографії зображень	19
1.3.2 Методи приховування даних в частотній області зображення.....	21
1.3.3 Методи шаблонного вбудовування даних на основі матричного представлення кодів Хеммінга	23
1.4 Методи стеганографічного аналізу частотної області зображень.....	28
1.4.1 Методи цільового стеганографічного аналізу частотної області зображень	28
1.4.2 Методи сліпого стеганографічного аналізу частотної області зображень	31
Висновки до розділу 1	36
2 МОДЕЛІ ТА МЕТОДИ ВБУДОВУВАННЯ ДАНИХ У ВЕЙВЛЕТ-КОЕФІЦІЄНТИ ЗОБРАЖЕНЬ	37
2.1 Узагальнені моделі та методи вбудовування даних у зображення.....	37
2.1.1 Узагальнені моделі та методи неадаптивного вбудовування даних у зображення.....	37

2.1.2 Узагальнені моделі та методи адаптивного вбудовування даних у зображення.....	40
2.1.3 Узагальнені моделі та методи витягування даних із стеганографічного зображення	43
2.2 Методи бінарної інтерпретації коефіцієнтів вейвлет-перетворення	44
2.2.1 Структура матриці коефіцієнтів вейвлет-перетворення	44
2.2.2 Метод бінарної інтерпретації вейвлет-коефіцієнтів $d = const$	46
2.2.3 Метод бінарної інтерпретації вейвлет-коефіцієнтів $d = var$	51
2.3 Оцінки допустимої ширини діапазону вбудовування для методу бінарної інтерпретації.....	54
2.4 Оцінки допустимого обсягу даних, вбудовуваних у вейвлет-коефіцієнти.....	62
Висновки до розділу 2	73
3 МЕТОДИ ШАБЛОННОГО ВБУДОВУВАННЯ ДАНИХ У ВЕЙВЛЕТ-КОЕФІЦІЄНТИ ЗОБРАЖЕНЬ	74
3.1 Метод шаблонного вбудовування даних з використанням кодів БЧХ.....	74
3.1.1 Метод шаблонного вбудовування даних на основі матричного представлення кодів БЧХ.....	75
3.1.2 Удосконалений метод шаблонного вбудовування на основі поліноміального представлення кодів БЧХ	78
3.1.3 Порівняльні оцінки методів шаблонного вбудовування на основі кодів БЧХ	79
3.2 Метод шаблонного вбудовування даних на основі запропонованої таблиці відповідності між таємними даними та значеннями шаблону	81
3.3 Критерій стеганографічної стійкості до активних атак	87
3.4 Метод адаптивного шаблонного вбудовування даних.....	97
3.4.1 Метод адаптивного вбудовування даних на основі показників вбудовування усіх блоків зображення	97
3.4.2 Оптимізація показників шаблонного вбудовування даних у блоки зображення.....	101
Висновки до розділу 3	105

4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ МЕТОДІВ ВБУДОВУВАННЯ ДАНИХ У ВЕЙВЛЕТ-КОЕФІЦІЄНТИ	106
4.1 Статистичний аналіз результатів вбудовування даних у вейвлет-коефіцієнти зображення з використанням розроблених методів бінарної інтерпретації.....	106
4.1.1 Непараметричні тести для спарених вибірок.....	106
4.1.2 Параметричні тести для спарених вибірок.....	110
4.1.3 Непараметричний тест для неспарених вибірок.....	119
4.2 Порівняльні оцінки методів бінарної інтерпретації вейвлет- коефіцієнтів на основі показників спотворень в області зображень.....	123
4.2.1 Порівняння законів розподілу спотворень пікселів зображень	123
4.2.2 Експериментальні дослідження спотворень в просторовій області зображень	128
4.2.3 Емпіричні оцінки допустимого обсягу даних, вбудованих у вейвлет-коефіцієнти.....	133
4.3 Оцінка ймовірності правильного витягування вбудованих даних.....	138
4.4 Експериментальні оцінки адаптивного методу шаблонного вбудовування даних у вейвлет-коефіцієнти зображень.....	140
4.4.1 Експериментальна оцінка параметрів функції ентропії детектування стегозображень	140
4.4.2 Експериментальна оцінка порогового параметра для методу адаптивного шаблонного вбудовування.....	143
4.5 Порівняльні характеристики методів шаблонного вбудовування даних у вейвлет-коефіцієнти зображень.....	144
Висновки до розділу 4	146
ВИСНОВКИ.....	147
ЛІТЕРАТУРА	148

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БЧХ	– код Боуза–Чоудхурі–Хоквінгхема
ДКП	– дискретне косинусне перетворення
КСМ	– комп’ютерні системи і мережі
НБ	– наймолодший біт
ЦВП	– цілочисельне вейвлет-перетворення
AD	– середня абсолютна різниця
CQ	– якість кореляції
$GSSNR$	– загальне сигма відношення сигнал–шум
$LMSE$	– середня квадратична помилка оператора Лапласа
MSE	– середня квадратична помилка
NC	– нормалізована взаємна кореляція
$PSNR$	– максимальне відношення сигнал–шум
SNR	– відношення сигнал–шум
$\lfloor x \rfloor$	– максимальне ціле число, менше x
$\ h\ _{L_1}$	– L_1 -норма вектора h

ВСТУП

Коло задач, що розв'язуються у сучасних комп'ютерних системах і мережах (КСМ), є надзвичайно широким. Однак основне призначення КСМ полягає у автоматизованому збиранні, зберіганні, обробленні та передаванні інформації. Одним з основних аспектів підвищення безпеки КСМ є забезпечення високого рівня захищеності інформації. Серед інших напрямків захисту інформації стеганографія має низку переваг, що обумовлені непомітністю її реалізації.

Стеганографія зображень є галуззю, що набула стрімкого розвитку протягом останніх років. Її ціль може бути окреслена як таємне та стійке до різноманітних перетворень приховування даних.

У розвиток стеганографії значний внесок зробили В. О. Хорошко [66–67], Г. Ф. Конахович [38], М. Є. Шелест [67], В. К. Задірака [29], Н. В. Кошкіна [29], А. В. Аграновский [1–2], В. Г. Грібунін [14], І. Н. Оков [15], М. Коста [96], К. Кашін [87], І. Кокс [97] та інші. Внесок зазначених вчених полягає в розробці та вдосконаленні методів приховування даних в зображення та аудіофайли. Проте розробка методів стеганографічного захисту інформації зазначеними вченими відбувалася без врахування взаємозв'язку вимог таємності та робастності.

Порушення таємності призводить до повної втрати стеганографічної захищеності даних в КСМ. Саме зазначена якість задає основні обмеження при застосуванні стеганографічних перетворень, що передбачають можливість пасивних атак. Забезпечення якості таємності в більшості робіт визначає можливість стеганографічного зображення (стегозображення) залишитися непоміченим, що відповідає показнику ймовірності (або ентропії) правильного детектування методами стеганографічного аналізу (стеганоаналізу) [2].

Другим важливим аспектом є вимога робастності, яка визначається ентропією таємних даних при витяганні, що відповідає пропускній здатності двійкового каналу. Така якість задає додаткові обмеження при використанні стеганографічних перетворень, що передбачають можливість активних атак [93].

Серед відомих моделей стеганографічних перетворень існують моделі, що враховують вимоги таємності [120]. Також існує низка підходів щодо моделювання, які враховують вимоги робастності [93].

Показники якостей таємності та робастності залежать від особливостей стежоконтейнера, використовуваного перетворення, методу вбудовування і т. д.

Вибір контейнера значним чином впливає на результати стеганографічного перетворення. Наприклад, факт вбудовування даних у зображення, що містять значні за розміром однотонні області, як правило, встановлюється за допомогою сучасних методів стеганоаналізу [81].

Вибір перетворення для вбудовування даних також значним чином впливає на якість таємності та робастності. Наприклад, використання більшості методів стеганографічного захисту інформації, що вбудовують дані в область зображень, приводить до незначних спотворень. Однак такі методи забезпечують невисоку стійкість до впливів з боку третьої особи. З іншого боку, використання методів вбудовування даних в частотну область зображень забезпечує меншу таємність, але значно більшу робастність порівняно з методами стеганографічного захисту інформації, що оперують з пікселями зображень [90].

Для різних методів вбудовування характерне різне співвідношення між якостями таємності та робастності за заданої пропускну здатності. Запропоновані вченими Д. Фрідріх та Д. Соукал [105] методи шаблонного вбудовування забезпечують високу таємність, однак є менш робастними порівняно з методом вбудовування даних в наймолодший біт (НБ).

Вказані особливості визначають стійкість стеганографічного захисту за умови активних атак в КСМ, що не враховано в сукупності жодною з відомих моделей стеганографічних перетворень і стеганографічних методів. Цей факт обумовлює актуальність досліджень, спрямованих на розробку методів та засобів забезпечення стеганографічної стійкості захисту інформації в КСМ до активних атак.

Розділ 1 написано В. А. Лужецьким та А. С. Васюрою, розділ 2.1 В. А. Лужецьким і В. В. Лукічовим. Основні наукові результати, викладені в розділах 2, 3 і 4, отримані під час дисертаційного дослідження В. В. Лукічовим.

1 МОДЕЛІ ТА МЕТОДИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

Процес стеганографічного захисту інформації в КСМ має низку особливостей, головною з яких є необхідність забезпечення стійкості до видів атак, що відповідають призначенню стеганографічних перетворень. На сьогоднішній день розроблено значну кількість методів стеганографічного захисту інформації в КСМ, але використання будь-якого з них має свої певні переваги та недоліки.

1.1 Види загроз безпеці інформації в комп'ютерних системах і мережах

Загроза інформаційній безпеці в КСМ реалізується, якщо КСМ вразлива і здійснюється атака на КСМ [12, 17].

Вразливість КСМ – характеристика, що робить можливим виникнення загрози. Чим вразливіша система, тим ймовірніший успіх віддаленої атаки.

Атака на КСМ – це пошук і використання супротивником вразливості системи, тобто реалізація загрози. В загальному випадку система повинна бути стійка як до випадкових, так і до зловмисних ворожих впливів [39, 55, 69].

Виділяють три основних види загроз безпеці КСМ: загрози розкриття, порушення цілісності та відмови в обслуговуванні (рис. 1.1). Загроза розкриття полягає в тому, що інформація стає відома супротивнику. У термінах комп'ютерної безпеки загроза розкриття має місце завжди, коли здійснюється доступ до деякої конфіденційної інформації, що зберігається в КСМ або передається від однієї системи до іншої [54, 65].

Порушення конфіденційності (розкриття) інформації – це перехоплення і розшифровка мережевих пакетів, тобто аналіз трафіка. Основною метою супротивника, як правило, є з'ясування паролів системи, що дозволяє віддалено звертатися до системи без додаткових заходів [43].

Загрозу порушення цілісності містить у собі будь-яка зловмисна зміна (модифікація або навіть видалення) даних, що зберігаються в КСМ або передаються з однієї системи в іншу. Зазвичай загрози розкриття піддаються більшою мірою державні структури, а загрози порушення цілісності – ділові або комерційні [31, 136].

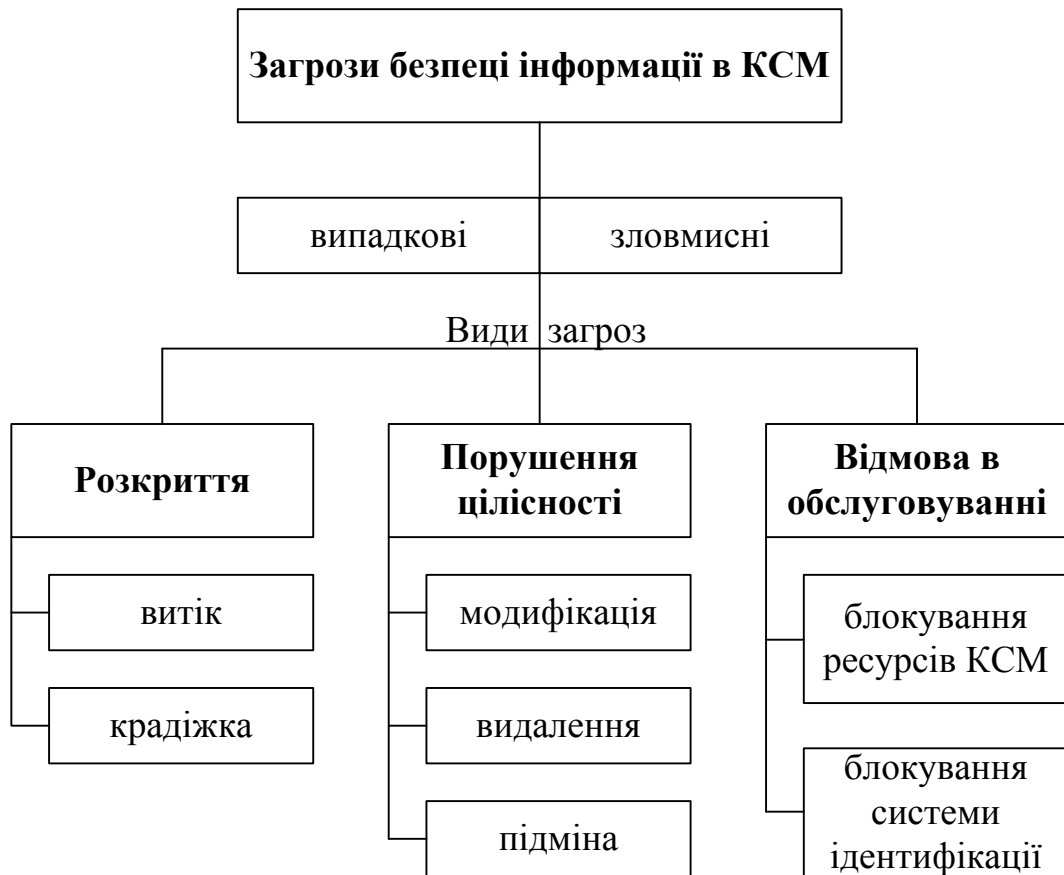


Рисунок 1.1 – Види загроз безпеці інформації в комп'ютерних системах і мережах

Загроза відмови в обслуговуванні виникає щоразу, коли в результаті певних дій блокується доступ до деякого ресурсу комп'ютерної системи. Блокування може бути постійним або викликати лише затримку запитуваного ресурсу. Запобігання загрозам безпеки інформації в КСМ реалізується за допомогою методів та засобів захисту інформації [73].

Серед методів, що використовуються для захисту інформації в КСМ, одними з найбільш поширених є методи захисних перетворень. Найбільш розповсюдженими методами захисних перетворень є криптографічні [26, 61, 100]. Ціль криптографії полягає в закритті змісту конфіденційних повідомлень [9]. На відміну від криптографічних результатів стеганографічних перетворень є приховування самого факту існування таких повідомлень [15, 67].

На рис. 1.2 наведено схеми передавання даних комп'ютерною мережею. При передаванні даних в КСМ без захисту ніякі додаткові перетворення не здійснюються, що обумовлює вразливість комп'ютерної мережі, яка побудована за таким принципом. При передаванні даних, захищених криптографічно, супротивник, аналізуючи трафік, має можливість дізнатися про сам факт передачі та блокувати канал. При передаванні даних, захищених стеганографічно, супротивнику невідомо про факт передачі захищених даних. Підтвердження цього факту вимагає проведення стеганоаналізу [80, 82, 109, 138].

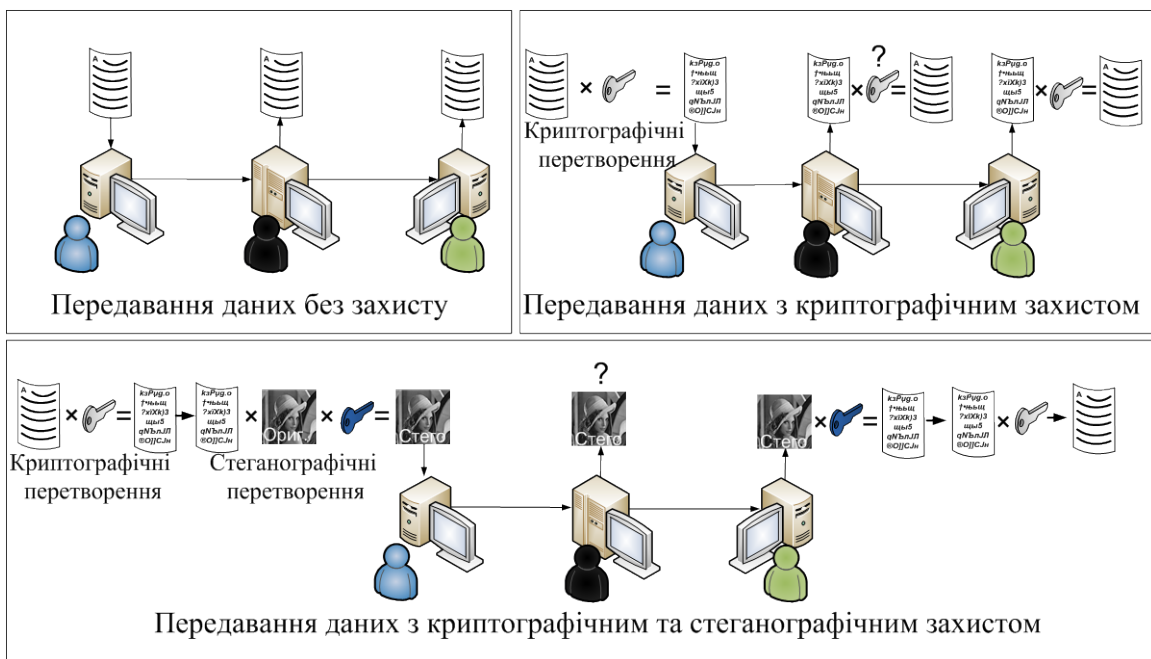


Рисунок 1.2 – Схеми передавання даних комп'ютерними мережами

Зазначені особливості дозволяють відмітити значні переваги стеганографічного захисту у порівнянні з криптографічним при реалізації політики безпеки в КСМ, що зменшує вразливість останніх [1, 20, 72, 95]. На практиці стеганографічний та криптографічний захист реалізують спільно: повідомлення перед вбудовуванням зашифровується.

Особливо популярним є напрямок цифрової стеганографії зображень, про що свідчать чисельні програмні засоби [117]. Найбільш універсальним описом процесу вбудовування даних у зображенні є математичні моделі.

1.2 Моделі стеганографічних перетворень

Опис стеганографічних перетворень за допомогою математичних моделей дозволяє пов'язати окремі компоненти, що необхідно для встановлення значень параметрів вбудовування даних з метою покращення необхідних характеристик.

1.2.1 Теоретико-множинна та структурна моделі стеганографічних перетворень. Однією з найбільш часто використовуваних математичних моделей для опису процесу вбудовування даних у зображення є теоретико-множинна модель [96, 103].

Надалі використовується $\tilde{\mathbf{I}}, \mathbf{W}, \mathbf{I}, \mathbf{D}$ – множини можливих стегоконтейнерів, ключів, контейнерів і приховуваних повідомлень, відповідно.

Контейнер – будь-які дані (файл, зображення, аудіо та ін.), призначені для приховування інформації за допомогою стеганографічного перетворення.

Стегоконтейнер – контейнер (стеготекст, стегозвук, стегозображення і т.п.), отриманий у результаті стеганографічного перетворення, що містить приховану інформацію.

Генерація стегоконтейнерів представляється таким чином:

$$F : \mathbf{I} \times \mathbf{W} \times \mathbf{D} \rightarrow \tilde{\mathbf{I}}, \quad \tilde{I} = F(I, W, D),$$

де $\tilde{I} \in \tilde{\mathbf{I}}, I \in \mathbf{I}, W \in \mathbf{W}, D \in \mathbf{D}$.

Функція F є складеною:

$$F = T \circ G,$$

де $G : \mathbf{W} \times \mathbf{D} \rightarrow \mathbf{C}$ і $T : \mathbf{I} \times \mathbf{C} \rightarrow \tilde{\mathbf{I}}$. Функція G може бути реалізована за допомогою криптографічно стійкого генератора псевдовипадкової послідовності з початкового значення W [33, 123]. Оператор T модифікує \mathbf{C} , у результаті чого отримується стегоконтейнер $\tilde{\mathbf{I}}$.

Недоліком такої теоретико-множинної моделі є неврахування проміжних етапів перетворень контейнера при вбудовуванні даних, таких, наприклад, як базисні перетворення, що широко використовую-

ються в обробці зображень, та бінарної інтерпретації отриманих коефіцієнтів базисних перетворень.

Структурна модель стеганографічних перетворень, використовувана для передачі даних за наявності як пасивного, так і активного супротивника [2, 38, 114, 140], зображена на рис. 1.3.

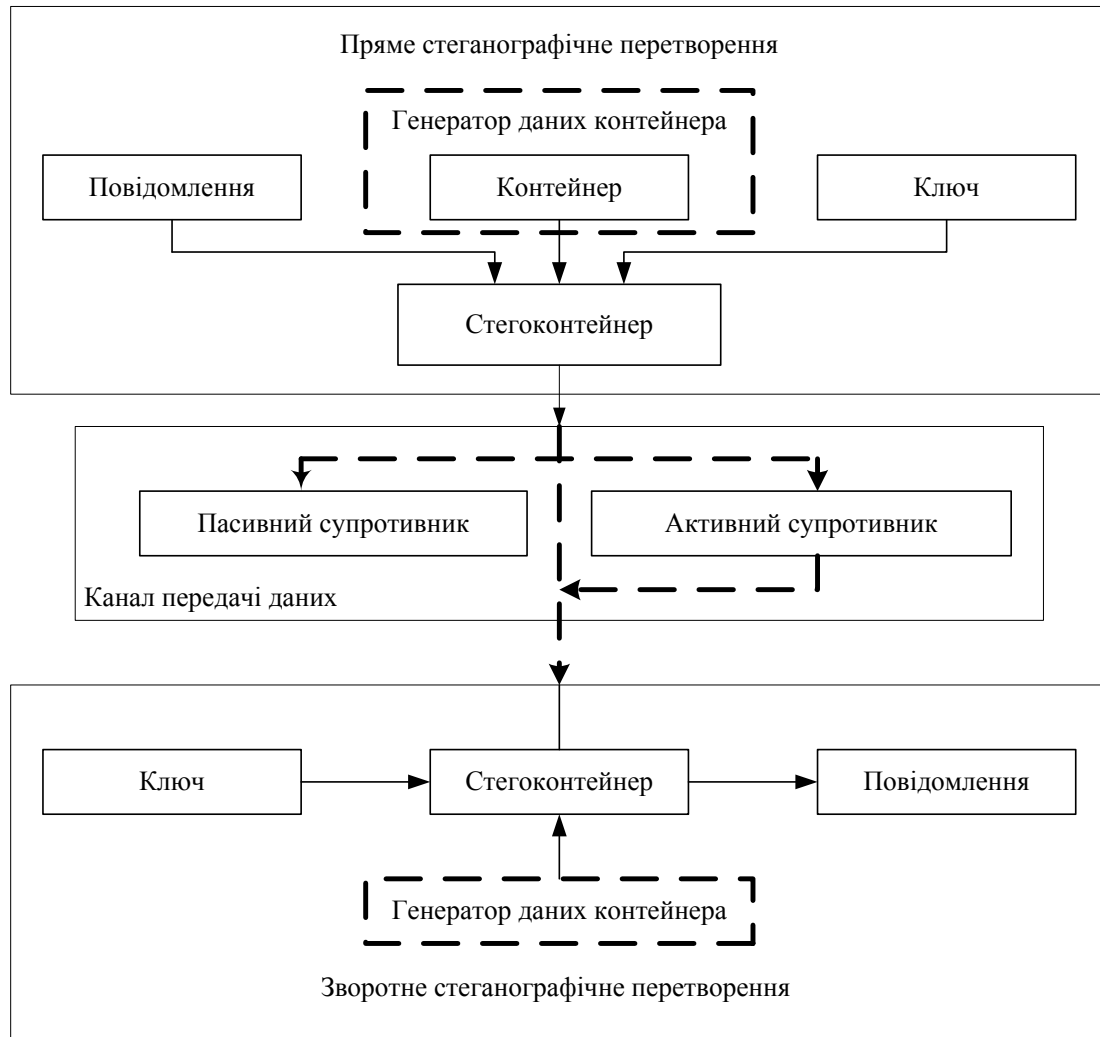


Рисунок 1.3 – Структурна модель стеганографічних перетворень

Відповідно до цієї схеми, на стороні передачі повідомлення приховується в контейнері за допомогою прямого стеганографічного перетворення. Отриманий модифікований контейнер відкритими каналах зв'язку відправляється приймальною стороною, де після його одержання, за допомогою зворотного стеганографічного перетворення, витягається вихідне повідомлення [87, 120, 145].

Завдання пасивного супротивника полягає у визначенні факту присутності в контейнері прихованих даних, при цьому припускається, що він може перехоплювати усі надіслані контейнери та аналізувати їх [29, 66, 98, 108]. Якщо пасивному супротивнику вдалося встановити факт присутності прихованого повідомлення в контейнері, він може прочитати його. Однак, як правило, перед прихованням повідомлення шифрується, і для його читання необхідне дешифрування. Активний супротивник має можливість вносити зміни в переданий по каналах зв'язку контейнер, при цьому передбачається, що не приймальна та не передавальна сторони не знають, який контейнер було змінено під час передачі. Найпростіший сценарій активного супротивника полягає у знищенні прихованої інформації без встановлення факту присутності повідомлення [89, 135].

Основним завданням розробки стеганографічних перетворень є забезпечення стійкості до спроб встановлення факту її використання. Однак відсутність стійкості до спроб знищення прихованого повідомлення значно знижує ефективність її практичного використання [93, 139, 147].

До недоліків цієї структурної моделі слід віднести відсутність зворотного зв'язку між процесами вбудовування та витягування.

1.2.2 Теоретико-ігрова модель стеганографічних перетворень з врахуванням активної протидії. Основні ідеї та результати класичної теорії ігор застосовні до стеганографії та дозволяють проводити оцінку і аналіз стійкості до атак в КСМ, що спрямовані на знищення прихованих даних [2, 19, 24, 38, 57, 84]. Для опису стеганографічних перетворень з врахуванням активної протидії можуть бути використані модель гри двох учасників з нульовою сумою.

Дійсна гра двох учасників G визначається сукупністю $\{S_1, S_2, P_1, P_2\}$, де S_1, S_2 – множина стратегій першого та другого учасників відповідно, $P_1: S_1 \times S_2 \rightarrow R$, $P_2: S_1 \times S_2 \rightarrow R$ – функції вигравів, що визначають вигреш першого і другого учасників для всіх припустимих стратегій.

У грі з нульовою сумою і двома учасниками вигреш одного гравця дорівнює програшу іншого, тобто $P_1(s, t) = -P_2(s, t)$, $\forall s, t \mid s \in S_1, t \in S_2$. Таким чином, у грі з нульовою сумою і двома гравцями гравці пере-

бувають у конфлікті один з одним, оскільки завдання першого гравця полягає у збільшенні виграшу, а другого – у його зменшенні [57, 59].

Гру двох учасників з нульовою сумою можна описати за допомогою двох множин чистих стратегій S_1 , S_2 та тільки однією функцією виграшів першого гравця, яку позначають $P(s, t) = P_1(s, t) = -P_2(s, t)$.

Стратегія гравця є оптимальною, якщо застосування цієї стратегії забезпечує йому найбільший виграш при будь-яких стратегіях іншого гравця. Оскільки перший гравець прагне по можливості збільшити значення функції виграшу, то

$$P_* = \max_{s \in S_1} \min_{t \in S_2} P(s, t),$$

де P_* – чиста нижня ціна гри, що показує, який мінімальний виграш може гарантувати перший гравець, застосовуючи свої чисті стратегії при будь-яких діях другого гравця, а відповідно цьому числу стратегія першого гравця називається максимінною стратегією [18, 57].

Оскільки другий гравець прагне по можливості зменшити значення функції виграшу, то

$$P^* = \min_{t \in S_2} \max_{s \in S_1} P(s, t).$$

де P^* – чиста верхня ціна гри, що показує, який максимальний виграш за рахунок своїх стратегій може собі гарантувати перший гравець.

Якщо $P_* = P^*$, то гра має сідлову точку в чистих стратегіях і чистій ціні гри P :

$$P = \max_{s \in S_1} \min_{t \in S_2} P(s, t) = \min_{t \in S_2} \max_{s \in S_1} P(s, t).$$

1.2.3 Теоретико-ігрова модель вбудовування даних в область зображень. Теоретико-ігрова модель стеганографічних перетворень передбачає, що на стороні відправника повідомлення приховується у контейнері за допомогою прямого стеганографічного перетворення, після чого модифікований контейнер відкритими каналами зв'язку відправляється приймальній стороні, де за допомогою зворотного стеганографічного перетворення витягається вхідне повідомлення. Завдання активного супротивника полягає в знищенні або модифікації прихованих у контейнері даних [114, 127, 130, 134].

Перший гравець намагається організувати прихований канал передачі даних, а другий – контрольне відкритий канал і намагається не допустити утворення прихованих каналів. Для цього він застосовує до всіх контейнерів перетворення, спрямоване на знищення прихованих даних [96, 143]. Передбачається, що другий гравець не аналізує контейнери окремо з метою виявлення або витягання прихованої інформації.

Чиста стратегія першого гравця x визначає спотворення, що вносяться у контейнер:

$$\mu_1(x) \leq d,$$

де $\mu_1(x)$ – значення спотворень, що вносяться першим гравцем за певною мірою спотворень; d – обмеження, що визначає максимальне допустиме значення спотворень за цією мірою.

Аналогічно, чиста стратегія другого гравця y визначає спотворення, що вносяться у стежоконтанейнер:

$$\mu_2(y) \leq d,$$

де $\mu_2(y)$ – значення спотворень, що вносяться другим гравцем за певною мірою спотворень.

Теоретико-ігрова модель стеганографічних перетворень з активним супротивником використовує модель двійкового каналу, відому з теорії зв'язку [35]. Пропускна здатність двійкового каналу з ймовірністю виникнення помилки p дорівнює $1 - H(p)$, де $H(p) = -p \log(p) - (1 - p) \log(1 - p)$ – ентропія [70, 92, 125]. Виграшем у цій грі є пропускна здатність цього каналу:

$$P(x, y) = \phi_1(x) \left(1 - H \left(\frac{\phi_2(y)}{N} \right) \right),$$

де $\phi_1(x)$ – функція, що визначає для кожній стратегії першого гравця кількість прихованих біт; $\phi_2(y)$ – функція, що визначає для кожної стратегії другого гравця кількість змінених (інвертованих) біт; N –

максимально можлива кількість бітів контейнера, які можна використати для приховання.

Повідомлення представляють собою послідовність псевдовипадкових бітів, які приховуються в растровому N піксельному зображенні з 2^l градаціями сірого.

Чиста стратегія першого гравця – це вектор з l додатних дійсних чисел $x = (x_0, x_1, \dots, x_{l-1})$ таких, що

$$\sum_{i=0}^{l-1} x_i 2^{i-1} \leq d,$$

де x_i – кількість бітів, які перший гравець приховує в i -ті біти представлення значень пікселів зображення.

Позиції приховуваних бітів у зображенні вибираються псевдовипадково і тому рівномірно розподілені серед N бітів кожного i -го представлення [90]. Приховування x_0 бітів у просторову область зображення, наприклад, в наймолодший біт (НБ) призведе в середньому до $x_0 / 2$ спотворень.

Чиста стратегія другого гравця визначається як вектор з l додатних дійсних чисел $y = (y_0, y_1, \dots, y_{l-1})$, таких, що

$$\sum_{i=0}^{l-1} y_i 2^i \leq d,$$

де y_i – кількість бітів, які другий гравець інвертує серед i -х бітів представлення значень пікселів зображення.

Позиції бітів, які інвертуються, вибираються псевдовипадково та рівномірно розподілені серед N можливих варіантів. Ймовірність того, що приховуваний біт буде інвертовано на i -му рівні представлення дорівнює y_i / N .

Функція виграшу гри приймає такий вигляд:

$$P(x, y) = \sum_{i=0}^{l-1} x_i (1 - H(y_i / N)).$$

За оптимальної стратегії другого гравця виконується [10, 19]:

$$2^{-i} (1 - H(y_i/N)) = 2^{-j} (1 - H(y_j/N)).$$

Отже, процес отримання оптимальної стратегії другого гравця $y^* = (y_0^*, y_1^*, \dots, y_{l-1}^*)$ описується таким чином: другий гравець спочатку додає шум у біти 0-го представлення, доки не буде виконано $H(y_0/N) = 1/2$ і продовжує додавати шум у 0-ве та 1-ше представлення, зберігаючи виконання рівності $1 - H(y_0/N) = 1/2(1 - H(y_1/N))$, доки не буде виконано $1 - H(y_0/N) = 1/2(1 - H(y_1/N)) = 1/4$, і так далі до досягнення межі спотворень d [24, 59, 91, 141].

За оптимальної стратегії першого гравця виконується:

$$\frac{x_j}{x_i} = \frac{2^{j-i} \log \frac{p_i^*}{1-p_i^*}}{\log \frac{p_j^*}{1-p_j^*}},$$

де $p_i^* = y_i^* / N$.

До переваг теоретико-ігрової моделі стеганографічних перетворень слід віднести: врахування активної протидії стеганографічному вбудовуванню; використання різних за значимістю рівнів представлення у зображенні.

Недоліками теоретико-ігрової моделі стеганографічних перетворень є неврахування пасивної стадії атаки. Моделлю передбачено зменшення пропускну здатності стежоканалів супротивником, однак для цього необхідні передумови, зроблені на основі демаскуючих ознак. Внаслідок попереднього зауваження використання допустимого рівня спотворень d не є достатньо обґрунтованим. Ця модель також не враховує інші, окрім просторових, перетворення вбудовування і, відповідно, перетворення спотворень [86, 97].

Таким чином, неврахування проміжних перетворень теоретико-множинною моделлю, неврахування зворотних зв'язків структурною моделлю, неврахування пасивної стадії атаки теоретико-ігровою моделлю з активним супротивником обумовлюють необхідність розробки узагальнених адаптивних моделей, що враховують ці недоліки.

1.3 Методи цифрової стеганографії зображень

Забезпечення стійкості стеганографічних перетворень до активних атак в КСМ є актуальною практичною задачею стеганографії. Методи цифрової стеганографії зображень здатні забезпечити високу робастність та таємність вбудовування, тому ці характеристики необхідно враховувати при забезпеченні стійкості до активних атак в КСМ [21, 94, 112, 142].

1.3.1 Задачі цифрової стеганографії зображень. Незважаючи на велике різноманіття методів приховування інформації в цифрових зображеннях, можна виділити два основних класи [113, 147]:

- методи приховування в просторовій області зображень;
- методи приховування в частотній області зображень.

При розробці перших методів приховування даних на основі зміни НБ або квантованих коефіцієнтів дискретного косинусного перетворення (ДКП) особливості області вбудовування не враховувалися. І сьогодні дані методи стеганографічного захисту інформації використовуються доволі широко, незважаючи на успішність виявлення навіть за малої пропускної здатності таємного каналу [105, 119].

Значно ускладнює виявлення модифікація методу вбудовування на основі НБ, яка передбачає збільшення або зменшення на 1 НБ кожного пікселя з рівною ймовірністю [147], що робить неефективними більшість стеганоаналітичних методів. Цей метод отримав назву вбудовування ± 1 та є універсальним відносно області використання.

Метод ± 1 є частинним випадком адитивного шумового вбудовування у просторовій області зображень. Найпоширенішими методами вбудовування повідомлень за значних пропускних здатностей (до 0,8 біта/піксель) є методи стохастичної модуляції. Вони реалізуються шляхом використання незалежних, ідентично розподілених шумів. Однак можна відмітити, що нові підходи [88, 92, 101, 128, 133] використовують адаптивні адитивні шумові генератори, де функція розподілу шуму визначається вмістом оригінального зображення.

З іншого боку забезпечення таємності при використанні методів адитивного шумового вбудовування вимагає уникання вбудовування в однотонні області [85, 102, 118, 146], що дозволяє визначити можливі області вбудовування при стеганоаналізі.

Перші методи стеганографічного захисту інформації, що враховували можливість стеганоаналітичних атак як, наприклад, метод вбудовування в НБ із збереженням статистики [97], OutGuess [147], модельно-орієнтовна стеганографія [139], Steghide та багато інших, зберігали основні статистичні закономірності, чого виявилось недостатньо для забезпечення стійкості до сучасних стеганоаналітичних атак в КСМ. Досягнення сучасного сліпого стеганоаналізу [104, 108] пояснюються використанням значної кількості різних показників, що ускладнює задачу адаптації при вбудовуванні.

Особливості розвитку стеганоаналізу полягають в тому, що кількість аналізованих властивостей постійно збільшується. Це пояснюється особливостями самого процесу отримання даних [4, 13, 16]. Наприклад, якщо аналізується цифрове зображення на кінцевому етапі формування, то завдання визначення області можливого вбудовування є надзвичайно складним, оскільки існує велика кількість складних залежностей між його складовими.

З іншого боку, відправник може володіти необробленим зображенням та вбудовувати дані під час JPEG-ущільнення. Реальні значення ДКП-коефіцієнтів кантуються та округлюються до цілих, кодується за Хаффманом та зберігаються у JPEG-файлі [8, 144]. Отже, відправник може визначити ті з реальних значень ДКП коефіцієнтів, що близькі до середини інтервалу квантування, та за потребою округлити їх до нижньої чи верхньої межі. Цей підхід отримав назву вимушеного квантування [92, 97].

Бажано уникати модифікації оригінального зображення, що реалізовано у [89], де нове мозаїчне зображення конструюється з блоків різних зображень, за рахунок чого представляються біти повідомлення. Існує ціла низка обмежень цього методу стеганографічного захисту інформації, які мають задовольнятися з метою забезпечення стеганографічної таємності. Вони пов'язані з одержанням подібних знімків однієї сцени, існуванням зв'язку між пікселями на межах блоків. Незважаючи на складність визначення вимог таємності цього методу, що пояснюється зв'язком з експериментальними умовами та апаратною частиною, описаний підхід є доволі перспективним [95, 147].

Щодо отримання оригінального зображення, важливими є такі зауваження. Наприклад, відновлені JPEG-зображення, як демонструє

ЛІТЕРАТУРА

1. Аграновский А. В. Основы компьютерной стеганографии / А. В. Аграновский, П. Н. Девянин, Р. А. Хади. – М. : Радио и связь, 2003. – 151 с.
2. Аграновский А. В. Оценка уровня скрытности встраивания данных в стеганографических системах первого поколения / А. В. Аграновский, А. В. Жижелев, Р. А. Хади, // Комплексная защита информации. – 2002. – № 2. – С. 321–333.
3. Айвазян С. А. Прикладная статистика: классификация и снижение размерности / С. А. Айвазян, В. М. Бухштабер, И. С. Енюков. – М. : Финансы и статистика, 1989. – 245 с.
4. Анисимов Б. В. Распознавание и цифровая обработка изображений / Б. В. Анисимов. – М. : Высшая школа, 1983. – 295 с.
5. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М. : Мир, 1986. – 576 с.
6. Болдин М. В. Знаковый статистический анализ линейных моделей / М. В. Болдин, Г. И. Симонова, Ю. Н. Тюрин. – М. : Наука. Физматлит, 1997. – 288 с.
7. Большев Л. Н. Таблицы математической статистики / Л. Н. Большев, Н. В. Смирнов. – М. : Наука, 1983. – 416 с.
8. Ватолин Д. Методы сжатия данных / Д. Ватолин, А. Ратушняк, М. Смирнов – М. : ДИАЛОГ-МИФИ, 2002. – 384 с.
9. Вербицкий О. В. Вступление к криптологии / О. В. Вербицкий, В. А. Герасименко, А. А. Скворцов. – Львов : Издательство научно-технической литературы, 1998. – 300 с.
10. Воробьёв Н. Н. Теория игр для экономистов-кибернетиков / Н. Н. Воробьёв. – М. : Наука, Главная редакция физико-математической литературы, 1985. – 272 с.
11. Галлагер Р. Теория информации и надежная связь / Р. Галлагер. – М. : Мир, 1974. – 351 с.
12. Герасименко В. А. Защита информации в автоматизированных системах обработки данных / В. А. Герасименко. – М. : Энергоатомиздат, 1994. – 345 с.
13. Гольденберг Л. М. Цифровая обработка сигналов : учеб. пос. для ВУЗов / Л. М. Гольденберг, Б. Д. Матюшкин, М. Н. Поляк. – М. : Радио и связь, 1990. – 256 с.

14. Грибунин В. Г. Теория и практика вейвлет-преобразования [Электронный ресурс] / В. Г. Грибунин – Режим доступа: <http://www.autex.spb.ru/wavelet/>
15. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – СПб. : Солон-Пресс, 2002. – 272 с.
16. Грузман И. С. Цифровая обработка изображений в информационных системах / И. С. Грузман, В. С. Киричук, В. П. Косых. – Новосибирск : НГТУ, 2000. – 166 с.
17. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М. : Яхтсмен, 1996. – 234 с.
18. Губко М. В. Теория игр в управлении организационными системами / М. В. Губко, Д. А. Новиков. – М. : Синтег, 2002. – 148 с.
19. Данилов В. И. Лекции по теории игр / В. И. Данилов. – М. : Российская экономическая школа, 2002. – 140 с.
20. Девянин П. Н. Теоретические основы компьютерной безопасности / П. Н. Девянин, О.О. Михальский, Д. И. Правиков. – М. : Радио и связь, 2000. – 412 с.
21. Девянин П. Н. Модели безопасности компьютерных систем : учеб. пос. для студ. высш. учеб. зав. / П. Н. Девянин. – М. : Академия, 2005. – 144 с.
22. Дмитриев В. И. Прикладная теория информации : учеб. пос. для ВУЗов / В. И. Дмитриев. – М. : Высш. школа, 1989. – 320 с.
23. Дубовой В. М. Моделирование систем контролю та керування / В. М. Дубовой. – Вінниця : УНІВЕРСУМ-Вінниця, 2005. – 187 с.
24. Дюбин Г. Н. Введение в прикладную теорию игр / Г. Н. Дюбин, В. Г. Суздаль. – М. : Наука, 1981. – 336 с.
25. Дьяконов В. MATLAB. Обработка сигналов и изображений. Специальный справочник / В. Дьяконов, И. Абраменкова. – СПб. : Питер, 2002. – 608 с.
26. Жельников В. Криптография от папируса до компьютера / В. Жельников. – М. : АБФ, 1996. – 335 с.
27. Журавлев Ю. И. «Распознавание». Математические методы. Программная система. Практические применения / Ю. И. Журавлев, В. В. Рязанов, О. В. Сенько. – М. : Фазис, 2006. – 420 с.
28. Загоруйко Н. Г. Прикладные методы анализа данных и знаний / Н. Г. Загоруйко. – Новосибирск : ИМ СО РАН, 1999. – 251 с.

29. Задірака В. К. Аналіз стійкості стеганографічних систем в моделі пасивного противника / В. К. Задірака, Н. В. Кошкіна, О. С. Олексюк // Искусственный интеллект. – 2004. – № 3. – С. 801–805.
30. Закс Л. Статистическое оценивание / Л. Закс. – М. : Статистика, 1976. – 598 с.
31. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая линия – Телеком, 2000. – 342 с.
32. Злотник Б. М. Помехоустойчивые коды в системах связи / Б. М. Злотник. – М. : Радио и связь, 1989. – 232 с.
33. Кан Д. Взломщики кодов / Д. Кан. – М. : Центрполиграф, 2000. – 472 с.
34. Кветний Р. Н. Основи моделювання та обчислювальних методів: навч. посіб. / Р. Н. Кветний. – Вінниця : ВНТУ, 2007. – 150 с.
35. Кедрус В. А. Основы теории информации и кодирования / В. А. Кедрус, И. В. Кузьмин. – К. : Вища школа, 1986. – 283 с.
36. Кларк Д. Кодирование с исправлением ошибок в системах цифровой связи / Д. Кларк, Д. Кейн. – М. : Радио и связь, 1987. – 392 с.
37. Кобзарь А. И. Прикладная математическая статистика / А. И. Кобзарь. – М. : Физматлит, 2006. – 816 с.
38. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.
39. Корнієнко Б. Я. Анализ действия и методов противодействия информационным угрозам типа «riskware» / Б. Я. Корнієнко, Л. М. Щербак // Захист інформації. – 2008. – № 1. – С. 54–59.
40. Кузнецов А. В. Кодирование в памяти с дефектными ячейками / А. В. Кузнецов, Б. С. Цыбаков // Проблемы передачи информации, 1974. – № 2. – С. 52–60.
41. Кузьмин И. В. Основы моделирования сложных систем : учеб. для ВУЗов / И. В. Кузьмин. – К. : Вища школа, 1981. – 359 с.
42. Липкин И. А. Статистическая радиотехника. Теория информации и кодирования / И. А. Липкин. – М. : Вузовская книга, 2002. – 232 с.

43. Лужецький В. А. Основи інформаційної безпеки / В. А. Лужецький, О. П. Войтович, А. Д. Кожухівський – Черкаси : ЧДТУ, 2008. – 243 с.
44. Лукічов В. В. Вдосконалення метода вбудовування даних на основі алгоритму вейвлет-ущільнення зображень / В. В. Лукічов, А. С. Васюра // «Методи та засоби кодування, захисту й ущільнення інформації», I Міжнародна науково-практична конференція, 15–17 травня 2007 р. : тези доп. – V, 2007. – С. 90–91.
45. Лукічов В. В. Метод вбудовування даних на основі алгоритму вейвлет-стиснення зображень / В. В. Лукічов, А. С. Васюра // «Автоматика-2006», XIII Міжнародної конференції з автоматичного управління, 25–28 вересня 2006 р. – IX, 2006. – С. 491–495.
46. Лукічов В. В. Метод вбудовування даних у зображення за можливості JPEG-стиснення / В. В. Лукічов, А. С. Васюра // Оптико-електронні інформаційно-енергетичні технології. – 2008. – Т. 16, № 2. – С. 42–47.
47. Лукічов В. В. Метод шаблонного вбудовування даних у вейвлет коефіцієнти на основі критерію стеганографічної стійкості / В. В. Лукічов, А. С. Васюра // Наукові праці Вінницького національного технічного університету. – 2009. – № 1. – Режим доступу до журн. : http://nbuv.gov.ua/e-journals/VNTU/2009-1/2009-1.files/uk/09asvoss_ua.pdf.
48. Лукічов В. В. Методи виявлення великих простих чисел / В. В. Лукічов, А. С. Васюра // Вісник Вінницького політехнічного інституту. – 2003. – № 6. – С. 333–339.
49. Лукічов В. В. Моделі адаптивного шаблонного вбудовування даних у вейвлет-коефіцієнти зображень з урахуванням активних стеганографічних атак / В. В. Лукічов // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2009. – № 2. – С. 127–134.
50. Лукічов В. В. Перевірка чисел на простоту і факторизацію / В. В. Лукічов, А. С. Васюра // Оптико-електронні інформаційно-енергетичні технології. – 2003. – № 1–2. – С. 21–26.
51. Лукічов В. В. Підвищення ефективності методу шаблонного вбудовування даних у зображення / В. В. Лукічов, А. С. Васюра // Наукові праці Вінницького національного технічного університету. – 2008. – № 3. – Режим доступу до журн. : http://www.nbuv.gov.ua/e-journals/VNTU/2008-3/2008-3.files/uk/08asvdii_ua.pdf.

52. Лукічов В. В. Стеганографічний захист інформації в комп'ютерних системах на основі шаблонного метода та інтегрального критерію стійкості та таємності / В. В. Лукічов // «Інтегровані інтелектуальні робототехнічні комплекси», II Міжнародна науково-практична конференція, 25–28 травня 2009 р. : тези доп. – V, 2009. – С. 250–251.

53. Лукічов В. В. Стеганографічний захист інформації на основі інтегрального критерію стійкості до активних JPEG-атак / В. В. Лукічов // «Методи та засоби кодування, захисту й ущільнення інформації», II Міжнародна науково-практична конференція, 22–24 квітня 2009 р. : тези доп. – IV, 2009. – С. 118–119.

54. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М. : Финансы и статистика; Электронинформ, 1997. – 368 с.

55. Михайлов С. Ф. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции : уч. пос. / С. Ф. Михайлов, В.А. Петров, Ю. А. Тимофеев. – М. : МИФИ, 1995. – 112 с.

56. Мокін Б. І. Математичні моделі робастної стійкості та чутливості нелінійних систем : моногр. / Б. І. Мокін, С. В. Юхимчук. – Вінниця : УНІВЕРСУМ-Вінниця, 1999. – 122 с.

57. Нейман Дж. Теория игр и экономическое поведение / Дж. Нейман, О. Моргенштерн. – М. : Наука, 1970. – 707 с.

58. Оппенгейм А. Цифровая обработка сигналов / А. Оппенгейм, Р. Шафер. – М. : Техносфера, 2006. – 856 с.

59. Оуэн Г. Теория игр / Г. Оуэн. – М. : Мир, 1971. – 368 с.

60. Петух А. М. Динаміка елементів зображення як інформативний параметр / А. М. Петух, Д. Т. Обідник, С. Г. Захаренков // «Автоматика-2006», XIII Міжнародної конференції з автоматичного управління, 25–28 вересня 2006 р. – IX, 2006. – С. 437–440.

61. Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – М. : АНО НПО «Профессионал», 2005. – 480 с.

62. Смоленцев Н. К. Основы теории вейвлетов. Вейвлеты в Matlab / Н. К. Смоленцев. – М. : LVR Пресс, 2005. – 304 с.

63. Третьяк Л. Н. Обработка результатов наблюдений: учеб. пос. / Л. Н. Третьяк. – Оренбург : ГОУ ОГУ, 2004. – 171 с.

64. Уидроу Б. Адаптивная обработка сигналов / Б. Уидроу, С. Стирнз. – М. : Радио и связь, 1989. – 440 с.
65. Фоменков Г. В. Методы и средства обеспечения безопасности в сети Интернет : науч.-практ. пос. / Г. В. Фоменков. – М. : ИКСИ, 1997. – 312 с.
66. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К. : Юниор, 2003. – 504 с.
67. Хорошко В. О. Основы комп'ютерної стеганографії : навч. пос. / В.О. Хорошко, В.О. Азаров В.О., М. Є. Шелест. – Вінниця : ВДГУ, 2003. – 143 с.
68. Шапиро С. Статистические модели в инженерных задачах / С. Шапиро, Г. Хан. – М. : Мир, 1969. – 365 с.
69. Шатт С. Мир компьютерных сетей / С. Шатт. – К. : ВНУ, 1996 – 288 с.
70. Шеннон К. Теория связи в секретных системах / К. Шеннон // Теории информации и кибернетики. – 1963. – № 2. – С. 333–402.
71. Шлезингер М. Десять лекций по статистическому и структурному распознаванию / М. Шлезингер, В. Главач. – К. : Наукова думка, 2004. – 355 с.
72. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности / А. Ю. Щербаков. – М. : Радио и Связь, 2001. – 325 с.
73. Юдін О. К. Захист інформації в мережах передачі даних : підручник МОН України [для студ. вищ. навч. закл.] / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. – К. : Дельфін, 2008. – 560 с.
74. Яковлев А. Н. Введение в вейвлет-преобразования : учеб. пос. / А. Н. Яковлев. – Новосибирск : НГТУ, 2003. – 104 с.
75. Ahumada A. Computational image quality metrics: a review / A. Ahumada // Society for Information Display International Symposium Digest of Technical Papers. – 1993. – Vol. 24. – P. 305–308.
76. Akaike H. A new look at the statistical model identification / H. Akaike // IEEE Transactions on Automatic Control. – 1974. – Vol. 19, № 6. – P. 716–723.
77. Akansu A. N. Multiresolution Signal Decomposition: Transforms, Subbands and Wavelets / A. N. Akansu, R. A. Haddad. – New York : Academic Press, 1992. – 402 p.

78. Antonini M. Image Coding Using Wavelet Transform / M. Antonini // IEEE Transactions on Image Processing. – 1992. – Vol. 1, № 2. – P. 205–220.
79. Arazi B. A Commonsense Approach to the Theory of Error Correcting Codes / B. Arazi. – Cambridge (MA): MIT Press, 1988. – 343 p.
80. Aura T. Practical invisibility in digital communication / T. Aura // The 1st International Information Hiding Workshop, May 30 – June 1, 1996. – V–VI, 1996. – P. 265–278.
81. Avcibas N. Image steganalysis with binary similarity measures / N. Avcibas, D. Memon, B. Sankur // International Conference on Image Processing, 22–25 Sept. 2002. – IX, 2002. – P. 645–648.
82. Back A. Traffic analysis attacks and trade-offs in anonymity providing systems / A. Back, U. Moeller, A. Stiglic // The 4th Information Hiding Workshop, 25–27 Apr. 2001. – IV, 2001. – P. 257–269.
83. Barberis M. Perceptual distortion metrics for JPEG images / M. Barberis, L. Semeria // Images and Video Compression. – 1998. – Vol. 15, № 3. – P. 176–183.
84. Barron R. J. The duality between information embedding source coding with side information and its implications – applications / R. J. Barron, B. Chen, G. W. Wornell // IEEE Transactions on Information Theory. – 2003. – Vol. 49, № 5. – P. 1159–1180.
85. Barten P. G. Evaluation of subjective image quality with the square-root integral method / P. G. Barten // Journal of Optical Society of America. – 1990. – Vol. 7. – P. 2024–2031.
86. Bohme R. Breaking Cauchy model-based JPEG steganography with first order statistics / R. Bohme, A. Westfeld, P. Samarati // The 9th European Symposium on Research in Computer Security, 13–15 Sept. 2004. – IX, 2004. – P. 125–140.
87. Cachin C. An Information-Theoretic Model for Steganography / C. Cachin // The 2nd Workshop of Information Hiding, 14–17 Apr. 1998. – IV, 1998. – P. 5–12.
88. Cardoso S. Blind signal separation: statistical principles / S. Cardoso // Proceedings of the IEEE. – 1998. – Vol. 86, № 10. – P. 2009–2025.

89. Chandramouli R. Adaptive steganography / R. Chandramouli, N. Memon // The 4th SPIE Conference on Security and Watermarking of Multimedia Contents, 29 Apr. 2002. – IV, 2002. – P. 108–124.

90. Chandramouli R. Analysis of LSB based image steganography techniques / R. Chandramouli, N. Memon // IEEE International Conference on Image Processing, 7–10 Oct. 2001. – X, 2001. – P. 1019–1022.

91. Chen B. Digital watermarking and information embedding using dither modulation / B. Chen, G. Wornell // The 2nd IEEE Workshop on Multimedia Signal Processing, 7–9 Dec. 1998. – XII, 1998. – P. 273–278.

92. Chen B. Dither modulation: A new approach to digital watermarking and information embedding / B. Chen, G. W. Wornell // Security and Watermarking of Multimedia Contents. – 1999. – Vol. 3657. – P. 342–353.

93. Chou J. A robust optimization solution to the data hiding problem using distributed source coding principles / J. Chou, S. Pradhan, L. Ghaoui // Conference on Image and Video Communications and Processing, 25–28 Jan. 2000. – I, 2000. – P. 327–348.

94. Clarke I. Freenet: A distributed anonymous information storage and retrieval system / I. Clarke, O. Sandberg, B. Wiley // Workshop on Design Issues in Anonymity and Unobservability, 25–26 July 2000. – VII, 2000. – P. 121–132.

95. Cole E. Hiding in plain sight: steganography and the art of covert communication / E. Cole. – Indianapolis : Wiley Publishing, 2003. – 335 p.

96. Costa M. Writing on dirty paper / M. Costa // Transactions on Information Theory. – 1983. – Vol. 29, № 3. – P. 439–441.

97. Cox I. Digital watermarking and steganography / I. Cox, J. Bloom, J. Fridrich. – Burlington : Morgan Kaufmann, 2008. – 593 p.

98. Craver S. On public-key steganography in the presence of an active warden / S. Craver. – New York : Academic Press, 1997. – 432 p.

99. Damera-Venkata N. Image quality assessment based on a degradation model / N. Damera-Venkata, T. D. Kite, W. S. Geisler // Transactions on Image Processing. – 2000. – Vol. 9, № 4. – P. 636–650.

100. Dang P. P. Image encryption for secure internet multimedia applications / P. P. Dang, P. M. Chau // Transactions on Consumer Electronics. – 2000. – Vol. 46, № 3. – P. 395–403.

101. Danova K. Spectral Image Distortion Map / K. Danova, P. Toivanen, V. Botchko // The 17th International Conference on Pattern Recognition, 23–26 Aug. 2004. – VIII, 2004. – P. 668–671.

102. Eckert M. P. Perceptual quality metrics applied to still image compression / M. P. Eckert, A. P. Bradley // Signal Processing. – 1998. – Vol. 70. – P. 177–200.

103. Eggers J. Scalar Costa scheme for information embedding / J. Eggers, R. Bauml, R. Tzschoppe // IEEE Transactions on Signal Processing. – 2003. – Vol. 51, № 4. – P. 1003–1019.

104. Farid H. Detecting hidden messages using higher-order statistics and support vector machines / H. Farid, S. Lyu // The 5th International Workshop on Information Hiding, 7–9 Oct. 2002. – X, 2002. – P. 340–354.

105. Fridrich J. Matrix Embedding for Large Payloads / J. Fridrich, D. Soukal // IEEE Transactions on Information Forensics and Security. – 2006. – Vol. 3, № 1. – P. 390–395.

106. Fridrich J. Minimizing the Embedding Impact in Steganography / J. Fridrich // ACM Multimedia and Security Workshop, 26–27 Sept. 2006. – IX, 2006. – P. 2–10.

107. Fridrich J. Practical steganalysis: State-of-the-art / J. Fridrich, M. Goljan // The 4th SPIE Conference on Security and Watermarking of Multimedia Contents, 29 Apr. 2002. – IV, 2002. – P. 212–214.

108. Fridrich J. Towards multi-class blind steganalyzer for JPEG images / J. Fridrich, T. Pevny // Lecture Notes in Computer Science. – 2005. – Vol. 3710. – P. 39–53.

109. Furht B. Multimedia security handbook / B. Furht, D. Kirovski. – Boca Raton : CRC Press, 2005. – 815 p.

110. Gelfand S. I. Coding for channel with random parameters / S. I. Gelfand, M. S. Pinsker // Problems of Information Transaction. – 1980. – Vol. 9, № 1. – P. 19–31.

111. Heegard C. On the capacity of computer memory with defects / C. Heegard, A. Gamal // IEEE Transactions on Information Theory. – 1983. – Vol. 29, № 5. – P. 731–739.

112. Hernandez J. R. Performance analysis of a 2-d multi pulse amplitude modulation scheme for data hiding and watermarking of still images / J. R. Hernandez, F. Perez-Gonzalez, J. M. Rodriguez // IEEE Journal of Selected Areas in Communications. – 1998. – Vol. 16, № 4. – P. 510–524.

113. Jonson N. Steganalysis of images created using current steganography software / N. Jonson, S. Jajodia // The 2nd Workshop of Information Hiding, 14–17 Apr. 1998. – IV, 1998. – P. 135–141.

114. Kipper G. Investigator's Guide to Steganography / G. Kipper. – Boca Raton : Auerbach Publications, 2004. – 240 p.

115. Kodovsky J. On Completeness of Feature Spaces in Blind Steganalysis / J. Kodovsky, J. Fridrich // ACM Multimedia and Security Workshop, 22–23 Sept. 2008. – IX, 2008. – P. 123–131.

116. Kogan J. Grouping Multidimensional Data: Recent advances in clustering / J. Kogan, C. Nicholas, M. Teboulle. – Heidelberg : Springer-Verlag, 2006. – 268 p.

117. Kunkelmann T. A scalable security architecture for multimedia communication standards / T. Kunkelmann, R. Reinema // IEEE International Conference on Multimedia Computing and Systems, 3–6 June 1997. – VI, 1997. – P. 660–661.

118. Lakhani G. Measuring Defects in Images Restored Using DCT Prediction Approaches / G. Lakhani, N. Zhong // The 11th IEEE Symposium on Computer-Based Medical Systems, 12–14 June 1998. – VI, 1998. – P. 175–183.

119. Liu Q. Improved Detection and Evaluation for JPEG Steganalysis / Q. Liu, A. Sung, M. Qiao // ACM Multimedia and Security Workshop, 7–8 Sept. 2009. – IX, 2009. – P. 873–876.

120. Lu C. Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property / C. Lu. – London : Idea Group, 2005. – 255 p.

121. Lukichov V. Improvement of Pattern Hiding Method of Data Application in JPEG-Files / V. Lukichov, A. Vasyura, Y. Zolotavkin // The 42nd Annual International Carnahan Conference on Security Technology, 13–16 Oct. 2008. – X, 2008. – P. 69–75.

122. Manoharan S. Using self-synchronizing codes to improve steganography / S. Manoharan // International Conference Internet and Multimedia Systems and Applications, 13–15 Aug. 2003. – VIII, 2003. – P. 43–57.

123. Mao W. Modern Cryptography: Theory and Practice / W. Mao. – New Jersey : Prentice Hall, 2003. – 345 p.

124. Martínez-Rach M. O. Quality Assessment Metrics vs. PSNR Under Packet Loss Scenarios in MANET Wireless Networks /

M. O. Martínez-Rach, O. López // ACM Multimedia 2007, International Workshop on Mobile Video, 28 Sept. 2007. – IX, 2007. – P. 31–36.

125. Marvel L. Spread Spectrum Image Steganography / L. Marvel, J. Boncelet // IEEE Transactions on Image Processing. – 1999. – Vol. 8, № 8. – P. 1075–1083.

126. Moulin P. Information-Theoretic Analysis of Information Hiding. / P. Moulin, J. O’Sullivan // IEEE Transactions on Information Theory. – 2003. – Vol. 49, № 3. – P. 563–593.

127. Neil F. Steganalysis: The Investigation of Hidden Information / F. Neil, S. Jajodia. – New York : Syracuse, 1998. – 313 p.

128. Pappas T. N. Perceptual criteria for image quality evaluation: [in Handbook of Image and Video Proc.] / T. N. Pappas, R. J. Safranek; ed. by A. Bovik. – London : Academic Press, 2000. – 423 p.

129. Pedrycz W. Knowledge-Based Clustering: From Data to Information Granules / W. Pedrycz. – New Jersey : John Wiley, 2005. – 316 p.

130. Perez-Gonzalez F. Performance Analysis of Existing and New Methods for Data Hiding with Known-Host Information in Additive Channels / F. Perez-Gonzalez, F. Balado, J. R. Hernandez // IEEE Transactions on Signal Processing. – 2003. – Vol. 51, № 4. – P. 960–980.

131. Petitcolas F. A. Information Hiding – A Survey / F. A. Petitcolas, R. J. Anderson, M. G. Kuhn // IEEE Special Issue on Protection of Multimedia Content. – 1999. – Vol. 87, № 7. – P. 1062–1078.

132. Pevniy T. Novelty Detection in Blind Steganalysis / T. Pevniy, J. Fridrich // ACM Multimedia and Security Workshop, 22–23 Sept. 2008. – IX, 2008. – P. 167–176.

133. Pitas I. A Method for Signature Casting on Digital Images / I. Pitas // International conference on image processing, 16–19 Sept. 1996. – IX, 1996. – P. 215–218.

134. Ramkumar M. Capacity Estimates for Data Hiding in Compressed Images / M. Ramkumar, A. N. Akansu // IEEE Transaction on Image Processing. – 2001. – Vol. 10, № 8. – P. 1252–1263.

135. Ramkumar M. Self-noise Suppression Schemes for Blind Image Steganography / M. Ramkumar, A. N. Akansu // SPIE International Symposium on Voice, Video and Data Communications, 2–5 Sept. 1999. – IX, 1999. – P. 421–433.

136. Ross J. A. Security Engineering: A Guide to Building Dependable Distributed Systems / J. A. Ross. – NY : John Wiley & Sons, 2001. – 217 p.
137. Ruanaidh J. Rotation, Translation and Scale Invariant Digital Image Watermarking / J. Ruanaidh, T. Pun // International conference on image processing, 26–29 Oct. 1997. – X, 1997. – P. 536–539.
138. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C / B. Schneier. – NY : John Wiley & Sons, 1996. – 481 p.
139. Sencar H. T. Data hiding fundamentals and applications / H. T. Sencar, M. Ramkumar, A. N. Akansu. – London : Elsevier, 2004. – 252 p.
140. Simmons G. J. The Prisoners' Problem and the Subliminal Channel / G. J. Simmons // Advances in cryptography, Lecture Notes in Computer Science. – 2002. – Vol. 2332. – P. 51–67.
141. Smithand J. R. Modulation and information hiding in images / J. R. Smithand, B. O. Comiskey // The 1st International Information Hiding Workshop, May 30 – June 1, 1996. – V–VI, 1996. – P. 207–226.
142. Voloshynovskiy S. Attack Modelling: Towards a Second Generation Benchmark / S. Voloshynovskiy, S. Pereira, V. Iquise // Signal Processing. – 2001. – Vol. 81, No. 6. – P. 1177–1214.
143. Voloshynovskiy S. On Reversibility of Random Binning Based Data-hiding Techniques: Security Perspectives / S. Voloshynovskiy, O. Koval, E. Topak // ACM Multimedia and Security Workshop, 26–27 Sept. 2006. – IX, 2006. – P. 89–96.
144. Wallace G. K. The JPEG Still Picture Compression Standard / G. K. Wallace // Multimedia Engineering, Digital Equipment Corporation. – 1991. – Vol. 12. – P. 675–681.
145. Wayner P. Disappearing cryptography. Information hiding: Steganography & watermarking / P. Wayner. – Burlington : Morgan Kaufmann, 2009. – 439 p.
146. Winkler S. A perceptual distortion metric for digital color images / S. Winkler // The International Conference on Image Processing, 4–7 Oct. 1998. – X, 1998. – P. 399–403.
147. Zeng W. Multimedia security technologies for digital rights management / W. Zeng, H. Yu, C. Lin. – London : Elsevier, 2006. – 494 p.

Наукове видання

Лукічов Віталій Володимирович
Лужецький Володимир Андрійович
Васюра Анатолій Степанович

**МЕТОДИ ТА ЗАСОБИ СТЕГАНОГРАФІЧНОГО
ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ
ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ**

Монографія

Редактор Н. Мазур
Оригінал-макет підготовлено В. В. Лукічовим

Підписано до друку 29.05.2014 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різнографічний. Ум. др. арк. 9,24
Наклад 300 (1-й запуск 1–75) прим. Зам № В2014-27

Вінницький національний технічний університет,
КІВЦ ВНТУ,
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-85-32.

Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано ФОП Барановська Т. П.
21021, м. Вінниця, вул. Порика, 7.
Свідоцтво суб'єкта видавничої справи
серія ДК № 4377 від 31.07.2012 р.