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

МЕТОДИ ТА ЗАСОБИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ

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 24.04.20014 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 шаблона, який дозволив збільшити пропускну здатність стегоканалу та забезпечити високу швидкість вбудовування.

УДК 004.056.55
ББК 32.97-018.2

ISBN 978-966-641-572-4

ЗМІСТ

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 вдосконалені 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 стегоконтейнера, 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 пропускної 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 стегонаграфічних 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 загрозі розкриття піддаються більшою мірою державні структури, а загрозі порушення цілісності – ділові або комерційні [31, 136].

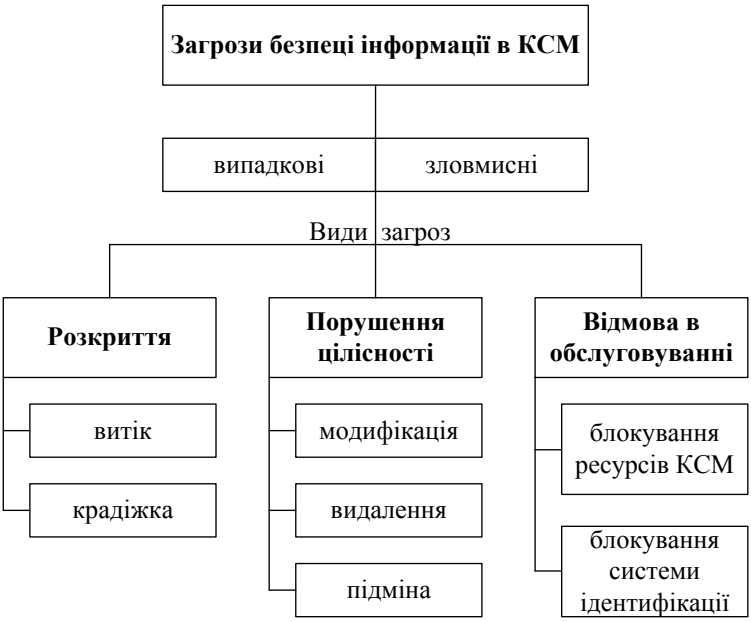

Рисунок 1.1 – Види загроз безпеці інформації
в комп'ютерних системах і мережах

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 результатом 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].

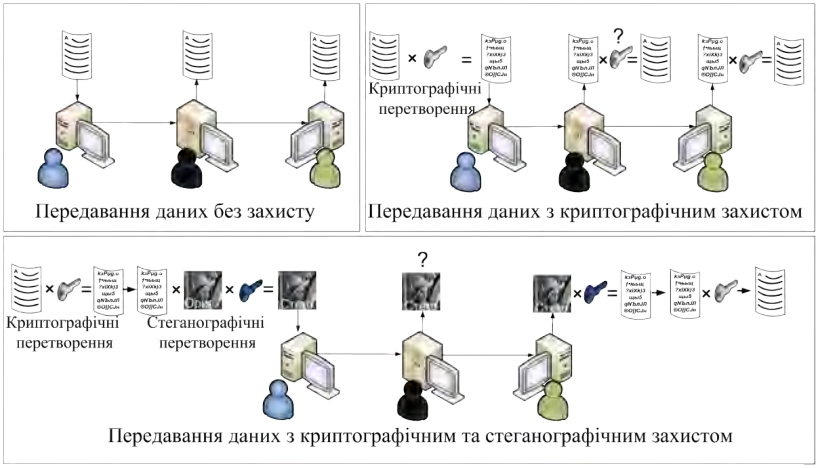

Рисунок 1.2 – Схеми передавання даних комп'ютерними мережами

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-множина 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:

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

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

Функція F є складеною:

$$F = T \circ G,$$

де $G: \mathbf{W} \times \mathbf{D} \to \mathbf{C}$ і $T: \mathbf{I} \times \mathbf{C} \to \tilde{\mathbf{I}}$. 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 використову-

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.

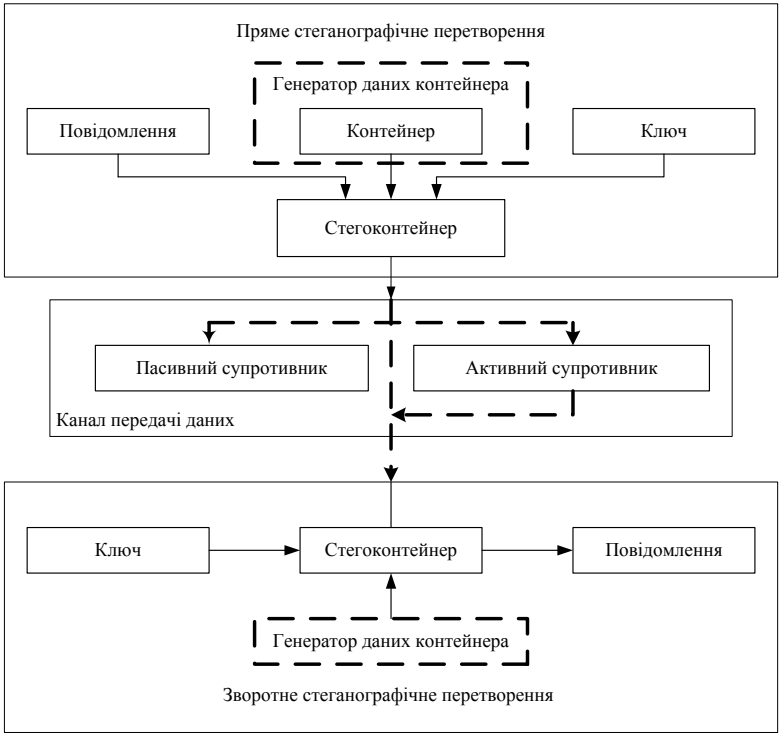

Рисунок 1.3 – Структурна модель стеганографічних перетворень

Відповідно до цієї схеми, на стороні передачі повідомлення приховується в контейнері за допомогою прямого стеганографічного перетворення. Отриманий модифікований контейнер відкритими каналах зв'язку відправляється приймальній стороні, 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 приховуванням 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, $P_1 : S_1 \times S_2 \to R$, $P_2 : S_1 \times S_2 \to R$ – функції виграшів, що визначають виграш першого і другого учасників для всіх припустимих стратегій.

У грі з нульовою сумою і двома учасниками виграш 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 – контролює 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:

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

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 стегоконтейнер:

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

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 $x = (x_0, x_1, ..., x_{l-1})$ таких, що

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

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 $y = (y_0, y_1, ..., y_{l-1})$, таких, що

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

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:

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

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

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

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

За оптимальної стратегії першого гравця виконується:

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

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 пропускної здатності стегоканалів супротивником, однак для цього необхідні передумови, зроблені на основі демаскуючих ознак. Внаслідок попереднього зауваження використання допустимого рівня спотворень d не є достатньо обгрунтованим. 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 піксела 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, кодуються 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 пікселами 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

Шановний читачу!

Умови придбання надрукованих примірників монографії наведені на сайті видавництва http://publish.vntu.edu.ua/get/?isbn=978-966-641-572-4

Уважаемый читатель!

Условия приобретения печатных экземпляров монографии приведены на сайте издательства http://publish.vntu.edu.ua/get/?isbn=978-966-641-572-4

Dear reader!

You may order this monograph at the Web page
http://publish.vntu.edu.ua/get/?isbn=978-966-641-572-4

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 різографічний. 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.