УДК 621.396

О.А. Смірнов, Є.В. Мелешко

*Кіровоградський національний технічний університет, Кіровоград*

# ДОСЛІДЖЕННЯ МЕТОДІВ СТЕГОАНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ

*В роботі проведено дослідження сучасних методів стегоаналізу цифрових зображень. Запропонована їх класифікація. Визначено напрямки подальших досліджень, які складаються з вдосконалення існуючих методів статистичного стегоаналізу та стегоаналізу з використанням нейронних мереж.*

***Ключові слова:*** *стегоаналіз, стеганографія, цифрові зображення, візуальний стегоаналіз, статистичний стегоаналіз, RS-аналіз, стиснення даних, нейронні мережі*

## Вступ

Цифрова стеганографія – раніше малодосліджена область захисту інформації, яка стрімко почала розвиватися в останні десятиріччя. Вона використовується для наступних цілей:

1. Вбудовування інформації з метою її прихованої передачі:

– використання спецслужбами для зв'язку з агентами без дипломатичного прикриття за рубежем;

– використання терористичними організаціями для передачі схованих повідомлень у кіберпросторі;

– використання фізичними і юридичними особами для приховування конфіденційної інформації.

2. Вбудовування цифрових водяних знаків (watermarking):

– для систем захисту авторських прав і DRM систем;

– у якості аналогового ЕЦП, забезпечуючи зберігання інформації про переданий підпис і спроби порушення цілісності контейнера.

3. Вбудовування ідентифікаційних номерів (fingerprinting), наприклад, у програмних продуктах, у системах цифрового друку й т.д.

4. Вбудовування заголовків (captioning), наприклад, у медичних картах, у системах цифрового друку й т.д.

При поєднанні з криптографією, стеганографія дозволяє значно підвищити захист інформації від несанкціонованого доступу.

У зв’язку з цим, стає актуальною задача дослідження існуючих методів стегоаналізу та виявлення перспективних напрямків їх розвитку.

Стегоаналіз дозволяє вирішити наступні важливі задачі:

– Визначити стійкість стеганографічного алгоритму до атак зловмисників.

– Запобігти несанкціонованій передачі таємної інформації методами стеганографії.

**Метою даної роботи** є дослідження основних методів стегоаналізу, введення їх класифікації та визначення перспективних напрямків розвитку.

## 1. Класифікація методів стегоаналізу

Стегоаналіз дозволяє виявити факт наявності прихованого повідомлення. Він як правило дає не точну відповідь про факт приховання повідомлення, а лише відповідь з певною ймовірністю. Помилкою першого роду являється випадок, коли порожній контейнер приймається за заповнений, помилкою другого роду – коли непорожній контейнер приймається за пустий. Деякі методи стегоаналізу також дозволяють одержати додаткову інформацію, таку як, наприклад, довжина стегоповідомлення. За певних умов також можливе вилучення повідомлення із стегоконтейнера.

Введемо наступну класифікацію методів стегоаналізу цифрових зображень.

1. За наявністю інформації про алгоритм стеганографії:

– направлені методи, призначені для виявлення даних прихованих конкретним алгоритмом;

– універсальні (або «сліпі») методи, що використовуються, коли алгоритм приховування даних невідомий.

2. За вихідними даними:

– методи пасивного стегоаналізу, що дозволяють визначити лише присутність або відсутність прихованих даних у контейнері;

– методи активного стеганоаналізу, що крім наявності прихованого повідомлення здатні визначити його довжину, місце розміщення у контейнері, деякі параметри алгоритму стеганографії, а також навіть вилучити повідомлення з контейнера у випадку застосування простих алгоритмів приховування інформації.

3. За способом визначення наявності прихованої інформації:

– візуальні методи, засновані на пошуку видимих викривлень зображень, а також візуальному аналізі їх бітових зрізів;

– статистичні методи, засновані на понятті «природного» контейнеру, їх суть полягає в оцінці ймовірності існування стегоповідомлення на основі критерію оцінки близькості досліджуваного контейнера до «природного»;

– методи засновані на стисненні даних, базуються на тому, що приховані дані статистично незалежні від контейнера, тому при стисненні об'єм одержаного архіву зростає в порівнянні з початковим порожнім контейнером;

– методи стегоаналізу засновані на використанні нейронних мереж.

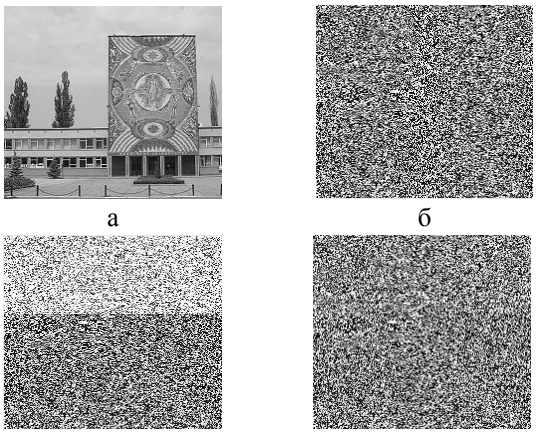
Розглянемо універсальні методи стегоаналізу розділені на групи в залежності від способу виявлення прихованої інформації.

## 2. Дослідження візуальних методів стегоаналізу

Візуальні методи засновані на здатності зорової системи людини аналізувати графічні образи та виявляти відмінності в порівнюваних зображеннях. Візуальні атаки ефективні при повному заповненні контейнеру: чим менше заповнений контейнер, тим складніше виявити факт прихованого повідомлення. Але частіше досліджується не саме зображення, а його бітові зрізи, тому що відмінності між порожнім та заповненим контейнером як правило візуально не проявляються. Якщо розглянути бітовий зріз, що містить найменші значимі біти, в деяких випадках можна побачити сліди прихованого повідомлення.

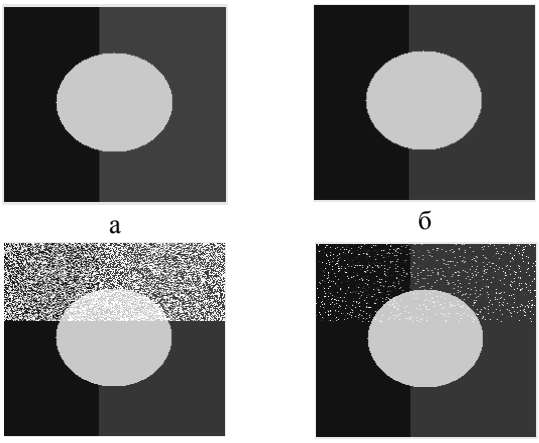
Для методів візуального аналізу бітових зрізів велике значення має алгоритм запису прихованої інформації та вид контейнеру. Якщо стегоповідомлення записувалося послідовно в кожний піксель контейнеру, то факт його наявності може бути встановлений з високою ймовірністю. Якщо пікселі для запису прихованої інформації вибиралися за допомогою генератора псевдовипадкових чисел, то дане завдання значно ускладнюється і залежить від того наскільки первісно був зашумлений контейнер. На рис. 1 та 2 наведені контейнери та їхні бітові зрізи, що містять найменш значимі біти у випадках порожніх, послідовно заповнених та хаотично заповнених контейнерів. Як видно з рисунків найменші значимі біти (НЗБ) зображень (рис. 1) самі по собі містять шум, що ускладнює візуальний аналіз. У випадку послідовного запису стегоповідомлення в даний контейнер, якщо він заповнений не повністю, різниця між заповненою та порожньою частинами помітна візуально, у хаотично заповненому контейнері наявність стегоповідомлення вже не помітна. Графічне зображення на рис. 2 не містить шуму у найменш значимих бітах. Приховати у ньому стегоповідомлення від візуального аналізу бітових зрізів видається малоймовірним. В обох наведених випадках, для послідовного та хаотичного заповнення контейнеру, сліди стегоповідомлення досить помітні.

Візуальні методи найбільш прості в реалізації, але малоефективні та незручні у використанні, так як зводиться до звичайного перегляду людиною зображення-контейнеру та його бітових зрізів з метою виявлення спотворень. Дозволяють виявити наявність стегоповідомлення тільки у випадку застосування найпростіших алгоритмів приховування даних та при значній заповненості контейнеру.



а б в г

Рис. 1. Візуальний стегоаналіз контейнеру з великою первісною зашумленістю:
а – зображення-контейнер; б – бітовий зріз НЗБ порожнього контейнеру; в – бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане послідовно в кожний піксель; г – бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане у пікселі, які обрані генератором псевдовипадкових чисел



а б в г

Рис. 2. Візуальний стегоаналіз контейнеру без первісної зашумленості:
а – зображення-контейнер; б – бітовий зріз НЗБ порожнього контейнеру; в – бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане послідовно в кожний піксель; г – бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане у пікселі, які обрані генератором псевдовипадкових чисел

## 3. Дослідження статистичних методів стегоаналізу

Найбільш поширені та різноманітні методи статистичного стегоаналізу. Статистичні методи базуються на понятті «природного» контейнера. Суть методів полягає в оцінюванні ймовірності існування стегоповідомлення на основі критерію оці-

нки близькості досліджуваного контейнера до «природного». Основним недоліком методів цього класу є саме припущення про існування «природного» контейнера. Основні методи статистичного стегоаналізу найбільш повно розглянуті в [8], серед важливих методів не згадуються там лише RS-аналіз, огляд та дослідження якого можна зустріти в [4, 5, 6] та «аналіз пар», який розглянуто в [6,7].

Розглянемо методи описані [8] та розташовані у порядку убування ступеня довіри позитивним результатам їхнього застосування (виявлення прихованої інформації).

**Метод оцінки числа переходів значень молодших біт у сусідніх елементах зображення**

У методі використовується знання, що між молодшими бітами сусідніх елементів і між ними й іншими бітами природних контейнерів є кореляційні зв'язки. При аналізі графічних файлів формату BMP як елементи аналізованої послідовності вибираються найменш значущі біти складових кольору поруч розташованих пікселів зображення. При дослідженні файлів формату JPEG – молодші біти сусідніх дискретних косинусних коефіцієнтів**,** відмінних від 0 і 1.

Залежність між бітами у відповідних розрядах елементів контейнера має марківский характер. При цьому параметри залежності визначаються номером розряду. Під «переходом» розуміють перехід значення і-го елемента послідовності в значення і + 1 елемента послідовності x, i = 1, 2, ..., n - 1, де n – довжина послідовності. Так як послідовності є двійковими, то аналізується чотири види переходів: з 0 в 0, з 0 в 1, з 1 в 0 і з 1 в 1. За отриманими результатами будується гістограма. Для кожного розряду перший стовбчик гістограми показує число переходів у потоці НЗБ із 0 в 0, другий стовбчик – з 0 в 1, третій стовбчик – з 1 в 0, четвертий стовбчик – з 1 в 1.

Для порожнього контейнера й контейнера, що містить вбудовану інформацію, число переходів у потоці НЗБ буде різним. Розподіл НЗБ стеганоконтейнера має, як правило, випадковий характер. Відповідно число переходів у потоці НЗБ для всіх станів буде приблизно однаковим, що не властиво порожньому контейнеру.

**Метод оцінки частот появи k-бітових серій у потоці НЗБ елементів контейнера**

Метод дозволяє оцінити рівномірність розподілу елементів у досліджуваній послідовності на основі аналізу частоти появи нулів і одиниць, і серій, що складаються з k біт. У бітовому представленні досліджуваної послідовності x підраховується, скільки разів зустрічаються нулі й одиниці (k = 1), серії-двійки (00, 01, 10, 11: k = 2), серії-трійки (000, 001, 010, 011, 100, 101, 110, 111: k = 3) і т.д. На основі результатів будується гістограма.

Для JPEG-зображень гістограма будується за значеннями частот появи бітових серій у потоці НЗБ дискретних косинусних коефіцієнтів, відмінних від -1, 0, 1.

Для незаповнених BMP і JPEG зображень не є характерним, щоб значення частот всіх компонентів перебували досить близько. При вбудовуванні інформації значення частот зближаються. Цей факт використовується при аналізі.

Результати роботи методу залежать від стеганографического перетворення, застосованого для вбудовування приховуваних даних, а також від їхнього обсягу. Як правило, виявлення факту приховування можливе при заповненості контейнера на 60% і вище.

**Метод аналізу розподілу пар значень на основі критерію $\chi^2$**

У методі використовується аналіз гістограми, отриманої за елементами зображення й оцінка розподілу пар значень цієї гістограми. Для BMP-файлів пари значень формуються значеннями пікселів зображення, для JPEG – квантуємими коефіцієнтами дискретного косинусного перетворення, які відрізняються за молодшим бітом. Молодші біти зображень не є випадковими. Частоти двох сусідніх елементів контейнера повинні перебувати досить далеко від значення частоти середнього арифметичного цих елементів. В «порожньому» зображенні ситуація, коли частоти елементів зі значеннями 2N і 2N + 1 близькі за значенням, зустрічається досить рідко. При вбудовуванні інформації дані частоти зближаються або стають рівними. Ідея атаки хі-квадрат полягає в пошуку цих близьких значень і підрахунку ймовірності вбудовування на основі того, як близько розташовуються значення частот парних і непарних елементів аналізуємого контейнера. Особливістю алгоритму є послідовний аналіз усього зображення й, відповідно, нагромадження частот елементів.

Результати роботи методу за критерієм хі-квадрат значною мірою залежать від способу приховування даних. При послідовному записі в НЗБ елементів контейнера метод забезпечує гарні результати, а при псевдовипадковому виборі молодших біт і розсіюванні повідомлення по всій довжині контейнера метод не спрацьовує.

У роботі [12] автор запропонував «блоковий» варіант даного методу. Від класичного методу він відрізняється тим, що аналізоване зображення розбивається на блоки певного розміру, які можуть як перетинатися, так і не перетинатися, і для кожного блоку розраховуються свої набори частот елементів і свої ймовірності приховування. Крім того, існує можливість вибору окремих областей зображення для їхнього наступного аналізу. Такий підхід дозволяє виявляти наявність інформації, прихованої псевдовипадковим чином.

**Метод аналізу гістограм, побудованих за частотами елементів зображення**

Метод дозволяє оцінити рівномірність розподілу елементів аналізованого зображення, а також визначити частоту появи конкретного елемента.

Якщо розкид частот появи елементів у кольорових складових BMP-зображення прагне до нуля, то контейнер містить приховані дані. У протилежному випадку контейнер вважається порожнім.

Для зображень у JPEG-форматі будується гістограма частот квантованих дискретних косинусних коефіцієнтів. Експериментально виявлено, що огибаюча гістограми порожнього зображення має більш гладкий характер у порівнянні з гістограмами зображень, що містять стегоповідомлення. Звичайно, залежно від характеру й ступеня стиснення зображення, гістограми можуть змінюватися – у них можуть з'являтися скачки й провали, але важливо те, що приховування інформації міняє загальний вид гістограм. Більшість стеганографічних програм, що працюють із JPEG, приховують дані в молодші біти дискретних коефіцієнтів, відмінних від 0 і 1. Як наслідок, частоти 0-х і 1-х DCT не змінюються, у той час як всі інші частоти або зменшуються, або збільшуються залежно від алгоритму вбудовування. При значних обсягах приховуваної інформації гістограми часто приймають східчастий характер, що нетипово для звичайних JPEG-зображень.

**Метод аналізу розподілу елементів зображення на площині**

Метод призначений для визначення залежностей між елементами досліджуваної послідовності.

На площину (поле) розміром $(2^R - 1)(2^R - 1)$, де R – розрядність елемента послідовності, наносяться точки з координатами $(x_i, x_{i+1})$, $x_i$ – елементи досліджуваної послідовності x, $i = 1, 2, \ldots, n - 1$, де n – довжина послідовності. За отриманою «картиною» проводиться аналіз

Якщо точки по всьому полю розташовані хаотично, то між елементами послідовності відсутні залежності, що характерно для контейнерів з вбудованими даними. У випадку незаповненого контейнера точки на полі будуть розташовані нерівномірно або утворювати «візерунки».

**Метод перевірки розподілу елементів на монотонність**

Метод дозволяє оцінити рівномірність розподілу елементів зображення за результатами аналізу довжин ділянок незростання й неубування елементів послідовності.

Досліджувана послідовність x графічно представляється у вигляді слідуючих один за одним непересічних ділянок незростання й неубування елементів послідовності.

Так як статистичні властивості стегоконтейнера близькі до властивостей випадкової послідовності, то ймовірність появи ділянки незростання (неубування) буде тим менше, чим більше його довжина n.

**Метод «аналіз пар» [6,7]**

Даний метод заснований на пошуку закономірності в ймовірностях появи значень яскравості в природних зображеннях і зображеннях з вбудованим стегоповідомленням. При заміні молодшого біта компонента кольору чергового пікселя зображення на черговий біт попередньо зашифрованого або стиснутого стегоповідомлення (тобто стегоповідомлення, що має властивості псевдовипадкової послідовності), значення яскравості пікселя модифікованого зображення або дорівнює значенню яскравості пікселя контейнера, або змінюється на одиницю з імовірністю ~1/2. Для пошуку слідів вбудовування відбувається аналіз закономірностей у частотах появи «сусідніх» значень яскравості. Такі пари значень («Pair of Values») розрізняються тільки значенням найменш значущого біта.

Значення яскравості, двійкове представлення якого закінчується нульовим бітом 1, називається «лівим» (L), а сусіднє з ним значення яскравості, двійкове представлення якого закінчується одиничним бітом – «правим» (R). Нехай кольорова гама вихідного контейнера включає 8 кольорів. Отже, при вбудовуванні повідомлення в НЗБ компонента кольору пікселів необхідно досліджувати статистичні характеристики в 4 парах номерів кольору.

Ймовірності появи лівих і правих номерів кольору в природних контейнерах, істотно відрізняються між собою у всіх парах, а в зображенні з убудованим стегоповідомлення ці ймовірності рівні. Це є явною ознакою наявності приховуваної інформації. Ступінь розходження між ймовірнісними розподілами елементів природних контейнерів і зображень із вбудованим стегоповідомлення може бути використана для оцінки ймовірності наявності стегоповідомлення у зображенні. Дану ймовірність зручно визначати з використанням критерію згоди $\chi^2$.

**Метод RS-аналізу [4, 5, 6]**

Одним з оригінальних методів статистичного стегоанализу є метод RS, вперше опублікований в 2001 р. колективом учених під керівництвом Дж. Фрідріх. Скорочення в назві розшифровується як Regular-Singular, тобто «регулярно-сингулярний».

Суть методу. Все зображення розбивається на групи по n пікселів $G(x_1, x_2,...,x_n)$ де n парне число, наприклад по 2 пікселя, що перебувають поруч по горизонталі. Для групи пікселів визначається функція регулярності або «гладкості» f(G), в якості такої функції можна вибрати, наприклад, дисперсію значень всередині групи, або просто суму перепадів значень суміжних пікселів. Під значенням пікселя розуміється ціле число від 0 до 255.

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| . \qquad (1)$$

Функція F(x) називається фліпінгом і має властивість F(F(x)) = x. Визначаються дві функції фліпінгу – $F_1$, відповідає інверсії молодшого біта пікселя, і $F_2$, що представляє собою інверсію з переносом у старший біт (додавання одиниці):

$F_1$: 0 ↔1, 2↔3, … , 254↔255,

$F_2$: 255↔0, 1↔2, 3↔4, ... , 253↔254, 255↔0.

При застосуванні фліпінгу до групи одержуємо перетворену групу пікселів. Далі, всі групи пікселів розділяються на класи в такий спосіб:

(1) Регулярні групи:

$$G \in R \Leftrightarrow f(F(G)) > f(G),$$

(2) Сингулярні групи:

$$G \in S \Leftrightarrow f(F(G)) < f(G),$$

(3) Невикористовувані групи:

$$G \in U \Leftrightarrow f(F(G)) > f(G).$$

Метод ґрунтується на статистичному припущенні, що для природного зображення, тобто незаповненого контейнера, характерно наступне:

$$R_M \cong R_{-M} \text{ та } S_M \cong S_{-M}. \qquad (2)$$

Припущення засноване на тому, що застосування $F_{-1}$ дасть той же розподіл, що й $F_1$ на зображенні, значення пікселів якого зсунуті на одиницю. Для звичайного зображення співвідношення між групами не повинне істотно змінюватися. Значна розбіжність між значеннями свідчить про застосування LSB-стеганографії для молодших біт зображення.

Розглянемо зміни молодших біт зображення при 100% перезаписі їх бітами повідомлення. Вбудовування випадкового повідомлення довжиною, рівною розміру зображення, призведе до того, що 50% молодших біт будуть інвертовані. Це, у свою чергу зведе до нуля різницю між значеннями RM і SM. Однак на R-M і S-M вбудовування повідомлення буде впливати прямо протилежно, і різниця цих величин буде пропорційна ступеню заповнювання контейнера, іншими словами довжині повідомлення.

На рис. 3 наведена діаграма для типового зображення. На осі абсцис розташована кількість інвертованих біт x, шукана довжина повідомлення p, на осі ординат – відносні значення регулярних і сингулярних груп по відношенню до спільного числа груп зображення.

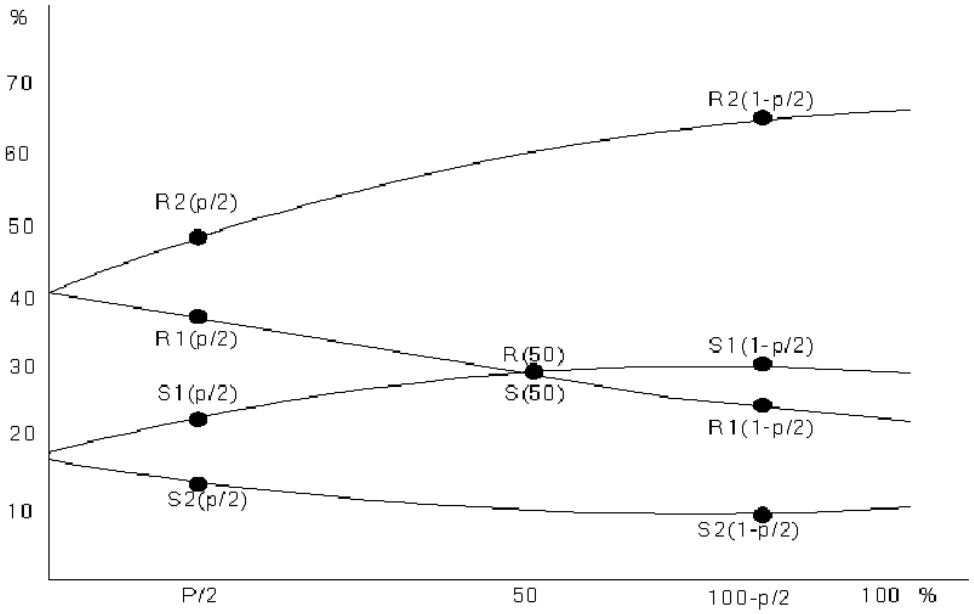



Рис. 3. RS-діаграма типового зображення

Припускаючи, що в зображення внесене повідомлення довжиною p біт, і при цьому 50% молодших біт, використаних для запису, будуть інвертовані, значення статистик буде одержане у точці p/2. Потім, якщо інвертувати всі молодші біти зображення й перерахувати статистики, на діаграмі вони будуть відповідати точкам кривих при x = 100-p/2. Повній рандомізації молодшої бітової площини відповідає точка 1/2**.** Тепер, якщо прийняти p/2 за нуль, а 100-p/2 за одиницю, а також використовувати апроксимацію кривих $R_{-M}$ і $S_{-M}$ прямими, а $R_M$ і $S_M$ параболами, можна вивести квадратне рівняння для знаходження координати точки перетину кривих $R_M$ і $S_M$:

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + \\ + d_0 - d_{-0} = 0.$$

Потім, довжина повідомлення p обчислюється як p = x/(x-1/2). Таким чином, вихідне значення довжини є відповіддю для даного методу.

Для дуже зашумлених і дрібнотекстурованих зображень різниця між кількістю регулярних і син-

гулярних груп контейнера мала. Відповідно, лінії в RS-діаграмі перетнуться під малим кутом і точність зменшиться. Методика RS-стегоаналізу точніша для повідомлень, стегоповідомлення-біти яких випадково розміщені в площині стегоконтейнера, чим для повідомлень, вбудованих локально.

У табл. 1 наведено типові значення розмірів виявлених повідомлень у пустих контейнерах для зображень різних типів [5].

Таблиця 1

Типові відсотки значень розмірів хибно виявлених повідомлень RS-аналізом

| Тип зображення | Хибно визначена довжина повідомлення у відсотках від об'єму контейнера |
|---|---|
| Фотографії, скановані зображення | = 1 % |
| Зображення з Інтернету, підготовлені до друку | = 15 ... 20 % |
| Дрібнотекстуровані зображення, високодеталізовані зображення | = 30 ... 100 % |

## 4. Дослідження методів стегоаналізу заснованих на стисненні даних

В [9, 10] запропоновано метод стегоанализу цифрових зображень на основі стиснення даних. В даному методі можуть застосовуватися широко розповсюджені програми-архіватори.

Ідея методу полягає в наступному: потік випадкових даних стискається гірше, ніж потік, де зустрічаються повторювані послідовності. Інформація, що включається в молодші біти контейнера, як правило, попередньо шифрується й, можливо, стискається, тому є псевдовипадковою. Ступінь стиснення контейнерів використовується для визначення наявності в них прихованої інформації.

Формально даний алгоритм виглядає в такий спосіб. Нехай $X = \{x_1, ..., x_N\}$ – послідовність байтів у полі даних зображення BMP, де $|X| = N$ – довжина послідовності.

Послідовність X розбивається на d рівних відрізків, а кожний відрізок позначається $X_i$, де i = 1, 2, ..., d. Нехай $\psi(X)$ – алгоритм стиснення, застосований до послідовності X. Далі визначається коефіцієнт стиснення відрізка n послідовності X алгоритмом $\psi$ за наступною формулою:

$$f(X, n) = \frac{|\psi(X_n)|}{|X_n|}. \qquad (3)$$

Нехай $\varphi(X)$ – псевдовипадкова зміна молодших біт всіх байтів послідовності X, що подається на вхід програми, а $Y = \varphi(X)$ – отримана з неї нова послідовність ("заповнений" контейнер). Початкова послідовність X повинна стискатися "сильніше" у порівнянні зі зміненою послідовністю Y.

Якщо відрізок $X_i$ послідовності X містить "приховану" інформацію, то коефіцієнт f(X,i) і відповідний йому f(Y,i) відрізняються несуттєво, і навпроти, "порожня" ділянка стискається краще "заповненої". Для визначення факту вбудовування інформації обчислюється різниця коефіцієнтів стиснення:

$$\delta(X, n) = |f(X, n) - f(Y, n)|, \qquad (4)$$

та вибирається граничне значення для величини $\delta$ і здійснюється оцінка кількості відрізків, на яких значення величини не перевищує поріг. Якщо таких відрізків більше d/2, то вважається, що вхідна послідовність X містила приховані дані, у протилежному випадку послідовність X вважається "порожньою". Поріг можна варіювати, регулюючи тим самим частоту помилок програми на порожніх і непустих контейнерах.

В [10] наводиться експериментальний аналіз алгоритму. У якості архіваторів використовувалися RAR, ZIP, GZIP, BZIP2. RAR показав мінімальну в порівнянні з іншими помилку 1-го роду. Архіватори ZIP і BZIP2 продемонстрували мінімальні помилки другого роду, для заповнених наполовину контейнерів. Найкращі результати були отримані з використанням архіватора ZIP, оскільки він найбільш вдало сполучив малі значення обох помилок тестів.

Автором методу емпірично були підібрані два значення: $\delta min = 0.8\%$ (рис. 4) і $\delta max = 1.6\%$ (рис. 5).

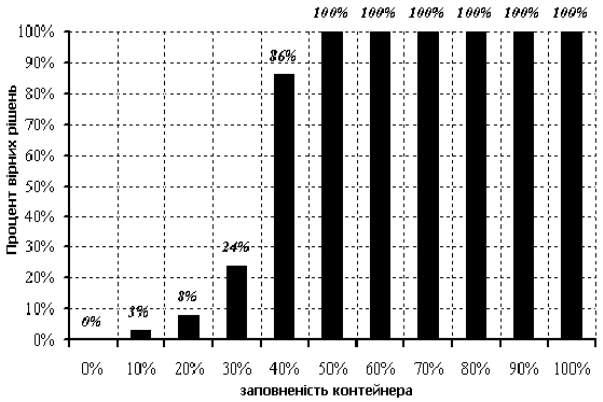



Рис. 4. Результати тестів з архіватором ZIP на "розкиданому" заповненні, $\delta = \delta_{min}$

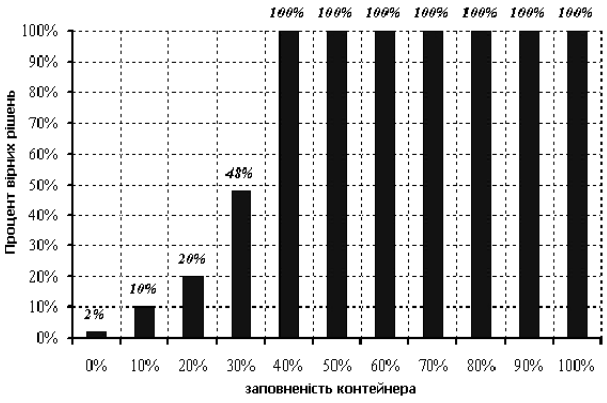



Рис. 5. Результати тестів з архіватором ZIP на "розкиданому" заповненні, $\delta = \delta_{max}$

Даний метод дозволяє виявляти факт внесення прихованих даних у зображення формату 24-біт BMP. Особливістю методу є наявність параметрів, що дозволяють регулювати чутливість алгоритму. Помилка при заповненні контейнера на 50% і більше не перевищує 3%. При заповненні контейнера менше ніж на 40% метод дає більше хибних, ніж вірних відповідей як видно з наведених рисунків.

## 5. Дослідження методів стегоаналізу заснованих на використанні нейронних мереж

Методи стегоаналізу засновані на використанні нейронних мереж малодосліджені. Вони використовують статистичні методи стегоаналізу в поєднанні з можливостями нейронних мереж до навчання та класифікації. Існуючі методи засновані на алгоритмах навчання з учителем. В якості векторів вхідних даних використовуються частотні форми представлення зображень, отримані за допомогою вейвлет-перетворень. В [11] було запропоновано використати для стегоаналізу нейронні мережі RBF. Даний метод відноситься до «сліпих» методів виявлення вбудованої інформації.

Одним з найважливіших етапів алгоритмів стегоаналізу заснованих на використанні нейронних мереж є вибір ознак за якими нейромережа буде робити висновок про наявність стеговставки. Простір пікселів зображення перетворюється в простір ознак і визначення наявності вбудованого повідомлення відбувається вже в просторі ознак. В [11] як ознаки були використані статистичні моменти в частотній області гістограм вейвлет-коефіцієнтів.

Використання статистичних характеристик гістограм зображень пояснюється легкістю моделювання гістограм за допомогою суми, як правило, двох випадкових нормальних змінних і повнотою представлення зображення. В частотній області відмінність стегоповідомлення від контейнера легше розрізнити (рис. 6).

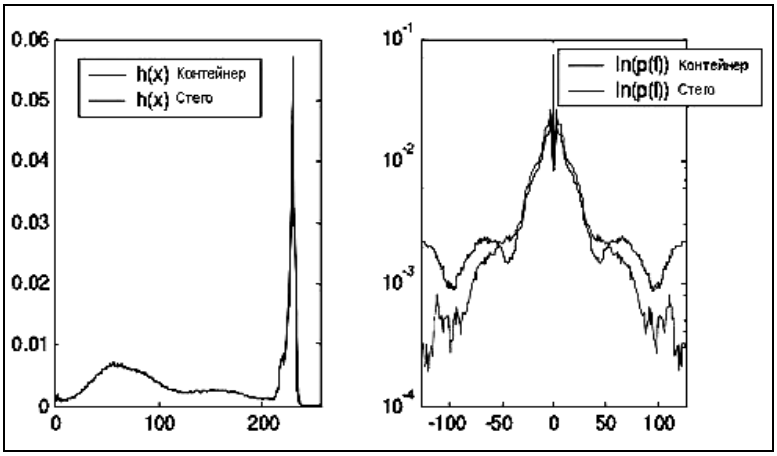



Рис. 6. Гістограма зображення в просторовій області (ліворуч) і в частотній області (праворуч)

Статистичні моменти в частотній області гістограм визначаються в такий спосіб:

$$M_n = \sum_{k=-N/2}^{N/2} |f_k|^n p(f_k), \qquad (5)$$

де n – порядок моменту, N – кількість відліків коефіцієнтів дискретного перетворення Фур'є (ДПФ) для гістограми, $f_к$ – k-та частота в ДПФ (k = -N/2,...-1,0,1,..N/2).

$$p(f_k) = \frac{|H(f_k)|}{\sum_{k=-N/2}^{N/2} |H(f_k)|}, \qquad (6)$$

де, $|H(f_k)|$ – амплітуда ДПФ гістограми $h(x_k)$,

$$H(f) = \int_{-\infty}^{\infty} h(x) e^{-j2\pi fx} dx, \qquad (7)$$

де h(x) – гістограма зображення, або інакше кажучи, кількість пікселів, що приймають значення x.

Кожний з n компонентів вхідного вектора подається на вхід m базисних функцій RBF-мережі і їхні виходи лінійно підсумовуються з вагами:

$$\{w_j\}_{j=1}^{m}.$$

Вихід RBF-мережі є лінійною комбінацією набору базисних функцій:

$$f(\bar{x}) = \sum_{j=1}^{m} w_j h_j(\bar{x}).$$

Якщо припустити, що параметри функції, зсув *c* і радіус *r* фіксовані, то завдання знаходження ваг вирішується методами лінійної алгебри. Цей метод називається методом псевдообернених матриць і він мінімізує середній квадрат помилки. Суть цього методу полягає в наступному.

Знаходиться інтерполяційна матриця H:

$$H = \begin{bmatrix} h_1(\bar{x_1}) \ldots h_m(\bar{x_1}) \\ \ldots\ldots\ldots\ldots \\ h_1(\bar{x_p}) \ldots h_m(\bar{x_p}) \end{bmatrix},$$

де m – число нейронів у прихованому шарі, p – розмір навчальної вибірки, n – число входів мережі.

На наступному етапі обчислюється інверсія добутку матриці H на транспортовану матрицю $H^T$:

$$A^{-1} = (H^T H)^{-1}.$$

Вектор ваг:

$$\overline{W} = A^{-1} H^T \overline{y}.$$

Якщо припущення про фіксовані параметри функції не виконуються, тобто крім ваг необхідно налаштувати параметри активаційної функції кожного нейрона (зсув функції й радіус) і задача стає нелінійною. Вирішувати її доводиться з використанням ітеративних чисельних методів оптимізації, зокрема, градієнтних методів.

Для навчання нейронних мереж в [11] було використано алгоритм навчання з учителем. Навчання без вчителя не було досліджене.

Для адекватного навчання RBF-мережі необхідно підготувати вхідні дані – провести аналіз за допомогою методу головних компонентів і стиснути діапазон по кожній ознаці до інтервалу [0,1].

В [11] наводяться наступні результати роботи RBF-мережі – ймовірність помилки в навчальній вибірці склала 0%, була побудована мережа, що складається з 400 нейронів. Імовірність помилки на контрольній вибірці – 10%.

## Висновки

В ході проведених досліджень було розглянуто основні методи стегоаналізу цифрових зображень, досліджено їх можливості та введено класифікацію. Перспективним напрямком подальших досліджень є вдосконалення існуючих методів статистичного стегоаналізу та стегоаналізу з використанням нейронних мереж та дослідження кількісних та якісних показників ефективності даних методів стегоаналізу.

## Список літератури


*1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.*

*2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.*

*3. Хорошко В.А.. Введение в компьютерную стеганографию / В.А. Хорошко, М.Е. Шелест. – К., 2002. – 140 с.*

*4. Корольов В.Ю. Планування досліджень методів стеганографії та стегоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л. Горінштейн // Вісник Хмельницького національного університету, №4, 2011. – С. 187– 196.*

*5. Корольов В.Ю. RS-стеганоаналіз. Принципи роботи, недоліки та концепція метода його обходу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко // Вісник Вінницького політехнічного інституту. – 2010. – № 6. – С. 66 – 71.*

*6. Кущ А.В. Использование алгоритмов стеганографии при проведении компьютерно-технической экспертизы / А.В. Кущ // VI Всероссийская межвузовская конференция молодых ученых – СПб: СПбГУ ИТМО, 2009.*

*7. Митекин В.А. Модифицированные методы статистического стегоанализа бинарных и полутоновых изображений / В.А. Митекин // Компьютерная оптика № 28 – Институт систем обработки изображений РАН: 2005 – С. 145 – 151.*

*8. Швидченко И.В. Методы стеганоанализа для графических файлов / И.В. Швидченко // Искусственный интеллект. – 2010. – № 4. – С. 697 – 705.*

*9. Жилкин М.Ю. Метод выявления скрытой информации, основанный на сжатии данных / М.Ю. Жилкин // Сборник тезисов и докладов восьмой Всероссийской конференции молодых ученых по математическому моделированию и информационным технологиям. –Новосибирск: 2007.*

*10. Жилкин М.Ю. Стегоанализ графических данных в различных форматах / М.Ю. Жилкин // Доклады ТУСУРа, №2 (18), часть 1, 2008. – С. 63 – 64.*

*11. Абденов А.Ж. Использование нейронных сетей в слепых методах обнаружения встроенной стеганографической информации в цифровых изображеннях / А.Ж. Абденов, Л.С. Леонов // Ползуновский вестник. – 2010. – С. 221 – 225.*

*12. Дрюченко М.А. Алгоритмы выявления стеганографического скрытия информации в jpeg-файлах / М.А. Дрюченко // Вест. Воронеж. гос. ун. Системный анализ и информационные технологии. – 2007. – № 1. – С. 21 – 30.*


*Надійшла до редколегії 12.03.2012*

**Рецензент:** д-р техн. наук проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

### ИССЛЕДОВАНИЕ МЕТОДОВ СТЕГОАНАЛИЗА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

А.А. Смирнов, Е.В. Мелешко

*В работе проведено исследование современных методов стегоанализа цифровых изображений. Предложена их классификация. Определены направления дальнейших исследований, которые состоят в усовершенствовании существующих методов статистического стегоанализа и стегоанализа с использованием нейронных сетей.*

***Ключевые слова:*** *стегоанализ, стеганография, цифровые изображения, визуальный стегоанализ, статистический стегоанализ, RS-анализ, сжатие данных, нейронные сети.*

### THE METHOD STUDY STEGOANALYSIS DIGITAL SCENES

A.A. Smirnov, E.V. Meleshko

*In work is organized study of the modern methods stegoanalysis digital scenes. Their categorization is offered. The certain directions of the further studies, which consist in improvement existing methods statistical stegoanalysis and stegoanalysis with use neural networks.*

***Keywords****: stegoanalysis, steganography, digital scenes, visual stegoanalysis, statistical stegoanalysis, RS-analysis, compression data, neural network.*