УДК 004.056 DOI: https://doi.org/10.33099/2304-2745/2023-1-77/130-135

Чистов В. І.[1] (0000-0002-4401-3773)
Несміян О. Ю., кандидат технічних наук[1] (0000-0002-3312-9439)
Опенько П. В., кандидат технічних наук, старший дослідник[2] (0000-0001-7777-5101)
Угринович О. І., кандидат військових наук, доцент[2] (0000-0001-7164-2700)

[1] – Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків;
[2] – Національний університет оборони України імені Івана Черняховського, Київ

Дослідження статистичних методів стегоаналізу цифрових зображень

Резюме. Для маскування факту передачі інформації в інформаційно-телекомунікаційних системах (ІТКС) широко застосовується велика кількість методів стеганографії. Для протидії стеганографічним алгоритмам приховування інформації актуальною задачею є розробка нових та удосконалення існуючих методів стегоаналізу.

Ключові слова: стеганографія; стегоаналіз; зображення-контейнер; методи стегоаналізу.

Постановка проблеми. На тлі російської збройної агресії проти України все більшого розповсюдження набуває практика використання державою-терористом методів впливу (в тому числі несилового) на критичну інфраструктуру нашої держави – об'єкти, знищення або пошкодження яких може мати тяжкі наслідки для населення, економіки, стабільного функціонування органів державної влади. Для проведення зазначених атак широке застосування знайшли стеганографічні системи зв'язку (ССЗ) [1], принцип роботи яких полягає в інтегруванні скритих каналів зв'язку у вже існуючі потоки даних в інформаційно-телекомунікаційних системах.

Для пошуку та нейтралізації ССЗ в процесі обробки даних, які передаються в ІТКС, використовуються різноманітні методи стегоаналізу [2]. Задача стегоаналізу зображень полягає в виявленні наявності прихованої інформації (стеганографічного контенту) в цифрових зображеннях. Іншими словами, стегоаналіз полягає в виявленні прихованого зображення, тексту або іншої інформації, які були заховані в цифровому зображенні без зміни візуального сприйняття зображення. Можливими діями після виявлення стеганографічного контенту можуть бути підвищення рівня захисту передачі чутливої інформації, виявлення шпигунської діяльності або контролю над використанням цифрових зображень відповідно до вимог авторського права. Висока імовірність виявлення прихованих повідомлень (стеганограм) забезпечується завдяки застосуванню складних в обчисленні методів пасивного стегоаналізу, заснованих на використанні статистичних моделей файлів-контейнерів [3, 4], що значно знижує швидкість обробки даних. Кожен з таких методів має ряд переваг та недоліків, внаслідок чого для аналізу різних видів контейнерів необхідно обирати ті методи стегоаналізу, які добре підходять для конкретного випадку, а послідовне застосування великої кількості методів до кожного контейнеру в рази збільшить і без того суттєвий час обробки повідомлень. З огляду на це важливим та актуальним завданням є дослідження існуючих методів стегоаналізу, визначення їх особливостей, переваг та недоліків з метою подальшого удосконалення.

Аналіз останніх досліджень і публікацій. Пошуком ефективних методів виявлення факту приховання повідомлень потенційним зловмисником в мультимедійних даних займаються відомі вітчизняні та закордоні вчені. В роботі [5] досліджуються сучасні методи квантової стеганографії. Робота [6] присвячена оцінці ефективності методів стеганографічного вбудовування інформації в спектральну область зображень. В роботі [7] основну увагу приділено загальним відомостям та перспективам розвитку комп'ютерної стеганографії. В роботі [8] автори розглядають принципи роботи, переваги та недоліки й концепцію обходу RS-стегоаналізу. Автор [9] досліджує методи виявлення стеганографічного приховування інформації в зображеннях, зокрема розглядає такі методи пасивного стегоаналізу як метод оцінки числа переходів значень молодших бітів у сусідніх елементах

контейнера, метод оцінки частот появи *k*-бітових серій у потоці найменш значущих бітів елементів контейнера, метод аналізу розподілу пар значень на основі критерію *Xi*-квадрат та інші.

Метою статті є дослідження статистичних методів стегоаналізу цифрових зображень, визначення їх особливостей та можливостей для подальшого удосконалення.

Виклад основного матеріалу. Стеганографія – це спосіб організації зв'язку (передачі повідомлень), при якому ховається сама наявність каналу зв'язку. Основними напрямками сучасної стеганографії є технологічна та інформаційна стеганографія, класифікація методів яких наведена на рис. 1.

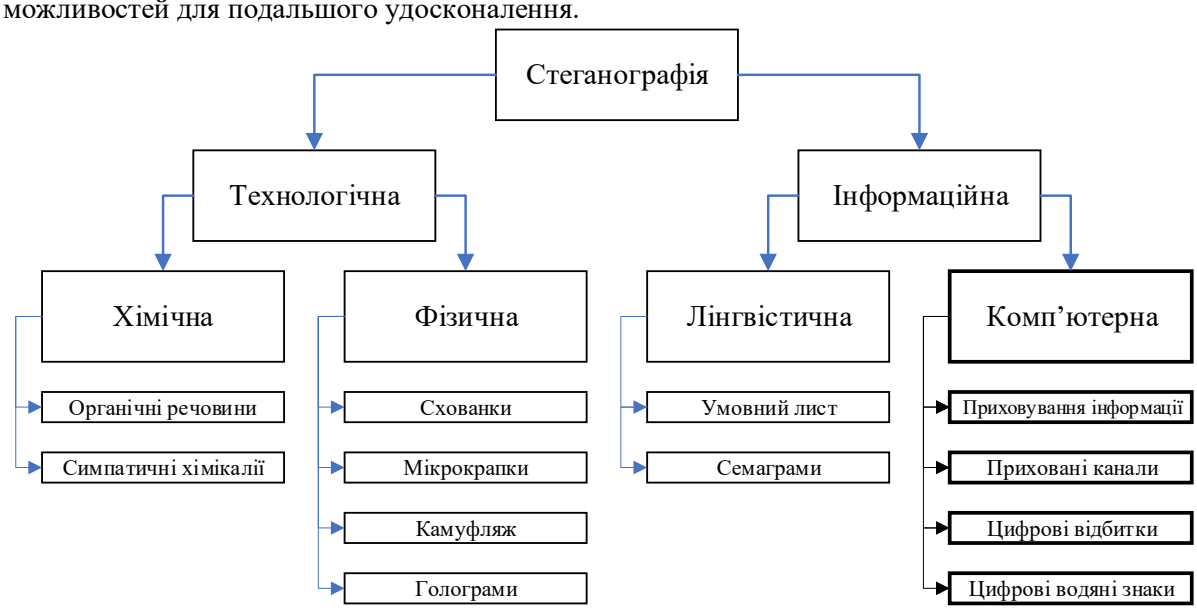

Рис. 1. Класифікація методів стеганографії

Технологічна стеганографія, як напрямок включає в себе методи, що використовують хімічні або фізичні властивості матеріальних носіїв інформації.

Методи хімічної стеганографії майже цілком зводяться до використання невидимих чорнил, які в свою чергу поділяються на органічні речовини та симпатичні хімікалії. Органічні речовини проявляються під впливом нагрівання (молоко, оцет, сік лимона, сеча тощо). Симпатичні чорнила являють собою хімічні речовини, які після висихання стають безбарвними, але в результаті впливу на них відповідних реагентів стають видимими. *Фізичні методи* полягають у використанні різного виду мікрокрапок, камуфляжів, схованок, голограм та кінограм. Також останнім часом фізичні методи є дуже корисними при дослідженні фізичних особливостей носіїв інформації, з метою приховування в них даних.

Інформаційна стеганографія ділиться на лінгвістичну та комп'ютерну. Лінгвістична стеганографія включає в себе семаграми та умовні листи. Семаграми є нічим іншим як таємними повідомленнями, в яких шифром служать будь-які символи, крім букв і цифр.

Умовні листи бувають трьох видів:

геометрична система – ключові букви або слова розташовуються у спеціально визначених місцях або точках перетину заздалегідь узгоджених між абонентами геометричних фігур;

жаргонний код – ключові слова (фрази) мають не ті значення що зазвичай, а текст складається максимально правдоподібно, щоб у разі його перехоплення не визвати підозр в аналітика;

пусковий шифр – ключовими буквами (словами) є лише деякі (наприклад кожна третя буква кожного другого слова), а решта служить в якості "пускових", для приховування таємного змісту повідомлення.

Методи стеганографії, які реалізовані на основі комп'ютерів та програмного забезпечення в рамках локальних або глобальних мереж є предметом вивчення комп'ютерної стеганографії. Вона охоплює такі питання як приховування інформації, яка зберігається на носіях або передається в інформаційно-телекомунікаційних мережах, організація прихованих каналів комп'ютерних мереж та систем, технології цифрових відбитків пальців та цифрових водяних знаків.

Структурна схема стегосистеми представлена на рис. 2. *Повідомлення* – це

будь-яка інформація (текст, зображення, аудіосигнал, тощо), вбудована у контейнер з метою її прихованої передачі. *Контейнер* – інформація, призначена для приховування в ній повідомлення. Вибір виду контейнера істотно впливає на надійність стегосистеми і можливість виявлення факту передачі прихованого повідомлення. *Ключ* (стегоключ) – секретний ключ, що використовується для приховування повідомлення. Залежно від рівня захищеності стегосистеми, в ній може бути один або кілька ключів. Під *стегоканалом* слід розуміти канал передачі даних, у якому відбувається приховування повідомлення методами стеганографії.

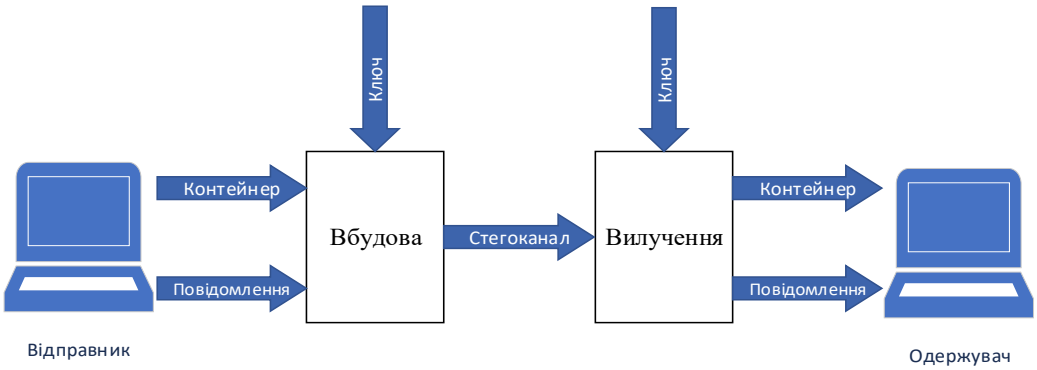

Рис. 2. Структурна схема стегосистеми

Статистику розподілу стеганографічних програм за типом файлів-контейнерів, які в них використовуються наведено на діаграмі (рис. 3).

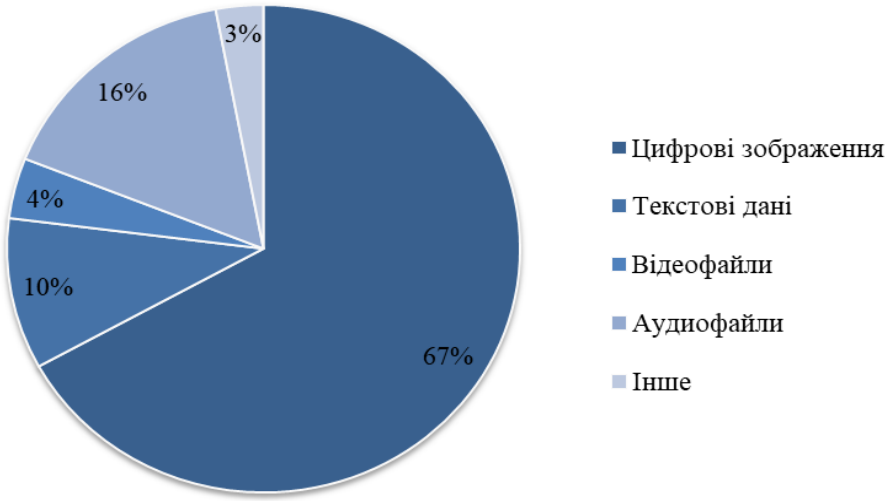

Рис. 3. Діаграма розподілу стеганографічних програм за видом файлів-контейнерів (за даними [2])

Виходячи з (рис. 3) можна зробити висновок, що найбільш розповсюдженим типом мультимедійних даних, які використовуються у ССЗ в якості файлів-контейнерів, є цифрові зображення. Це пояснюється тим, що статистична модель цифрових зображень займає місце між “простою” статистичною моделлю аудіофайлів та багатовимірною моделлю відеофайлів [4]. Виходячи з цього, використання зображень-контейнерів (ЗК) у ССЗ може дозволити досягти певного балансу між об’ємом інформації, яка приховується та стійкістю стеганограм до атак (стегоаналізу).

Стегоаналіз (стеганоаналіз) – розділ стеганографії; наука про виявлення факту передачі інформації, прихованої за допомогою алгоритмів стеганографії.

Відомо, що в залежності від вихідних даних, які використовуються, методи стегоаналізу можна умовно поділити на дві групи (рис. 4):

1. Методи, що призначені для атак на конкретні контейнери (заздалегідь відомі)

алгоритмами стенографії. До цієї групи входять сигнатурні та схемні методи.

Сигнатурні методи шукають послідовності бітів, які притаманні певним стеганографічним програмам та алгоритмам. Такий стегоаналіз часто займає великий часовий проміжок, в зв'язку з тим, що існує необхідність розпізнання сигнатури для відповідної стего-програми з великої кількості файлів, що вкраплювались з її алгоритмом. *Схемні методи* перевіряють гіпотези про наявність вкраплення інформації зі заздалегідь відомою стегосистемою.

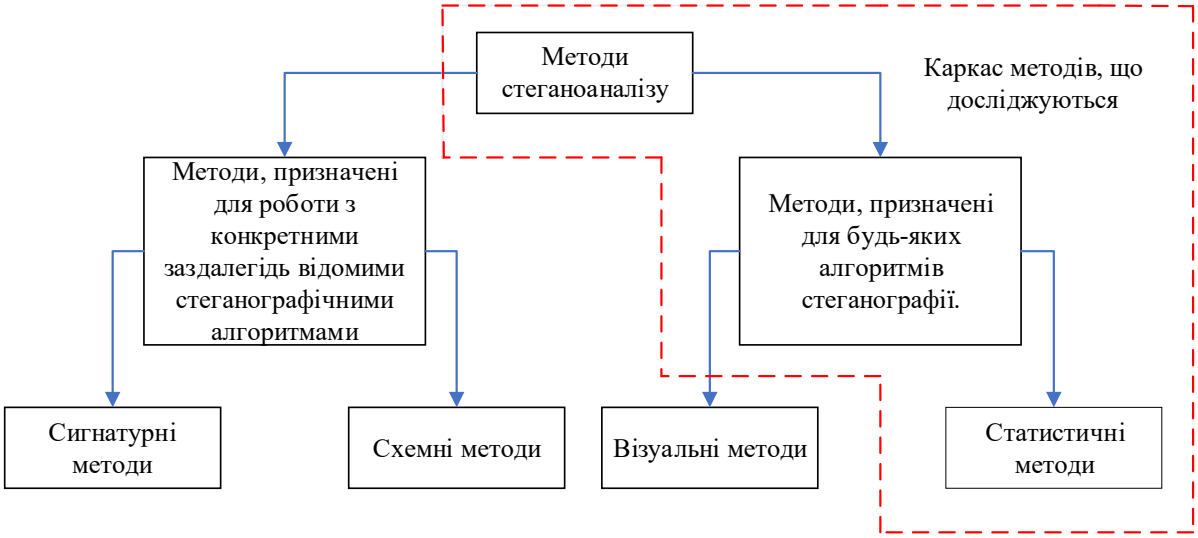

Рис. 4. Класифікація методів стегоаналізу, в залежності від вихідних даних

2. Методи, що призначені для атак на будь-які алгоритми стеганографії. При застосуванні даних методів стегоаналіз не вимагає знань про стеганографічний алгоритм, що використовується. Найбільш відомі методи зазначеної групи, як правило, побудовані на основі алгоритмів, що вимагають навчання на серіях із порожніх та заповнених контейнерів. Вони в свою чергу поділяються на візуальні та статистичні.

Основою *візуальних методів* є виявлення людиною або комп'ютером наявних в зображеннях вкраплень. Контроль неозброєним оком буде успішним у випадку стеганографічного вкраплення даних в однотонні фрагменти зображення. Комп'ютерні програми в свою чергу розкладають зображення на індивідуальні бітові площини. Такі площини складаються з одного біту пам'яті на піксель зображення, і є характерним місцем зберігання вбудованої інформації. У випадку незвичного зовнішнього вигляду у відображенні площини молодшого двійкового розряду, робиться висновок про ймовірне вкраплення в зображення прихованих даних.

Принцип *статистичних методів* полягає в існуванні поняття "оригінального" контейнера. Аналітик оцінює ймовірність існування стеганограми з невідомою стегосистемою на основі критерію оцінки наближення контейнера що досліджується до "оригінального" за його статистичною поведінкою (наприклад числом переходів значень молодших бітів елементів зображення або частотою появи певних серій в потоці молодших бітів елементів зображення).

До переваг цієї групи методів відноситься необмежена сфера застосування, що досить істотно як при перевірці гіпотези про наявність стеганографічного вкладення з невідомою стегосистемою, так і при розробці схемних методів стегоаналізу [9].

З урахуванням вищесказаного, основний акцент досліджень авторами зроблено саме на статистичних методах стегоаналізу цифрових зображень.

Основою методу оцінки числа переходів значень молодших бітів у сусідніх елементах контейнера, що описаний в [9], служить факт наявності кореляційної залежності між молодшими бітами прилеглих елементів, та між цими елементами і іншими бітами "оригінальних" контейнерів. Аналізуються чотири види (0→0, 0→1, 1→0 і 1→1) переходів значень i-го елемента послідовності в значення $i+1$ елемента послідовності x, $i=1,2,...,n-1$, де n – довжина послідовності. За отриманими результатами будується та аналізується гістограма з чотирьох стовпців, кожен з яких відповідає кількості одного з видів переходів у потоці найменш значущих бітів. Для пустого і заповненого контейнера

кількість переходів у потоці найменш значущих бітів буде різним.

У [8] розглянута концепція RS-аналізу, яка полягає в тому, що для більшості зображень рівень найменш значущих бітів є випадковим, проте, разом з тим пов'язаним з іншими бітовими рівнями нелінійною залежністю. Зображення розділяється на групи суміжних відліків з подальшим обчисленням дискримінаційної функції та виконанням переставних операцій для кожної з них. В подальшому групи розбиваються на класи (*R* – регулярні, *S* – сингулярні, *U* – невикористані). Значення для *R* та *S* груп наносяться на *RS*-діаграму та будуються криві, обчислюється їх екстраполяційний перетин. За перетином визначається існування або не існування секретного повідомлення. За координатами перетину розраховується довжина повідомлення.

У методі аналізу розподілу пар значень з урахуванням критерію *Xi*-квадрат, розглянутому в [9], використовується аналіз гістограми, отриманої за елементами зображення та оцінка розподілу пар значень цієї гістограми. Молодші біти в зображеннях є випадковими. Частоти двох сусідніх елементів контейнера повинні бути досить далекі від значення частоти середнього арифметичного цих елементів. При наявності вбудованої інформації ці частоти стають рівними або зближуються.

Таблиця 1

Порівняння методів статистичного стегоаналізу цифрових зображень

Метод/ параметр	Принцип роботи	Формати зображень, з якими працює	Типи алгоритмів, з якими працює	Переваги	Недоліки
Xi-квадрат	Порівняння реального розподілу даних з очікуваним розподілом, що знаходиться за допомогою статистичних методів.	BMP, PNG, JPEG, TIFF	LSB, F5, JSteg, OutGuess, Masking and filtering	Може виявляти стеганографію на різних рівнях (рівень бітів, блоків, файлів); можливість виявлення стеганографії в різних форматах даних (текст, зображення, звук); можливість виявлення навіть дуже малих змін контейнері.	Підвищена складність обчислень; залежність від вибору моделі розподілу; підвищена вразливість до криптографічних методів; ефективність суттєво зменшується за відсутності оригіналу зображення.
RS-аналіз	Визначення статистичних відхилень між оригіналом зображення та зображенням зі стеганографічною інформацією за допомогою методів Річардсона та Шифера.	BMP, PNG, JPEG	LSB, Masking, Outguess, F5, JSteg, Modulo-based methods	Висока точність виявлення стеганографічних вставок при відсутності великого рівня зашумленості; можливість виявлення стеганографії в різних форматах даних (текст, зображення, звук).	Високі вимоги до розміру зображення; обчислювальна складність.
Метод оцінки числа переходів значень молодших бітів (метод Гілберта)	Використання методу Гілберта для порівняння кількості переходів між 0 та 1 в оригінальній та модифікованій послідовностях бітів	BMP, JPEG, PNG, GIF	LSB, M&F, Randomized LSB, Outguess, F5, JSteg	Швидка обробка даних; низький рівень помилок	Ефективність суттєво зменшується за відсутності оригіналу зображення; не здатний до виявлення низько бітових стеганографічних вставок.

Висновки. Таким чином, у статті проведено дослідження трьох статистичних методів стегоаналізу цифрових зображень. Метод оцінки числа переходів значень молодших бітів у сусідніх елементах контейнера показує добру швидкість обробки даних та низький рівень помилок. В той же час його ефективність суттєво зменшується за відсутності оригіналу зображення та він виявляється не здатним до виявлення низько бітових стеганографічних вставок. Точність RS-аналізу залежить від рівня зашумленості зображення-контейнеру, але при малій зашумленості дозволяє надійно виявляти повідомлення в різних форматах даних (текст, зображення, звук). Також методика RS-аналізу є складною в обчисленні. Метод аналізу розподілу пар значень за критерієм Хі-квадрат може виявляти стеганографію на різних рівнях (рівень бітів, блоків, файлів), але його ефективність суттєво зменшується за відсутності оригіналу зображення.

Перспективами подальших досліджень є продовження аналізу слабких та сильних сторін статистичних методів стегоаналізу цифрових зображень з метою їх подальшого вдосконалення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Geers K. Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn : NATO CCD COE Publications, 2015. 175 p.
2. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / 1st Edition. New York : Cambridge University Press, 2009. 437 p. ISBN 978–0–521–19019–0.
3. Fridrich J., Kodovsky J. Rich Models for Steganalysis of Digital Images // IEEE Transactions on Information Forensics and Security. 2012. Volume 7, Issue 3. P. 868–882.
4. Kodovský J., Fridrich J. Steganalysis of JPEG images using rich models // Proc. SPIE 8303, Media Watermarking, Security, and Forensics – Editors Memon Nasir D., Alattar Adnan M., Delp Edward J.;
5. Конахович Г., Шевченко О., Кінзерявий В., Хохлачова Ю. Сучасні методи квантової стеганографії // Захист інформації. 2012. № 2 (51). С. 82–93.
6. Конахович Г. Оцінка ефективності методів стенографичної вбудови інформації в спектральну область зображень // Автоматизовані системи управління та прибори автоматики. 2015. № 168. С. 59–63.
7. Комп'ютерна стеганографія / В. Задирака, І. Сергієнко, І. Коваленко, П. Андон. Київ : Наукова думка, 2010. С. 736–747. (Стан та перспективи розвитку інформатики в Україні).
8. Королёв В., Полиновский В., Герасименко В. RS-стеганоаналіз. Принципи роботи, недоліки та концепція метода його обходу // Вісник Вінницького політехнічного інституту. 2010. № 6. С. 66–71.
9. Швідченко І. В. Методи виявлення стеганографічного приховання інформації в зображеннях // Вісник національного університету "Львівська політехніка". Серія: Автоматика, вимірювання та керування. 2012. № 41. С. 198–203.

Стаття надійшла до редакційної колегії 18.02.2022

Research of statistical methods of steganalysis of digital images

Annotation

The practice of using terrorist state methods of influencing critical infrastructure facilities of Ukraine through the use of steganographic communication systems has become more widespread. The principle of operation of steganographic communication systems is to integrate covert communication channels into existing data flows in information and telecommunication systems.

To search for and neutralize such systems in the process of data processing, various methods of steganalysis are used. Given this, an important and urgent task is to study the existing methods of steganalysis, determine their features, advantages and disadvantages in order to further improve them.

The article studies three statistical methods of steganalysis of digital images.

The method for estimating the number of transitions of the values of the least significant bits in neighboring elements of the container shows a good data processing speed and a low error rate.

At the same time, its effectiveness is significantly reduced in the absence of the original image and it is not capable of detecting low-bit steganographic inserts.

The accuracy of RS-analysis depends on the level of noise in the image-container, but with low noise it can reliably detect messages in different data formats (text, image, sound).

Also, the RS-analysis technique is difficult to calculate.

The method of analyzing the distribution of pairs of values by the Chi-square criterion can detect steganography at different levels (the level of bits, blocks, files), but its effectiveness is significantly reduced in the absence of the original image.

Keywords: steganography; steganalysis; container image; methods of steganalysis.