Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод підвищення стійкості
водяних знаків у цифрових зображеннях

(тема)

Виконав:
студент II курсу, групи КСМм-19-1
Пересада Р.А.
(прізвище, ініціали)

Спеціальність
123 – Комп'ютерна інженерія
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп'ютерні системи та мережі
(повна назва освітньої програми)

Керівник: доц. Ільїна І.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 – Комп'ютерна інженерія
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові Пересаді Роману Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод підвищення стійкості водяних знаків у цифрових зображеннях

затверджена наказом по університету від " 30 " жовтня 2020 р. № 1487Ст

2. Термін подання студентом роботи до екзаменаційної комісії 14 грудня 2020 р.

3. Вхідні дані до роботи Набір зображень BMP формату; методи статистичного аналізу

4. Перелік питань, що потрібно опрацювати в роботі

Методи вбудовування в просторові області зображень;

Загальні критерії вибору контейнерів;

Статистичні аналітичні методи стеганографічні аналізу для виявлення lsb стеганографії

Дослідження статистичних властивостей зображення при встановленні інформації в молодшу бітову площину

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайди презентації – 17 слайдів.

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд методів вбудовування в просторові	03.11.20-09.11.20	
	області зображень		
2	Вибір та обгрунтування загальних критерів	10.11.20-17.11.20	
…	вибору контейнерів		
3	Вибір інструментальних засобів	18.11.20-23.11.20	
4	Проведення експериментів	24.11.20-01.12.20	
5	Оформлення матеріалів атестаційної роботи	02.12.20-07.12.20	
6	Подання атестаційної роботи керівникові та	08.12.20-09.12.20	
	її попередній захист		
7	Подання атестаційної роботи на рецензування	10.12.20-11.12.20	

Дата видачі завдання 02 листопада 2020 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Ільїна І.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 85 с., 31 рис., 2 дод., 15 джерел.

СТЕГАНОГРАФІЧНА СИСТЕМА, BMP, LSB, КОНТЕЙНЕР, КОЛЬОРОВІСТЬ, ДИСПЕРСІЯ, ЕНТРОПІЯ, XI-КВАДРАТ, RS-МЕРА.

Метою атестаційної роботи є дослідження статистичних властивостей цифрових зображень, що забезпечують найкращу стійкість стеганографічної системи, що використовує цифрові зображення в якості контейнерів для вбудовування секретного повідомлення.

У ході виконання атестаційної роботи досліджені властивості цифрових зображень, на які слід спиратися при виборі цифрових зображень в якості контейнера при розробці стеганостойкіх систем. В якості методу вбудовування інформації в просторові області зображень обраний метод заміни найменш значущих біт.

Науково-практичне значення: результати роботи можуть бути використані при практичній розробці стеганографічних систем, що володіють високою стеганографічної стійкістю.

ABSTRACT

Master’s thesis: 85 pages, 31 figures, 2 appendices, 15 sources.

STEGANOGRAPHIC SYSTEM, BMP, LSB, CONTAINER, COLOR, DISPERSION, ENTROPY, XI-SQUARE, RS-MEASURE..

The major goal of this thesis is study of the statistical properties of digital images that provide the best stability of the steganographic system that uses digital images as containers for embedding a secret message.

During the certification work, the properties of digital images, which should be relied on when choosing digital images as a container in the development of quilt-resistant systems, were studied. The method of replacing the least significant bits is chosen as a method of embedding information in the spatial area of images.

Scientific and practical significance: the results can be used in the practical

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

LSB – Least Significant Bit

RGB – Red Green Blue

JPEG – Joint Photographic Experts Group

BMP – Bitmap Picture

RS – Regular-Singular, то есть «регулярно-сингулярный».

TIFF – Tagged Image File Format

PNG – Portable Network Graphics

ВСТУП

У всі часи протягом історії людства завдання захисту інформації від несанкціонованого доступу залишалася актуальною і в даний час залишається не вирішеною до кінця. Уже в стародавньому світі виділилося два основних напрямки вирішення цього завдання, існуючі і по сьогоднішній день: криптографія і стеганографія. Метою криптографії є приховування вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії ховається сам факт існування таємного повідомлення.

Сильним поштовхом до розвитку стеганографії послужило те, що в більшості країн на криптографію накладаються певні обмеження: так, наприклад, потрібна передача ключів від систем шифрування, що використовуються на державному рівні. Обов'язкова так само реєстрація та ліцензування криптографічних систем незалежно від того, є вони апаратними або програмними засобами. Стеганографія не підпадає під дію зазначених обмежень та є при цьому ефективним способом приховування даних.

Методи стеганографії застосовуються не тільки для прихованої передачі повідомлень, але і використовують для захисту авторських або майнових прав на цифрове зображення, фотографії або інші оцифровані твори мистецтва. Переваги, які дають представлення і передача повідомлень в цифровому вигляді, можуть виявитися закресленими легкістю, з якою можливо їх злодійство або модифікація. Тому розробляються різні заходи захисту інформації, організаційного і технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у вбудовуванні в об'єкт, що захищається невидимих міток - цифрових водяних знаків. Вони можуть містити багато корисної інформації: коли створений файл містить інформацію, тих хто володіє авторськими правами, як вступити в контакт з автором і т.д. Всі внесені дані можуть розглядатися як вагомі докази при розгляді питань і судових розглядів про авторство або для

доведення факту нелегального копіювання і часто мають вирішальне значення.

Найбільш поширеним на сьогоднішній день методів цифрової стеганографії є метод, що полягає у вкладенні приховуваного повідомлення в зображення шляхом модифікації найменш значущих біт (LSB). Цифрові зображення представляють собою матрицю пікселів. Піксель - це одиничний елемент зображення. Він має фіксовану розрядність двійкового представлення.

Наприклад, в найпростішій чорно-білій картинці кожний піксель описується одним байтом, який кодуться яскравістю пікселя: нуль - чорний, 255 - білий, все інше - градації сірого. Якщо змінити будь-який байт такого файлу або, що те ж саме, окремі біти цього байта, то відповідний йому піксель змінить яскравість. При цьому зміна різних бітів впливає на яскравість пікселя по-різному: перший дуже сильно, другий слабкіше, а останній, восьмий біт може додати до байту (а значить, і пікселю) тільки одиницю. Нормальна людина не помістить зміну яскравості точки на одну (1/255) градацію сірого. А значить, абсолютно не важливо, які останні біти кожного байта. І їх можна обнуляти, переставляти, замінювати, картинка при цьому буде здаватися однаковою.

Переваги методу полягають в його простоті і порівняно з великим обсягом вбудованих даних. Однак він має два серйозних недоліки:

Приховане повідомлення легко зруйнувати. Для цього необхідно просто записати в один або два молодших біта кожного байта графічного зображення нулі або одиниці, тоді, якщо картинка не містила прихованого повідомлення, то видимих спотворень не з'явиться, а якщо в зображенні було приховано повідомлення, то воно буде зіпсовано. Тобто, ті ж переваги, які використовуються для приховування інформації, можуть бути використані і для непомітної боротьби зі стеганографії.

Чи не забезпечену таємність вбудовування інформації. Порушнику точно відомо місце розташування всього повідомлення. У разі перехоплення

інформації, якщо у перехоплювача виникне підозра, на те, що в зображенні приховано якесь повідомлення, йому неважко буде витягти цю інформацію, так як кількість можливих способів вилучення невелика.

Метою даної роботи є дослідження властивостей природних зображень-контейнерів, що забезпечують найкращу секретність вбудовування інформації в результаті застосування статистичних методів стеганографічного аналізу.

1 ОСНОВНІ ПОЛОЖЕННЯ СТЕГАНОГРАФІЇ

1.1 Основні визначення

Стеганографію можна розділити на 3 складових:

- класична стеганографія - включає в себе всі "некомп'ютерні методи".
- комп'ютерна стеганографія - напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи.
- цифрова стеганографія - напрям класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів. Використовується надмірність аудіо- і візуальної інформації [1].

Саме цифрова стеганографія має найбільший інтерес, з точки зору захисту інформації, як найбільш перспективний напрямок. Її розглянемо докладніше.

Основні положення стеганографії:

- методи приховування повинні забезпечувати автентичність і цілісність файлу.
- передбачається, що криптографу повністю відомі можливі стеганографічні методи.
- безпека методів ґрунтується на збереженні стеганографічних перетворенням основних властивостей відкрито переданого файлу при внесенні до нього секретного повідомлення і деякої невідомої противнику інформації - ключа.
- навіть якщо факт приховування повідомлення став відомий противнику через спільника, витягнути саме секретне повідомлення є складна обчислювальна задача [1].

Незважаючи на численні відкриті публікації та щорічні конференції, тривалий час стеганографія не мала сформованої термінології. Основні

поняття стеганографії були узгоджені в 1996 р на 1-й Міжнародній конференції по прихованню даних - Information Workshop on Information Hiding '96. Проте, навіть таке основоположне поняття як «стеганографія» різними фахівцями трактується неоднаково [2].

Наведемо визначення найбільш важливих, з точки зору стеганографії, термінів.

Стеганосистема - система, що здійснює вбудову та виділення однієї бітової послідовності з іншого. Послідовність, що підлягає прихованню, називається повідомленням. Послідовність, в яку здійснюється вбудова, називається контейнером. Якщо в контейнер не вбудовується повідомлення, то він називається порожнім, інакше - заповненим. Як правило, в складі стеганосистеми додатково виділяють підсистеми, такі як прекодер, стеганокодер, стеганодетектор, декодер [3]. Порівняно недавно була розроблена математична модель стеганосистеми.

У будь-який стеганосистемі важливу роль відіграє стеганографічний протокол - порядок дій, до яких вдаються дві або більше сторін, з метою вирішення певних завдань [4].

Цифровий водяний знак (ЦВЗ) - впроваджена в мультимедійний сигнал інформація, призначення якої - аутентифікація вмісту, охорона прав власника, захист від копіювання та інше.

Стеганосистема утворює стеганоканал, за яким передається заповнений контейнер. Цей канал вважається підданим впливам з боку порушників. Дотримуючись [5], в стеганографії зазвичай розглядається постановка задачі у вигляді «проблема ув'язнених», бажаючих таємно обмінюватися повідомленнями за допомогою передачі їх в прихованому вигляді. Пасивний порушник може лише виявити факт наявності стеганоканала і (можливо) читати повідомлення. Діапазон дій активного порушника значно ширше. Приховане повідомлення може бути їм видалено або зруйновано. В цьому випадку сторона, що передає і, можливо, приймаюча сторона дізнаються про

факт втручання. Дії злочинного порушника найбільш небезпечні. Він здатний не тільки руйнувати, а й створювати помилкові повідомлення.

При побудові стеганосистеми повинні враховуватися наступні положення, багато з яких лежать в основі критеріїв ефективності стеганографічних алгоритмів зображень:

- стеганосистема повинна мати прийнятну обчислювальну складність реалізації;
- заповнений контейнер повинен бути візуально однаковим з незаповненим;
- повинна забезпечуватися необхідна пропускна здатність (що особливо актуально для стеганосистем прихованої передачі даних);
- методи приховування повинні забезпечувати автентичність і цілісність секретної інформації для авторизованої особи;
- потенційний порушник має повне уявлення про стеганосистеми і деталі її реалізації, єдине, що йому невідомо, - це ключ, за допомогою якого тільки його власник може встановити факт наявності і зміст прихованого повідомлення;
- якщо факт існування прихованого повідомлення стає відомим порушнику, це не повинно дозволити останньому витягти його до тих пір, поки ключ зберігається в таємниці;
- порушник повинен бути позбавлений будь-яких технічних та інших переваг в розпізнанні або, по крайній мірі, розкритті змісту секретних повідомлень [3].

1.2 Методи вбудовування в просторові області зображень

Алгоритми, які здійснюють приховування даних в просторової області, впроваджують ЦВЗ в області вихідного зображення. Їх перевагою є те, що для впровадження ЦВЗ немає необхідності виконувати обчислювально громіздкі лінійні перетворення зображень. ЦВЗ впроваджується за рахунок

маніпуляцій яскравістю або складовими кольору $(r(x,y),g(x,y),b(x,y))$. Розглянемо деякі з цих алгоритмів [8].

1.2.1 Вбудова в незначні елементи контейнера

Цифрові зображення представляють собою матрицю пікселів. Молодший значущий біт зображення несе в собі найменше інформації. Відомо, що людина зазвичай не здатна помітити зміну в цьому біті. Фактично, він є шумом. Тому його можна використовувати для вбудови інформації. Переваги даного методу полягають в його простоті і порівняно великому обсязі вбудованих даних [6].

1.2.2 Метод Kutter

Нехай зображення має RGB-кодування. Вбудова виконується в канал синього кольору, так як до синього кольору система людського зору найменш чутлива. Нехай s_i - біт, що вбудовується, $I=\{R,G,B\}$ - контейнер, $p=(x,y)$ - псевдовипадкова позиція, в якій виконується вбудова. Секретний біт вбудовується в канал синього кольору шляхом модифікації яскравості

$$l(p)=0,299r(p)+0.587g(p)+0.114b(p) \tag{1.1}$$

$$b'(p)=\begin{cases} b(p)+ql, if\ s_i=0 \\ b(p)-ql, if\ s_i=1 \end{cases} \tag{1.2}$$

де q - константа, яка визначає енергію вбудованого сигналу. Її величина залежить від призначення схеми. Чим більше q, тим вище робастність вкладення, але тим сильніше його помітність. Максимальне відхилення синьої кольорової складової за умови незмінності двох інших кольрів

становить 9-26%. Колірна компонента кожного пікселя описується одним байтом. Зміна відбувається по масці 11100011, тобто модифікації підлягають 4, 5 або 6 біти. Відхилення інтенсивності кольору в даному випадку не перевищує 6,3%, а загальна зміна яскравості пікселя не перевищує 1% [6].

1.2.3 Метод Bruyndonckx

ЦВЗ є рядком біт. Для підвищення завадостійкості застосовується код БЧХ. Впровадження здійснюється за рахунок модифікації яскравості блоку 8 × 8 пікселів. Процес вбудови здійснюється в три етапи:

- класифікація, або поділ пікселів всередині блоку на дві групи з приблизно однорідними яскравостями.
- розбиття кожної групи на категорії. Для цього на блоки накладаються маски, різні для кожної групи і кожного блоку. Призначення масок полягає в забезпеченні таємності впровадження
- модифікація середніх значень яскравості кожної категорії в кожній групі [6].

1.2.4 Метод Langelaar

Алгоритм працює з блоками 8 × 8. Спочатку створюється псевдовипадкова маска нулів і одиниць такого ж розміру $pat(x, y) \in \{0,1\}$. Далі кожен блок B ділиться на два субблока B_0 і B_1, в залежності від значення маски. Для кожного субблока обчислюється середнє значення яскравості l_0 і l_1. Далі вибирається деякий поріг α, і біт ЦВЗ вбудовується в такий спосіб:

$$s = \begin{cases} 1, l_0 - l_1 > +\alpha \\ 0, l_0 - l_1 < -\alpha \end{cases} \tag{1.3}$$

Якщо ця умова не виконується, змінюємо значення яскравості пікселів

субблока B_1. Для вилучення біта ЦВЗ обчислюються середні значення яскравості субблоків – $l\wedge_0$ і $l\wedge_1$. Різниця між ними дозволяє визначити потрібний біт: [6]

$$s = \begin{cases} 1, l\wedge_0 - l\wedge_1 > 0 \\ 0, l\wedge_0 - l\wedge_1 < 0 \end{cases} \quad (1.3)$$

1.2.5 Метод Pitas

ЦВЗ є двовимірний масив біт розміром з зображення, причому число одиниць в ньому дорівнює числу нулів. Існує кілька версій алгоритму, запропонованого Пітасом. Спочатку пропонувалося вбудовувати біт ЦВЗ в кожен піксель зображення, але пізніше було вирішено використовувати для цієї мети блоки розміром 2 × 2 або 3 × 3 пікселя, що робить алгоритм більш робастниv до стиснення або фільтрації. ЦВЗ складається із зображенням: $l\wedge(x,y) = l(x,y) + \alpha s(x,y)$. У разі використання для впровадження блоків детектор ЦВЗ обчислює середнє значення яскравості цього блоку. Звідси з'являється можливість нерівномірного впровадження ЦВЗ в пікселі, тобто величина α ≠ const. Таким чином можна отримати ЦВЗ, оптимізований за критерієм робастності до процедури стиснення алгоритмом JPEG. Для цього в блоці 8 × 8 елементів заздалегідь обчислюють «ємність» кожного пікселя (з урахуванням ДКП і матриці квантування JPEG). Потім ЦВЗ впроваджують відповідно до обчисленої ємністю. Ця оптимізація проводиться раз і назавжди, і знайдена маска застосовується для будь-якого зображення [6].

1.2.6 Метод Rongen

Також, як і в попередньому алгоритмі, ЦВЗ нагадує двовимірну матрицю одиниць і нулів з приблизно рівним їх кількістю. Пікселі, в які

можна впроваджувати одиниці (тобто робастні до спотворень), визначаються на основі деякої характеристичної функції (характеристичні пікселі). Ця функція обчислюється локально, на основі аналізу сусідніх пікселів. Характеристичні пікселі становлять приблизно 1/100 від загального числа, так що не всі одиниці ЦВЗ вбудовуються саме в ці позиції. Для підвищення кількості характеристичних пікселів в разі необхідності пропонується здійснювати невелике спотворення зображення. Детектор знаходить значення характеристичних пікселів і порівнює з наявними у нього ЦВЗ. Якщо в зображенні ЦВЗ не міститься, то в характеристичних пікселах кількість одиниць і нулів буде приблизно порівну [6].

1.2.7 Метод Patchwork

В основі алгоритму Patchwork лежить статистичний підхід. Спочатку псевдовипадковим чином на основі ключа вибираються два пікселя зображення.

Потім значення яскравості одного з них збільшується на деяке значення (від 1 до 5), значення яскравості іншого зменшується на те ж значення. Далі цей процес повторюється велике число разів (~ 10000) і знаходиться сума значень всіх різниць. За значенням цієї суми судять про наявність чи відсутність ЦВЗ в зображенні. Авторами також запропоновані поліпшення основного алгоритму для підвищення його робастності. Замість окремих пікселів пропонується використовувати блоки, або patches. Звідси і назва алгоритму. Алгоритм Patchwork є досить стійким до операцій стиснення зображення, його усічення, зміни контрастності. Основним недоліком алгоритму є його нестійкість до афінних перетворень, тобто поворотам, зрушення, масштабування. Інший недолік полягає в малій пропускної здатності. Так, в базовій версії алгоритму для передачі 1 біта прихованого повідомлення потрібно 20000 пікселів [6].

1.2.8 Метод Bender

Алгоритм, заснований на копіюванні блоків з випадково вибраної текстурної області в іншу, що має подібні статистичні характеристики. Це призводить до появи в зображенні повністю однакових блоків. Ці блоки можуть бути виявлені в такий спосіб:

- аналіз функції автокореляції стегозображення і знаходження його піків;
- зсув зображення відповідно до цих піків і віднімання зображення з його копії після зсуву;
- різниця в місцях розташування блоків, що були скопійовані повинна бути близька до нуля. Тому можна вибрати певний поріг і значення, менші за цей поріг по абсолютній величині, вважати блоками, які шукали.

Так як копії блоків ідентичні, то вони змінюються однаково при перетвореннях всього зображення.

Якщо зробити розмір блоків досить великим, то алгоритм буде стійким по відношенню до більшості з не геометричних спотворень. У проведених експериментах показана робастний алгоритму до фільтрації, стиску, поворотам зображення. Основним недоліком алгоритму є виняткова складність знаходження областей, блоки з яких можуть бути замінені без помітного погіршення якості зображення. Крім того, в даному алгоритмі як контейнер можуть використовуватися тільки досить текстурні зображення [6].

1.3 Класифікація стеганографічних атак

Суб'єктивна атака. Аналітик уважно розглядає зображення (слухає аудіозапис), намагаючись визначити "на око", чи є в ньому приховане повідомлення. Ясно, що подібна атака може бути проведена лише проти абсолютно незахищених стеганосистем. Тим не менш, вона, напевно,

найбільш поширена на практиці, принаймні, на початковому етапі розкриття стегосистеми.

Атака на основі відомого заповненого контейнера. В цьому випадку у порушника є одне або кілька стего. В останньому випадку мається на увазі, що вбудована прихована інформація здійснювалося відправником одним і тим же способом. Завдання аналітика може складатися у виявленні факту наявності стеганоканала (основна), а також в його добуванні або визначення ключа. Знаючи ключ, порушник отримає можливість аналізу інших повідомлень.

Атака на основі відомого вбудованого повідомлення. Цей тип атаки в більшій мірі характерний для систем захисту інтелектуальної власності, коли в якості водяного знака використовується відомий логотип фірми. Завданням аналізу є отримання ключа. Якщо відповідне приховане повідомлення заповненого контейнер невідоме, то завдання вкрай важко вирішити.

Атака на основі обраного порожнього контейнера. В цьому випадку аналітик здатний змусити відправника користуватися запропонованим йому контейнером. Наприклад, запропонований контейнер може мати великі однорідні області (однотонні зображення), і тоді буде важко забезпечити секретність впровадження.

Атака на основі відомої математичної моделі контейнера або його частини. При цьому атакуючий намагається визначити відміну підозрілого повідомлення від відомої йому моделі. Наприклад, припустимо, що біти всередині відліку зображення корельовані. Тоді відсутність такої кореляції може служити сигналом про наявний прихованому повідомленні. Завдання впровадження повідомлення полягає в тому, щоб не порушити статистики контейнера. Той хто впроваджує і атакує можуть мати у своєму розпорядженні різні моделі сигналів, тоді в інформаційно-прихованому протиборстві переможе краща модель [5].

Атака на основі відомої математичної моделі природного контейнера становить найбільший інтерес для даної наукової роботи і може бути в

подальшому застосована для дослідження статистичних властивостей контейнера, що дозволяють забезпечити найбільшу стійкість стеганографічної системи.

1.4 Аналіз методу заміни найменш значущих біт

Суть методу заміни найменш значущого біта (Least Significant Bits - LSB) полягає в приховуванні інформації шляхом зміни останніх бітів зображення, які кодують колір на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини. В BMP зображення зберігається як матриця значень відтінків кольору для кожної точки зображення. Якщо кожна з компонент простору RGB (їх ще називають каналами кольору) зберігається в одному байті, вона може набувати значень від 0 до 255 включно, що відповідає 24-х бітної глибині кольору.

Особливість зору людини полягає в тому, що воно слабо розрізняє незначні коливання кольору. Для 24-х бітного кольору зміна в кожному з трьох каналів одного найменш значимого біта (тобто крайнього правого) призводить до зміни менш ніж на 1% інтенсивності даної точки, що дозволяє змінювати їх непомітно для ока на свій розсуд.

Принцип роботи стеганографічного методу полягає в наступному. Нехай, є 24-х бітове зображення в градаціях сірого. Піксель кодується 3 байтами, і в них розташовані значення каналів RGB. Змінюючи найменш значущий біт, змінюємо значення байта на одиницю. Такі градації, мало того, що непомітні для людини, можуть взагалі не відобразитися при використанні низькоякісних пристроїв виведення.

Наведений нижче приклад показує, як повідомлення може бути приховано в перших восьми байтах, що відносяться до трьох пикселів в 24-бітного зображення:

```
Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
A: 01000001
Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001) .
```

Приклад 1.1 – Приховане повідомлення

У прикладі підкреслені ті три біта, які були фактично змінені. Застосування стеганографічного методу LSB в середньому вимагає, що тільки половина біт зображення-контейнера були змінені.

Невелика модифікація цієї стеганографічної техніки дозволяє використовувати для вбудовия повідомлення два або більш молодших бітів на байт. Це збільшує обсяг прихованої інформації в об'єкті-контейнері, але скритність сильно знижується, що полегшує виявлення стеганографії. Інші варіації цього методу включають в себе нівелювання статистичних змін в зображенні. Деякі інтелектуальні програми для виявлення стеганографії перевіряють області, які складаються з одного суцільного кольору. Для підвищення скритності слід уникнути запису змін в ці пікселі.

Переваги методу:

- розмір файлу-контейнера залишається незмінним;

- при заміні одного біта в каналі синього кольору впровадження неможливо помітити візуально;

- можливість варіювати пропускну здатність, змінюючи кількість замінних біт.

Недоліки методу:

- приховане повідомлення легко зруйнувати, наприклад, при стисненні або відображенні.

- не забезпечено таємність вбудовування інформації. Точно відомо місце розташування зашифрованої інформації. Для подолання цього недоліку можна вбудовувати інформацію не в усі пікселі зображення, а лише до деяких з них, що визначаються за псевдовипадковому закону відповідно до

ключа, відомого тільки законному користувачеві. Пропускна здатність при цьому зменшується [7].

Зроблено короткий аналіз існуючих методів вбудовування інформації в просторові області цифрових зображень, заснованих на маніпуляції яскравістю або колірними складовими зображень. В якості переваг наведених методів можна виділити відсутність необхідності виконувати обчислювальної громіздкості лінійні перетворення зображень, що відповідає одній з положень побудови стеганосистем. Одним з найбільш часто використовуваних методів вбудови інформації в просторові області зображень є метод заміни найменш значущих біт цифрових зображень, який в подальшому може бути використаний в роботі в якості використовуваного методу вбудови інформації. Зміна кількості замінних біт дозволяє варіювати пропускну здатність стеганографічної системи, однак, існує необхідність дослідження можливості використання старших біт для вбудовування інформації.

2 АНАЛІЗ КРИТЕРІЇВ ВИБОРУ КОНТЕЙНЕРА

2.1 Загальні критерії вибору контейнерів

Істотний вплив на надійність стегосистеми і можливість виявлення факту передачі прихованого повідомлення надає вибір контейнера.

За протяжністю контейнери можна поділити на два типи: безперервні (потокові) і обмеженою (фіксованою) довжини. Особливістю потокового контейнера є те, що неможливо визначити його початок або кінець. Більш того, немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти, що призводить до необхідності включати повідомлення, які приховуються в потік біти в реальному масштабі часу, а самі біти для приховування вибираються за допомогою спеціального генератора, що задає відстань між послідовними бітами в потоці.

У безперервному потоці даних найбільша трудність для одержувача - визначити, коли починається приховане повідомлення. При наявності в потоковому контейнері сигналів синхронізації або кордонів пакета, приховане повідомлення починається відразу після одного з них. У свою чергу, для відправника можливі проблеми, якщо він не впевнений в тому, що потік контейнера буде достатньо довгим для розміщення цілого таємного повідомлення.

При використанні контейнерів фіксованої довжини відправник заздалегідь знає розмір файлу і може вибрати біти для приховання в підходящої псевдовиападковаї послідовності. З іншого боку, контейнери фіксованої довжини, як це вже зазначалося вище, мають обмежений обсяг і іноді повідомлення може не помістится в файл-контейнер.

Інший недолік полягає в тому, що відстані між приховують бітами рівномірно розподілені між найбільш коротким і найбільш довгим заданими відстанями, в той час як справжній випадковий шум буде мати

експоненціальне розподіл довжин інтервалу. Звичайно, можна породити псевдовипадкові експоненціальні розподілені числа, але цей шлях зазвичай занадто трудомісткий. Однак на практиці найчастіше використовуються саме контейнери фіксованої довжини, як найбільш поширені і доступні.

Можливі такі варіанти контейнерів:

- контейнер генерується самою стегосистемою. Такий підхід можна назвати конструюючою стеганографією.

- контейнер вибирається з деякого множини контейнерів. В цьому випадку генерується велика кількість альтернативних контейнерів, щоб потім вибрати найбільш підходящий контейнер, який використовується для приховування повідомлення. Такий підхід можна назвати селектірующей стеганографією. В даному випадку, при виборі оптимального контейнера з множини згенерованих, найважливішою вимогою є природність контейнера. Єдиною ж проблемою залишається те, що навіть оптимально організований контейнер дозволяє заховати незначну кількість даних при дуже великому обсязі самого контейнера.

- контейнер надходить ззовні. В даному випадку відсутня можливість вибору контейнера і для приховування повідомлення береться перший-ліпший контейнер, не завжди підходить до вбудови повідомленням. Назвемо це безальтернативною стеганографією [5].

В даний час більшість досліджень в області стеганографії присвячено використанню в якості стеганоконтейнерів цифрових зображень. Це обумовлено наступними причинами:

- існуванням практично значущої задачі захисту фотографій, зображень, відео від незаконного тиражування і розповсюдження;

- відносно великим обсягом цифрового представлення зображень, що дозволяє впроваджувати повідомлення великого обсягу або підвищувати скритність застосування;

- заздалегідь відомим розміром контейнера, відсутністю обмежень, що накладаються вимогами реального часу;

- наявністю в більшості реальних зображень текстурних областей, що мають шумову структуру і добре підходять для вбудовування інформації;
- слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, вмісту в ньому шуму, спотворень поблизу контурів;
- добре розробленими в останнім часом методами цифрової обробки зображень.

Треба відзначити, що остання причина викликає і значні труднощі в забезпеченні скритності секретних повідомлень: чим більш досконалими стають методи стиснення, тим менше залишається можливостей для вбудовування сторонньої інформації [3].

2.2 Класифікація критеріїв вибору контейнера для LSB-методу

Від вибору контейнера залежить обсяг секретного повідомлення, а також стійкість стегоконтейнера до різних видів аналізу: візуального або статистичного. Способів приховування даних багато, однак, проблема вибору підходящого контейнера до сих пір не вирішена. При дослідженні було знайдено всього кілька джерел, в яких зачіпалася дана проблема.

Вибір контейнера повинен розглядатися з точки зору способу застосування даних, так як саме він визначає біти, які будуть модифіковані на біти повідомлення. Також має враховуватися той факт, що існують методи аналізу, що дозволяють виявити секретне повідомлення.

На даному етапі досліджень вибір контейнера зроблений для методу заміни молодших біт (LSB-методу), на основі якого зроблено більшість програм впровадження повідомлень. Враховувався вплив візуального стеганоаналізу, як початкового етапу аналізу контейнера на наявність повідомлення [8].

Класифікація критеріїв вибору контейнера:

- відмова від загальновідомих зображень в якості контейнера, як, наприклад, зображення «Джоконда»;
- відмова від використання в якості контейнера зображень, конвертованих з JPEG-формату в формат BMP;
- отримання зображення за допомогою фотоапарата або сканера, а не за допомогою графічних редакторів;
- великий розмір контейнера;
- відсутність корисної складової на молодших бітових площинах зображення;
- зашумленность;
- відсутність плавних переходів і монотонних областей;
- «строкатість»;
- велике число перепадів яскравості;
- наявність великої кількості пікселів, відтінки кольорів яких погано розрізняються оком людини (зелений, жовтий).

Ці критерії в достатній мірі враховують всі особливості контейнера, необхідні для отримання стеганоустойчивого контейнера до візуального стеганоаналізу для методу заміни молодших біт [9].

2.3 Кольори зображення як критерій вибору контейнера

На візуальну прихованість даних впливає кольоровість зображення, тобто наявність колірних областей того чи іншого кольору. Це пояснюється нерівномірної чутливістю людського ока до малих змін різних довжин хвиль видимого діапазону. Людське око має властивість порога розрізнення кольорів при невеликих колірних відмінностях, тобто він сприймає колір і його «сусідній» колір як один. Величина цього порога неоднакова для різних кольорів. Цей ефект представлений на рисунку 2.1:

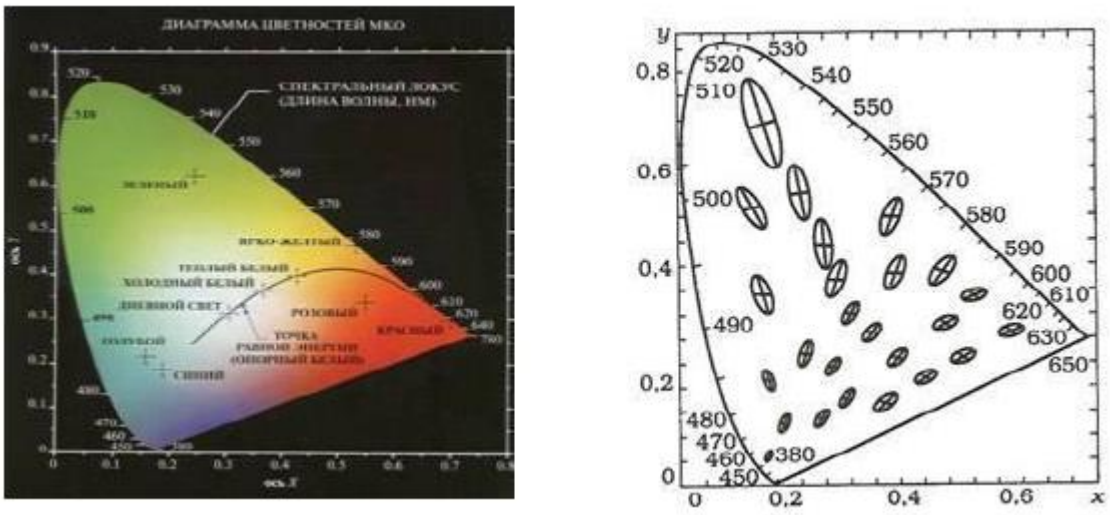

Рисунок 2.1 – Діаграма яскравості і порогові еліпси

Таким чином, заміна однакової кількості молодших біт червоною, синьою області буде більш небезпечною для виявлення виробленої заміни оком, ніж молодших біт жовтої або зеленої області за рахунок різного порога розрізнення цих кольорів. Вибір контейнера, який містить найбільші області зеленого, жовтого і їх сумішей з білим кольором забезпечить найкращу скритність даних з точки зору візуального стеганоаналіза [4].

2.4 Критерій ефективності в стеганографії зображень

Під терміном «ефективність» в стеганографії будемо розуміти можливість вирішення за допомогою цифрових зображень основних завдань стеганографії: швидко і таємно передавати великі обсяги інформації. Існує дуже велика кількість факторів, що впливають на ефективність стеганографії цифрових зображень.

Серед цих чинників можна виділити групу технічних критеріїв ефективності, які піддаються строгому математичному опису і мають певний набір чисельних характеристик. Як приклад такого критерію можна привести ставлення максимального розміру вбудованого повідомлення, що не

приводить до спотворення зображення, до розміру самого контейнера.

З іншого боку, існують критерії ефективності, що не піддаються технічним описом, але як і раніше грають виняткову роль у формуванні поняття «ефективність». Розглядаючи кілька графічних форматів, можна стверджувати, що застосовувати один з них ефективніше, ніж інший. Причиною для цього може бути те, що один з форматів має набагато більшого поширення (в тому числі, в мережі Інтернет), ніж інші. Більш того, використання деяких форматів для нетипових для них цілей саме по собі може бути підозрілим і провокувати атаки. Наприклад, викладені на сайт в мережі Інтернет фотографії друзів в форматі BMP (мають розмір порядку декількох мегабайт) викличуть підозру у відвідувачів (адже сучасні алгоритми стиснення дозволяють стискати фотографії в 20-30 разів з прийнятною втратою якості). До того ж, для деяких форматів (наприклад, згаданий вище формат BMP) розроблений найширший спектр методів та інструментів стеганоаналіза, і ці формати є більш уразливими, а значить і менш ефективними з точки зору стеганографії.

Проаналізуємо найважливіші критерії ефективності застосування цифрових зображень в стеганографії.

Скритність або стеганографічна стійкість. Задоволення вимогу скритності є обов'язковим для абсолютно будь-який стеганосистем. У застосуванні до графічної стеганосистеми, стійкість пов'язана зі змінами (спотвореннями), що вносяться в вихідне зображення при встановленні повідомлення. Вимога стійкості вважається невиконаним, якщо зображення піддається атаці за допомогою простого візуального аналізу. Дана стеганосистема володіє вкрай низькою ефективністю і не може знайти практичного застосування, так як не відповідає мінімальному рівню безпеки (рисунок 2.2).

1 2

Рисунок 2.2 – Результат роботи алгоритму, що не відповідає вимогам стійкості: 1 - вихідне зображення, 2 - зображення з вбудованим повідомленням

Як правило, при створенні стеганографічних алгоритмів, найбільший обсяг досліджень пов'язаний саме із забезпеченням скритності. Проводяться експерименти, що дозволяють встановити, як зміна тієї чи іншої частини файлу-контейнера впливає на результуюче зображення. Стійкість стеганографічного алгоритму в значній мірі визначається розмірами вбудованого повідомлення.

Розмір вбудованого повідомлення. Ефективність використання цифрового зображення для зберігання секретної інформації в значній мірі визначається максимальним можливим розміром секретного повідомлення. Як правило, чисельно цей критерій характеризується процентним співвідношенням між обсягом вбудованого повідомлення і вихідним обсягом контейнера. Відносно зображень, дана величина варіюється в залежності від використовуваного графічного формату.

Головним «обмежувачем» максимального розміру повідомлення для конкретного графічного файлу виступає описана вище вимога скритності. У стеганографії є фундаментальна залежність між стійкістю вбудови та розміром вбудованого повідомлення. Ця залежність має обернено пропорційний характер: чим більший об'єм вбудованого в заздалегідь

заданий контейнер повідомлення, тим нижче надійність приховування цієї інформації в контейнері (рисунок 2.3).

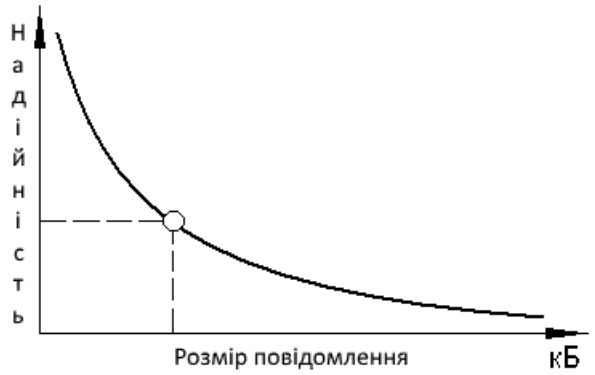

Рисунок 2.3 – Залежність надійності приховування інформації від обсягу повідомлення

Здавалося б, наведена закономірність не дозволяє збільшувати ефективність стеганографічного вбудовування інформації шляхом нарощування розміру повідомлення. Але це не так. Існує кілька методів підвищення розмірів повідомлення без шкоди стійкості, про які йтиметься далі.

Стійкість до модифікації заповненого контейнера (стиску). Стійкість до модифікації характеризує ймовірність відновлення повідомлення, за умови певної модифікації заповненого контейнера. Окремим випадком модифікації є стиснення з втратами. Особливе значення цей фактор ефективності має для технологій впровадження цифрових водяних знаків.

Модифікація заповненого контейнера може здійснюватися як ненавмисно (стиснення, помилки при передачі файлу по каналу зв'язку з перешкодами), так і навмисно (спроба порушити авторські права шляхом знищення ЦВЗ). Підвищення стійкості до стиснення здійснюється шляхом ретельного дослідження алгоритмів компресії з метою визначення областей контейнера, що не піддаються модифікаціям. Дієвим методом боротьби з навмисним руйнуванням ЦВЗ може вважатися вбудовування інформації в ту

область файлу-контейнера, зміна якої призводить до деградації зображення. Традиційним і досить потужним способом боротьби з «перешкодами» може служити збільшення надмірності вбудованого повідомлення.

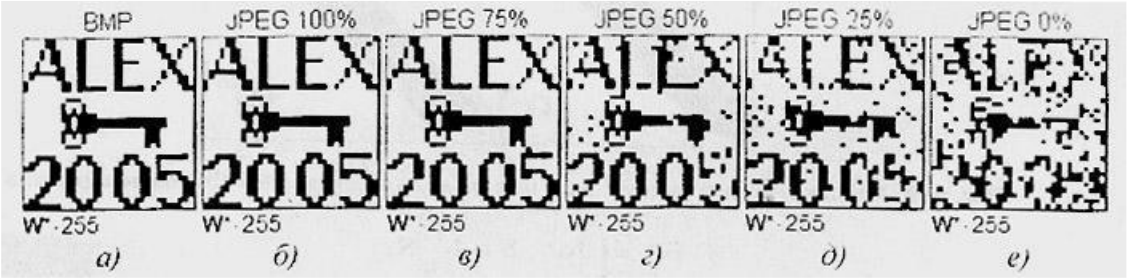

Рисунок 2.4 – Спотворення ЦВЗ при стисненні: а) - вихідний ЦВЗ; б) - е) - ЦВЗ, витягнутий контейнера, стисненого з різним ступенем

Обсяг обчислень, необхідний для вбудови повідомлення в цифрове зображення.

Незважаючи на стрімке зростання можливостей сучасних комп'ютерів, проблема обчислювальної складності алгоритмів вбудовування продовжує грати ключову роль в деяких областях застосування стеганографії. Це, як правило, інформаційні системи реального часу, де часові рамки виконання алгоритму сильно обмежені. Як приклад, можна навести гіпотетичний прихований канал голосового зв'язку, що працює за допомогою вбудови аудіоінформації в потік графічних файлів, що передаються по мережі. Очевидно, що в даному випадку, щоб уникнути втрати якості переданої інформації, пакети даних (цифрові зображення) повинні готуватися (заповнюватися повідомленнями) і можуть бути доставлені негайно.

Варто відзначити, що більшість стеганографічних алгоритмів не володіють великою обчислювальною складністю. Проте, спроби збільшення деяких параметрів ефективності (скритність, розмір повідомлення), можуть значно збільшувати обсяги обчислень і обмежувати використання алгоритму в системах реального часу.

Використовуваний графічний формат. Значною мірою ефективність застосування цифрових зображень в стеганографії залежить від формату їх зберігання.

У комп'ютерної стеганографії як контейнер може виступати практично будь-який файловий формат, проте найбільш поширеним типом носія є файли зображення формату BMP. Це пояснюється тим, що для цілей стеганографії найкращими є файли форматів, в яких використовуються методи стиснення без втрат (такі види стиснення типові для зображень формату BMP, TIFF, PNG, TGA, і ін.). Також позитивною стороною на користь вибору формату BMP виступає висока якість зображення і простота формату.

Варто відзначити, що при роботі з форматами файлів, що використовують стиснення з втратами, таким як JPEG, зазвичай все одно виконують перетворення потоку даних JPEG в потік даних BMP. З позиції стеганографії файли даного формату дозволяють приховувати порівняно великі обсяги інформації [10].

У даній роботі в якості контейнера розглядається 24-бітове растрове зображення в системі кольоровості RGB формату BMP. Кожна колірна комбінація тони (пікселя) являє собою комбінацію значень яскравості трьох складових кольорів - червоного (R), зеленого (G) і синього (B), які займають кожен по 1 байту (разом з 3 байта на точку). Таким чином, яскравість кожної складової записується 8 - бітовим числом і може змінюватися в діапазоні від 0 до 255 (комбінація (0, 0, 0) відповідає чорному кольору, комбінація (255, 255, 255) - білому).

Використання BMP-файлів обумовлено тільки лише простотою їх програмної обробки, - все отримані результати з легкістю можуть бути перенесені на випадок зображень в файлах інших форматів.

Сформульовано основні вимоги до вибору контейнера для стеганографічного приховування даних методом найменш значущих біт цифрового зображення, заснованих на властивостях цифрових зображень.

Представлені вимоги до вибору контейнера є важливими умовами, що дозволяють позбавити порушника явних переваг у виявленні факту приховування інформації і необхідні для задоволення умов ефективності в стеганографії, що використовує цифрові зображення в якості контейнерів. Критерії ефективності, описані в поточній чолі, можна виділити в дві умовні групи: технічні критерії і критерії, що не піддаються технічним описом. В якості технічного критерію оцінки ефективності, можна привести приклад ставлення максимального розміру вбудованого повідомлення, що не приводить до спотворення зображення, до розміру самого контейнера. У свою чергу, використовуваних графічний формат, що не піддається строгому математичному опису, є важливою умовою ефективності в стеганографії. Таким чином, обидві групи є рівнозначними умовами оцінки ефективності стеганографічної системи.

Отримані результати в подальшому можуть бути використані при дослідженні можливості вбудовування інформації в бітові площини зображень.

3 СТАТИСТИЧНІ АНАЛІТИЧНІ МЕТОДИ СТЕГАНОГРАФІЧНІ АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ LSB СТЕГАНОГРАФІЇ

Раніше розглянуті теоретичні оцінки стійкості стеганосистем, наприклад, теоретико-інформаційні, припускають, що той хто приховує інформацію і порушник володіють необмеженими обчислювальними ресурсами для побудови стеганосистем і, відповідно, стеганоатак на них, дотримуються оптимальних стратегій приховує перетворення і стеганоаналіз, мають у своєму розпорядженні нескінченним часом для передачі і виявлення приховуваних повідомлень та інше. Зрозуміло, такі ідеальні моделі того хто приховує інформацію і порушника застосовуються для реалій практичних стеганосистем. Тому розглянемо відомі до теперішнього часу практичні оцінки стійкості деяких стеганосистем, що реально використовуються для приховування інформації.

В останні роки з'явилися програмно-реалізовані стегосистеми, що забезпечують приховування інформації в цифрових відео- і аудіофайли. Такі програми вільно поширюються, легко встановлюються на персональні комп'ютери, сполучаються із сучасними інформаційними технологіями і не вимагають спеціальної підготовки при їх використанні. Вони забезпечують вбудовування тексту в зображення, зображення в зображення, тексту в аудіо-сигнал і т.п. В сучасних телекомунікаційних мережах типу Інтернет передаються дуже великі потоки мультимедійних повідомлень, які потенційно можуть бути використані для приховування інформації. Однією з найбільш актуальних і складних проблем цифрової стеганографії є виявлення факту такого приховування. В реальних умовах найбільш типовим видом атаки порушника є атака тільки зі стего, так як справжній контейнер йому зазвичай невідомий. У цих умовах виявлення прихованого повідомлення можливо на основі виявлення порушень залежностей, властивих природним контейнерів. Практичний стеганоаналіз цифрових стеганосістем є дуже

молодою наукою, однак в його арсеналі вже є ряд методів, що дозволяють з високою ймовірністю виявляти факт наявності стеганоканала, утворених деякими запропонованими до теперішнього часу стеганосистемам. Серед методів практичного стеганоаналіза найбільший інтерес представляє клас статистичних атак.

Порушення статистичних закономірностей природних контейнерів є одним з найбільш перспективних підходів для виявлення факту існування прихованого каналу передачі інформації є підхід, який представляє введення в файл приховується. При цьому підході аналізуються статистичні характеристики досліджуваної послідовності і встановлюється, чи схожі вони на характеристики природних контейнерів (якщо так, то прихованої передачі інформації немає), або вони схожі на характеристики стего (якщо так, то виявлено факт існування прихованого каналу передачі інформації). Цей клас стеганоатак є імовірнісним, тобто вони не дають однозначної відповіді, а формують оцінки типу "дана досліджувана послідовність з ймовірністю 90% містить приховане повідомлення". Імовірнісний характер статистичних методів стеганоаналіза не є істотним недоліком, так як на практиці ці методи часто видають оцінки ймовірності існування стеганоканала, що відрізняються від одиниці або нуля на нескінченно малі величини.

3.1 Атака на основі аналізу статистики Хі-квадрат

У методі використовується аналіз гістограми, отриманої за елементами зображення і оцінка розподілу пар значень цієї гістограми. Для BMP-файлів пари значень формуються значеннями пікселів зображення, для JPEG-квантуемого коефіцієнтами дискретного косинусного перетворення, які відрізняються по молодшому біту. Молодші біти зображень не є випадковими. Частоти двох сусідніх елементів контейнера повинні знаходитися досить далеко від значення частоти середнього арифметичного цих елементів. У «порожньому» зображенні ситуація, коли частоти елементів

зі значеннями 2N і 2N + 1 близькі за значенням, зустрічається досить рідко. При встановленні інформації дані частоти зближуються або стають рівними.

Ідея атаки хі-квадрат полягає в пошуку цих близьких значень і підрахунку ймовірності вбудови на основі того, як близько розташовуються значення частот парних і непарних елементів аналізованого контейнера.

Особливістю алгоритму є послідовний аналіз всього зображення і, відповідно, накопичення частот елементів.

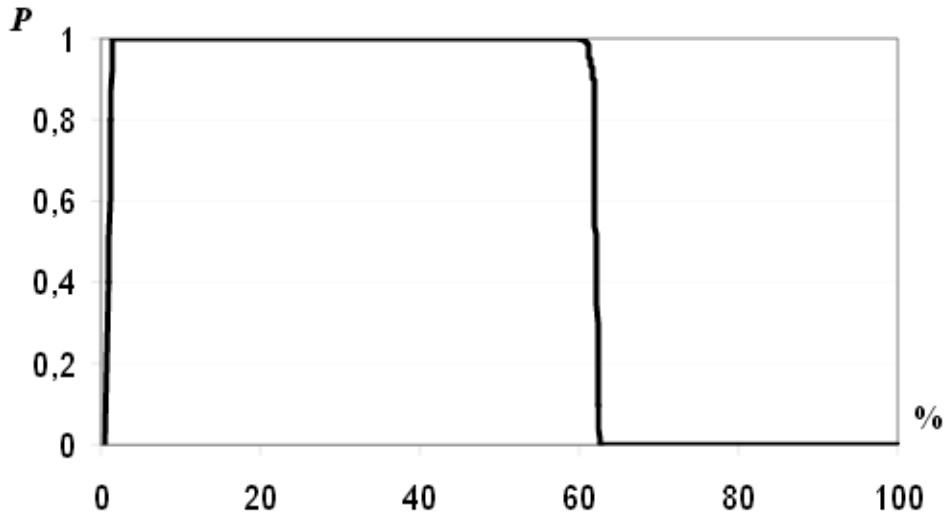

Рисунок 3.1 – Імовірність вбудови за критерієм Хі-квадрат при аналізі стегоконтейнера, отриманого методом послідовної заміни.

Метод Хі-квадрат є універсальним, так як підходить для аналізу зображень, створених різними програмами приховування. Однак результати роботи методу за критерієм Хі-квадрат в значній мірі залежать від способу приховування даних.

При послідовному записі в НЗБ елементів контейнера метод забезпечує хороші результати (рисунок 3.1), а при псевдовипадковому виборі молодших біт і розсіюванні повідомлення по всій довжині контейнера метод не спрацьовує [11].

3.2 Стеганоаналіз різниці на основі подвійної статистики

Одним з оригінальних методів статистичного стеганоаналіза є метод RS, вперше опублікованих в 2001 р колективом вчених під керівництвом Дж.Фрідріх. Скорочення в назві розшифровується як Regular-Singular, тобто «регулярно-сингулярних».

Суть методу полягає в наступному. Всі зображення розбивається на групи по n пікселів G (x, x2, ..., xn), де n парне, наприклад по 2 пікселя, що знаходяться 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 розуміємо ціле число від 0 до 255:

$$f(x_1, x_2, ..., x_n) = \sum_{i=1}^{n-1} | x_{i+1} - x_i | \qquad (3.1)$$

Функція *F (x)* називається фліппінгом і має властивість *F (F (x))=x*. Визначимо дві функції фліппінга – F_1, відповідає інверсії молодшого біта пікселя, і F_{-1}, що представляє собою інверсію з перенесенням в старший біт (додаток одиниці):

$$F_1 : 0 \leftrightarrow 1, 2 \leftrightarrow 3, ..., 254 \leftrightarrow 255 \qquad (3.2)$$

$$F_{-1} : 255 \leftrightarrow 0, 1 \leftrightarrow 2, 3 \leftrightarrow 4, ..., 253 \leftrightarrow 254, 255 \leftrightarrow 0 \qquad (3.3)$$

При застосуванні фліппінга до групи отримуємо перетворену групу пікселів. Далі, поділимо все групи пікселів на класи наступним чином:

$$\textit{Регулярні групи}: G \in R \Leftrightarrow f(F(G)) > f(G) \tag{3.4}$$

$$\textit{Сингулярні групи}: G \in I \Leftrightarrow f(F(G)) > f(G) \tag{3.5}$$

$$\textit{Невикористані групи}: G \in U \Leftrightarrow f(F(G)) > f(G) \tag{3.6}$$

Надалі нас буде цікавити співвідношення між групами в зображенні. Визначимо кількість груп потрапили в той чи інший клас як R_M, S_M, U_M, і R_{-M}, S_{-M}, U_{-M}, де індекси M і -M означають відповідно застосування і для отримання розподілу. Наша мета - визначити яким чином впровадження повідомлення методом LSB буде впливати на вищеописану статистику груп пікселів.

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

$$R_m \cong R_{-m} \; i \; S_m \cong S_{-m} \tag{3.7}$$

Припущення базується на тому, що застосування дасть той же розподіл, що і на зображенні, значення пікселів якого зрушені на одиницю. Для звичайного зображення співвідношення між групами не повинно істотно змінюватися. Значна розбіжність між значеннями свідчить про застосування LSB-стеганографії для молодших біт зображення.

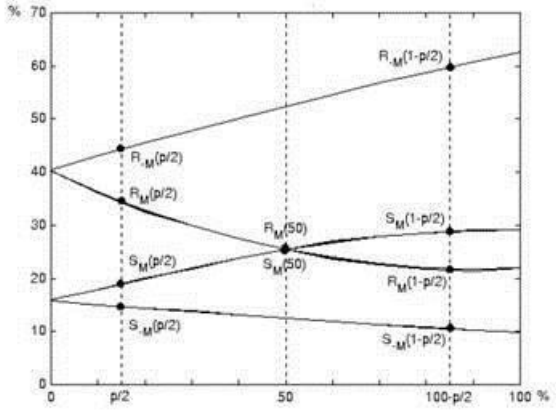

Рисунок 3.2 – RS-діаграма типового зображення

Розглянемо зміни молодших біт зображення при 100% перезапису їх бітами повідомлення. Впровадження випадкового повідомлення довжиною, що дорівнює розміру зображення, призведе до того, що 50% молодших біт будуть інвертовані. Це, в свою чергу зведе до нуля різницю між значеннями і. Однак на і впровадження повідомлення буде впливати прямо протилежно, і різниця цих величин буде пропорційна ступеню заповненості контейнера, іншими словами довжині повідомлення. На рисунку 3.2 приведена RS-діаграма для типового зображення. На осі абсцис розташовано кількість інвертованих біт x, шукана довжина повідомлення p, на осі ординат - відносні значення регулярних і сингулярних груп по відношенню до загальної кількості груп зображення [7,12].

Методу аналізу на основі Хі-квадрат є універсальним методом стеганографічного аналізу і заснований на порівнянні частот сусідніх елементів зображення. Даний метод показує гарні результати при використанні послідовного вбудовування інформації в елементи контейнера. Однак суттєвим недоліком даного методу є те, що при псевдовипадковому вбудовування даних метод не може бути застосований.

Метод RS є досить новим методом стеганоаналіза, заснованому на аналізі співвідношення між групами в цифровому зображенні. Даний метод дозволяє уникнути недоліки, властиві методу аналізу на основі Хі-квадрат,

так як він не залежить від методу вбудовування інформації в просторові області зображень.

Надалі ці методи можуть бути використані в ході наукової роботи для дослідження можливості вбудовування інформації в бітові області зображень в якості критерію стеганографічної стійкості системи.

4 ОЦІНКА СТЕГАНОГРАФІЧНІ ЄМКОСТІ БІТОВИХ ПЛОЩИН СТЕГАНОКОНТЕЙНЕРОВ

Однією з важливих задач стеганографії є вибір відповідного контейнера. Незважаючи на велику кількість досліджень в даній області, вибір контейнера для стеганографічного приховування даних все ще освітлений в недостатній мірі.

Метою даної наукової роботи є дослідження статистичних властивостей природних зображень-контейнерів, що дозволяє забезпечити найкращу стійкість стеганографічної системи.

В якості досліджуваного формату цифрових зображень був обраний формат BMP. Вибір даного формату цифрових зображень був обумовлений тим, що він забезпечує можливість вбудовування більшої кількості даних і не використовує алгоритмів стиснення зображення. Останнє є важливим фактом, тому що вбудовування інформації в цифрове зображення відбувається в найменш значущий біт, що при використанні зображень з різними алгоритмами стиснення може привести до втрати або пошкодження вбудованої інформації.

В ході роботи було проаналізовано понад 100 різних зображень формату BMP. Досить часто при виборі відповідного контейнера для стеганографії, зображення поділяють на різні групи. Однак ці поділу є досить умовними, тому в ході даної роботи зображення не піддавалися на розділення по групах. Науковий інтерес представляють лише статистичні властивості досліджуваних зображень. До всіх досліджуваних зображень пред'являлися наступні вимоги.

1. Зображення повинні бути вихідним файлом, а не бути отриманими шляхом конвертації інших цифрових форматів зображень у формат BMP.
2. Зображення не повинні бути створені з використанням будь-яких графічних редакторів.

3. Всі зображення повинні мати однаковий розмір, що виключить вплив розміру зображення на отримані результати.

Вбудовування інформації в досліджувані зображення відбувалося за коштами методу LSB, яким є досить популярним методом вбудовування в стеганографії і має на увазі використання найменш значущі біти зображення. Одним із серйозних помилок в стеганографії є те, що молодші біти зображень є нічим іншим, як шумом. Однак це зовсім не так, між молодшими бітами зображень встановлюються цілком певні залежності, які змінюються при стеганографічному приховуванні інформації.

Для визначення цих змін, в роботі використовується метод дослідження статистики розподілу Хі-квадрат і RS-метод стеганографічного аналізу. Таким чином, зображення з найменшим відхиленням даних оцінок між природним і стегаконтейнером буде найкращим з точки зору стеганографічного приховування інформації.

В ході дослідження були вивчені залежності оцінок Хі-квадрат і RS від статистичних властивостей природних зображень-контейнерів, таких як монотонність, ентропія і дисперсія зображення.

4.1 Дослідження статистичних властивостей зображення при встановленні інформації в молодшу бітову площину

Впровадження інформації буде здійснюватися в молодшу бітову площину цифрового зображення за засобами LSB методу. Розглянемо залежність зміни статистики Хі - квадрат від монотонності зображення. За монотонність будемо приймати величину, що характеризує відносне відсоткове співвідношення колірних відтінків зображення.

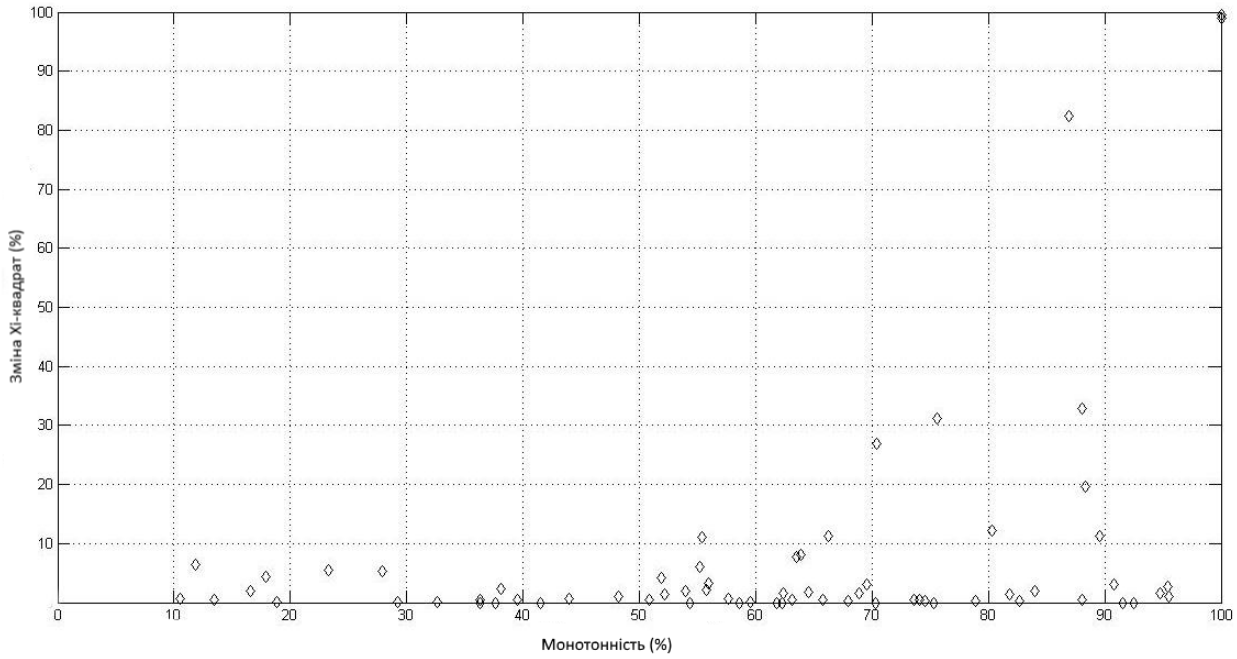

Рисунок 4.1 – Залежність зміни статистики Хі-квадрат від монотонності зображення

На основі графіка (рисунок 4.1) можна зробити висновок, що найбільш підходящими зображеннями в якості стегоконтейнер є зображення, що володіють найменшою монотонністю. Максимальна зміна статистики Хі-квадрат (100%) знаходиться в точці, де монотонність зображення досягає 100%. Таким чином, аналізуючи таку характеристику як "монотонність" зображення, зображення містять більшу кількість областей монотонної заливки, є менш бажаними в якості стегоконтейнер і забезпечують погану скритність вбудованого повідомлення.

Однак, однією характеристики зображення недостатньо, щоб визначити найбільш підходящі при виборі зображень в якості контейнера. Важливими статистичними характеристиками цифрового зображення є ентропія і дисперсія.

Залежність зміни Хі-квадрат від ентропії молодшої бітової площини зображення представлені на рисунку 4.2.

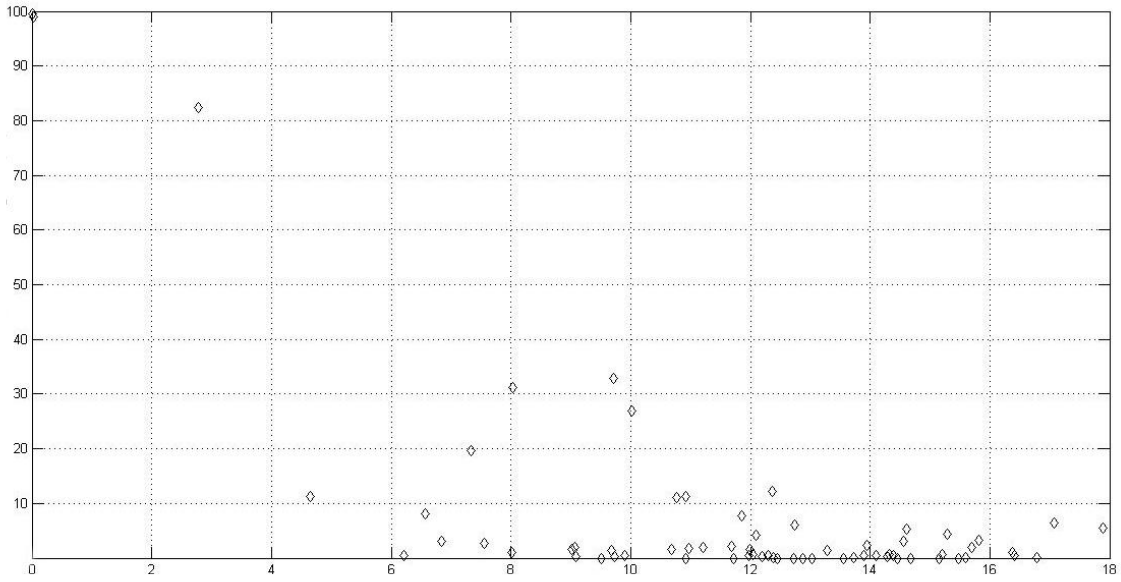

Рисунок 4.2 – Залежність зміни Хі-квадрат від ентропії молодшої бітової площини

На графіку видно, що зміна Хі-квадрат зменшується зі збільшенням ентропії досліджуваних зображень. Виходячи з цього можна зробити висновок, що критерій Хі-квадрат природного зображення і зображення, що містить Стего, ближче у тих зображень, ентропія яких вище. Так як ентропія цифрового зображення характеризує величини яскравості варіацій зображення, то система, яка використовує в якості контейнера строкаті зображення з великою кількістю дрібних деталей, забезпечує більшу надійність.

Для визначення розкиду значень молодших біт використовується математична величина - дисперсія. Недоліком методу визначення дисперсії є чутливість до розміру зображення. Сусідні пікселі двох однакових зображень з різним дозволом відрізняються кількістю пікселів, що припадають на однакові фрагменти зображення. Чим менше розмір зображення, тим більше будуть відрізнятися два сусідніх пікселів, ніж у такого ж зображення більшого розміру. Саме тому в даній роботі було прийнято використовувати зображення однакового розміру. На рисунку 4.3 представлена залежність зміни Хі-квадрат і дисперсії зображення.

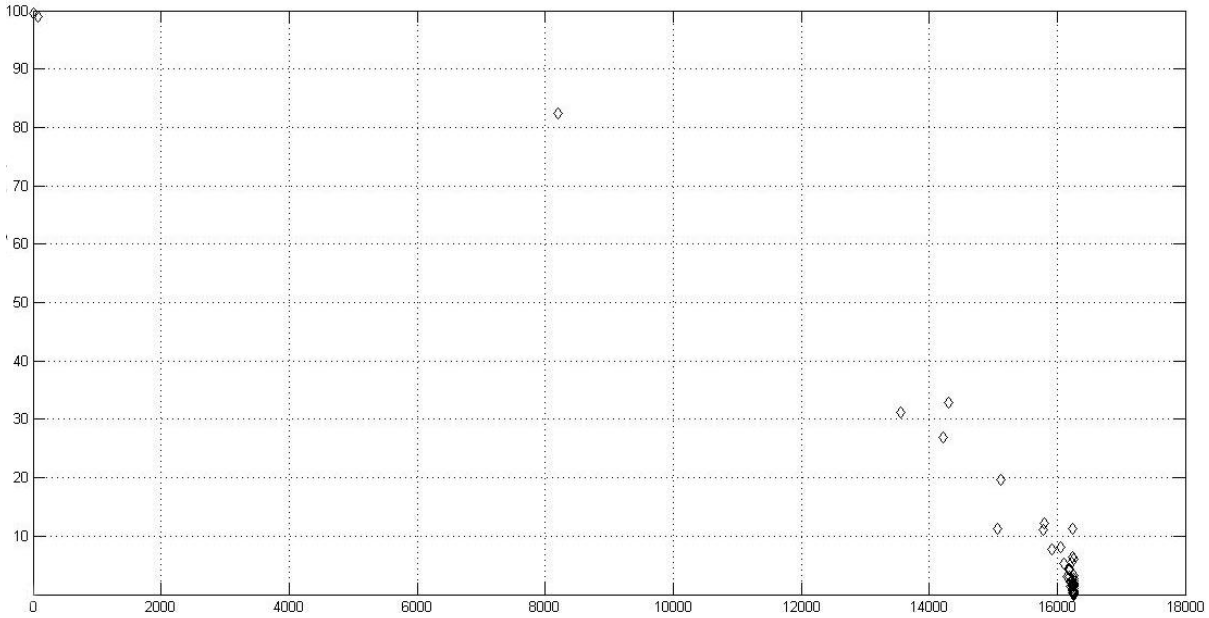

Рисунок 4.3 – Залежність зміни Хі-квадрат від дисперсії молодшої бітової площини

Результати аналізу залежності зміни (рисунок 4.3) Хі-квадрат від дисперсії зображення показують, що зі збільшенням дисперсії зображення, різниця Хі-квадрат природного контейнера і контейнера, що містить стего, зменшується. Таким чином, зображення, що володіють більшою дисперсією в молодшій бітової площині, є найбільш придатними в якості контейнера для вбудовування секретної інформації.

Підводячи підсумки стеганографічної атаки на основі критерію Хі-квадрат, можна помітити, що найбільш підходящими як стегоконтейнер є зображення, що володіють меншою монотонністю і великими ентропією і дисперсією.

Розглянемо залежності RS - стеганоаналіза від статистичних властивостей зображень, представлених вище, тобто монотонності, ентропії і дисперсії. Як вже було помічено раніше RS - стеганоаналіз є досить ефективним методом для виявлення стеганографічного приховування інформації в цифрових зображеннях.

На рисунку 4.4 і рисунку 4.5 представлені залежності змін регулярних і сингулярних груп від монотонності зображень.

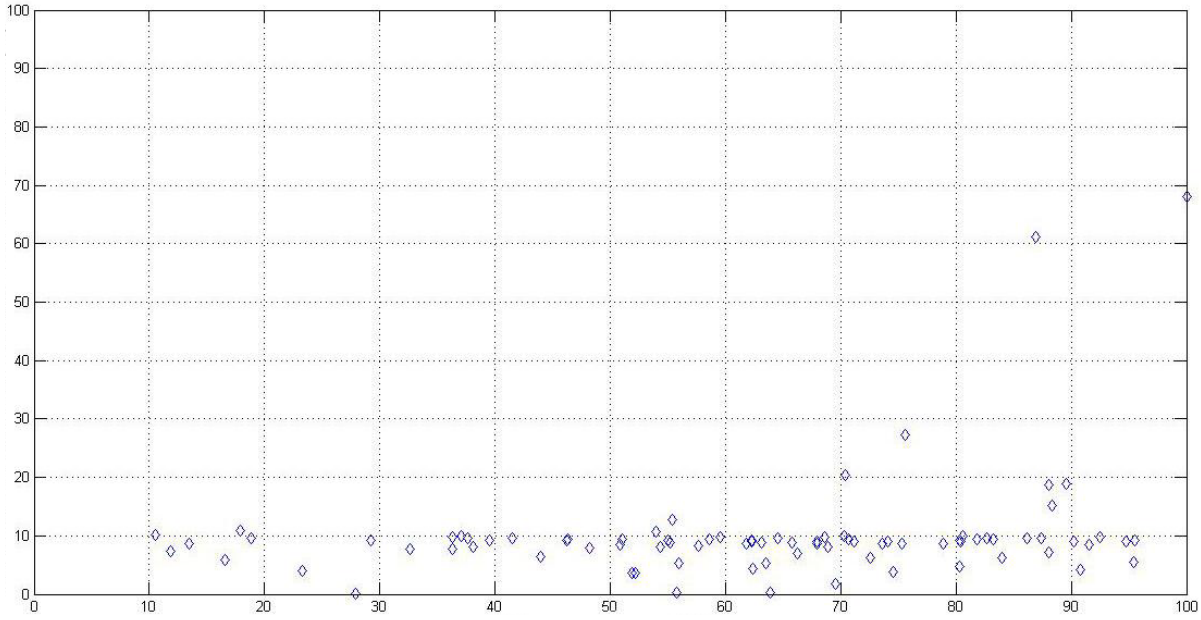

Рисунок 4.4 – Залежність зміни процентного співвідношення регулярних груп від монотонності

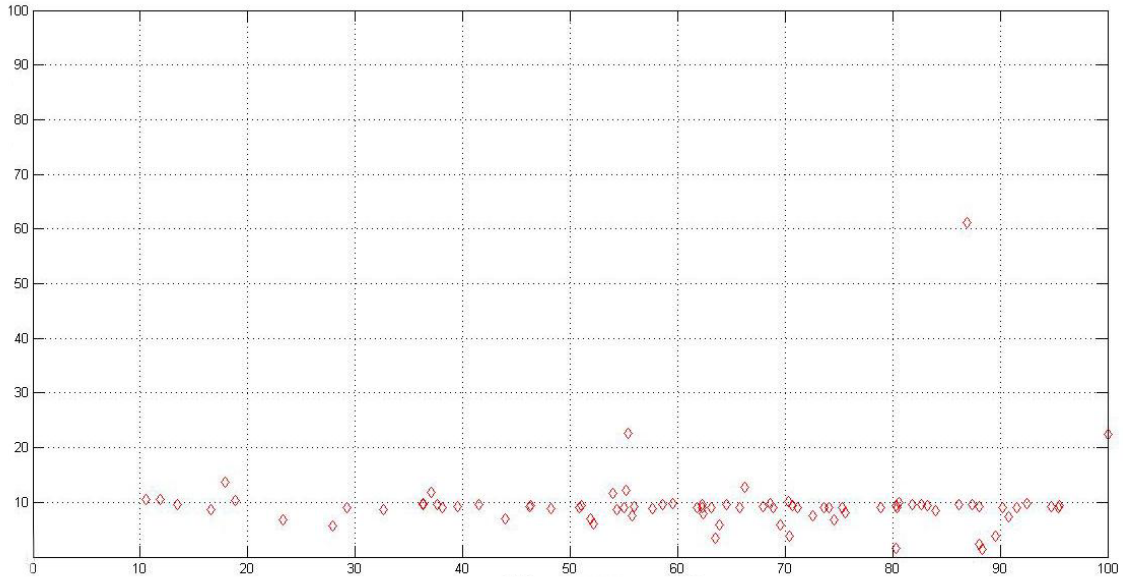

Рисунок 4.5 – Залежність зміни процентного співвідношення сингулярних груп від монотонності

Аналіз залежностей на рисунке 4.4 і рисунке 4.5 показує, що RS-метод є менш чутливим до монотонності зображення, тому дана характеристика зображення не є об'єктивною в разі застосування RS-методу при виборі стегоконтейнер.

Звернемося до ентропії зображення і проаналізуємо поведінку методу в даному випадку. Аналіз отриманих результатів показує, що, як і в випадку з методом аналізу, заснованого на критерії Хі-квадрат, найбільш підходящими зображеннями в якості стегоконтейнер, є зображення, що володіють більшою ентропією. Зміна регулярних і сингулярних груп природних і стего-контейнерів менше у зображень з більшою ентропією в молодшій бітової площини рисунке 4.6 і 4.7.

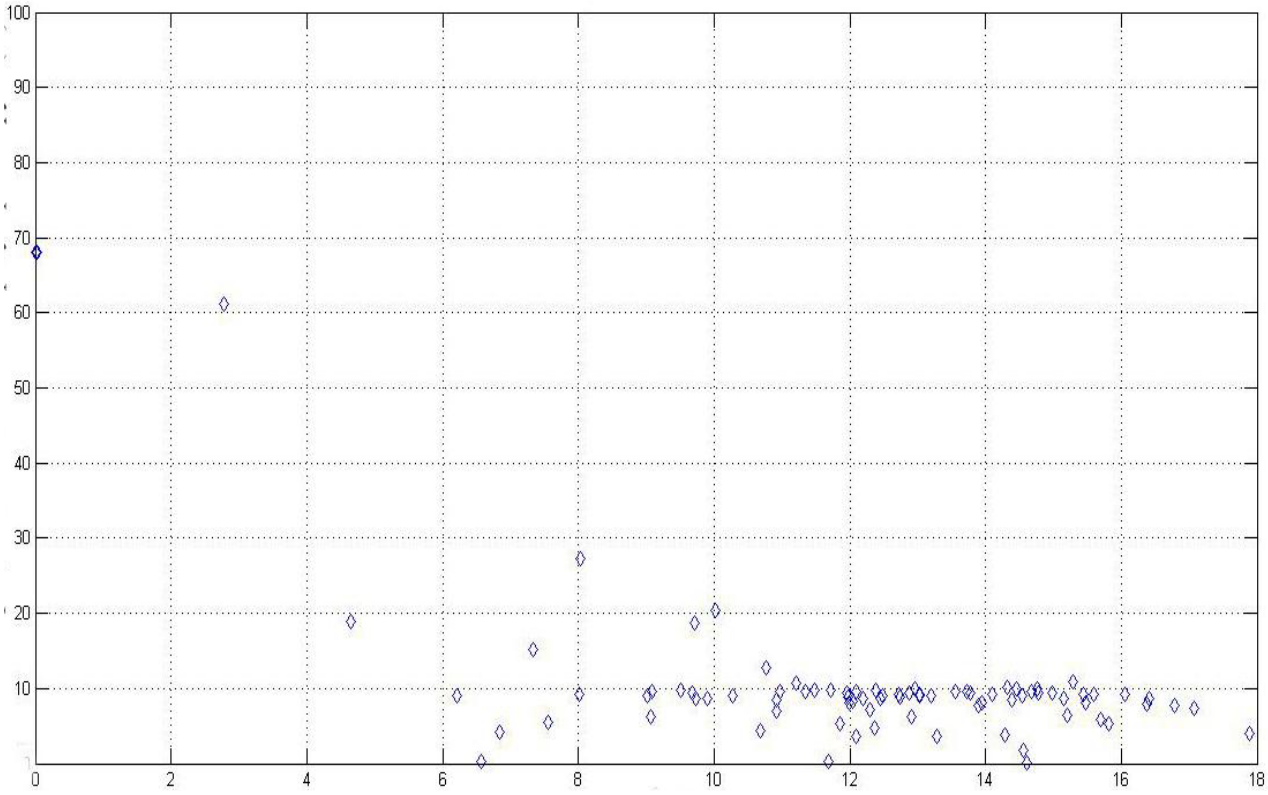

Рисунок 4.6 – Залежність зміни процентного співвідношення регулярних груп від ентропії молодшої бітової площини

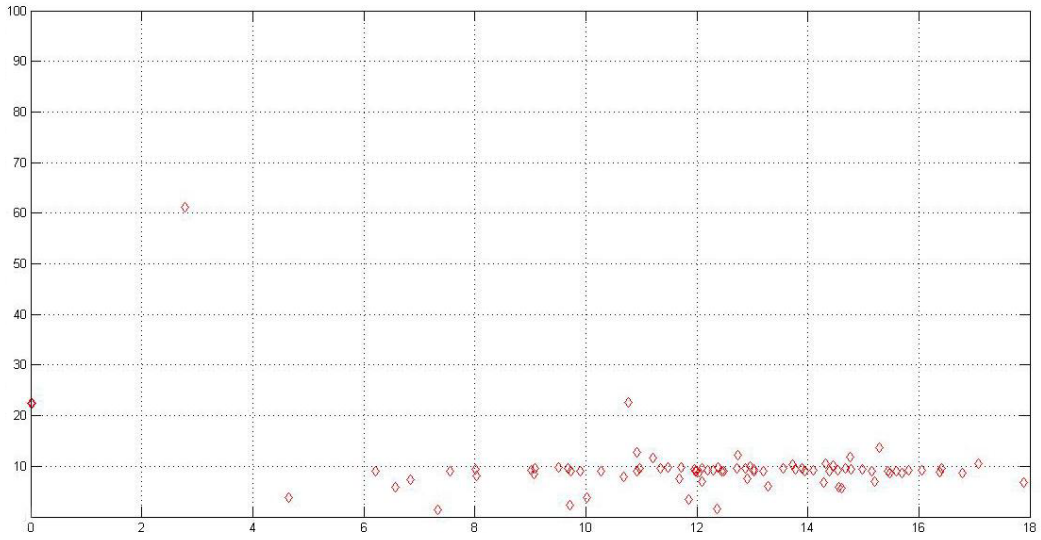

Рисунок 4.7 – Залежність зміни процентного співвідношення сингулярних груп від ентропії молодшої бітової площини

Аналіз залежності RS - стегоаналіза від дисперсії зображення (рисунок 4.8 і рисунок 4.9) також показав, що, як і в методі аналізу на основі критерію Хі -квадрат, зображення з більшою дисперсією найбільш підходящі в якості контейнера для методу LSB.

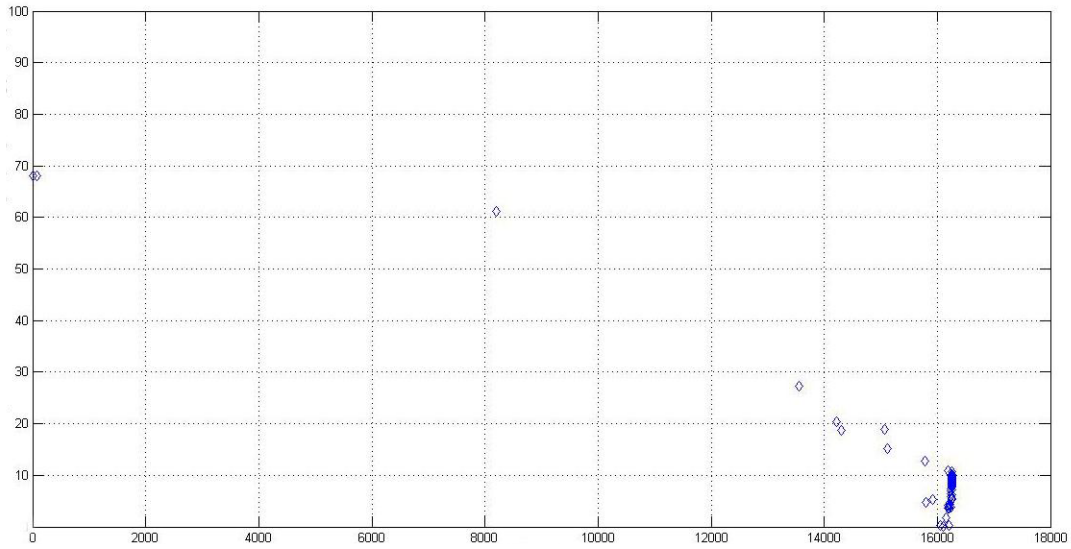

Рисунок 4.8 – Залежність зміни процентного співвідношення регулярних груп від дисперсії молодшої бітової площини

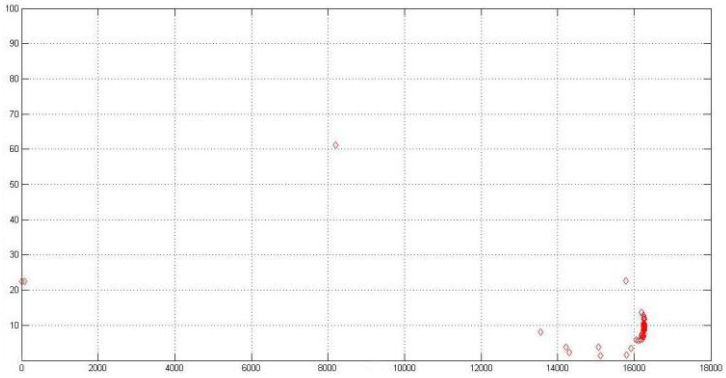

Рисунок 4.9 – Залежність зміни процентного співвідношення сингулярних груп від дисперсії молодшої бітової площини

4.2 Дослідження статистичних властивостей цифрових зображення при встановленні інформації в другу бітову площину

Одним із суттєвих недоліків методу LSB є невелика кількість інформації можливе вбудувати в разі використання виключно найменш значущих біт цифрового зображення. Таким чином, постає необхідність вивчення можливості задіяння найбільш значущих біт зображення для вбудовування інформації. Розглянемо результати вбудовування повідомлення у другі біти зображення. На малюнку 4.10 показана залежність зміни критерію Хі-квадрат від дисперсії зображення.

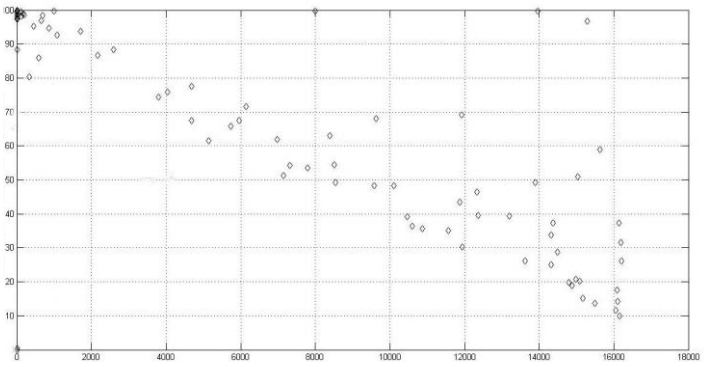

Рисунок 4.10 – Залежність зміни Хі-квадрат від дисперсії другий бітової площини

Дисперсії другий бітової площині зміна показника Хі-квадрат зменшується. Однак, аналізуючи значення дисперсії другий бітової площини, можна помітити, що розкид значень дисперсії збільшується в порівнянні з молодшою бітової площиною. На рисунках 4.11 і 4.12 показані результати роботи методу регулярних - сингулярних груп. Результати є схожими з результатами роботи методу Хі-квадрат, і показують, що найбільш підходящими зображеннями в якості контейнера є зображення, що володіють найбільшим значенням дисперсії другий бітової площини зображення.

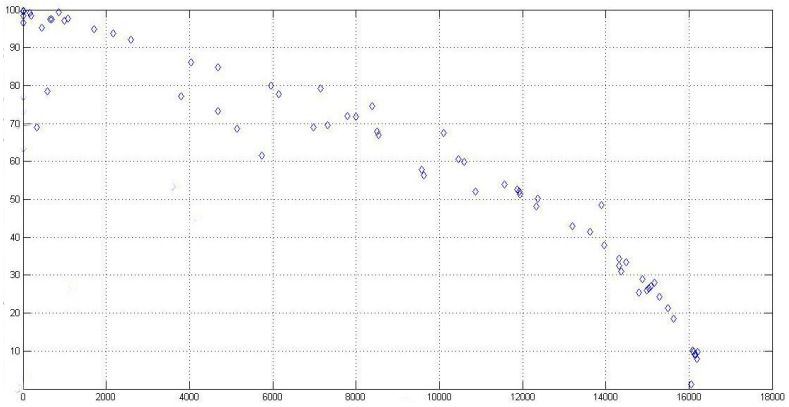

Рисунок 4.11 – Залежність зміни процентного співвідношення регулярних груп від дисперсії другий бітової площини

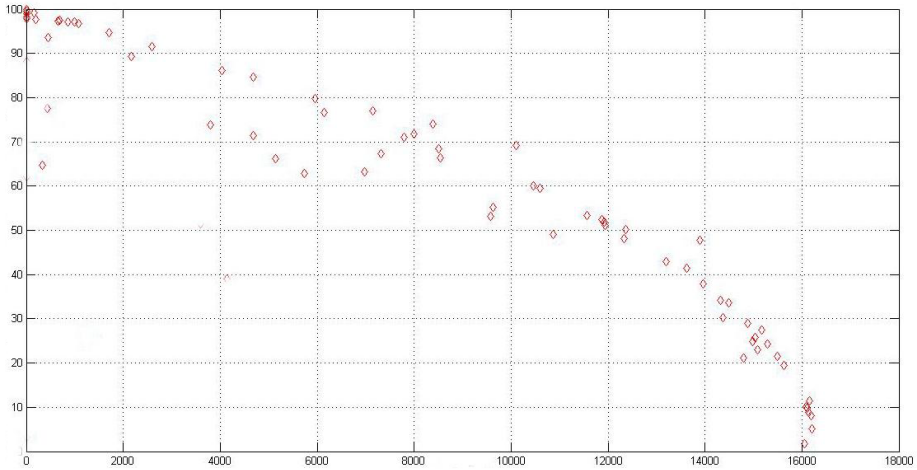

Рисунок 4.12 – Залежність зміни процентного співвідношення сингулярних груп від дисперсії другий бітової площини

Розглянемо результати роботи методу Хі-квадрат і RS методу щодо ентропії зображення. На рисунке 4.13 представлена залежність зміни Хі - квадрат від ентропії.

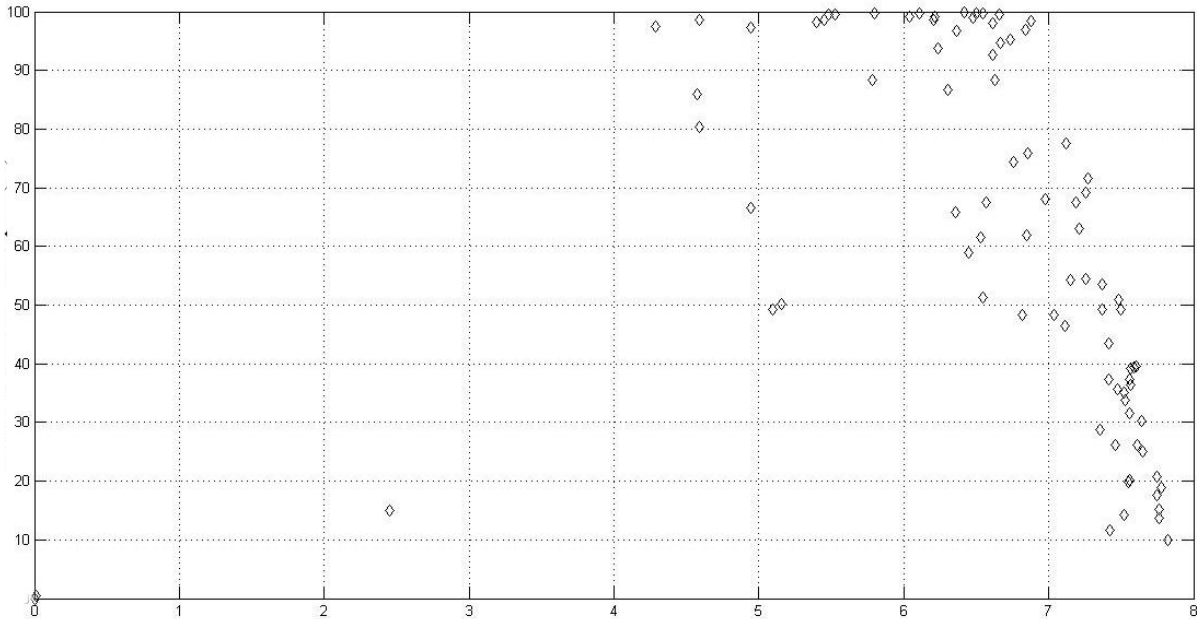

Рисунок 4.13 – Залежність зміни критерію Хі-квадрат від ентропії другий бітової площини

Так само, як і в випадку вбудовування в найменш значущі біти зображення, при встановленні в другу бітову площину найбільшою стійкістю до статистичного методу аналізу Хі - квадрат мають зображення з великим значенням ентропії в другій бітової площині. Як можна помітити, чисельне значення ентропії другий бітової площини зменшується щодо молодшої бітової площині, що робить другі біти менш привабливими для вбудовування в порівнянні з молодшими бітами.

RS методу стеганоаналіза щодо ентропії цифрового зображення показує схожі результати: найбільшою стеганографічної стійкістю володіють зображення з великим значенням ентропії другий бітової площині (рисунок 4.14 і рисунок 4.15).

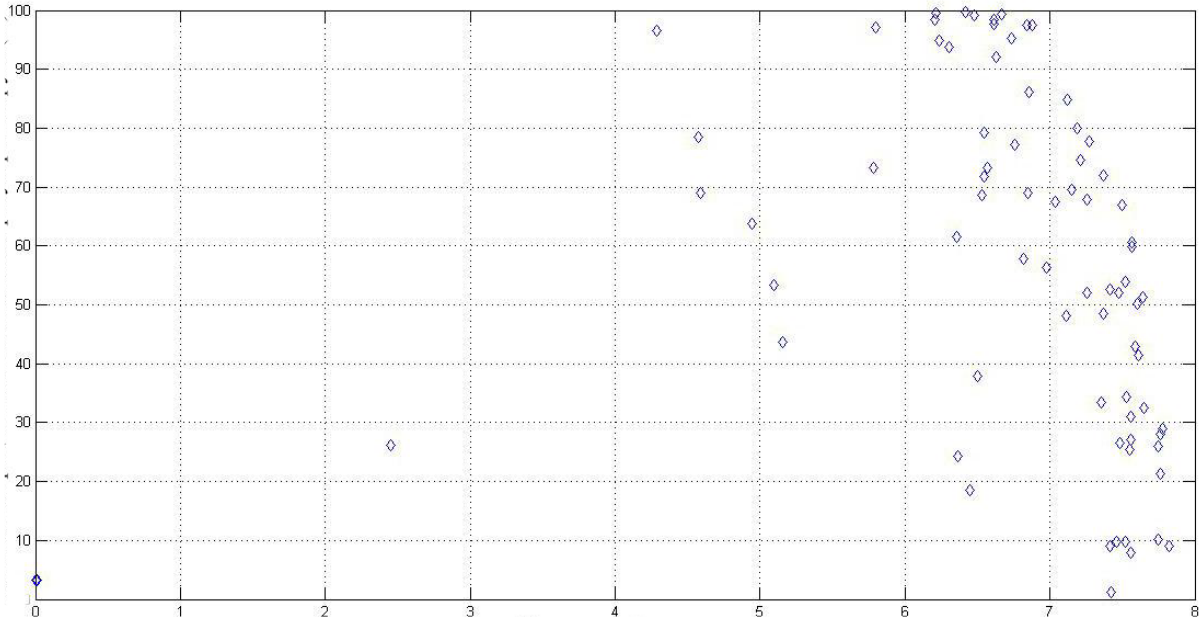

Рисунок 4.14 – Залежність зміни процентного співвідношення регулярних груп від ентропії другий бітової площини

Таким чином, в разі необхідності задіяння другого біта цифрового зображення для вбудовування стеганографічного повідомлення, необхідно віддавати переваги зображенням, що володіє більшою дисперсією і ентропією в другій бітової площині. Однак використання другого біту зображення підвищує шанс виявлення факту впровадження повідомлення засобами аналізу бітових зрізів зображення.

4.3 Дослідження статистичних властивостей цифрових зображення при встановленні інформації в третю бітову площину

Проаналізуємо можливість використання третіми бітової площини цифрових зображень для стеганографічного приховування даних.

На рисунку 4.15 представлена залежність зміни критерію Хі - квадрат від дисперсії.

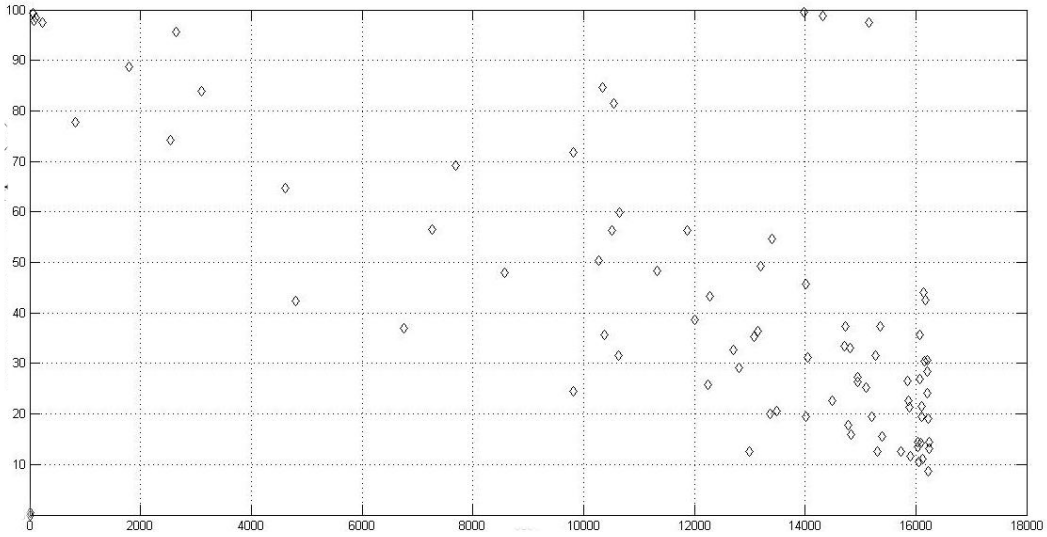

Рисунок 4.15 – Залежність зміни процентного співвідношення регулярних груп від ентропії другий бітової площини

З залежності на рисунку 4.16 можна побачити, що, як і у випадку з більш молодшими бітовими площинами, найбільшою стеганографічної стійкістю володіють зображення з великим значенням дисперсії.

Розглядаючи поведінку методу RS, можна прийти до аналогічного висновку (рисунок 4.16 і рисунок 4.17).

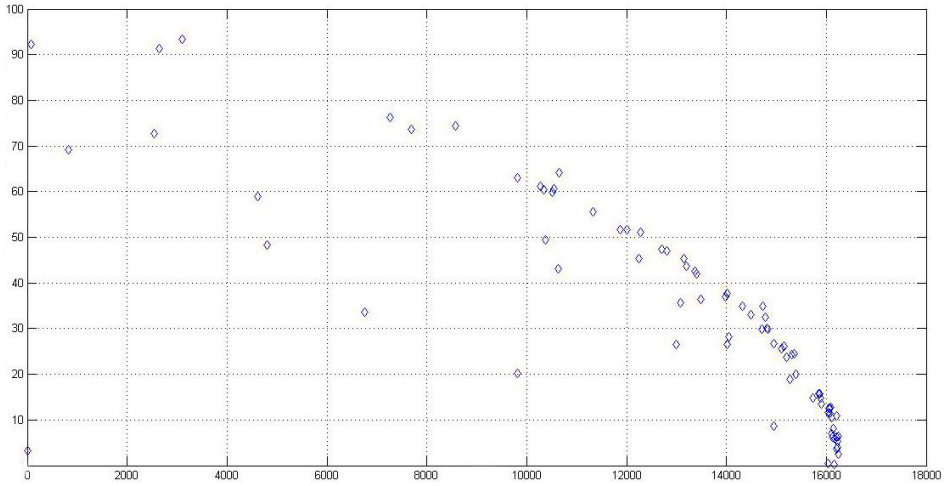

Рисунок 4.16 – Залежність зміни процентного співвідношення регулярних груп від дисперсії третьої бітової площини

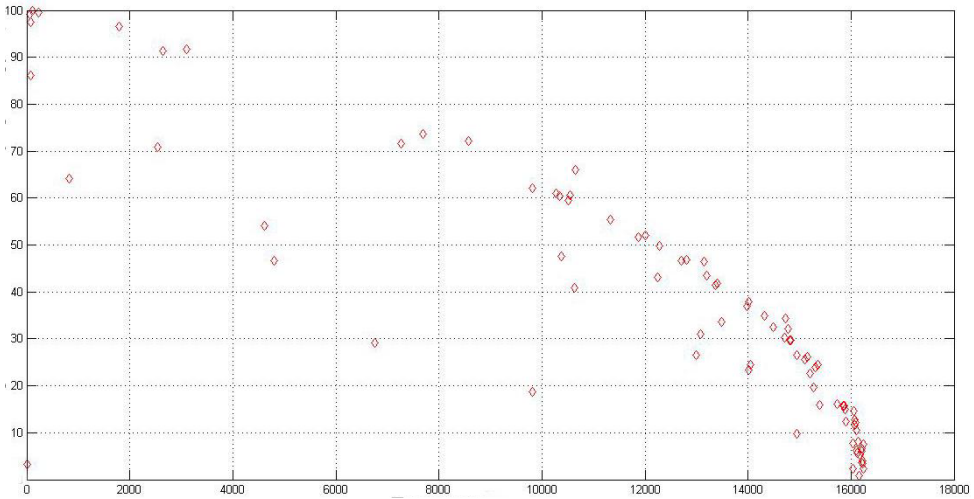

Рисунок 4.17 – Залежність зміни процентного співвідношення сингулярних груп від дисперсії третьої бітової площини

Розглянемо далі залежність критерію Хі - квадрат і регулярних, сингулярних груп від ентропії. На рисунку 4.18 представлена залежність Хі - квадрат від ентропії третьої бітової площини зображення. Як і в попередніх випадках впровадження інформації в бітові площини зображень, найбільшою стійкістю, як стеганографічної системи, володіє цифрове зображення, ентропія якої вище.

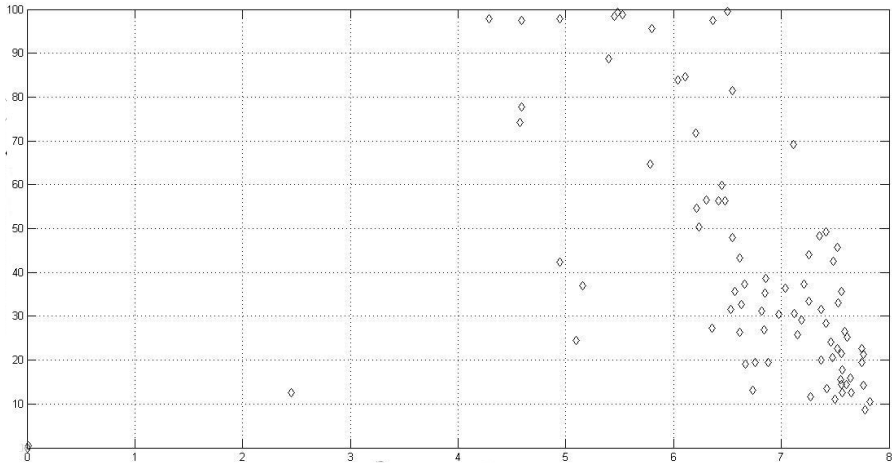

Рисунок 4.18 – Залежність зміни критерію Хі - квадрат від ентропії третьої бітової площини

Аналіз результатів роботи RS методу (рисунок 4.19 і 4.20), також показують, що для найбільшої надійності цифрового зображення в якості контейнера, для впровадження інформації в третю бітову площину необхідно використовувати зображення, що володіють найбільшою ентропією в третіх бітах.

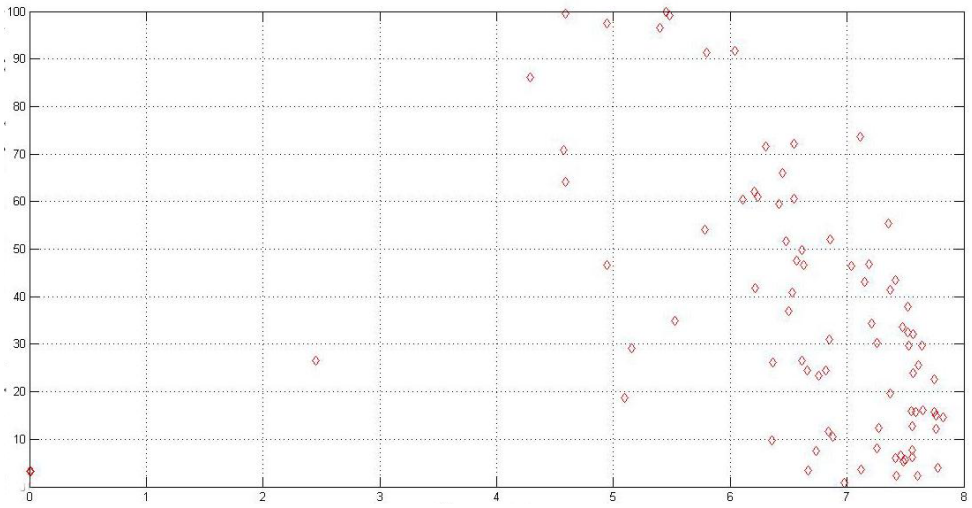

Рисунок 4.19 – Залежність зміни процентного співвідношення регулярних груп від ентропії третьої бітової площини

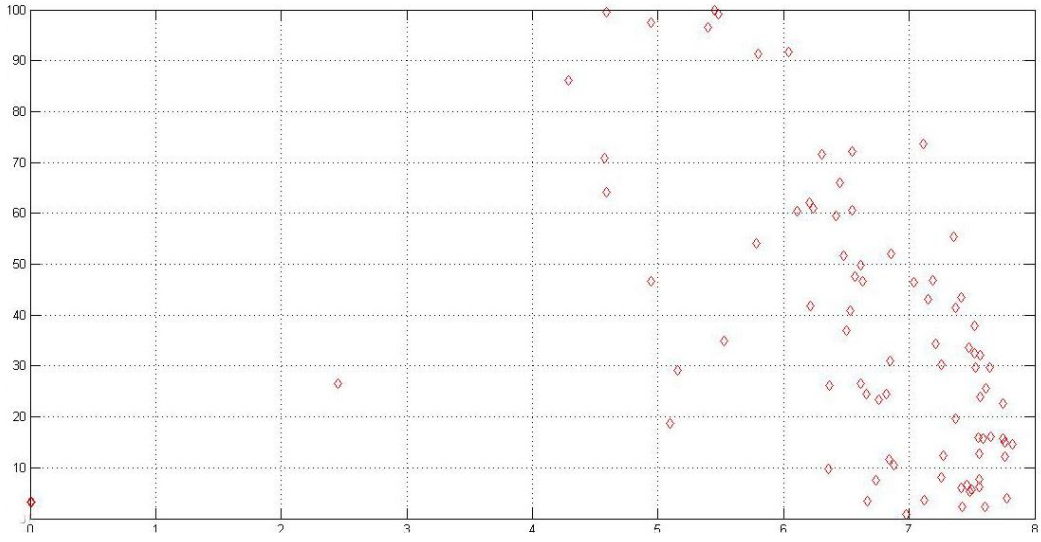

Рисунок 4.20 – Залежність зміни процентного співвідношення сингулярних груп від ентропії третьої бітової площини

4.4 Дослідження статистичних властивостей цифрових зображення при встановленні інформації в четверту бітову площину

Для отримання більшої кількості статистичних даних досліджуємо статистичні властивості цифрових зображень для вивчення можливості вбудовування інформації в четверті біти. Четверті біти вносять значний вклад у формування зображення, що робить їх використання досить небезпечним для виявлення стеганографічного приховування інформації в зображенні-контейнері.

Як і у випадку з менш значущими бітами, аналіз проводиться за коштами методів стегоаналіза Хі-квадрат і RS. На рисунку 4.21 представлена залежність зміни статистики Хі-квадрат від дисперсії четвертої бітової площині.

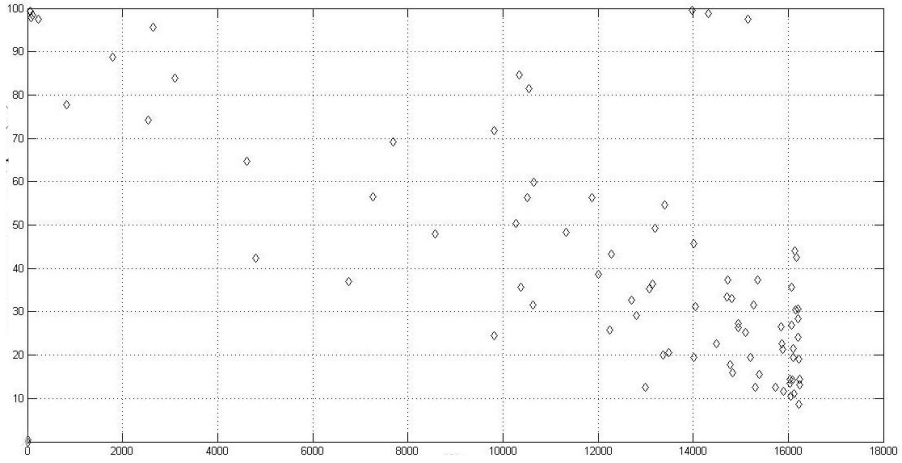

Рисунок 4.21 – Залежність зміни Хі-квадрат від дисперсії четвертої бітової площини

Аналіз залежності показує, що найменша зміна статистичних показників Хі-квадрат показують цифрові зображення, четверті біти яких мають більшу дисперсією. Однак слід зазначити, що значення дисперсії

четверте бітових площин досліджуваних зображень все більше вирівнюються відносно один одного.

Розглянемо залежність зміни регулярних і сингулярних груп зображень щодо значень дисперсії (рисунок 4.22 і рисунок 4.23).

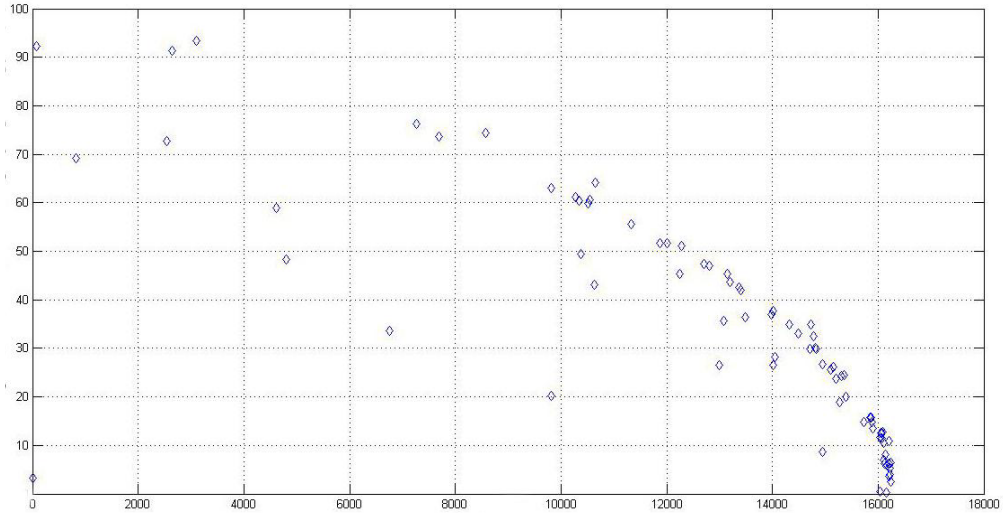

Рисунок 4.22 – Залежність зміни процентного співвідношення регулярних груп від дисперсії четвертої бітової площини

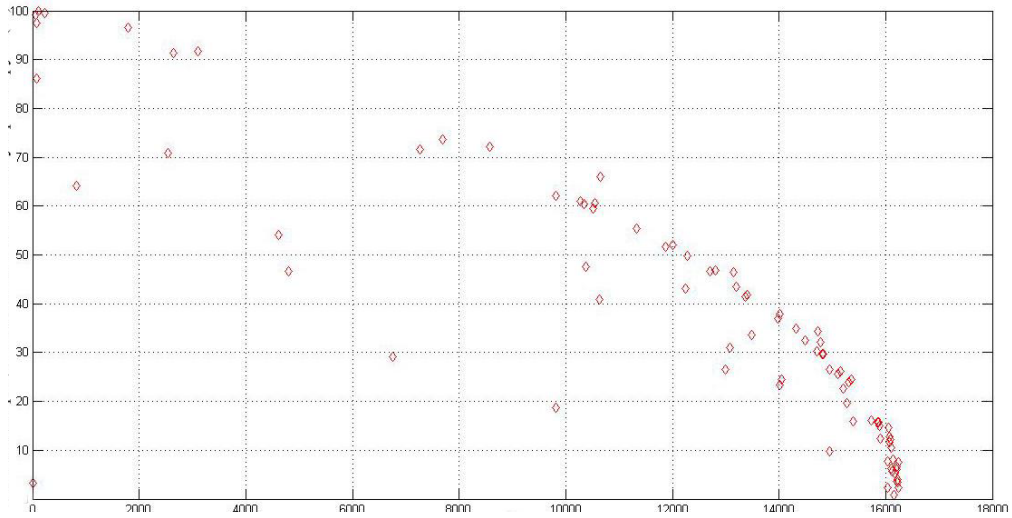

Рисунок 4.23 – Залежність зміни процентного співвідношення сингулярних груп від дисперсії четвертої бітової площини

Отримані дані RS аналізу показують, що, як і в разі аналізу зміни Хі-квадрат, зображення, що володіють більшою дисперсією в четвертій бітової площині, є більш стійкими до статистичних методів стеганоаналіза.

Далі на рисунку 4.24 представлена залежність зміни Хі-квадрат від ентропії четвертої бітової площині зображень.

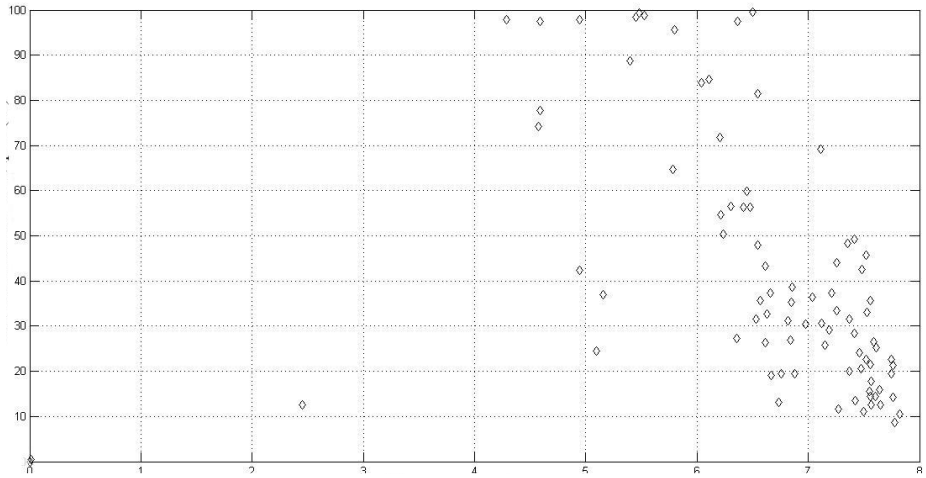

Рисунок 4.24 – Залежність зміни Хі-квадрат від ентропії четвертої бітової площини

Чи не складно помітити, що значення ентропії четвертої бітової площини досліджуваних зображень ще більше вирівнялися один щодо одного, в порівнянні зі значеннями ентропії третьої або другий бітових площин. Незважаючи на це, результат аналізу залежності на рисунку 4.24, що при виборі зображення-контейнера для вбудовування в четверті біти, слід звертати пильнішу увагу на зображення, що володіють великим значенням ентропії в цих бітах.

Яким чином зміни регулярних і сингулярних груп RS стегоаналіза, при встановленні в четверні біти цифрових зображень, залежать від ентпропіі показано на рисунках 4.25 і 4.26. При необхідності задіяння четверте біт зображення для приховування секретних даних, слід використовувати зображення, що володіють максимальним значенням ентропії четвертих біт.

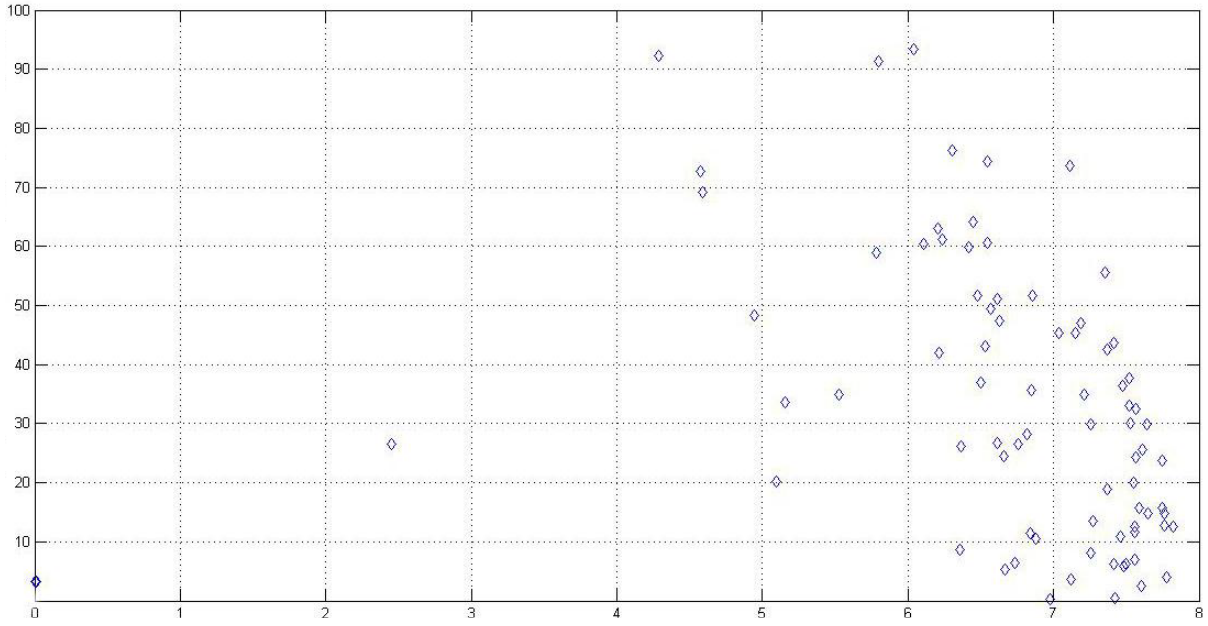

Рисунок 4.25 – Залежність зміни процентного співвідношення регулярних груп від ентропії четвертої бітової площини

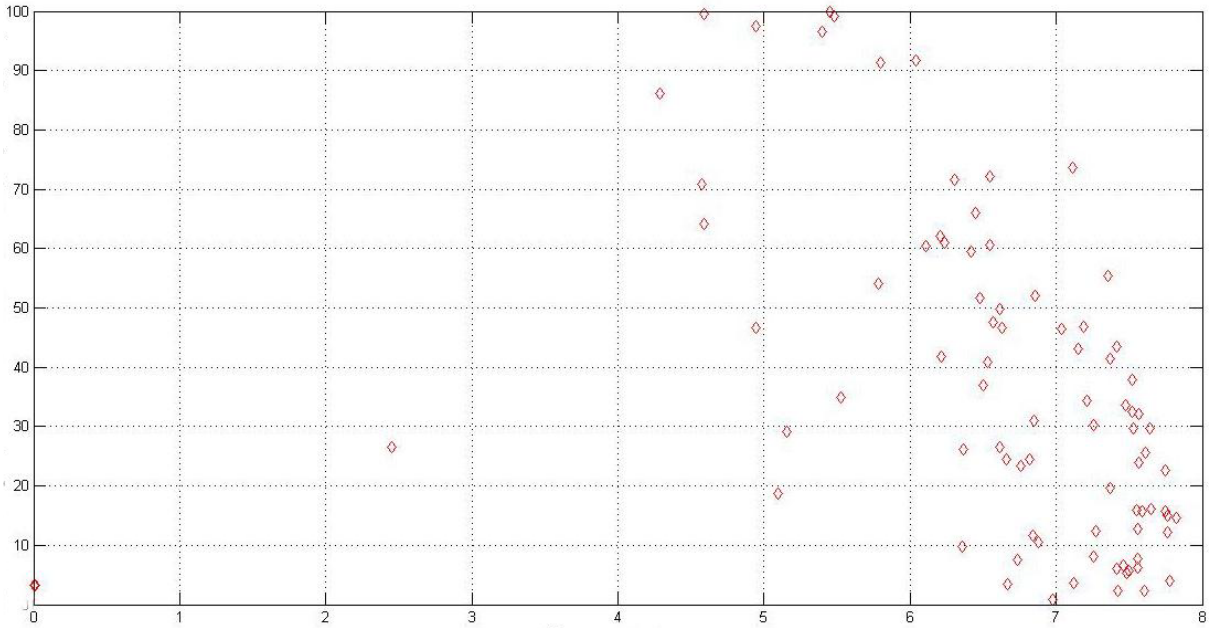

Рисунок 4.25 – Залежність зміни процентного співвідношення сингулярних груп від ентропії четвертої бітової площини

ВИСНОВКИ

Мета цієї роботи полягає у визначенні характеристик цифрових зображень-контейнерів, які забезпечують найбільшу стійкість стеганографічної системи. Для досягнення зазначеної мети, було вирішено ряд теоретичних і практичних завдань. В ході проведених досліджень отримані наступні основні результати.

1. Зроблено короткий огляд методів вбудови інформації в просторові області цифрових зображень. Дана коротка характеристика існуючих методів.

2. Розглянуто принцип дії LSB методу для стеганографічної системи на основі цифрових зображень. Сформовано загальний список вимог і критеріїв вибору зображень-контейнерів для алгоритмів стеганографічного приховування інформації на основі методу LSB. На основі сформульованих вимог додосліджуваних зображень-контейнерів обрані зображення формату BMP.

3. Проведено дослідження статистичних характеристик цифрових зображень BMP формату, зображення отримані за допомогою цифрового фотоапарата шляхом конвертації з RAW формату. Конвертація з RAW формату, не призначеного для безпосередньої візуалізації, в формат BMP відбувається без втрати якості зображення. В якості досліджуваних характеристик були обрані монотонність, ентропія і дисперсія зображень. Дослідження зміни статистичних характеристик зображень проведено методами оцінки критерію Хі-квадрат і RS методом стегоаналіза. На основі отриманих даних можна зробити висновок, що найбільшою стеганографічної стійкістю володіють зображень з найбільшою ентропією і дисперсією молодшої бітової площини, з підвищенням монотонності зображення стійкість стеганографічної системи падає, погіршується.

4. Аналіз дисперсії бітових площин показав, що молодші бітові площини тестованих зображення володіють досить великими близькими показниками дисперсії порядку 16000. Мінімальне значення дисперсії

молодших бітових площин становить близько 6000, що відповідає ймовірності виявлення повідомлення методу RS аналізу в 60 відсотків. Зі збільшенням біта вбудовування збільшується розкид значень дисперсії досліджуваних зображень. RS метод стегоаналіза показує, що при показниках дисперсії прагнуть до 0, ймовірність виявлення прихованої інформації, що міститься в зображенні, прагне до 100 відсотків. Таким чином, наведені дані про дисперсії підтверджують теорію випадковості молодших біт і показують їх перевагу найбільш старшим бітам при встановленні інформації методом LSB. При виникненні необхідності задіяння старших біт при LSB стеганографії, слід більш уважно ставитися до вибору зображення в силу великих разбросів показників дисперсії різних зображень і віддавати переваги зображенням, що володіють найбільшою дисперсією в цих бітах.

5. Аналіз даних про ентропії показує, що її відносна величина молодших бітових площин є більшою у порівнянні зі старшими бітами. Максимальна відносне значення молодших бітових площин становить близько 18, в свою чергу максимальне значення ентропії другий бітової площини зменшилася більш ніж в два рази. Максимальна ймовірність виявлення впровадження повідомлення в молодший біт зображення становить близько 60 відсотків при значенні ентропії дорівнює 3. При залученні найбільш старших біт зображень, ймовірність виявлення в 60 відсотків досягається при відносному значенні ентропії близько 6. Необхідно відзначити, що зі збільшенням біта вбудовування, відносне значення ентропії бітових площин тестованих зображень прагне до максимального значення. Підводячи підсумок, можна зробити висновок, що, як і в випадку з дисперсією зображень, при виборі зображення в якості контейнера для стеганографічного приховування даних методом LSB, слід вибирати зображення з великими значеннями ентропії в бітових площинах.

Результати представлені для цифрових зображень формату BMP, проте можуть бути адаптовані і на інші формати.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Овчарук, І. В., and А. А. Пристінська. "Аналіз чутливості зорового сприйняття інформації людиною на основі стеганографічного методу LSB." Водний транспорт 1 (2019): 151-158.

2. Fedoseev, V. (2017). A model for data hiding system description. In 3rd International Conference on Information Technology and Nanotechnology (pp. 65-71).

3. Sudana, I. Ketut. "Penggunaan Microsoft Office Powerpoint Sebagai Media Pembelajaran Untuk Meningkatkan Motivasi Dan Hasil Belajar Pendidikan Agama Hindu Kelas V Sekolah Dasar Negeri 1 Yangapi Tahun Pelajaran 2018/2019." Cetta: Jurnal Ilmu Pendidikan 3.3s (2020).

4. Мушко, В. В. "Стеганографические методы защиты информации.№ УД-7121/уч." (2019).

5. Коржик, В. И., Анфиногенов, С. О., Кочкарёв, А. И., Федянин, И. А., Жувикин, А. Г., Флаксман, Д. А., & Алексеев, В. Г. (2017). Цифровая стеганография и цифровые водяные знаки.

6. КУСТОВ, В. Н.; ПРОЦКО, Д. К. Программная модель стеганографа на основе модификации метода замены наименее значащих битов. In: Вестник научных конференций. ООО Консалтинговая компания Юком, 2017. p. 54-61.

7. J. Fridrich, R. Du, and L. Meng, “Steganalysis of LSB Encoding in Color Images”, ICME 2000, New York City.

8. Пересада Р.А., Бологова Н.М. АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ СТІЙКОСТІ ВОДЯНИХ ЗНАКІВ У ЦИФРОВИХ ЗОБРАЖЕННЯХ. Збірник тез доповідей восьмої міжнародної науково-технічної конференції «Проблеми інформатизації»: с. 57.

9. J. Fridrich, G. Miroslav, R. Du Steganalysis Based on JPEG Compatibility. - SUNY Binghamton, New York, 2001. - 6 с

10. Разинков Е.В. Стойкость стеганографических систем /Е.В.Разинков, Р.Х.Латыпов //Учёные записки Казан.гос.ун-та. –Казань, 2009. –Т. 151,No 2

11. Westfeld A. Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos and S-Tools-and Some Lessons Learned / A. Westfeld, A. Pfitzmann // 3rd International Workshop on Information Hiding (2000)

12. J. Friedrich, G. Miroslav, R. Du. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghampton, New York: SUNY, 2001.

13. Фисенко В.Т., Фисенко Т.Ю. Компьютерная обработка и распознавание изображений: учеб. пособие. - СПб.: СПбГУ ИТМО, 2008

14. Кустова В. Н. и Федчука А. А. "Методы встраивания скрытых сообщений" ("Защита информации. Конфидент", №3, 2000