Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Сокальський Сергій Миколайович,
група РЗ-171

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Розробка методу вибору стеганографічного контейнера в умовах атак проти вбудованого повідомлення

Спеціальність:
125 Кібербезпека
Спеціалізація, освітня програма Кібербезпека

Керівник:
Кобозєва Алла Анатоліївна,
д.т.н., професор

Одеса – 2022

Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
Спеціалізація, освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ
_____
д.т.н.,проф. А.А.Кобозєва
«___»_____2022р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Сокальському Сергію Миколайовичу

1.Тема роботи: *Розробка методу вибору стеганографічного контейнера в умовах атак проти вбудованого повідомлення*,
керівник роботи *Кобозєва Алла Анатоліївна, д. т. н., професор*,
затверджені наказом ректора від „____”_____ 20___ р. №_____ .
2. Зміст роботи*: аналіз предметної області, постановка задачі, визначення поняття захищеної інформації, розробка методу вибору контейнера, експериментальне дослідження ефективності розробленого методу.*
3. Перелік ілюстративного матеріалу: *структурна схема стеганосистеми, приклади стеганограм, таблиця ефективності розробленого методу та його аналога.*

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Дата видачі завдання “_____”_____2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз літератури за темою випускної кваліфікаційної роботи*	*29.08.2022*	*виконано*
2	*Розробка методу вибору контейнера в умовах атак проти вбудованого повідомлення*	*15.09.2022*	*виконано*
3	*Програмна реалізація алгоритму*	*01.10.2022*	*виконано*
4	*Розробка користувацькогоінтерфейсу програмного продукту*	*15.10.2022*	*виконано*
5	*Підготовка тексту роботи*	*01.11.2022*	*виконано*
7	*Підготовка презентації та доповіді*	*12.11.2022*	*виконано*
8	*Попередній захист*	*02.12.2022*	*виконано*
9	*Нормоконтроль, рецензування*	*15.12.2022*	*виконано*
10	*Занесення роботи в електронний архів*	*18.12.2022*	*виконано*
11	*Допуск до захисту*	*19.12.2022*	*виконано*

Здобувач вищої освіти _____ *Сокальський С.М.*

Керівник роботи _____ *Кобозєва А.А.*

АНОТАЦІЯ

Кваліфікаційна робота на тему «Метод вибору стеганографічного контейнера в умовах атак проти вбудованого повідомлення» на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітня програма: Кібербезпека, містить 13 рисунків, 1 таблицю, 1 додаток, 26 літературних джерел за переліком посилань. Робота виконана на 62 сторінках загального тексту і 47 сторінках основного тексту.

Метою роботи є підвищення стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки методу вибору контейнера з кінцевої сукупності наявних цифрових зображень, що забезпечує для повідомлення, що передається, мінімальну або близьку до мінімально можливої для аналізованих зображень чутливість сформованого стеганоповідомлення до збурних дій при обраному стеганографічному алгоритмі.

Поставлена мета досягається шляхом теоретичного дослідження збурень формальних параметрів матриці контейнера в результаті стеганоперетворення й активних атак, що дало можливість для введення нового формального представлення для інформації, захищеної від збурної дії E, як різниці малорангових апроксимацій матриць контейнера й стеганоповідомлення. Ефективність розробленого методу практично в 3 рази перевищує ефективність кращого з наявних аналогів і залишається високою, незалежно від використовуваного для стеганоперетворення стеганографічного методу. Значимість отриманого результату полягає в забезпеченні за рахунок використання розробленого методу підвищення стійкості стеганосистеми до атак проти вбудованого повідомлення.

Результатом кваліфікаційної роботи є програмний продукт, що реалізує метод вибору стеганографічного контейнеру, в умовах атак проти вбудованого повідомлення.

СТЕГАНОГРАФІЧНИЙ МЕТОД, ЦИФРОВЕ ЗОБРАЖЕННЯ, ВИБІР КОНТЕЙНЕРА, СТІЙКІСТЬ СТЕГАНОСИСТЕМИ, СИНГУЛЯРНЕ ЧИСЛО, СИНГУЛЯРНИЙ ВЕКТОР.

ANNOTATION

Qualification work on the topic "Method of choosing a steganographic container in the face of attacks against an embedded message" for the second (master's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 13 figures, 1 table, 1 appendix, 26 references in the list of references. The work is performed on 62 pages of the general text and 47 pages of the main text.

The aim of the work is to increase the resistance of a steganographic system to attacks against an embedded message by developing a method for selecting a container from a finite set of available digital images, which ensures for the transmitted message the minimum or close to the minimum possible for the analyzed images the sensitivity of the generated steganomessage to disturbing actions with the selected steganographic algorithm.

This goal is achieved by a theoretical study of perturbations of the formal parameters of the container matrix as a result of steganotransformation and active attacks, which made it possible to introduce a new formal representation for information protected from disturbing action E, as a difference of low-rank approximations of the container matrices and the steganomessage. The efficiency of the developed method is almost 3 times higher than the efficiency of the best of the available analogues and remains high, regardless of the steganographic method used for steganotransformation. The significance of the result is to ensure by using the developed method to increase the resistance of the steganosystem to attacks against the embedded message.

The result of qualification work is a software product that implements a method for selecting a steganographic container in the face of attacks against an embedded message.

STEGANOGRAPHIC METHOD, DIGITAL IMAGE, CONTAINER SELECTION, STEGANOGRAPHIC SYSTEM RESISTANCE, SINGULAR NUMBER, SINGULAR VECTOR.

ЗМІСТ

ВСТУП

На сьогоднішній день задача захисту інформації від несанкціонованого доступу, несанкціонованої зміни стає все більш складною та охоплює всі сфери людської діяльності. Одним із найперспективніших напрямів у забезпеченні інформаційної безпеки є стеганографія. Істотно впливає на надійність стеганосистеми, її стійкість носій – контейнер, в якості якого у роботі розглядається цифрове зображення. Вибір контейнера дозволяє максимально забезпечити вимоги, що висуваються до одержуваного стеганоповідомлення, що робить задачу вибору контейнера важливою та актуальною при побудові стеганосистеми.

Метою роботи є підвищення стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки методу вибору контейнера з кінцевої сукупності наявних цифрових зображень, що забезпечує для повідомлення, що передається, мінімальну або близьку до мінімально можливої для аналізованих зображень чутливість сформованого стеганоповідомлення до збурних дій при обраному стеганографічному алгоритмі.

Для досягнення поставленої мети в роботі розв’язуються наступні ***задачі***:

1. Обгрунтувати вибір формального представлення процесу стеганоперетворення;
2. Обгрунтувати вибір сукупності формальних параметрів матриці цифрового зображення, які має сенс аналізувати для оцінки обсягу захищеної ДІ в стеганоповідомленні, та спосіб їх врахування;
3. Обгрунтувати спосіб аналізу обраної сукупності формальних параметрів матриці цифрового зображення для оцінки обсягу захищеної ДІ в стеганоповідомленні;
4. Обгрунтувати співвідношення для кількісної оцінки обсягу захищеної додаткової інформації в стеганоповідомленні;
5. Розробити метод вибору контейнера з кінцевої сукупності наявних цифрових зображень, ефективність якого не буде залежити від специфики конкретного

стеганографічного алгоритму, який задіюється при отриманні стеганоповідомлень;

6. Провести оцінку ефективності, зокрема порівняльну, розробленого методу вибору контейнера.

Поставлена мета була досягнута шляхом: теоретичного дослідження збурень формальних параметрів матриці контейнера, отриманих за допомогою її нормального сингулярного розкладання та однозначно визначаючих матрицю, в результаті стеганоперетворення та активних атак, що дало можливість для введення нового формального представлення для інформації, захищеної від збурної дії E, як різниці малорангових апроксимацій матриць контейнера і стеганоповідомлення, де ранг апроксимацій визначається кількістю сингулярних чисел матриці контейнера, що мають достатню відокремленість по відношенню до E.

Об’єкт дослідження: процеси прихованої (стеганографічної) передачі даних.

Предмет дослідження: методи вибору контейнера, що забезпечує певні характеристики стеганоповідомлення.

Методи дослідження: Для розробки теоретичного базису методу вибору контейнера з наявної сукупності ЦЗ використовувалися матричний аналіз, теорія збурень, обчислювальна лінійна алгебра; при безпосередній розробці методу, відповідного алгоритму та оцінки його ефективності використовувалися обчислювальні методи, стеганографічні методи, методи обробки цифрових зображень, методи комп’ютерного моделювання.

Наукова новизна. Вперше на основі введеного визначення захищеної від збурної дії E додаткової інформації у вигляді різниці малорангових апроксимацій матриць контейнера і стеганоповідомлення, розроблено метод вибору контейнера з кінцевої сукупності наявних цифрових зображень, що забезпечує для повідомлення, що передається, мінімальну або близьку до мінімально можливої для аналізованих зображень чутливість сформованого стеганоповідомлення до збурних дій при обраному стеганографічному алгоритмі, який дозволив

підвищити стійкість стеганографічної системи до атак проти вбудованого повідомлення.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні здобувачем отриманих результатів до конкретного методу та відповідного алгоритму, що може бути використаним у якості складової комплексної системи захисту інформації будь-якого закладу, підприємства. Ефективність розробленого методу перевищує ефективність кращого з аналогів: максимальне відхилення коефіцієнта кореляції *NC* для додаткової інформації, що є кількісним показником чутливості стеганоповідомлення до збурних дій, від максимального значення для контейнерів з заданої множини склало 3.9%, що практично в 3 рази менше значення цього показника для найкращого з аналогів, що говорить про підвищення стійкості стеганосистеми загалом до атак проти вбудованого повідомлення при використанні запропонованого методу. Практичною перевагою розробленого методу є забезпечувана ефективність використання його результатів – обраних контейнерів, отриманих в умовах збурної дії E, для атак меншої сили. Ефективність розробленого методу залишається високою, незалежно від використовуваного для стеганоперетворення стеганографічного методу.

Робота складається із вступу, трьох розділів, висновку, переліку посилань та додатку.

У вступі обґрунтовано актуальність дослідження та сформульована мета роботи.

У першому розділі виконано огляд предметної області, а саме розглянуті питання щодо загального поняття стеганосистеми, поняття її стійкості, а також розглянуто питання задачі вибору стеганографічного контейнера.

У другому розділі обгрунтовано поняття захищеної додаткової інформації, формалізовано процес стеганоперетворення, який не залежить від конкретики вибраного стеганографічного методу, а також запропоновано новий метод вибору контейнера, проведено оцінку ефективності його алгоритмічної реалізації, в тому числі, порівняльну.

У третьому розділі описане середовище розробки, яке було використане для реалізації програмного продукту, виконаний опис використаних функцій та засобів і створена інструкція із практичного використання створеного продукту.

Основні положення та результати поданої роботи опубліковані в науковому інформаційно-аналітичному журналі «Проблеми регіональної енергетики», що включений до наукометричних баз Scopus та Web of Science [1].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальне поняття стеганосистеми

Складовою будь-якої сучасної комплексної системи захисту інформації є стеганографічна система [2-6] (рис.1.1), що дозволяє приховати сам факт наявності секретної інформації «під маскою» контейнера, що не привертає увагу, в якості якого при організації прихованого (стеганографічного) каналу зв'язку в сьогоднішній стеганографії використовуються, як правило, цифрові контенти – зображення (ЦЗ), відео, аудіо. Аналіз тенденцій розвитку комп'ютерної стеганографії показує, що найближчими роками інтерес до неї буде тільки посилюватись [7], основними причинами чого є: обмеження (аж до заборони) на використання криптозасобів у ряді країн світу, проблеми захисту прав власності на інформацію, яка представлена у цифровому вигляді, обсяги та цінність якої безперервно зростають.

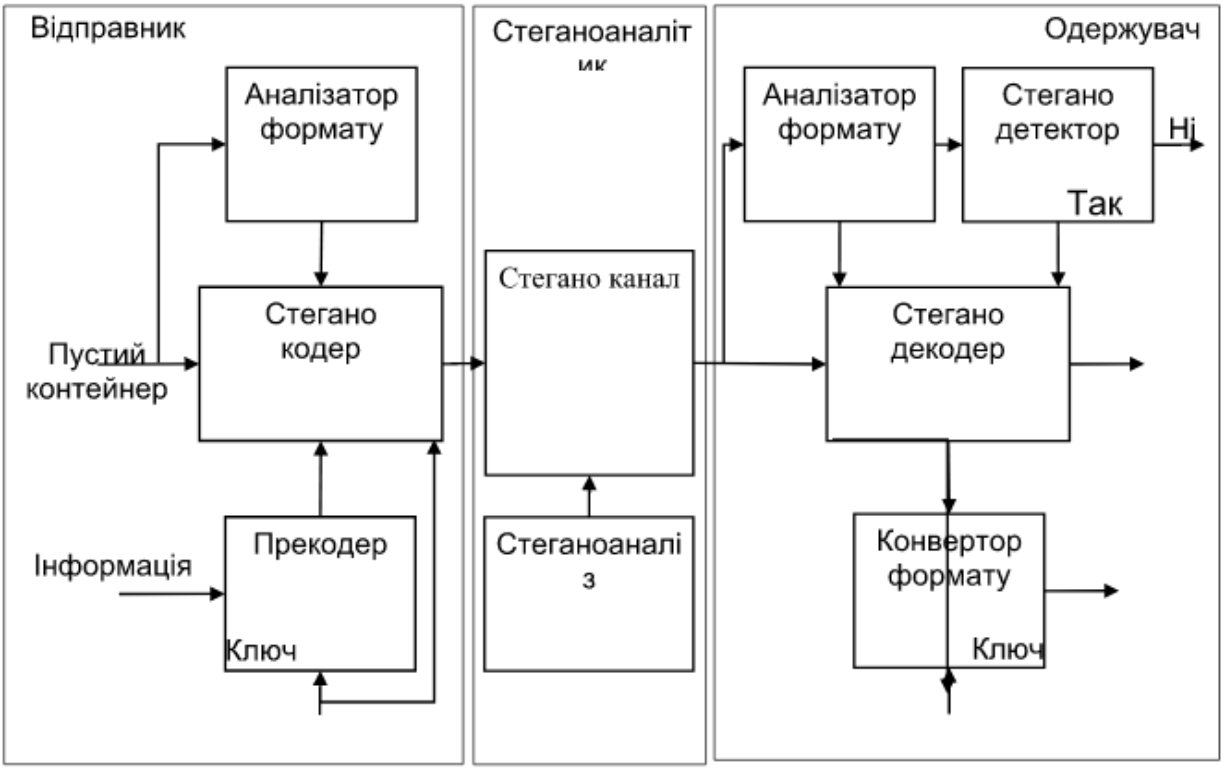


Рисунок 1.1 - Структурна схема стеганосистеми та стеганоаналізу

Стеганографія є найбільш перспективним напрямком у забезпеченні безпеки інформації в сучасних системах та мережах [8].

Процес стеганографування загалом складається з декількох етапів [9]: вибір (якщо такий можливий) контейнера, в якості якого у цій роботі розглядається ЦЗ, оскільки суттєвий вплив на надійність стеганосистеми, можливість виявлення факту передачі прихованого повідомлення, на інші її характеристики оказує саме носій; попереднє кодування переданої інформації, в результаті якого, як правило, виходить бінарна цифрова послідовність – додаткова інформація (ДІ); безпосереднє вбудовування ДІ в контейнер, результатом чого є стеганоповідомлення (СП).

Контейнери загалом поділяються на два типи: потоковий та фіксований. Потоковий являє собою послідовність бітів, яка постійно змінюється, і додаткова інформація вбудовується в нього в реальному масштабі часу. У випадку використання такого контейнеру заздалегідь не ясно, чи вистачить місця вбудувати усю додаткову інформацію, яку потрібно передати. Фіксований контейнер представляє собою цифровий контент із заздалегідь визначеними незмінними розмірами і характеристиками, і тому є можливість попереднього обчислення обсягу інформації, яку можна буде цілком вбудувати у обраний контейнер. В даній роботі будуть розглядатися саме фіксовані контейнери.

Використовувані при організації прихованого каналу зв'язку контейнери можуть бути [9]: випадковими, нав'язаними та обраними. При цьому очевидно, що саме обраний контейнер дозволить максимально забезпечити вимоги, що висуваються до одержуваному СП. Так існує важлива можливість підбору контейнера таким чином, щоб він у своєму оригінальному вигляді вже містив потрібну ДІ відповідно до використовуваного секретного ключа, тим самим анулюючи для стеганоаналітика ймовірність виявлення факту наявності ДІ (проте на практиці така можливість використовується вкрай рідко через значну обчислювальну складність її реалізації).

Єдиної думки про те, яким має бути «ідеальний» контейнер, немає [10], та вона й не може бути сформованою, оскільки пріоритетні вимоги, що ставляться до СП, для різних умов його отримання та використання так само різні [9,11]. Завдання вибору контейнера завжди вирішується з урахуванням

пріоритетності вимог, що висуваються до СП у конкретних умовах його використання, серед яких: забезпечення надійності сприйняття (СП не повинно візуально відрізнятися від контейнера), стійкість до стеганоаналізу, стійкість до атак проти вбудованого повідомлення [9,12] тощо.

Вважається, що саме атаки проти вбудованого повідомлення заслуговують на сьогодні найбільшої уваги. Справді, надійність сприйняття СП зобов'язаний забезпечувати кожен контейнер, що входить до області застосування використовуваного стеганографічного алгоритму. Якщо це не так, то такий стеганоалгоритм просто не має права на існування. Стеганоаналітична атака (відмінна від візуальної) вимагає від атакуючого наявності специфічних програмних, технічних засобів виявлення (наявності) прихованої інформації, а також відповідної кваліфікації, що явно звужує коло таких атак. Що ж до атак проти вбудованого повідомлення, то вони можуть бути проведені без будь-якого специфічного обладнання, програмного забезпечення, специфічної кваліфікації атакуючого, наприклад, атака стисненням із втратами, що робить такі атаки поширеними, надзвичайно актуальними, одними з тих, з якими треба боротися насамперед, у тому числі, за рахунок вибору контейнера, що забезпечує малу чутливість СП до збурних дій.

Під чутливістю СП тут і далі розуміється чутливість задачі декодування ДІ.

Додаткова інформація, призначена для подальшого вбудовування в контейнер, має бути представлена у бітовому вигляді. Доцільно використати шифрування ДІ за допомогою стійкого криптографічного методу. Це дозволить підвищити стійкість та захищеність стеганосистеми.

1.2 Поняття стійкості стеганосистеми

Поняття стійкості стеганографічної системи, на відміну від поняття стійкості криптографічної системи, може розумітися по-різному. Це пояснюється як і недостатнім практичним і теоретичним опрацюванням питань щодо безпеки

стеганосистеми, так і великою кількістю різноманітних стеганографічних завдань щодо інформаційної безпеки.

Схожістю із криптосистемами є те, що стеганосистеми також оцінюються за допомогою їх стійкості. Під поняттям стійкості розуміється здатність стеганосистеми приховати від кваліфікованого зловмисника, який може спостерігати за передачею стеганоповідомлень по каналу зв'язку, факт наявності прихованого під «маскою» контейнерів вбудованої інформації, здатність протистояти атакам, спрямованим на знищення або пошкодження додаткової інформації, а також здатність підтвердити або спростувати справжність прихованої інформації.

Оскільки задача стеганосистеми і криптосистеми відрізняється, тому поняття стійкості і злому цих систем є різними. У випадку використання криптографічної системи стійкою є така система, коли зловмисник, який володіє криптограмою, ніяк не може дізнатись вміст того, що в ній міститься, а стеганосистема є стійкою тоді, коли зловмисник не може встановити сам факт існування прихованого повідомлення. У відповідності до здатності протистояти пасивним атакам, стеганосистеми поділяють на:

- Теоретично стійка стеганосистема – система, для злому якої не існує теоретично розробленого стеганоаналітичного алгоритму.
- Практично стійка стеганосистема – система, для злому якої не існує практично реалізованого стеганоаналітичного метода.
- Нестійка стеганосистема – система, для злому якоє існує практично реалізований метод.

Далі розглянемо класифікацію атак на стеганосистему:

- Атака з стеганоповідомленням – у користуванні зловмисника є одне або декілька стеганоповідомлень, і він намагається дізнатися, чи містять вони приховану інформацію. У такому випадку порушнику дуже важко скомпрометувати систему, оскільки без наявності пустих контейнерів або фрагментів прихованої інформації можна отримати багато неправдивих розшифрувань, серед яких не можна виділити правильне.

- Атака з відомим контейнером – атака яка дає порушнику набагато більше шансів для злому системи, порівняно із першою атакою, оскільки в його розпорядженні є одна або декілька пар пустого контейнера та відповідного стеганоповідомлення.
- Атака із вибраним контейнером – у випадку такої атаки зловмисник нав'язує для використання у стеганоперетвореній свій контейнер, який має кращі для стеганоаналізу і компрометування системи характеристики, аніж випадковий контейнер. Також існує покращення цієї атаки – атака із адаптивно вибраним контейнером. При такій атаці порушник нав'язує для стеганосистеми свій контейнер, і при отриманні результатів отриманого стеганоповідомлення він пропонує на основі цих результатів іще один більш підходящий контейнер. І так до встановлення факту передачі прихованої інформації, або до спростування його.
- Атака із відомим повідомленням – атака на стеганосистему в умовах, коли зловмиснику відомий вміст одного або декількох стеганоповідомлень. У такому випадку зловмиснику набагато легше скомпрометувати систему, аніж коли він намагається за допомогою цих самих стеганограм виявити факт існування прихованого каналу зв'язку, коли йому невідомий зміст прихованої інформації.
- Атака із вибраним повідомленням – атака, коли зловмисник нав'язує для використання своє повідомлення, щоб він мав змогу встановити факт існування прихованого каналу зв'язку, або щоб дізнатися стеганоключ. Також можлива атака із адаптивно вибраним повідомленням. В такому випадку порушник постійно нав'язує своє повідомлення для стеганосистеми, щоб послідовно все більш впевнено констатувати факт використання прихованого каналу зв'язку.

В добавок до вище перерахованих атак можна сказати, що зловмисник може проводити різноманітні комбінації цих атак. Ймовірність злому стеганосистеми росте із обсягом інформації про цю систему, якою володіє порушник. Такою інформацією може бути інформація про контейнери, об'єм прихованої інформації або можливість нав'язування своїх контейнерів або повідомлень для системи.

Додатково стійкість стеганосистеми може бути поділена на стійкість до виявлення факту використання прихованого каналу зв’язку, стійкість до встановлення використовуваного стеганографічного ключа, стійкість до нав’язування своїх контейнерів та повідомлень системі і стійкість до встановлення змісту стеганограми при її наявності.

У випадку якщо система являється стійкою до факту виявлення передачі прихованого повідомлення можна з впевненістю сказати, що така система є стійкою і до встановлення змісту перехопленої стеганограми. Але не навпаки, система може бути стійкою до виявлення змісту стеганоповідомлення у той час, коли є нестійкою до факту виявлення використання прихованого каналу зв’язку. Стійкою до нав’язування свої контейнерів і повідомлень системою є така, що не дозволяє зловмиснику скомпрометувати систему шляхом аналізу отриманих стеганограм на основі своїх контейнерів або повідомлень, що були цілеспрямовано вибрані для цієї задачі і мають найкращі для цього характеристики. Стеганографічна система, що не є стійкою до встановлення стеганоключа може бути повністю скомпрометована злочинцем, який не лише встановить факт наявності прихованого каналу зв’язку, але й зможе підроблювати стеганограми, видаючи їх за справжні.

Важливим фактором при використані стеганографічної системи є дотримання умов, за яких отримана стеганограма не буде порушувати надійність сприйняття, адже стеганосистема, яка може бути скомпрометована за допомогою візуальної оцінки заповненого контейнера є вкрай нестійкою.

Якщо зловмисник має можливість встановлення секретного ключа вбудовування цифрового водяного знака (ЦВЗ), то він може вбудувати цей ЦВЗ на будь який цифровий контент. Це ставить під сумнів або всю систему ЦВЗ або ЦВЗ даного автора, а це ставить під сумнів законність прав власника на те, що йому насправді належить. Ця проблема має дійсно велику практичну значимість у питаннях забезпечення авторських прав на цифрові контенти.

У випадку симетричної системи ЦВЗ потрібно, щоб декодер використовував конфіденційний ключ виявлення ЦВЗ. Такі декодери проблематично вбудовувати

у пристрої для масового використання. А у випадку несиметричної системи потрібно забезпечити неможливість встановлення секретного ключа вбудовування ЦВЗ із відкритого ключа перевірки ЦВЗ. Ці вимоги досить схожі із тими, які ставляться до криптографічних систем цифрового підпису. У випадку використання несиметричної системи, за умови забезпечення вищезгаданої умови, важливим є і унеможливлення обходу системи перевірки ЦВЗ, щоб користувач не міг безкоштовно переглядати платний контент.

Важливо вказати, що побудова несиметричних систем ЦВЗ або інших стеганосистем викликає деякі практичні проблеми. По-перше, побудова таких систем є набагато складнішою у обчисленнях при практичній реалізації. По-друге, окрім вимог, що висуваються для стійкості відкритого ключа, є ще проблема забезпечення стійкості системи до різноманітних спроб зловмисника спотворення ЦВЗ. Такі системи побудовані на основі однонаправлених функцій із потайним ходом, в результаті використання яких будь-які малі спотворення вихідного повідомлення призводять до істотного розмноження помилок в отримуваному повідомленні. А в стеганосистемі використання таких методів підтвердження достовірності ЦВЗ неможливе тому, що їх застосування демаскує прихований канал зв’язку, а також тому, що активний порушник може вибрати таку збурну дію, що доступні стеганографу методи підвищення достовірності можуть виявитись неефективними.

1.3 Задача вибору контейнера

Як було зазначено вище, основна увага в сучасних стеганографічних системах приділяється забезбеченню стійкості до атак проти вбудованого повідомлення. Підвищити ймовірність цього забезпечення можливо шляхом вибору контейнера з певними характеристиками.

Завдання вибору контейнеру знаходиться в полі зору багатьох сучасних вчених-стеганографів. Так у [13] розглядається питання вибору контейнера для підвищення безпеки стеганографічної системи. Дані контейнера моделюються як процес Гауса-Маркова. Основна ціль вибору контейнера – забезпечення або

підвищення стійкості стеганосистеми до стеганоаналізу. Питання стійкості до атак проти вбудованого повідомлення у роботі не піднімаються, як і в [10], де розглядається питання вибору контейнера з певного набору ЦЗ для заданого секретного повідомлення з метою забезпечення високої якості візуального сприйняття СП, а також стійкості до стеганоаналізу. Вибір здійснюється шляхом двокрокової процедури. На першому кроці відбувається фільтрація потенційних контейнерів з урахуванням їх гістограм. На другому - аналізуються характеристики інтенсивності пікселів, виділених попередньо блоків. Для підвищення ймовірності збереження надійності сприйняття СП при вбудовуванні ДІ проводяться додаткові геометричні перетворення блоків, що, хоч і забезпечує ефективний вибір контейнера відповідно до висунутих вимог, але ніяк не гарантує стійкості формованого СП до збурних дій.

У [14] розглянуто питання вибору контейнера для забезпечення максимально можливої стійкості стеганосистеми до пасивних атак, при цьому велика увага приділена форматам, у яких зберігаються контейнери. Питання стійкості до активних атак знову ігнорується. При цьому якийсь конкретний метод вибору контейнера у роботі взагалі не пропонується.

У [15] вибір контейнера робиться для одного стеганометода Бенгама-Мемона-Ео-Юнга, який автори попередньо модифікують, використовуючи для вбудовування інформації замість області дискретного косинусного перетворення область дискретного вейвлет-перетворення. Вибір контейнера тут зводиться до формулювання вимог до ЦЗ, тобто, по суті – до отримання обмежень на область використання модифікованого методу і не може розглядатися як варіант розв'язання задачі в цілому.

У [16] був запропонований метод, що дозволяє з наявної множини контейнерів вибрати той, який забезпечить відносну стійкість одержуваного СП до передбачуваних атак проти вбудованого повідомлення. Значною перевагою методу є відсутність обмежень на область застосування не тільки в сенсі використовуваного стеганографічного алгоритму, але і в сенсі конкретики атак

проти вбудованого повідомлення, внаслідок чого цей метод заслуговує на особливу увагу.

Метод заснований на можливості формального представлення стеганоперетворення контейнера з $n \times n$-матрицею F, незалежно від використовуваного стеганометода та обраної області для вбудови ДІ (просторової, області перетворення), у вигляді:

$$\bar{F} = F + \Delta F \quad (1)$$

де F - n×n-матриця СП, ΔF - n×n-матриця обурення, яка виникла в результаті вбудовування ДІ у контейнер. У роботі введено поняття обсягу захищеної від збурної дії Е інформації (ЗІ) з використанням понять захищеного від Е власного вектора (ВВ), що відповідає власному значенню (ВЗ) з достатньою абсолютною відокремленістю, для матриці розглянутого цифрового контенту після її попередньої симетризації. У [16] показано, що в основному зі зростанням величини обсягу ЗІ зростає і стійкість СП до атак проти вбудованого повідомлення. Однак зазначена залежність не є прямою, тут можлива ситуація, коли ЦЗ-контейнеру з максимальним обсягом ЗІ відповідало СП, кількісний показник стійкості якого визначається об'ємом правильно декодованої інформації, був значно меншим максимально можливого значення цього показника для розглянутої множини контейнерів. Причини цього частково були досліджені в [17], де була зроблена спроба врахувати та усунути виявлені недоліки, допущені в [16], серед яких: необґрунтоване використання абсолютних відокремленостей ВЗ матриці при розрахунку обсягу ЗІ; умова вибору захищених ВВ, що не використовує індивідуальні характеристики зображення та ін. Але до підвищення ефективності процесу вибору контейнера це практично не призвело, причиною чого є те, що зміни, внесені до принципу розрахунку обсягу ЗІ стосувалися лише дуже незначної частини ВЗ, ВВ, які враховувалися під час розрахунків. При цьому ВЗ з найбільшою абсолютною відокремленістю та відповідних їм ВВ, які є нечутливими до будь-яких збурних дій, це не торкнулося. Крім того, видалення з розгляду ВЗ у будь-якій якості, проведене в роботі, є «кроком назад» у процесі підвищення ефективності вибору контейнера, порівнюючи з [16], оскільки

призводять до ігнорування сукупності параметрів, збурення яких є складовою частиною формального представлення результату стеганоперетворення [16].

Таким чином, завдання вибору з наявної сукупності потенційних ЦЗ контейнерів такого, що для заданої ДІ забезпечить найменшу чутливість до збурних дій сформованого СП, є такою, що не має остаточного рішення, залишається актуальною для підвищення ефективності стеганосистеми в цілому.

Метою роботи є підвищення стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки методу вибору контейнера з кінцевої сукупності K наявних ЦЗ, що забезпечує для заданої ДІ мінімальну або близьку до мінімально можливої для ЦЗ з K чутливість формованого СП до збурних дій при вибраному стеганографічному алгоритмі. При цьому ефективність розробленого методу не повинна залежати від конкретики використовуваного при формуванні СП стеганоалгоритму.

Як основний показник ефективності методу вибору контейнера будемо розглядати відхилення кількісного показника (визначуваного нижче) чутливості СП до збурних дій, сформованого на основі обраного контейнера, від максимально можливого значення цього показника з усієї множини K.

2 РОЗРОБКА МЕТОДУ ВИБОРУ СТЕГАНОГРАФІЧНОГО КОНТЕЙНЕРА

2.1. Формалізація процесу стеганоперетворення та введення поняття захищеної інформації

Мета роботи може бути досягнута тільки при використанні загальної формалізації процесу стеганоперетворення, ніяк не пов'язаної зі специфікою конкретного стеганографічного алгоритму, чому очевидно задовольняє (1). Співвідношення (1) з врахуванням того, що для симетричної матриці вона повністю і однозначно визначається набором ВЗ та ВВ, отриманих в результаті нормального спектрального розкладання [16], дозволяє зробити наступний висновок: результат будь-якого стеганоперетворення для контейнера із симетричною матрицею формально може бути представлений у вигляді сукупності збурень ВЗ і ВВ, що відбулися при вбудовуванні ДІ в контейнер, що використовується в [16] при визначенні поняття ЗІ. Однак, розрахунок обсягу ЗІ відповідно з [16,17] вимагає попередньої симетризації матриці ЦЗ. Принцип симетризації, запропонований у [16] та збережений у [17]:

$$F = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix} A = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix}, B = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix}$$

призводить до того, що в кожній із двох отриманих симетричних матриць A, B, які ставляться у відповідність квадратній матриці F довільної структури, вноситься лише половина (верхній/нижній трикутник) оригінальної F, що, крім додаткової обчислювальної роботи, призводить до того, що одержувані шляхом нормального спектрального розкладання ВВ та ВЗ визначають не оригінальну матрицю, а її специфічну модифікацію, будучи додатковим джерелом похибки методу вибору контейнера як в [16], так і в [17]. У зв'язку з цим, відштовхуючись від (1) та враховуючи, що результат будь-якого стеганоперетворення може бути представлений також у вигляді сукупності збурень сингулярних чисел (СНЧ) та сингулярних векторів (СНВ), отриманих шляхом нормального сингулярного розкладання матриці контейнера, оскільки для матриці з різними СНЧ таке

розкладання завжди існує і єдине [18] (на відміну від «класичного» сингулярного розкладання), очевидно є доцільно замінити набір формальних параметрів, що фігурували в [16,17] для визначення кількісної оцінки обсягу ЗІ, на набір СНЧ і СНВ відповідної матриці, про доцільність чого також говорить порівнянність властивостей цього набору параметрів з набором ВЗ та ВВ симетричної матриці з точки зору чутливості до збурних дій [19].

Побудуємо для довільної n×n-матриці F нормальне сингулярне розкладання:

$$F = U\Sigma V^T, \quad (2)$$

де U, V - ортогональні матриці, стовпці яких u_i, v_i, $i = \overline{1,n}$, є лівими та правими СНВ відповідно, при цьому ліві СНВ додатково є лексикографічно позитивними [18]; $\Sigma = diag(\sigma_1, \ldots, \sigma_n)$, $\sigma_1 \geq \ldots \geq \sigma_n \geq 0$ – СНЧ F. СНЧ довільної F, як і ВЗ симетричної матриці, є добре обумовленими через співвідношення [19]: $\max_i|\sigma_i(F) - \sigma_i(F+E)| \leq \|E\|_2$, де 2 $\|\cdot\|_2$ – спектральна матрична норма, E – n×n матриця збуреня, мірою ж чутливості до збурних дій СНВ u_i досі вважалася відокремленість

$$svdgap(i,F) = \min_{i\neq j}\left|\sigma_i - \sigma_j\right| \quad (3)$$

відповідного СНЧ σ_i відповідно до формули [20]:

$$\sin 2\theta_i \leq 2\|E\|_2 / svdgap(i,F) \quad (4)$$

де θ_i - кут повороту u_i в результаті збурної дії E. Очевидно, що співвідношення (4) дає оцінку зверху для кута θ_i тільки тоді, коли його права частина менше чи дорівнює 1. Інакше поведінка вектора u_i після атаки непередбачувана. Виникнення цієї ситуації для конкретного СНВ залежить від величини $svdgap(i,F)$ (3). У зв'язку з цим будемо говорити, що СНЧ σ_i матриці F має достатню відокремленість щодо збурної дії E , якщо

$$svdgap(i,F) \geq 2\|\mathrm{E}\|_2 \,. \quad (5)$$

При формальному представленні результату вбудови ДІ в контейнер F у вигляді сукупності збурень СНЧ та СНВ актуальним є питання, як ці отримані збурення відреагують на атаку проти вбудованого повідомлення, формальним представленням якої є матриця E. Очевидно, що декодування ДІ можна провести безпомилково тільки в тому випадку, коли всі збурення СНЧ та СНВ, отримані у

процесі стеганоперетворення, не змінилися в результаті атаки. СНВ, що відповідають СНЧ, для яких (5) не виконуються, на практиці можуть сильно «постраждати» в результаті атаки Е, змінивши свій напрямок порівняно з положенням у матриці СП настільки сильно (аж до протилежного напряму), що частина ДІ, результатом вбудови якої було збурення цих СНВ, буде спотворена аж до повного знищення. Тут потрібно відзначити, що все ж таки цей процес неконтрольованої випадкової зміни напрямів деяких СНВ в результаті атаки Е не носить виключно негативний характер, коли збурення СНВ буде дуже значним, неадекватним збурній дії. Справді, як випливає з формули (4), її права частина дає лише верхню межу можливих значень для $\sin 2\theta_i$, що ніяк не забороняє $\sin 2\theta_i$ відповідати малому куту повороту u_i навіть при малій відокремленості відповідного СНЧ (Рис.2.1). Це частково пояснює наявність стійких до атак проти вбудованого повідомлення стеганометодів, які дозволяють досить ефективно декодувати вбудовану ДІ в умовах (значних) збурних дій, зберігаючи при цьому надійність сприйняття формованого СП. Однак, відсутність математичного інструменту апріорної оцінки реального збурення СНВ, відповідних СНЧ з недостатньою по відношенню до Е відокремленістю та практична непередбачуваність їхньої поведінки, що ілюструє рис.2.1, змушує для досягнення мети, поставленої у роботі, зупинитися лише на тих сингулярних трійках (σ_i, u_i, v_i) матриці ЦЗ, які відповідають СНЧ із достатньою відокремленістю. Назвемо ці трійки захищеними стосовно Е. Розглянемо можливість та спосіб їх використання для визначення ЗІ.

В [16] для кількісної оцінки обсягу ЗІ розглядалися безпосередньо кути повороту вибраних (захищених від Е) ВВ, як ваговий коефіцієнт - абсолютні відокремленості відповідних ВЗ. Однак з урахуванням абсолютних відокремленостей ВЗ ми отримуємо не реальні кути повороту ВВ, а лише верхню межу для величини цього кута, аналогічно (4): $\sin 2\theta_i \le 2\|E\|_2 / gap(i,F)$, де θ_i - кут повороту u_i в результаті збурної дії Е, $gap(i,F)$ – абсолютна відокремленість ВЗ λ_i: $gap(i,F) = \min_{i \neq j} \left| |\lambda_i| - |\lambda_j| \right|$, що говорить про недоцільність

використання абсолютної відокремленості ВЗ як вагового коефіцієнта, більше того, її використання призводить до того, що кількісно обсяг ЗІ невиправдано збільшується, даючи пріоритетні позиції контейнерам, які практично не є такими. В силу цього, проводячи аналогічні міркування для СНЧ, було вирішено відмовилися від ідеї використання безпосередньо при оцінці обсягу ЗІ відокремленостей СНЧ. Однак, враховуючи, що, як зазначено вище, результат стеганоперетворення формально представляється у вигляді збурень СНЧ та СНВ матриці контейнера, очевидним є необхідність сукупного врахування цих збурень щодо визначення поняття ЗІ, але не адитивного, а як деякого інтегрального параметра, який би не штучно, а природнім шляхом враховував взаємозв'язок та взаємовплив збурень окремих формальних параметрів (СНЧ, СНВ), необхідно присутній за будь-якої збурної дії в силу однозначності нормального сингулярного розкладу матриці. Справді, нехай матриця F отримала збурення E. Побудуємо для F + E нормальне сингулярне розкладання (2):

$$F + \mathrm{E} = (U + \Delta U)(\Sigma + \Delta\Sigma)(V + \Delta V)^T, \quad (6)$$

де $\Delta U, \Delta\Sigma, \Delta V$ – збурення відповідно матриць U, Σ, V при збурній дії E, причому:

$$\Delta U \neq 0, \Delta\Sigma \neq 0, \Delta V \neq 0. \quad (7)$$

Дійсно, збурна дія E ≠ 0 обурює всі або деякі елементи f_{ij} початкової n×n-матриці F, змінюючи в загальному випадку енергію N(F) відповідного сигналу. Враховуючи, що N(F) може бути розрахована відповідно до формули:

$$N(F) = \sum_{i,j=1}^{n} f_{ij}^2,$$

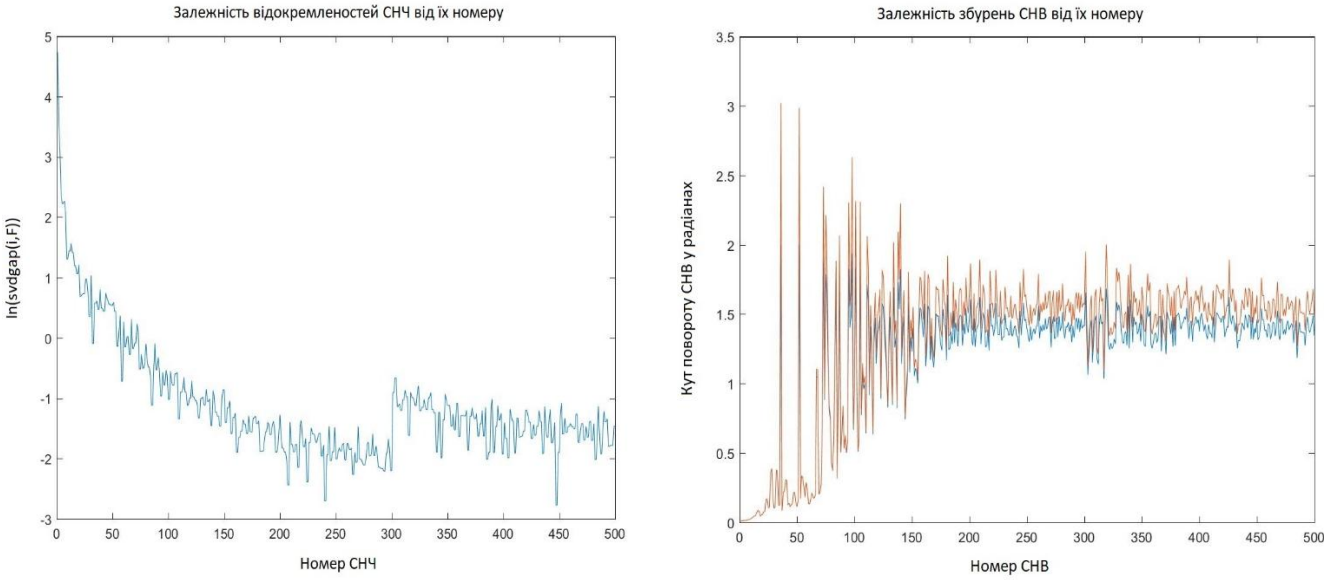
зміна f_{ij} призведе до зміни СНЧ F, наслідком чого є: $\Delta\Sigma \neq 0$. Два інших співвідношення в (7) пояснюються обов'язковою наявністю в межах матриці будь-якого ЦЗ чутливих до збурних дій СНВ, що реагують на будь-яку дію, аж до округлень під час обчислень. З (6) для невиродженої обуреної матриці F + E безпосередньо випливає, що $\Delta\Sigma = (U + \Delta U)^T(F + E)(V + \Delta V) - \Sigma$,

$\Delta U = (F + E)(V + \Delta V)(\Delta\Sigma + \Sigma)^{-1} - U$, $\Delta V = (F + E)^{-1}(U + \Delta U)(\Delta\Sigma + \Sigma) - V$.

Такий взаємозв'язок підтверджує доцільність викладеного нижче.

У процесі стеганоперетворення та наступних атак проти вбудованого повідомлення кожна із сингулярних трійок (σ_i, u_i, v_i) матриці контейнера може одержати збурення. Однак, як було зазначено вище, який-небудь «контроль» над спотворенням впровадженої ДІ ми маємо лише для захищених трійок. Позначимо M - безліч індексів СНЧ з достатньою по відношенню до E відокремленістю.

Нехай для (σ_k, u_k, v_k) $k \in M$. Кожна така трійка визначає матрицю $F_k = \sigma_k u_k v_k^T$, для якої $rank(F_k) = 1$.



а – графік залежності абсолютних відокремленостей СНЧ від їх номеру;

б – графік залежності збурень СНВ від їх номеру в умовах E, сформованої випадковим чином.

Рисунок 2.1 – Відповідність збурень СНВ матриці ЦЗ абсолютним відокремленостям її СНЧ

Оскільки в ЦЗ для СНЧ із значною відокремленістю, яка на практиці і фігурує як достатня, спостерігається її монотонне спадання зі зростанням номера СНЧ (рис.2.1(а)), то сукупність СНЧ з достатньою відокремленістю представляє з себе, як правило, множину послідовних СНЧ, а M містить послідовні натуральні числа від 1 до деякого m. Сума матриць, що відповідають захищеним трійкам, на практиці задовольняє співвідношення

$$\sum_{k\in M} F_k = \sum_{k=1}^{m} F_k = \sum_{k=1}^{m} \sigma_k u_k v_k^T , \quad (8)$$

тобто, є малоранговою апроксимацією F рангу m [19]. Саме ця апроксимація і розглядається як «поле, захищене від E», для вбудови ДІ, причому в силу

однозначності нормального сингулярного розкладання F, це «поле» ніяк не обмежує вибір реальної області ЦЗ-контейнера, яка використовується для стеганоперетворення - просторової, частотної, інших областей перетворення.

Формальне визначення та кількісний вираз для ЗІ отримаємо наступним чином. Нехай F і $\bar{F}$ – матриЦЗ контейнера та СП, $\bar{F} = \bar{U}\bar{\Sigma}\bar{V}^T$ – нормальне сингулярне розкладання для $\bar{F}$, в результаті якого отримані $\bar{\sigma}_i, \bar{u}_i, \bar{v}_i, i = \overline{1,n}$, - СНЧ, ліві та праві СНВ СП відповідно. Захищені від Е збурення сингулярних трійок, отримані в результаті стеганоперетворення, відповідають індексам із М.

Визначення. Захищена від збурної дії Е ДІ визначається різницею апроксимацій рангу m для матриць F контейнера та $\bar{F}$ СП:

$$S = \sum_{k=1}^{m} \bar{\sigma}_k, \bar{u}_k, \bar{v}_k{}^T - \sum_{k=1}^{m} \sigma_k u_k v_k^T \quad (9)$$

де m – максимальний індекс серед СНЧ F , які мають достатню по відношенню до Е відокремленість.

Формула (9) визначає шуканий інтегральний параметр, який дозволяє оцінити виникаючі в результаті стеганоперетворення збурення СНЧ і СНВ в сукупності, які нас цікавлять, враховуючи їх безпосередній взаємозв'язок та взаємовплив, крім того, очевидним є тут відсутність будь-якого зв'язку з конкретикою використовуваного для вбудови ДІ стеганографічного метода, що відповідає меті роботи.

Як кількісну характеристику для ЗІ пропонується використовувати спектральну матричну норму $\|S\|_2$. Зауважимо, що тут немає принципової різниЦЗ, яку саме матричну норму розглядати, враховуючи співвідношення, що пов'язують спектральну норму з нормою Фробеніуса $\|S\|_F$, нормами $\|S\|_1$, $\|S\|_\infty$ [19]. Проте з огляду на те, що саме спектральна норма фігурує в оцінках чутливості як ВЗ, ВВ, так і СНЧ, СНВ, вибір зроблено на її користь.

Очевидно, що більше $\|S\|_2$, тим більше сукупне збурення захищених сингулярних трійок, що відбулося в результаті стеганоперетворення, буде відносно «захищено» від Е, тим більший обсяг ДІ, формальним представленням вбудови якої є це збурення, буде збережено, а чутливість СП буде менше, що і враховується в нижче запропонованому методі вибору контейнера.

Враховуючи різке зменшення відокремленості при переході від СНЧ із максимальними значеннями до СНЧ із меншими значеннями (рис.2.1(а)), співвідношення (5) та прийняте визначення для ЗІ, можна теоретично припустити, що отримувана оцінка обсягу ЗІ $\|S\|_2$ оже виявитися недостатньо ефективною у разі, якщо ЦЗ матиме лише одне СНЧ (очевидно - σ_1) з достатньою по відношенню до Е відокремленістю. Справді, оскільки для σ_1 в оригінальних ЦЗ маємо: $\sigma_1 >> \sigma_i$, $i = \overline{2,n}$, типова ілюстрація чого представлена на рис.2.2 для ЦЗ розміром 50×50 пікселів, а *svdgap(1,F)* >> *svdgap(i,F),* $i = \overline{2,n}$ (рис.2.1(а)), це призводить до того, що перші СНВ u_1 ,v_1 відповідно до (4) практично не збурюються під впливом Е [21] (кут повороту такого вектора від початкового положення можна порівняти з нулем), наслідком чого є: $\|S\|_2 \approx 0$ для будь-якого з таких ЦЗ.

Однак така ситуація (рис.2.3 (NC відповідає формулі (10)) може мати місце тільки в тому випадку, коли передбачається, що СП піддаватиметься значній збурній дії Е, аж до порушення його надійності сприйняття. Візуалізація величини збурної дії, що фіксує порушення надійності сприйняття СП, наведена на прикладі (рис.2.4). Однак навіть у цьому випадку відхилення параметра NC, що характеризує чутливість СП до дії Е, для СП, побудованого на основі контейнера з максимальним обсягом ЗІ, від максимально можливого значення NC для всіх розглянутих зображень склало лише 5,5%. (Рис.2.3). Зауважимо, що на практиці таке обмеження не є критичним, оскільки при застосуванні атак проти вбудованого повідомлення, враховуючи незацікавленість порушника у тому, щоб його дії негайно були виявлені, атака буде відбуватися з збереженням надійності сприйняття збуреного СП, тобто не може мати значну $\|E\|_2$.

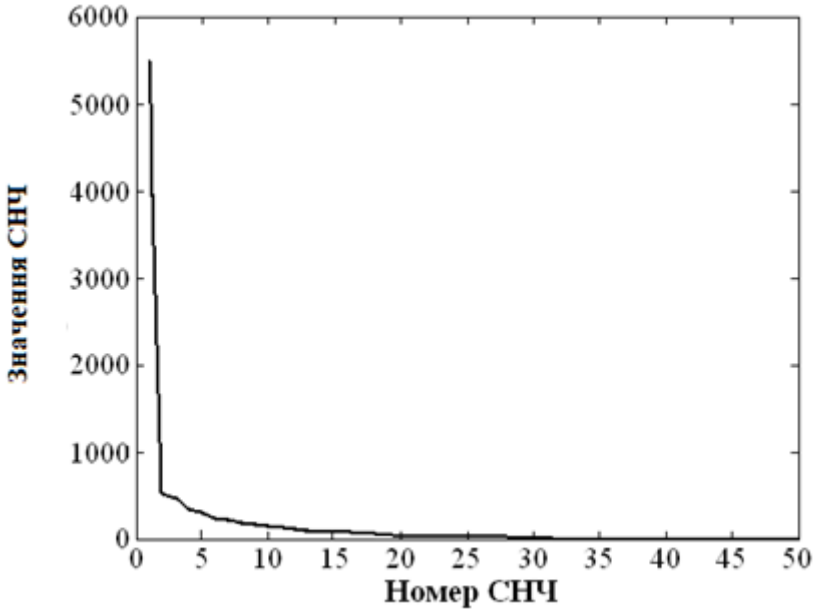


Рисунок 2.2 – Графік залежності значення СНЧ від його номеру для оригінального ЦЗ

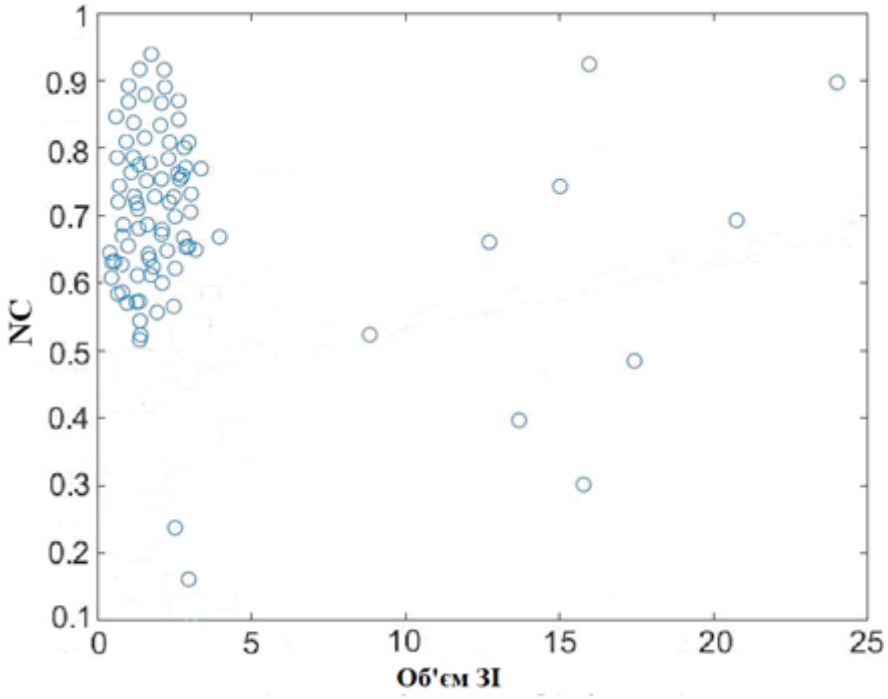


Рисунок 2.3 – Залежність коефіцієнта NC від об’єму ЗІ при використанні стеганометода [22] в умовах мультиплікативного шуму з D=0.004[3]

Рисунок 2.4 - ілюстрація можливого порушення надійності сприйняття ЦЗ при розглянутій збурній дії: а – оригінальне ЦЗ; б – ЦЗ, на яке було накладено мультиплікативий шум з *D=0.0044*

2.2 Метод вибору стеганографічного контейнера в умовах атак проти вбудованого повідомлення

З урахуванням всього вищевикладеного, основні кроки запропонованого методу вибору контейнера з наявної множини ЦЗ для заданого секретного повідомлення, що дає максимально можливу або близьку до максимально можливої стійкість по відношенню до збурної дії E, наступні:

Нехай K - безліч ЦЗ-контейнерів, з яких відбувається вибір, $p_1, p_2 \ldots p_l$ - бінарна послідовність – результат попереднього кодування повідомлення, що пересилається, M_S - Розглянутий для застосування ДІ стеганометод, E – формальне подання передбачуваної атаки проти вбудованого повідомлення.

Крок 1. Для кожного ЦЗ $F \in K$:

1.1. Побудувати нормальне сингулярне розкладання (2) для F;

1.2. Визначити відокремленості (3) для отриманих СНЧ;

1.3. Визначити множину M індексів СНЧ з достатньою відокремленістю по відношенню до збурення E;

1.4. Побудувати для F апроксимацію (8) рангу m;

1.5. Виконати вбудовування ДІ $p_1, p_2 \dots p_l$ за допомогою вибраного стеганографічного методу M_S в контейнер F. Результат – СП з матрицею $\bar{F}$;

1.6. Побудувати нормальне сингулярне розкладання (2) для $\bar{F}$;

1.7. Побудувати для $\bar{F}$ апроксимацію (8) рангу m;

1.8. Побудувати матрицю ЗІ S (9);

1.9. Визначити $\|S\|_2$;

Крок 2. Серед всіх ЦЗ множини K визначити таке F_V, для якого матриця S_V (9) відповідатиме відношенню:

$\|S_V\|_2 = \max_{F \in K} \|S\|_2$.

ЦЗ S_V - шуканий контейнер.

2.3 Оцінка ефективності розробленого методу вибору контейнера

Результати обчислювального експерименту з тестування розробленого методу в умовах різних атак проти вбудованого повідомлення, різних стеганометодів, що використовуються для вбудови ДІ, а також результати порівняльного аналізу з методом [16] наведено на рис.2.5, де відображено залежність між обсягом ЗІ та чутливістю СП до збурних дій, кількісним показником якої взято коефіцієнт кореляції NC між вбудованою ДІ $p_1, p_2, \dots p_t, p_i \in \{0,1\}, i = \overline{1,t}$, та декодованою $\overline{p_1}, \overline{p_2}, \dots \overline{p_t}, \overline{p_l} \in \{0,1\}, i = \overline{1,t}$, ДІ [23]:

$$NC = \frac{\sum_{i=1}^{t} p_i' \times \bar{p}_i'}{t}, \quad (10)$$

де $p_i' = 1, \bar{p}_i' = 1$, якщо $p_i = 1, \bar{p}_i = 1$, і $p_i' = -1, \bar{p}_i' = -1$, якщо $p_i = 0, \bar{p}_i = 0$.

На отриманих графіках (рис.2.5 (а, в, д)) для розробленого методу для будь-яких стеганометодів, будь-яких збурних дій можна помітити деякий «розкид»: для ЦЗ-контейнерів, які мають близькі або навіть рівні значення обсягу ЗІ значення параметра NC відрізняються між собою. Це пов'язане із наступним. Очевидно, що не всі СНВ з тих, які відповідають СНЧ з достатньою відокремленістю, є нечутливими до збурних дій. Більш того, на підставі наявного досвіду видно, що

відокремленість СНЧ не є мірою чутливості відповідного СНВ до збурних дій навіть у випадку (5) [20]. Очевидно, це можна стверджувати лише для тих СНВ, СНЧ які мають дуже значну відокремленість, перетворюючи праву частину (4) практично в нуль:

$$\sin 2\theta_i \leq \frac{2\|E\|_2}{svdgap(i,F)} \approx 0. \quad (11)$$

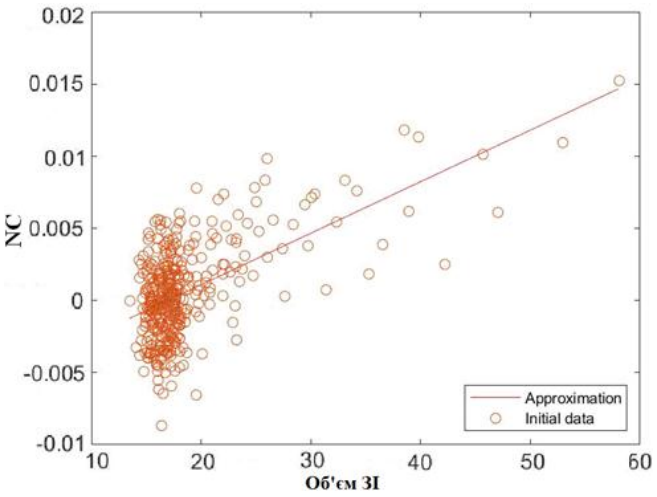
У такому разі відповідний СНВ без варіантів буде нечутливий до збурення E (у припущенні, що кут θ_i повороту СНВ гострий). Однак навіть якщо виконується (5), це не гарантує адекватну реакцію СНВ на збурення: при малій збурній дії кут його повороту θ_i може бути далекий від нуля, а величина кута визначатиметься не тільки вбудовуванням ДІ, а й збуреннями, не пов'язаними безпосередньо із стеганоперетворенням, наприклад, похибками округлень. Такі збурення захищених векторів дають ілюзію значного обсягу ЗІ, що не відповідає дійсності. Все вищесказане пояснює і те, що при максимальному обсязі ЗІ відповідний контейнер може давати СП, стійкість якого не є максимальною з можливих для множини *K* (хоча вона очевидно буде близька до максимальної).

Для покращення результатів роботи методу, зменшення розкиду значень NC при близьких значеннях обсягу ЗІ очевидно слід було б використовувати при аналізі сингулярні трійки (σ_i, u_i, v_i), в яких усі вхідні параметри є гарантовано нечутливими до збурних дій. Для забезпечення нечутливості вибраних для аналізу сингулярних трійок треба було б посилити умову достатності відокремленості СНЧ:

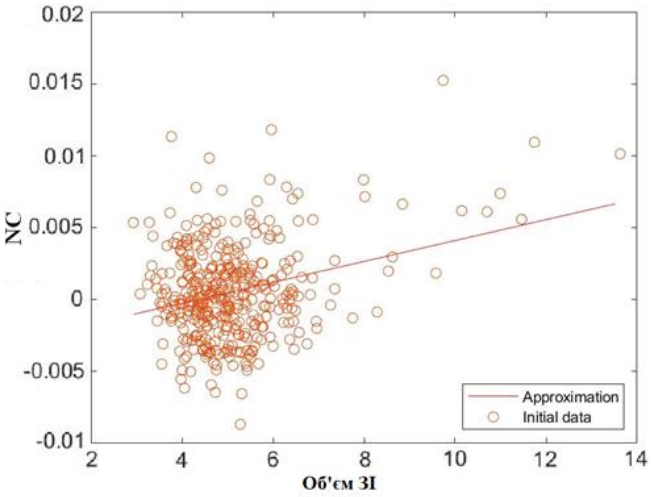
$$svdgap(i,F) \gg 2\|E\|_2, \quad (12)$$

проте на практиці використання (12) призведе до того, що в процесі аналізу систематично буде задіяна лише дуже мала (до одного) кількість СНЧ, що, як зазначалося вище, є небажаним.

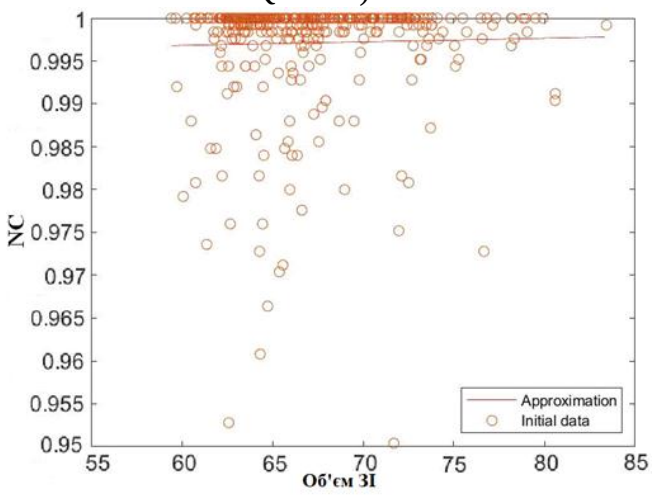
Однак слід зауважити, що хоча на практиці розкид і має місце, але при найбільшому обсязі ЗІ метод завжди вибирає контейнер, який забезпечує малу або близьку до найменшої чутливість СП до атак проти вбудованого повідомлення (рис.2.5, табл.2.1).



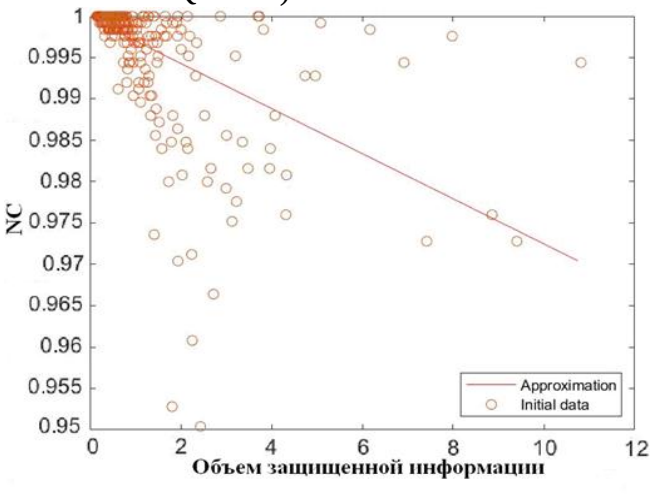
а – розроблений метод (стеганометод LSB[24], атака стисненням QF = 75)



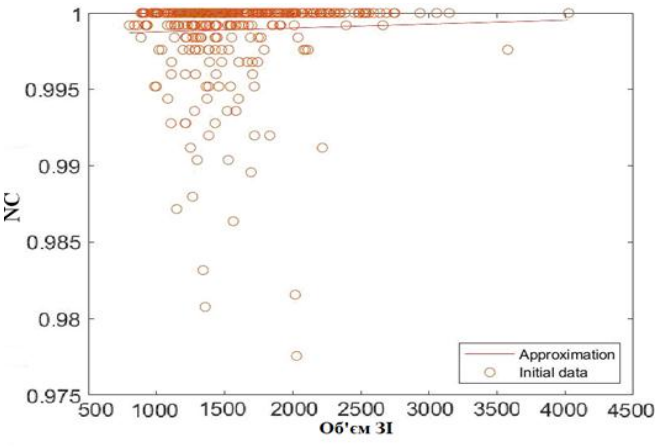
б – метод [16] (стеганометод LSB[24], атака стисненням QF = 75)



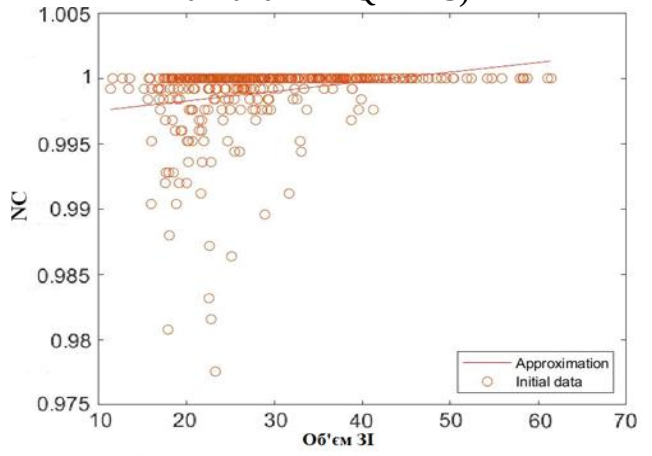
в – розроблений метод (стеганометод [25], атака стисненням QF = 75)



г - метод [16] (стеганометод [25], атака стисненням QF = 75)



д – розроблений метод ((стеганометод [22], атака - накладання гауссівського шуму з D=0.0005)



е - метод [16] ((стеганометод [22], атака - накладання гауссівського шуму з D=0.0005)е

Рисунок 2.5 – Графіки залежності коефіцієнта NC від об’єму ЗІ для різних стеганоалгоритмів, використаних для вбудовування ДІ, і різних атак проти вбудованого повідомлення

Результати порівняльного аналізу розробленого методу с аналогом приведені в табл. 1.

Таблиця 1 – Порівняння ефективності запропонованого методу і його аналога [16]

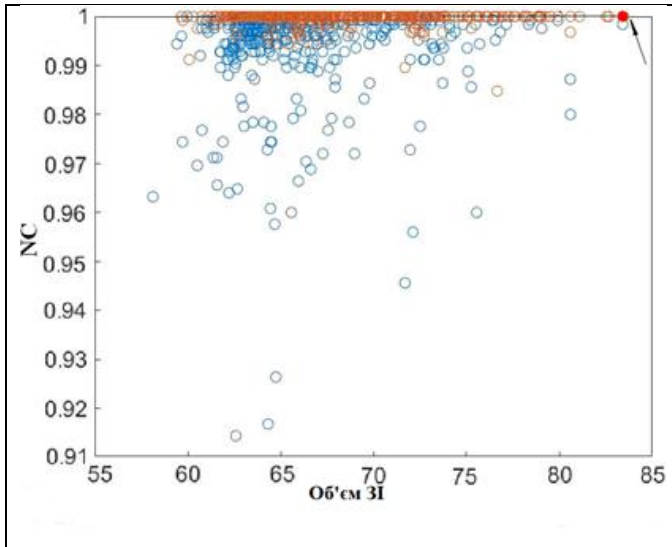
Стеганометод	Збурна дія	Значення *NC*, що відповідає максимальному об'єму ЗІ		Максимальне значення NC в умовах експерименту
		Метод [16]	Запропонований метод	
Метод LSB (просторова область вбудовування ДІ) [24]	Стиснення з втратами з *QF*=75	0.0101	0.0152	0.0152
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	0.0211	0.0211	0.0211
	Мультиплікативний шум с *D*=0.0005	0.4267	0.4267	0.4267
Метод з кодовим управлінням вбудовування ДІ (просторова область вбудовування ДІ) [25]	Стиснення з втратами з *QF*=75	0.9944	0.9992	1
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	0.7496	0.8568 (на 14.3%)	0.8651
	Мультиплікативний шум с *D*=0.0005	1	1	1
Метод модифікації максимального СНЧ (вбудовування ДІ - область сингулярного розкладання) [22]	Стиснення з втратами з *QF*=75	1	1	1
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	1	1	1
	Мультиплікативний шум с *D*=0.0005	1	1	1
Метод Коха і Жао (частотна область вбудовування ДИ) [26]	Стиснення з втратами з *QF*=75	1	1	1
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	0.9752	0.9608	1
	Мультиплікативний шум с *D*=0.0005	1	1	1

Результати обчислювального експерименту демонструють високу ефективність запропонованого методу для кожного з розглянутих стеганометодів вбудовування ДІ (які навмисно були обрані так, щоб перевірити ефективність

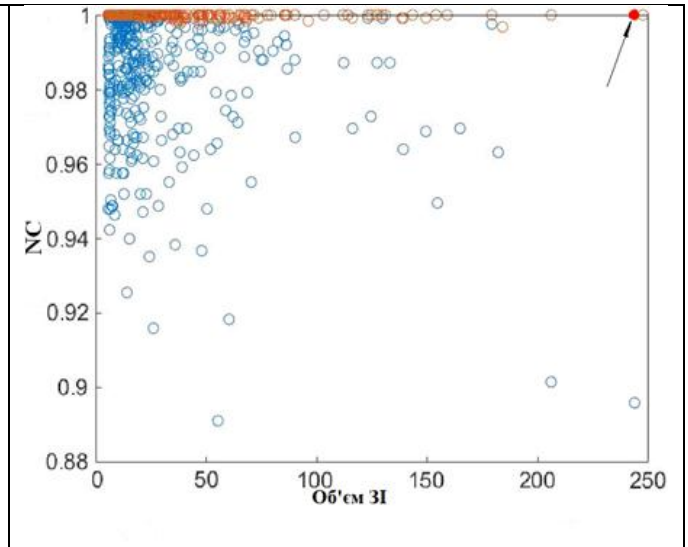
розробленого методу при використанні різних областей стеганоперетворення), що відповідає теоретичним очікуванням, перевагу розробленого методу порівняно з аналогом. У новому методі максимальна відмінність стійкості (коефіцієнта NC) СП, отриманого на підставі контейнера з максимальним обсягом ЗІ, від максимально можливого в умовах експерименту NC склало 3.9%, в той час, як для методу [16] ця відмінність максимально 11.6% (табл.2.1). По рис.2.5 очевидним є можливість порушення у методі [16] загального тренду збільшення NC з збільшенням обсягу ЗІ для візуалізації якого використовується лінійна апроксимація отриманих даних. Розроблений метод практично скрізь дає показник NC для СП, побудованого на основі обраного контейнера з максимальним обсягом ЗІ, не менше ніж дає метод [16]. Виняток становить лише метод Koch and Zhao, де контейнер, обраний новим методом, забезпечує гірший результат стійкості, проте цей програш незначний (менше 1.5%), при цьому відмінність у новому методі від максимального за експериментом NC складає лише 3.9%.

Запропонований у роботі метод має дуже важливу у практичному сенсі перевагу , порівняно з аналогами. Виходячи з введеного визначення ЗІ, можна стверджувати, що ЦЗ-контейнери, які були обрані для збурних дій певної сили E, можуть бути ефективно використані в умовах, коли сила такого впливу знижується: $\|S\|_2$ зменшується (рис.2.6).

Стрілками на рис.2.6 відзначені ЦЗ для експериментів з меншою силою збурної дії, які були визначені як такі, що мають найбільший обсяг ЗІ в експерименті з більшою силою збурної дії. Як видно, ЦЗ або збігаються (рис.2.6(а)), або відрізняються дуже незначно з погляду обсягу ЗІ (рис.2.6(б)). Це призводить до того, що принципово можна розглянути при роботі запропонованого методу збурні дії максимальної або значної сили, які не порушують надійності сприйняття ЦЗ. Вибрані для них один раз контейнери із заданої множини ЦЗ можуть використовуватися у всіх випадках більш слабких атак проти вбудованого повідомлення без попереднього пошуку.



а – стеганометод з кодовим управлінням



б – метод Коха і Жао

Рисунок 2.6 - Графіки залежності *NC* від об’єма ЗІ в умовах атаки стисненням з *QF*=70 (синій колір), *QF*=85 (червоний колір)

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ ВИБОРУ СТЕГАНОГРАФІЧНОГО КОНТЕЙНЕРА В УМОВАХ АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

3.1 Засоби реалізації програмного продукту

Для програмної реалізації методу вибору стеганографічного контейнера в умовах атак проти вбудованого повідомлення, було використано програмне середовище Matlab.

Matlab пропонує користувачеві велику колекцію методів, функцій та засобів, що спеціалізуються на вирішенні задач із різних областей математики. Усі розрахунки та змінні у Matlab представлені в математичній формі, що дозволяє дуже добре відображати їх візуально. Через це ця система є фаворитом в області розробки, моделювання та удосконалення математичних алгоритмів.

Оскільки основний тип даних, який використовується у Matlab, є багатовимірний масив, то проблеми і задачі, що базуються на матричних обчисленнях у Matlab виконуються набагато швидше, ніж у його аналогів, що дає перевагу Matlab у питанні обробки цифрових зображень.

Назва Matlab походить від поєднання двох слів – матрична та лабораторія. Архітектура Matlab була розроблена таким чином, щоб можна було з легкістю отримати доступ до спеціальних програмних комплексів з матричних обчислень.

Matlab завжди прагнув розвиватись у напрямку потреб для кожного користувача. Тому Matlab є чудовим інструментом для пізнання у різноманітних галузях, навіть у промисловості, де Matlab є засобом для реалізації високонавантажених досліджень, проведення аналізу даних та побудови професійних застосувань.

У Matlab велику роль відведено тулбоксам. Це пакети функцій та засобів, що спрямовані для вирішення задач у певній області математики. Прикладом такого тулбокса є Image Processing Toolbox [27]. Такі пакети є надзвичайно важливим компонентом системи, адже містять у собі реалізації відомих методів, що були добре протестовані. Вони постійно доповнюються новими функціями і створюються нові такі пакети.

Головні складові системи Matlab:

Мова. Оскільки основним типом даних у Matlab є масив, то він надає можливість будувати як прості та швидкі програми з матричними розрахунками, так і складні програми із об’єктно-орієнтованим підходом та паралельними обчисленнями.

Середовище розробки. Для користувача Matlab пропонує дружелюбний до новачка інтерфейс, а також можливість відслідковувати зміну змінних у процесі обчислень та інтерфейс для візуального відображення данних.

Керована графіка. Matlab надає можливість побудови двохвимірної та трьохвимірної графіки для відображення даних, що фігурують у обчисленні. Також є можливість встановлення та налаштування різноманітних параметрів та властивостей зовнішнього вигляду графіків.

Бібліотека функцій математики. Matlab містить у собі велику колекцію різноманітних функцій та засобів, що реалізують як найпростіші математичні операції, такі як додавання та віднімання, так і більш складні, наприклад, матричний добуток.

Інтерфейс програм. Matlab надає можливість користувачеві взаємодіяти із іншими мовами. Наприклад, взаємодія із мовою С.

3.2. Технологія реалізації програмного продукту

Image Processing Toolbox містить у собі багату колекцію методів та функцій, необхідних для зчитування, обробки та аналізу цифрових зображень. Тому вона ідеально підходить для розробки та тестування програмних продуктів націлених на роботу із цифровими зображенями. Основним типом даних у Matlab є багатовимірні масиви, що і робить Matlab одним із найкращих середовищ для опрацювання зображень.

Image Processing Toolbox дає можливість користувачеві працювати із різними колірними моделями цифрових зображень. Також в цьому тулбоксі є методи, що реалізовують конвертацію зображення із одного формату або колірної моделі до іншого. Тулбокс також може реалізувати зменшення та збільшення кількості кольорів за допомогою різних відомих алгоритмів.

Важливим моментом при опрацюванні ЦЗ є його попередня обробка. Прикладом однієї із таких обробок реалізованих в тулбоксі є підвищення якості картинки, за допомогою функції вирівнювання гістограми, або зміна діапазону яскравості чи контрастування цифрових зображень та методи маскування.

Далі наведено опис функцій та приклад їх використання у реалізації програмного продукту:

Перш за все, для реалізації розробленого алгоритму потрібно вибрати папку з вхідною множиною контейнерів, із якої слід обрати найкращий. Для цього було створено діалогове вікно вибору папки із контейнерами, а також вікно вибору папки, у яку буд е зберігатись, як результат, найкращий контейнер:

```
path_countainer = uigetdir('','Виберіть папку з контейнерами');
path_result = uigetdir('','Виберіть папку для зберігання результатів');
```

Далі потрібно було визначити кількість файлів у папці для подальшого їх аналізу за допомогою циклу. Для цього ми використали функцію dir(), що приймає в якості вхідного параметру шлях до папки, а повертає список змісту папки:

```
a=dir(path_countainer);
amount_img=size(a,1)-2;
```

Також було зчитано файл, у якому зберігається інформація, що має бути передана по прихованому каналу зв'язку. Функція readmatrix дозволяє зчитати файл та записати його вміст у змінну у вигляді матриці:

```
D=readmatrix('hiden_inf.txt');
```

Далі був запущений цикл з такою ж кількістю ітерацій, як і файлів у обраній папці. Для цього використалась конструкція for. Цей цикл складається із двох частин, у першій вказується кількість ітерацій циклу, а у другій тіло циклу, що буде виконуватись на кожній ітерації:

```
for k=1:1:amount_img
...
end
```

На кожній ітерації циклу була використана функція imread(). Ця функція приймає в якості вхідних параметрів шлях до файлу, який потрібно зчитати, та

його назву, а повертає матрицю обраного зображення. У випадку зчитування повноколірного зображення у змінну записується трьохвимірна матриця, яка складається із трьох матриць розміром, відповідним до розміру зображення, що відповідають кожному із трьох кольорів колірної моделі RGB:

```
I=string(path_countainer)+'\img('+num2str(k)+')'+string(img_format);
F=imread(I);
```

Далі були визначені розміри зображення за допомогою функції size(), і обрані такі максимальні величини для обрізання ЦЗ, щоб можна було проаналізувати зображення, при розбиванні його на блоки розміром 8х8, цілком. Функція size() приймає на вхід два параметра: змінну, розмір якої потрібно визначити, а також скаляр, який відповідає за те, яку розмірність змінної буде повернено:

```
m = size(F, 1);
n = size(F, 2);
```

Функція fix() повертає ціле значення від частки. Це потрібно для визначення такого максимального розміру зображення, що може бути націло поділене на блоки певного розміру:

```
m=(fix(m/8))*8;
n=(fix(n/8))*8;
```

Далі за допомогою функції imcrop() було обрізане ЦЗ до потрібних розмірів. Ця функція приймає на вхід зображення, що потрібно обітнути, та прямокутник із заданим розміром та координатами лівого верхнього кута, у формі якого і буде обрізане зображення:

```
F=imcrop(F,[0,0,n,m]);
```

Далі із тривимірної матриці зчитаного повноколірного зображення була виділена та матриця кольору, що обере користувач:

```
F=F(:,:,color);
```

Потім за допомогою конструкції switch case відбувається вбудовування ДІ у пустий контейнер згідно вибраного користувачем стеганографічного алгоритму. Ця конструкція являє з себе спрощений вигляд конструкції if else, що дозволяє

визначити тіло функції, яке потрібно виконати, виходячи із того, яке значення приймає змінна, подана у якості умови оператора switch:

```
switch chosed_method
    case 1
       stego=uint8(stego_jk(F,D));
    case 2
       stego=uint8(stego_sign(F,D));
    case 3
       stego=uint8(stego1(F,D));
    case 4
       stego=uint8(stego_lsb(F,D));
end
```

Потім за допомогою такої ж самої конструкції відбувається моделювання атаки на стеганоповідомлення за допомогою ймовірної збурної дії, яку також має можливість обрати користувач. Потрібно зазначити, що в випадку обрання шуму, як типу атаки на стеганоповідомлення, використовується функція imnoise(). Ця функція дозволяє у якості вхідного параметру вказати тип шуму, наприклад, гауссівський чи мультиплікативний, а також налаштувати властивості обраного шуму, такі як математичне очікування чи дисперсія:

```
switch chosed_noise
    case 1
       stego_noise=imnoise(stego,'gaussian',0,noise_par);
       orig_noises=imnoise(F, 'gaussian',0,noise_par);
       view = imnoise(view, 'gaussian',0,noise_par);
    case 2
       stego_noise=imnoise(stego,'speckle',noise_par);
       orig_noises=imnoise(F, 'speckle',noise_par);
       view = imnoise(view, 'speckle',noise_par);
    case 3
       stego_noise=imnoise(stego,'poisson');
```

```
            orig_noises=imnoise(F, 'poisson');
            view = imnoise(view, 'poisson');
        case 4
            stego_noise=imnoise(stego,'salt & pepper');
            orig_noises=imnoise(F, 'salt & pepper');
            view = imnoise(view, 'salt & pepper');
    end
```

Також був окремо прописаний код, якщо в якості збурної дії було обрано стиснення. Для цього стеганоповідомлення було збережено у окремій папці у форматі з втратами з обраним коефіцієнтом якості за допомогою функції imwrite():

```
    if chosed_noise==5
        stego_jpg_path=['D:\dyp\dyp\stegoQF75\img' num2str(k) '.jpg'];
        imwrite(stego,stego_jpg_path,"Quality",noise_par);
        stego_jpg=imread(stego_jpg_path);
        orig_jpg_path=['D:\dyp\dyp\QF75\img' num2str(k) '.jpg'];
        imwrite(F,orig_jpg_path,"Quality",noise_par);
        orig_jpg=imread(orig_jpg_path);
        path = ['D:\dyp\dyp\view.jpg'];
        imwrite(view,path,"Quality",noise_par);
        view=imread(path);
      else
        stego_noise_path=['D:\dyp\dyp\stego_noise\img' num2str(k) '.tif'];
        imwrite(stego_noise, stego_noise_path);
        orig_noises_path=['D:\dyp\dyp\noises\img' num2str(k) '.tif'];
        imwrite(orig_noises,orig_noises_path);
      end
```

Потім за допомогою функцій switch та if else було декодовано ДІ із стеганоповідомлення, виходячи із того, який стеганоалгоритм був обраний користувачем:

```
if chosed_noise == 5
    switch chosed_method
    case 1
       decode_inf=destego(stego_jpg);
    case 2
       decode_inf=destego_sign(stego_jpg);
    case 3
       decode_inf=destego1(stego_jpg,F);
    case 4
       decode_inf=destego_lsb(stego_jpg);
    end
else
    switch chosed_method
    case 1
       decode_inf=destego(stego_noise);
    case 2
       decode_inf=destego_sign(stego_noise);
    case 3
       decode_inf=destego1(stego_noise,F);
    case 4
       decode_inf=destego_lsb(stego_noise);
    end
end
```

За допомогою попередньо визначеної функції nc() було вирахувано коефіцієнт кореляції декодованої інформації, та тієї що передавалась для стеганоперетворення:

```
NC(k)=nc(decode_inf,D);
```

Далі було вирахувано об’єм захищеної інформації також за допомогою попередньо визначених функцій:

```
if chosed_noise ==5
```

```
        [obyom(k), count(k)]=def_obyom(F,stego,orig_jpg);
        [obyom_exp(k), count_exp(k)]=def_obyom_exp(F,stego,orig_jpg);
    else
        [obyom(k), count(k)]=def_obyom(F,stego,orig_noises);
        [obyom_exp(k), count_exp(k)]=def_obyom_exp(F,stego,orig_noises);
    end
```

За допомогою наступного коду було відсортовано масив, у якому зберігались значення об’ємів ЗІ. Для цього була використана функція sort(). Вона повертає вказаний в якості вхідного параметру масив, у якому елементи були відсортовані в порядку зростання:

```
    NC_exp=NC;
    sortOb_exp = sort(obyom_exp);
    for i=1:1:amount_img
       for j=1:1:amount_img
         if(sortOb_exp(i)==obyom_exp(j))
            sortNC_exp(i)=NC_exp(j);
         end
      end
    end
```

І за допомогою відсортованого масиву було обрано та кількість найкращих контейнерів, яку вказав користувач. Обрані контейнери були записані у папку, яку користувач вказав:

```
    ans_amount = str2num(get(handles.edit1,'String'));
    for i=amount_img-ans_amount+1:1:amount_img
       for j = 1:1:amount_img
          if(sortOb_exp(i)==obyom_exp(j))
             answer(count)=j;
             count = count+1;
          end
       end
```

```
end
for i=1:1:ans_amount
   I=string(path_countainer)+'\img ('+num2str(answer(i))+')'+string(img_format);
   F=imread(I);
   m = size(F, 1);
   n = size(F, 2);
   x=fix((n-s)/2);
   y=fix((m-s)/2);
   F=imcrop(F,[x,y,s-1,s-1]);
   path = string(path_result)+'\img ('+num2str(i)+')'+string(img_format);
   imwrite(F,path)
end
```

Для графічного відображення результатів обчислення було вирішено створити на інтерфейсі програмного продукту осі, і будувати на них графіки залежності коефіцієнту NC від об’єму ЗІ для обраної вибірки контейнерів:

```
axes(handles.axes2)
plot(obyom_exp, NC, 'o')
title('Залежність NC від обєму захищенної інформації')
xlabel('Обєм захищенної інформації')
ylabel('NC')
```

За допомогою функції axes() в якості вхідного параметру вказується та пара осей, яка буде зроблена обраною для відображення на ній графічного представлення даних.

Функція plot() будує на обраній парі осей графік залежності однієї множини від іншої, котрі передані як вхідні параметри цієї функції.

Функції title(), xlabel() та ylabel() налаштовують зовнішній вигляд графіка, а саме вказують його назву, та назви для осей.

Також для відслідковування забезпечення зберігання надійності сприйняття стеганоповідомлення після атаки на нього, було вирішено відображувати деяке

атаковане стеганоповідомлення на інтерфейсі. Це було реалізовано за допомогою функції imshow():

```
handles.axes3.Visible = true;
axes(handles.axes3)
imshow(uint8(view))
```

Також для зміни вікна налаштувань атаки на стеганоповідомлення при виборі певного типу атаки був написаний наступний код:

```
if(get(hObject, 'Value')==5)
   set(handles.edit3, 'Enable','on');
   set(handles.text9,'String','Коеф. стиснення:');
   set(handles.edit3,'String','75');
elseif(get(hObject, 'Value')==3||get(hObject, 'Value')==4)
   set(handles.edit3, 'Enable','off');
   set(handles.text9, 'String','Відхилення:');
   set(handles.edit3,'String','0.0001');
else
   set(handles.edit3, 'Enable','on');
   set(handles.text9, 'String','Відхилення:');
   set(handles.edit3,'String','0.0001');
end
```

Він реалізовує блокування поля для вводу дисперсії шуму у випадку, коли для обраного шуму це неможливо. А також реалізовує зміну назви параметру, який можна налаштувати, між переключанням атаки шумом та атаки стисненням.

3.3 Інструкція з експлуатації програмного продукту

У програмному продукті, реалізованому для розв’язку задачі вибору контейнера в умовах атак на стеганоповідомлення, було створено користувацький інтерфейс для облегшення роботи із програмою та взаємодії із користувачем (рис. 3.1).

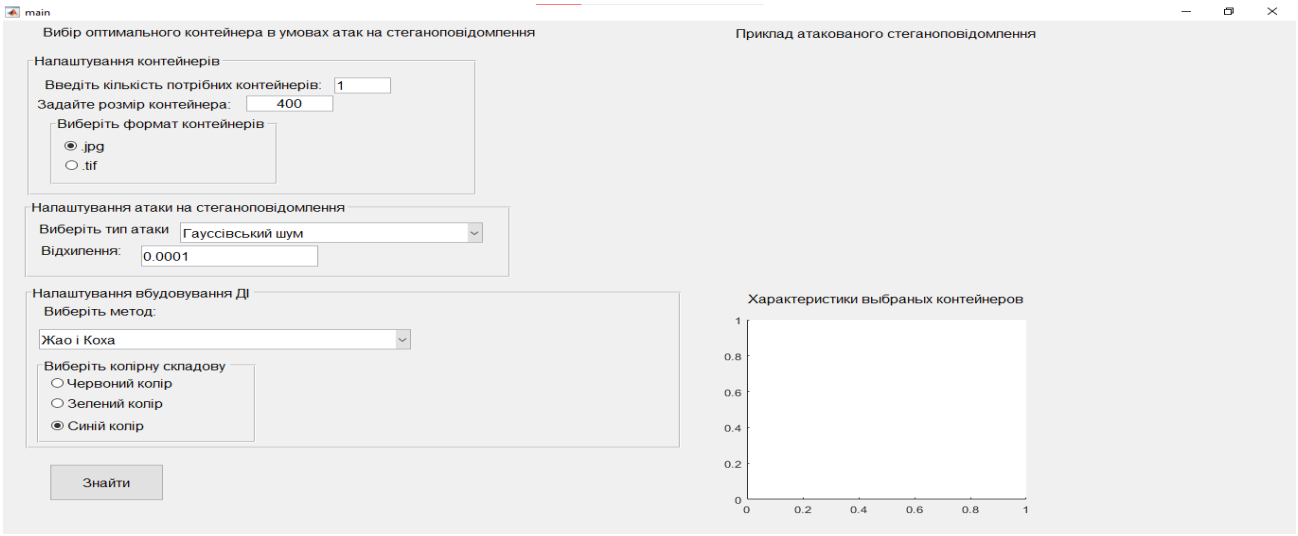


Рисунок 3.1 – Загальний вигляд користувацького інтерфейсу

Оскільки задачею, поставленою перед реалізованим продуктом, є вибір контейнера із скінченної множини, то найкращим рішенням для вводу такої множини у умови задачі є вибір папки із зображеннями за допомогою діалогового вікна (рис. 3.2). Також для зручності практичного використання, обраного програмою, найкращого контейнеру, було вирішено зберігати його у окремій папці, попередньо обрізавши його до потрібних розмірів. Було реалізовано відповідне діалогове вікно для обрання папки для результатів (рис. 3.3).

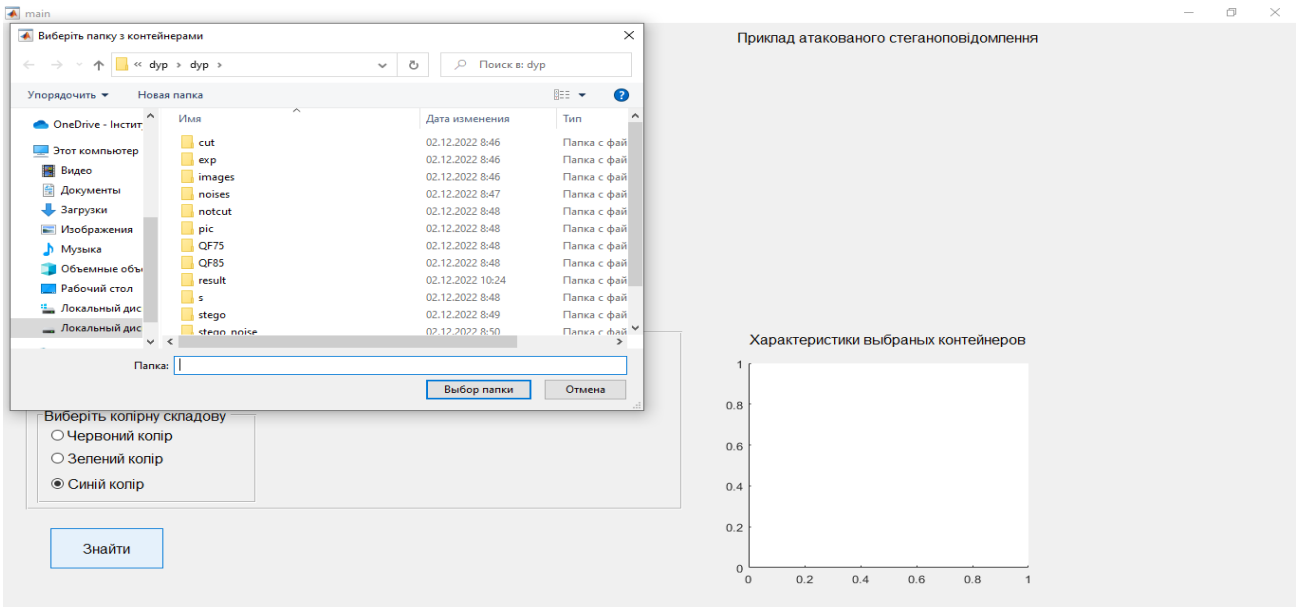


Рисунок 3.2 – Діалогове вікно вибору папки із початковою множиною контейнерів

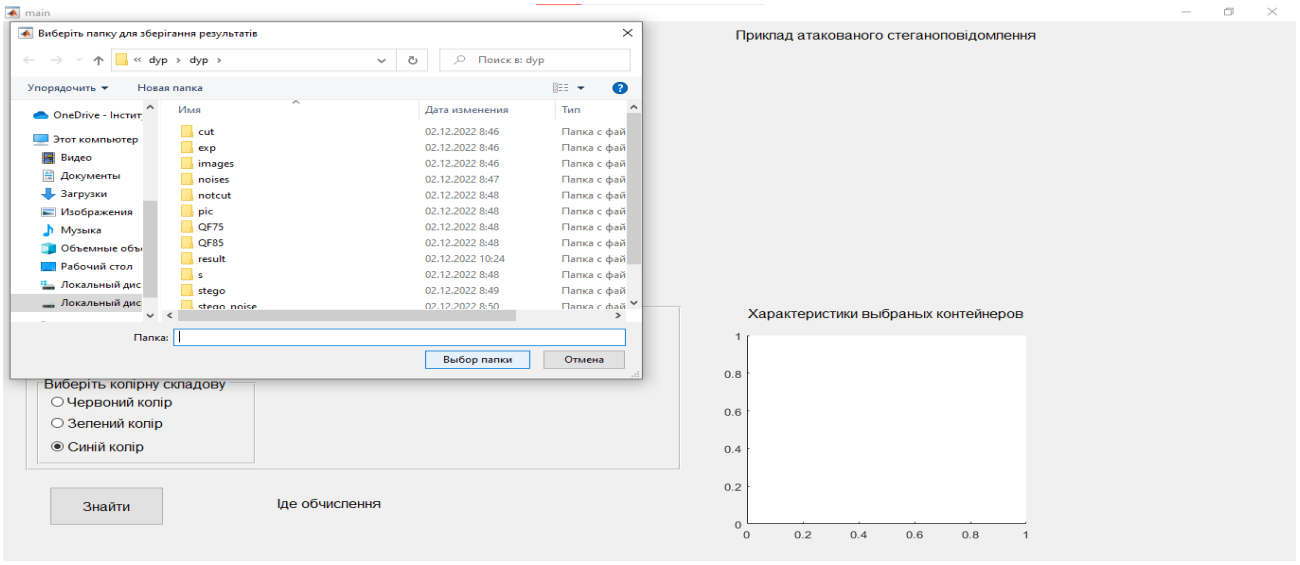


Рисунок 3.3 – Діалогове вікно вибору папки для подальшого запису результуючих контейнерів

Також було реалізовано для користувача ряд можливостей, щодо налаштування умов задачі, таких як: налаштування формулювання результуючих контейнерів, налаштування стеганоалгоритму, що вбудовує ДІ у контейнери, та налаштування атаки на стеганоповідомлення, що поділяється на налаштування шуму чи стиснення, залежно від того, що обере користувач. Наприклад, для реалізації можливості вибору стеганографічного методу було обрано випадаючий список (рис. 3.4), як і для вибору типу атаки на стеганоповідомлення (рис. 3.5).

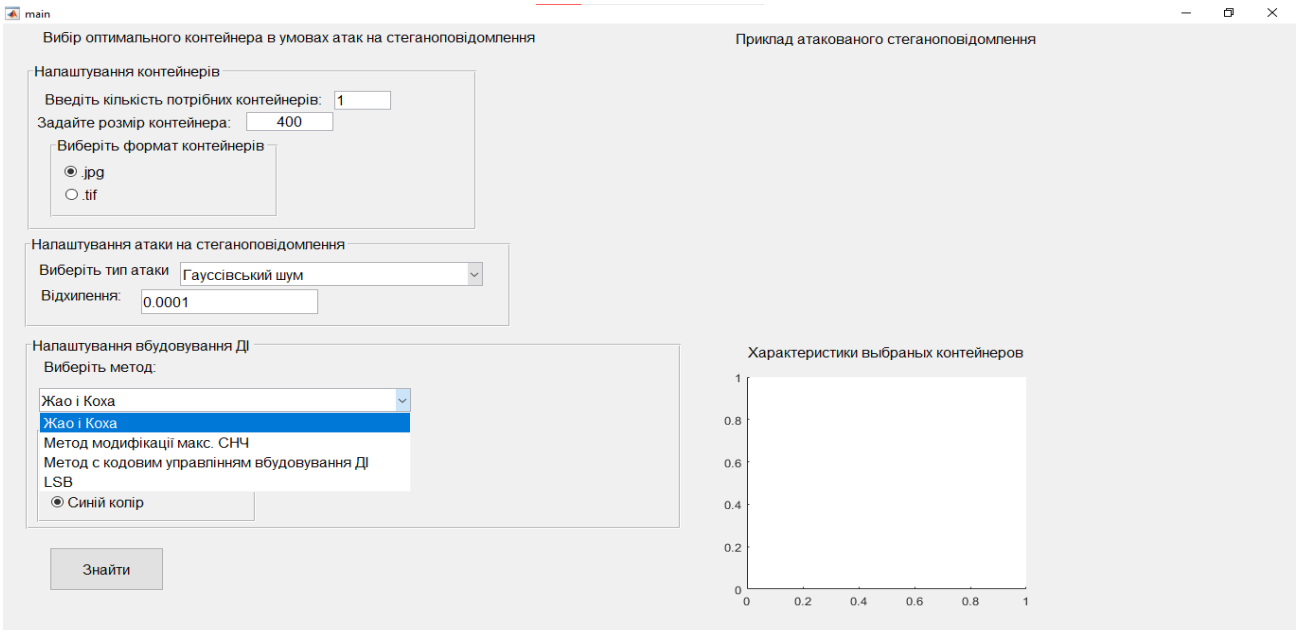


Рисунок 3.4 – Випадаючий список вибору стеганографічного методу

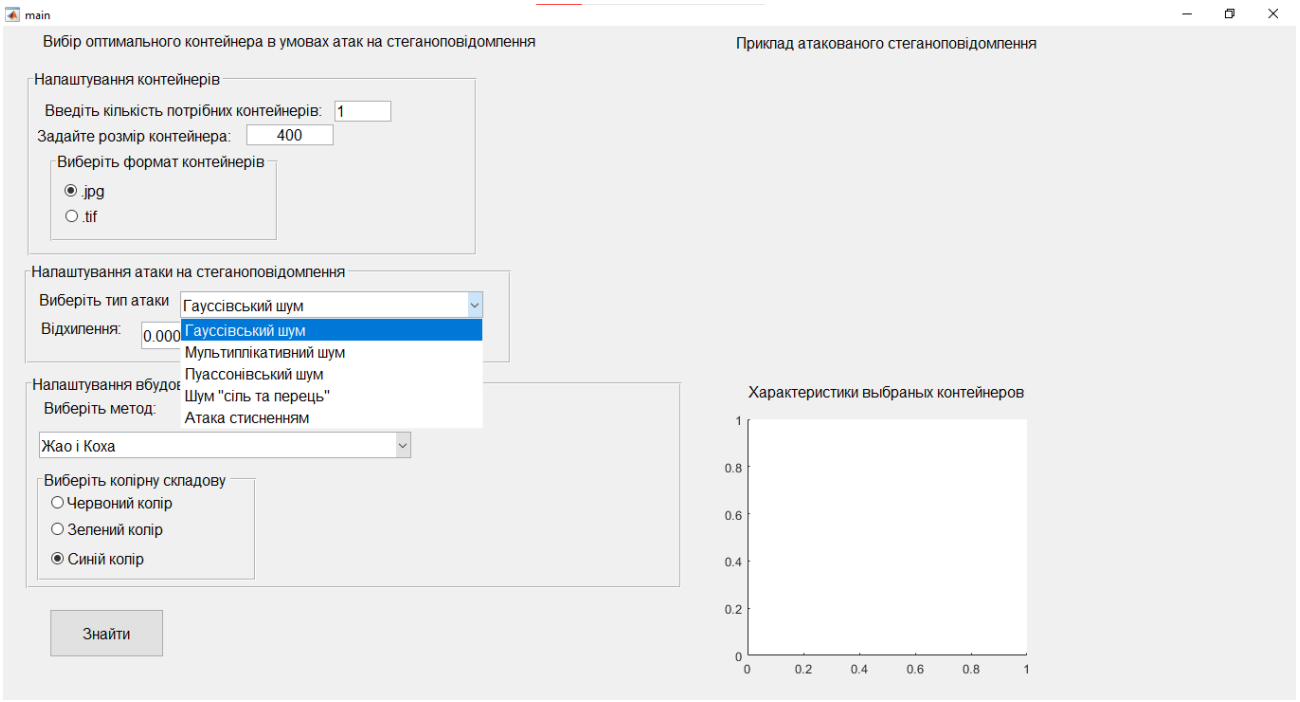


Рисунок 3.5 – Випадаючий список вибору атаки на стеганоповідомлення

Після того, як було обрано вхідну множину контейнерів, обрано папку для результатів та налаштовано усі умови задачі - програма виконає обчислення, результати яких можна побачити на інтерфейсі (рис. 3.5), та виведе приклад атакованого стеганоповідомлення, для того, щоб користувач міг відслідковувати умову збереження надійності сприйняття стеганоповідомлення після атаки на нього.

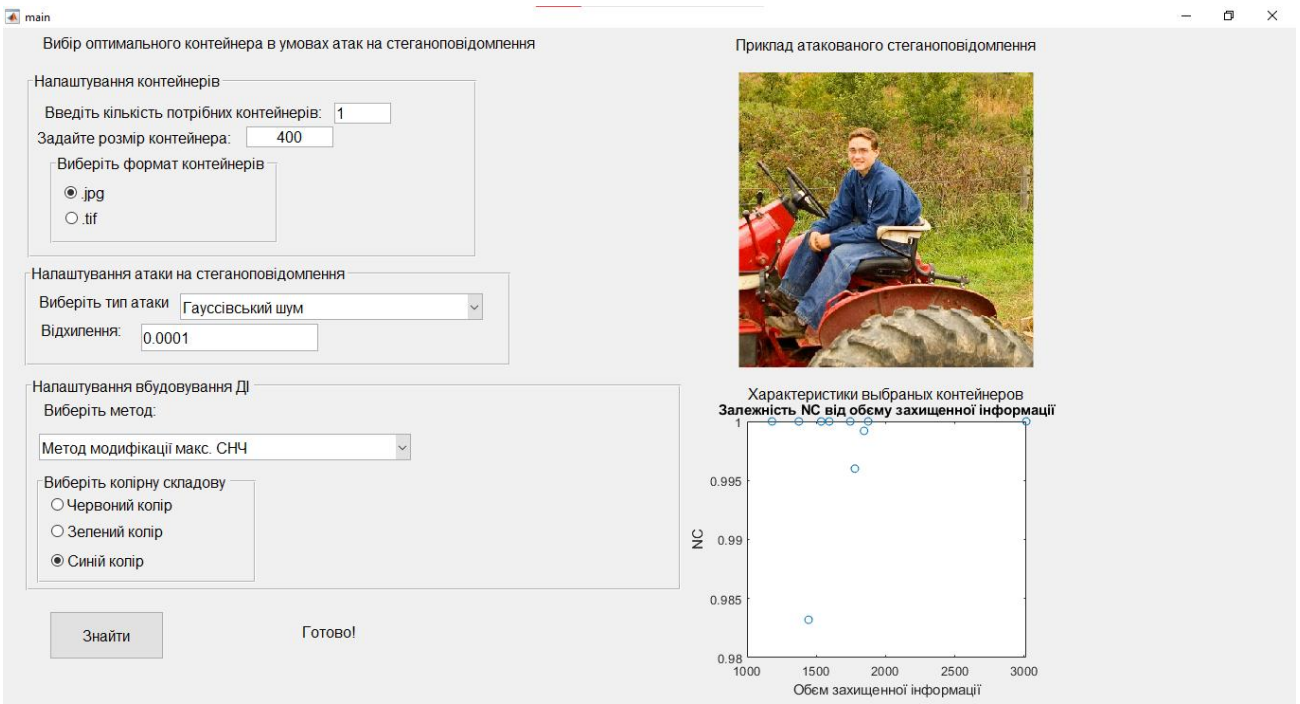


Рисунок 3.5 – Інтерфейс програми після виконання обчислювань

Після виконання обчислювань, необхідних для отримання результатів, програма запише вказану кількість найкращих контейнерів у вказану для цього папку (рис. 3.6). Ці контейнери готові до використання.

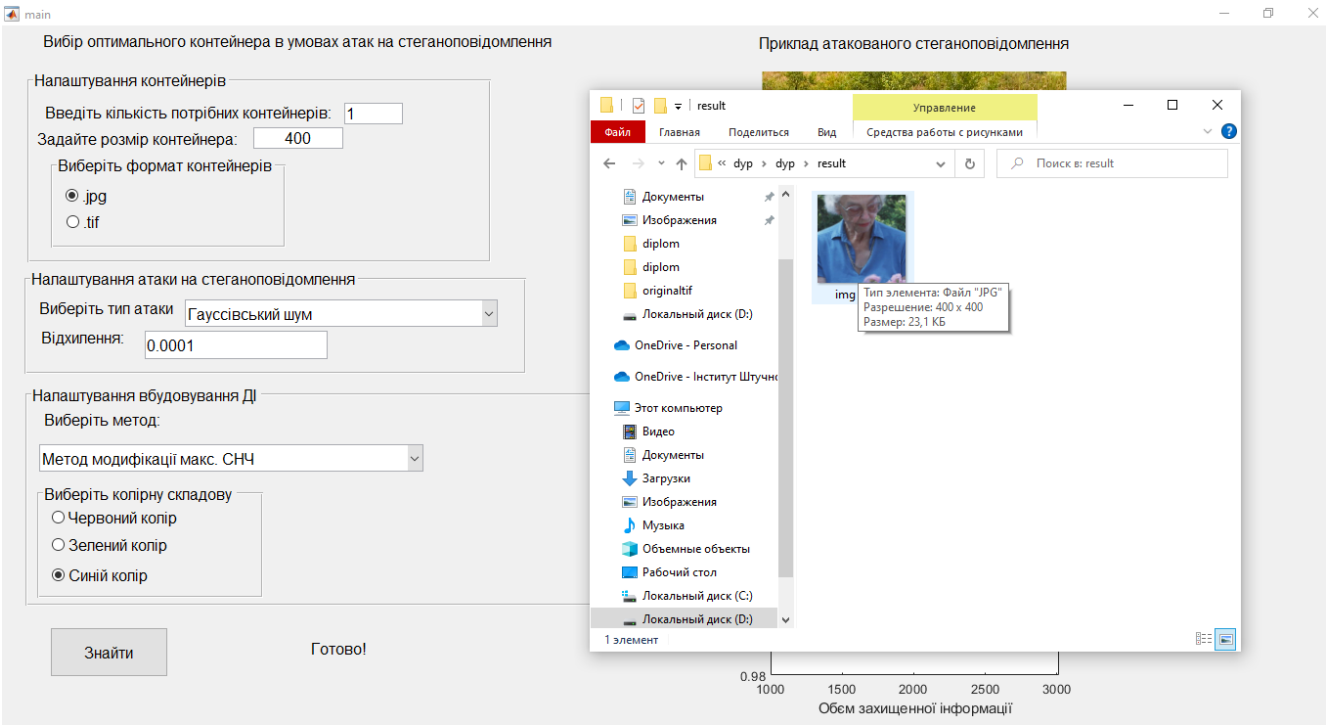


Рисунок 3.6 – Вміст папки, обраної для запису результатів, після виконання обчислень

ВИСНОВКИ

У роботі вирішено важливу науково-практичну задачу підвищення стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки методу вибору контейнера з скінченної сукупності наявних цифрових зображень, що забезпечує для повідомлення, що передається, мінімальну або близьку до мінімально можливої для аналізованих зображень чутливість сформованого стеганоповідомлення до збурних дій при обраному стеганографічному алгоритмі.

Розроблений та програмно реалізований метод заснований на аналізі збурень малорангових апроксимацій матриці контейнера в процесі стеганоперетворення. Ефективність запропонованого методу загалом перевищує ефективність аналогів, та залишається високою, незалежно від використовуваного для вбудови ДІ стеганографічного методу. Так максимальне відхилення коефіцієнта NC, що є кількісним показником чутливості СП до збурних дій, від максимального значення для контейнерів із заданої множини становило 3.9%, у той час, як для кращого з аналогів таке відхилення становить 11.5%, що говорить про значне підвищення ефективності процесу вибору контейнера в результаті використання нового методу (в умовах розглянутого критерію). Практичною перевагою розробленого методу є ефективність використання його результатів, отриманих в умовах збурної дії Е, для атак меншої сили.

Запропонований метод дозволяє підвищити в цілому стійкість стеганосистеми до атак проти вбудованого повідомлення при його використанні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бобок И.И., Кобозева А.А., Сокальский С.Н. Задача выбора стеганографического контейнера в условиях атак против встроенного сообщения. URL: https://journal.ie.asm.md/assets/files/07_04_56_2022.pdf

2. Torten R., Reaiche C., Boyle S. The impact of security awarness on information technology professionals' behavior. *Computers & Security*. 2018. Vol. 79. P. 68-79.

3. Alqahtani F. Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*. 2017. Vol. 124. P. 691-697

4. Mandal P.C., Mukherjee I., Goutam P., Chatterji B.N. Digital image steganography: A literature survey. *Information Sciences.* 2022. Vol. 609, P.1451-1488

5. Taher M. M., Ahmad A.R.B.HJ, Hameed R.S., Mokri S.S. A literature review of various steganography methods. *Journal of Theoretical and Applied Information Technology*. 2022. Vol.100. No 5 . P.1412-1427.

6. Gupta D., Gupta S., Gupta R. Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*. 2021. Vol. 30.2. P. 63-87.

7. Zielińska E., Mazurczyk W., Szczypiorski K. Trends in steganography. *Communications of the ACM*. 2014. Vol.57(3). P.86-95. URL: https://www.researchgate.net/publication/262248599_Trends_in_steganography.

8. Unseen to Seen by Digital Steganography: Modern-Day Data-Hiding Techniques. 2021. DOI: 10.4018/978-1-7998-7160-6.ch001 In book: Multidisciplinary Approach to Modern Digital Steganography. URL: https://www.researchgate.net/publication/351828629_Unseen_to_Seen_by_Digital_Steganography_Modern-Day_Data-Hiding_Techniques.

9. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009. 220 с.

10. Abed S., Al-Roomi S. A., Al-Shayeji M. Efficient cover image selection based on spatial block analysis and DCT embedding. *Journal on Image and Video Processing*. 2019. No. 1. https://doi.org/10.1186/s13640-019-0486-8

11. Mohammed A. M., Rossilawati S., Shukur Z., Hasan M. K. A Review on Text Steganography Techniques. *Mathematics*. 2021, No.9, 2829. URL: https://doi.org/10.3390/math9212829

12.URL:https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1034&context=ceendiss 2013.

13. Selecting Cover for Image Steganography by Correlation Coefficient URL: DOI. 10.1109/ETCS.2010.33.

14. Mustafayeva E. Principles Of Choosing Containers For Steganographic Systems. *Int. J. of 3D Printing Tech. Dig. Ind.* 2020. No.4(3). P.264-229. URL: https://www.researchgate.net/publication/358524150_Principles_Of_Choosing_Containers_For_Steganographic_Systems.

15. Nikishova A.V., Omelchenko T.A., Makedonskij S.A. Steganographic embedding in containers-images. *IOP Conf. Series: Journal of Physics: Conf. Series 1015*. 2018. 042041 doi: 10.1088/1742-6596/1015/4/042041 URL: https://iopscience.iop.org/article/10.1088/1742-6596/1015/4/042041/pdf.

16. Кобозева, А.А., Нариманова Е.В. Оценка чувствительности стеганосообщений к возмущающим воздействиям. *System Research & Information Technologies*. 2008. No 3. P 52-65.

17. Надвоцький О.Ю. Метод розв’язку задачі про вибір контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій. *Інформатика та математичні методи в моделюванні*. 2021. Т.11, №3. С.216-226.

18. Bergman C., Davidson J. Unitary embedding for data hiding with the SVD. – *Security, steganography, and watermarking of multimedia contents VII, SPIE* 2005. Vol. 5681,

19. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.

20. Demmel J. Accurate singular value decompositions of structured matrices. *SIAM Journal on Matrix Analysis and Applications*. 2000. Vol.21,No.2. P.562-580.

21. Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. *Transport and Telecommunication Journal.* 2016. 17(2). P. 128–137.

22. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию. *Інформационная безопасность*. 2012. №2(8). С. 99-106.

23 Lin W.-H. A blind watermarking method using maximum wavelet coefficient quantization. *Expert Systems with Applications.* 2009. Vol. 36, No. 9. P. 11509–11516.

24. URL: https://www.ijltet.org/wp-content/uploads/2015/02/60.pdf.

25. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, No. 3. P. 147-161.

26 URL: https://www.researchgate.net/publication/283463767.

27. Image Processing Toolbox. URL: https://www.mathworks.com/products/image.html.

Дотаток А. Лістинг програмного коду

```
function varargout = main(varargin)
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @main_OpeningFcn, ...
                   'gui_OutputFcn',  @main_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
    gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
    gui_mainfcn(gui_State, varargin{:});
end
function main_OpeningFcn(hObject, eventdata, handles, varargin)
handles.output = hObject;

guidata(hObject, handles);

function varargout = main_OutputFcn(hObject, eventdata, handles)
varargout{1} = handles.output;

function pushbutton1_Callback(hObject, eventdata, handles)
path_countainer = uigetdir('','Виберіть папку з контейнерами');
set(handles.text18,'String','Іде обчислення');
```

```
path_result = uigetdir('','Виберіть папку для зберігання
результатів');

a=dir(path_countainer);

amount_img=size(a,1)-2;

img_format = handles.uibuttongroup4.SelectedObject.String;

D=readmatrix('hiden_inf.txt');

for k=1:1:amount_img

    I=string(path_countainer)+'\img
('+num2str(k)+')'+string(img_format);

    F=imread(I);

    view = F;

    m = size(F, 1);

    n = size(F, 2);

    s=str2num(handles.edit4.String);

    x=fix((n-s)/2);

    y=fix((m-s)/2);

    F=imcrop(F,[x,y,s-1,s-1]);

    view=imcrop(view,[x,y,s-1,s-1]);

    color = handles.uibuttongroup5.SelectedObject.Value;

    F=F(:,:,color);

    chosed_method = get(handles.popupmenu4,'Value');

    switch chosed_method

        case 1

            stego=uint8(stego_jk(F,D));

        case 2

            stego=uint8(stego_sign(F,D));

        case 3

            stego=uint8(stego1(F,D));

        case 4

            stego=uint8(stego_lsb(F,D));

    end

    stego_path=['D:\dyp\dyp\stego\img' num2str(k) '.tif'];
```

```
    imwrite(stego,stego_path);
    chosed_noise = get(handles.popupmenu3,'Value');
    noise_par = str2num(get(handles.edit3,'String'));
    switch chosed_noise
        case 1
            stego_noise=imnoise(stego,'gaussian',0,noise_par);
            orig_noises=imnoise(F, 'gaussian',0,noise_par);
            view = imnoise(view, 'gaussian',0,noise_par);
        case 2
            stego_noise=imnoise(stego,'speckle',noise_par);
            orig_noises=imnoise(F, 'speckle',noise_par);
            view = imnoise(view, 'speckle',noise_par);
        case 3
            stego_noise=imnoise(stego,'poisson');
            orig_noises=imnoise(F, 'poisson');
            view = imnoise(view, 'poisson');
        case 4
            stego_noise=imnoise(stego,'salt & pepper');
            orig_noises=imnoise(F, 'salt & pepper');
            view = imnoise(view, 'salt & pepper');
    end
    if chosed_noise==5
        stego_jpg_path=['D:\dyp\dyp\stegoQF75\img' num2str(k)
'.jpg'];
        imwrite(stego,stego_jpg_path,"Quality",noise_par);
        stego_jpg=imread(stego_jpg_path);
        orig_jpg_path=['D:\dyp\dyp\QF75\img' num2str(k) '.jpg'];
        imwrite(F,orig_jpg_path,"Quality",noise_par);
        orig_jpg=imread(orig_jpg_path);
        path = ['D:\dyp\dyp\view.jpg'];
        imwrite(view,path,"Quality",noise_par);
```

```
        view=imread(path);
    else
        stego_noise_path=['D:\dyp\dyp\stego_noise\img' num2str(k)
'.tif'];
        imwrite(stego_noise, stego_noise_path);
        orig_noises_path=['D:\dyp\dyp\noises\img' num2str(k)
'.tif'];
        imwrite(orig_noises,orig_noises_path);
    end
    if chosed_noise == 5
        switch chosed_method
        case 1
            decode_inf=destego(stego_jpg);
        case 2
            decode_inf=destego_sign(stego_jpg);
        case 3
            decode_inf=destego1(stego_jpg,F);
        case 4
            decode_inf=destego_lsb(stego_jpg);
        end
    else
        switch chosed_method
        case 1
            decode_inf=destego(stego_noise);
        case 2
            decode_inf=destego_sign(stego_noise);
        case 3
            decode_inf=destego1(stego_noise,F);
        case 4
            decode_inf=destego_lsb(stego_noise);
        end
    end
```

```
    NC(k)=nc(decode_inf,D);
    if chosed_noise ==5
        [obyom(k), count(k)]=def_obyom(F,stego,orig_jpg);
        [obyom_exp(k),
count_exp(k)]=def_obyom_exp(F,stego,orig_jpg);
    else
        [obyom(k), count(k)]=def_obyom(F,stego,orig_noises);
        [obyom_exp(k),
count_exp(k)]=def_obyom_exp(F,stego,orig_noises);
    end
end
NC_exp=NC;
sortOb_exp = sort(obyom_exp);
for i=1:1:amount_img
    for j=1:1:amount_img
       if(sortOb_exp(i)==obyom_exp(j))
           sortNC_exp(i)=NC_exp(j);
       end
   end
end
axes(handles.axes2)
plot(obyom_exp, NC, 'o')
title('Залежність NC від обєму захищенної інформації')
xlabel('Обєм захищенної інформації')
ylabel('NC')
count = 1;
ans_amount = str2num(get(handles.edit1,'String'));
for i=amount_img-ans_amount+1:1:amount_img
    for j = 1:1:amount_img
        if(sortOb_exp(i)==obyom_exp(j))
            answer(count)=j;
            count = count+1;
```

```
        end
    end
end
for i=1:1:ans_amount
    I=string(path_countainer)+'\img
('+num2str(answer(i))+')'+string(img_format);
    F=imread(I);
    m = size(F, 1);
    n = size(F, 2);
    x=fix((n-s)/2);
    y=fix((m-s)/2);
    F=imcrop(F,[x,y,s-1,s-1]);
    path = string(path_result)+'\img
('+num2str(i)+')'+string(img_format);
    imwrite(F,path)
end
handles.axes3.Visible = true;
axes(handles.axes3)
imshow(uint8(view))
handles.text18.String = 'Готово!'

function popupmenu1_Callback(hObject, eventdata, handles)
str = get(hObject, 'String');

popupmenu1 contents as cell array
function popupmenu1_CreateFcn(hObject, eventdata, handles)
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end
```

```
function pushbutton2_Callback(hObject, eventdata, handles)

function popupmenu2_Callback(hObject, eventdata, handles)

function popupmenu2_CreateFcn(hObject, eventdata, handles)

if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))

    set(hObject,'BackgroundColor','white');

end

function pushbutton4_Callback(hObject, eventdata, handles)


function edit1_Callback(hObject, eventdata, handles)

function edit1_CreateFcn(hObject, eventdata, handles)

if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))

    set(hObject,'BackgroundColor','white');

end



function pushbutton3_Callback(hObject, eventdata, handles)


function edit2_Callback(hObject, eventdata, handles)

function edit2_CreateFcn(hObject, eventdata, handles)

if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))

    set(hObject,'BackgroundColor','white');

end

function figure1_SizeChangedFcn(hObject, eventdata, handles)

function popupmenu3_Callback(hObject, eventdata, handles)

if(get(hObject, 'Value')==5)

    set(handles.edit3, 'Enable','on');

    set(handles.text9,'String','Коеф. стиснення:');

    set(handles.edit3,'String','75');

elseif(get(hObject, 'Value')==3||get(hObject, 'Value')==4)
```

```
    set(handles.edit3, 'Enable','off');
    set(handles.text9, 'String','Відхилення:');
    set(handles.edit3,'String','0.0001');
else
    set(handles.edit3, 'Enable','on');
    set(handles.text9, 'String','Відхилення:');
    set(handles.edit3,'String','0.0001');
end


function popupmenu3_CreateFcn(hObject, eventdata, handles)
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end


function popupmenu4_Callback(hObject, eventdata, handles)
function popupmenu4_CreateFcn(hObject, eventdata, handles)
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end




function edit3_Callback(hObject, eventdata, handles)
function edit3_CreateFcn(hObject, eventdata, handles)
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
    set(hObject,'BackgroundColor','white');
end
```

```
function uibuttongroup4_ButtonDownFcn(hObject, eventdata, handles)

function radiobutton2_CreateFcn(hObject, eventdata, handles)

function uibuttongroup4_SelectionChangedFcn(hObject, eventdata,
handles)

function uibuttongroup4_CreateFcn(hObject, eventdata, handles)

function radiobutton1_CreateFcn(hObject, eventdata, handles)

hObject.Value = true;


function radiobutton3_Callback(hObject, eventdata, handles)


function radiobutton4_Callback(hObject, eventdata, handles)


function edit4_Callback(hObject, eventdata, handles)

function edit4_CreateFcn(hObject, eventdata, handles)

if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))

    set(hObject,'BackgroundColor','white');

end

function pushbutton1_ButtonDownFcn(hObject, eventdata, handles)

function uibuttongroup5_SelectionChangedFcn(hObject, eventdata,
handles)
```