МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України

На правах рукопису

КОСТИРКА ОЛЕСЯ ВІКТОРІВНА

УДК 004.056.5: 517.983.28

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ В УМОВАХ АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

05.13.21 — системи захисту інформації

Дисертація на здобуття наукового ступеня кандидата технічних наук

Науковий керівник
Рудницький Володимир Миколайович
доктор технічних наук,
професор

Черкаси — 2014

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДІ	додаткова інформація
ДВП	дискретне вейвлет-перетворення
ДКП	дискретне косинусне перетворення
КІ	конфіденційна інформація
ОП	основне повідомлення
ОПр	область перетворення
ПО	просторова область
СА	стеганографічний алгоритм
СНВ	сингулярний вектор
СНЧ	сингулярне число
СП	стеганоповідомлення
СПр	стеганоперетворення
ЦЗ	цифрове зображення

ВСТУП

Актуальність теми. Організація інформаційної безпеки сьогодні носить системний комплексний характер, що поєднує в собі законодавчі, морально-етичні, фізичні, адміністративні, технічні, програмні, криптографічні й стеганографічні заходи. Тому розвиток і вдосконалення комплексної системи захисту інформації неможливо без наявності в її складі ефективної стеганографічної системи, що ґрунтується на сучасних стеганографічних алгоритмах.

У даний момент стеганографія переживає етап свого бурхливого розвитку, пов'язаний з багатьма об'єктивними й суб'єктивними причинами, серед яких обмеження й навіть заборона на законодавчому рівні в деяких країнах світу (у тому числі, в Україні) використання криптографії. Особливістю стеганографії є те, що вона не передбачає прямого оголошення факту існування прихованої інформації, що захищається. Ця обставина дозволяє в рамках традиційно існуючих інформаційних потоків, інформаційного середовища вирішувати задачі організації прихованого каналу зв’язку.

Вагомий внесок у розвиток стеганографії належить відомим в області інформаційної безпеки вченим з України й пострадянського простору: А.В.Аграновському, В.Г.Грібуніну, В.К.Задираці, А.А.Кобозєвій, В.А.Мухачьову, І.Н.Окову, І.В.Туринцеву, В.О.Хорошку, М.Є.Шелесту та ін., а також їх закордонним колегам, у числі яких C.Bergman, J.Davidson, J.Fridrich, W.-H.Lin, D.Kumar та ін.

У процесі стеганографування конфіденційна інформація (КІ) після попереднього кодування, результатом якого є додаткова інформація (ДІ), вбудовується в контейнер, чи основне повідомлення (ОП), результатом чого є стеганоповідомлення (СП). СП відкрито пересилається по каналу зв'язку. Найбільш підходящими об'єктами-контейнерами, враховуючи специфіку сучасної стеганографії, що має «комп'ютерний» характер, є цифрові

зображення, файли аудіо й відеоданих. У роботі як контейнер використовується цифрове зображення (ЦЗ).

При розробці нових і вдосконаленні існуючих стеганографічних алгоритмів (СА), що використовуються при організації прихованого каналу зв'язку, гостро встають питання забезпечення ними різних вимог, серед яких одною з основних, але не вирішених до кінця залишається задача забезпечення стійкості алгоритму до різних збурних дій — атак проти вбудованого повідомлення. До таких атак відносяться, зокрема, накладання різних шумів на СП, фільтрація, стиск СП із втратами та ін.

Протягом привалого часу вважалося, що для забезпечення стійкості стеганографічних методів і алгоритмів кращою для вбудови додаткової інформації є область перетворення (ОПр) зображення, зокрема, частотна область. Завдяки цьому розробки стійких стеганоалгоритмів у просторовій області (ПО) ЦЗ були нечисленними, безсистемними, не мали потрібного математичного фундаменту.

У результаті сучасних наукових досліджень було показано, що забезпечення стійкості СА не залежить прямо від того, у якій області контейнера — просторовій або перетворення відбувається вбудова ДІ. Будь-які зміни, що відбуваються при вбудові ДІ в будь-якій області контейнера (ПО, ОПр) однозначно відбиваються у вигляді певних змін в інших областях (ОПр, ПО), що приводять до тих же результатів стосовно стійкості. При цьому просторова область має певні переваги при організації стеганоперетворення. Зокрема, процес вбудови/декодування ДІ в просторовій області ЦЗ дозволяє зменшити обчислювальну складність та обчислювальну похибку, що накопичується в процесі стеганоперетворення і декодування, в порівнянні з аналогічною організацією цих процесів в ОПр, за рахунок відсутності передобробки/постобрабки контейнера/стеганоповідомлення. Це говорить про принципову можливість забезпечення більш високої стійкості для СА, що працюють у ПО, у порівнянні зі стеганоалгоритмами, що працюють в областях перетворення контейнера.

Просторова область зображення-контейнера при розробці стеганоалгоритмів, стійких до збурних дій, на сьогоднішній день незаслужено відійшла на другий план. Серед причин цього: відсутність до цього моменту формальних достатніх умов забезпечення такої стійкості в просторовій області ЦЗ; більш проста реалізації існуючих достатніх умов стійкості в областях перетворення контейнера.

Усе це гальмує процес підвищення ефективності в умовах атакуючих дій, яка на сьогоднішній день, як свідчать відкриті джерела, залишається недостатньою при організації прихованого каналу зв’язку, для розроблюваних СА, які мають незначну обчислювальну складність за рахунок відсутності додаткових операцій для переходу із одної області зображення в іншу при організації стеганоперетворення/декодування ДІ.

Таким чином, задача розробки стійких стеганоалгоритмів, що працюють у просторовій області ЦЗ-контейнера, є важливою, а тема дисертаційного дослідження «Підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення» *актуальною.*

Зв'язок роботи з науковими програмами, планами, темами.

Тема дисертаційної роботи безпосередньо пов'язана з напрямками наукових досліджень, які сформульовані у п.1.2.7 – теорія й комп'ютерні технології інформаційної безпеки «Основних наукових напрямків і найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009–2013 роки», затверджених указом МОН України й НАН України № 1066/609 від 26.11.2009.

Тема дисертаційної роботи відповідає Переліку пріоритетних тематичних напрямків наукових досліджень і науково-технічних розробок у сфері інформаційних і комунікаційних технологій на період до 2015 р., затвердженому Постановою №942 Кабінету Міністрів України від 7 вересня 2011 р., а також «Концепції наукового забезпечення діяльності Міністерства надзвичайних ситуацій України» і «Концепції наукової діяльності Академії пожежної безпеки імені Героїв Чорнобиля МНС України на 2010–2015 роки».

Результати дисертаційної роботи включені в НДР «Методи та засоби захисту інформації МНС України» (ДР № 0112U003579), в якій автор брав участь як виконавець.

Мета роботи — підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення шляхом розробки стеганографічних методів і алгоритмів для організації прихованого каналу зв'язку, що працюють у просторовій області контейнера, стійких до збурних дій.

В роботі під ефективністю стеганосистеми розуміється ефективність СА, на основі якого вона побудована; ефективність СА визначається його стійкістю до атак проти вбудованого повідомлення – збурних дій; стійкість СА кількісно оцінюється стандартним чином: за допомогою коефіцієнта кореляції NC для ДІ.

Для досягнення поставленої мети необхідно розв'язати наступні **задачі:**

1. На основі аналізу сучасних стійких до атак проти вбудованого повідомлення стеганоалгоритмів виявити недоліки при забезпеченні їх стійкості, зокрема, при організації стеганоперетворення в просторовій області зображення-контейнера.
2. Серед областей зображення (просторової, перетворення) обрати ту, яка має переваги для вбудови/декодування додаткової інформації.
3. Виявити відповідності між збуреннями параметрів цифрового зображення, що формалізують процес стеганоперетворення, які забезпечують стійкість стеганоалгоритму до збурних дій, у просторовій області й областях перетворення контейнера, на основі яких отримати формальну достатню умову стійкості стеганоалгоритму до збурних дій у просторовій області зображення-контейнера.
4. Отримати оцінки збурень матриць стеганоповідомлення в процесі атак проти вбудованого повідомлення, на підставі яких з урахуванням необхідності забезпечення надійності сприйняття стеганоповідомлення отримати кількісні оцінки можливих збурень параметрів контейнера в просторовій області при стеганоперетворенні.

5. Розробити на основі отриманої достатньої умови й кількісних оцінок можливих збурень параметрів контейнера в результаті стеганоперетворення стеганометоди й алгоритми, стійкі до збурних дій незалежно від формату контейнера, які працюють у просторовій області зображення, оцінити характер їх стійкості: до атак проти вбудованого повідомлення, у тому числі, комплексних атак; до стеганоаналізу.

Об'єкт дослідження - процеси організації прихованого каналу зв’язку.

Предмет дослідження - стійкі до атак проти вбудованого повідомлення стеганографічні системи.

Методи дослідження. Для встановлення відповідності між збуреннями параметрів цифрового зображення, що формалізують процес стеганоперетворення, які забезпечують стійкість стеганоалгоритму до збурних дій, у просторовій області й областях перетворення, отримання формальної достатньої умови стійкості стеганоалгоритму до атак проти вбудованого повідомлення у просторовій області контейнера використовувалися матричний аналіз, методи цифрової обробки зображень, обчислювальна лінійна алгебра, теорія збурень. Для отримання кількісних оцінок можливих збурень яскравості пікселів зображення-контейнера в результаті стеганоперетворення, оцінок збурень блоків матриць стеганоповідомлення в процесі активних атак використовувалися методи обробки зображень, чисельні методи, методи обчислювальної лінійної алгебри. При розробці стеганографічних методів та алгоритмів, що їх реалізують, для оцінки їх ефективності, обчислювальної складності й виявлення внутрішнього паралелізму використовувалися теорія алгоритмів, основи паралельних обчислень.

Вірогідність основних наукових результатів, висновків і рекомендацій підтверджувалася чисельними експериментами, збігом результатів чисельних експериментів з відомими експериментальними даними інших досліджень, відповідністю отриманих теоретичних результатів з результатами обчислювальних експериментів.

Наукова новизна отриманих результатів полягає у наступному:

1. *Вперше* на основі встановленої відповідності між збуреннями параметрів цифрового зображення в просторовій області й областях перетворення отримана формальна достатня умова забезпечення стійкості стеганоалгоритму до збурних дій у просторовій області зображення-контейнера, що відрізняє її від існуючих. Це дозволило розробити теоретичні основи стійких до атак проти вбудованого повідомлення стеганометодів й алгоритмів.
2. *Вперше* на основі отриманої достатньої умови стійкості до збурних дій розроблені стеганометоди і поліноміальні стеганоалгоритми, які дали можливість підвищити ефективність стеганографічної системи в умовах атак проти вбудованого повідомлення, в порівнянні з сучасними аналогами, завдяки використанню для стеганоперетворення/декодування додаткової інформації просторової області зображення.
3. *Отримали подальший розвиток* умови забезпечення стійкості стеганоалгоритмів до атак проти вбудованого повідомлення за рахунок незалежності вимог, що висуваються отриманою достатньою умовою стійкості до стеганоперетворення, від формату контейнера та конкретного виду збурної дії: стійкість відповідних алгоритмів визначається величиною спотворення матриці стеганоповідомлення при атаці. Це забезпечило високу ефективність розроблених стеганоалгоритмів незалежно від виду атаки і формату зображення-контейнера (з/без втрат), у тому числі, в умовах комплексних атак, на відміну від переважної більшості існуючих.
4. *Отримали подальший розвиток* методи розробки стійких до збурних дій стеганоалгоритмів, за рахунок якісного і кількісного обгрунтування переваг просторової області зображення для організації стеганоперетворення, в порівнянні з областями перетворення, отримання оцінок збурень параметрів контейнера/стеганоповідомлення в просторовій області в результаті стеганоперетворення/збурної дії, що забезпечують розробленим алгоритмам разом із високою стійкістю надійність сприйняття стеганоповідомлення, що часто порушується сучасними аналогами. Отримані оцінки можуть бути

використані для розробки нових стійких стеганоалгоритмів для організації прихованого каналу зв'язку.

Практичне значення отриманих результатів.

Практична цінність роботи полягає в доведенні отриманих наукових результатів до конкретних алгоритмів, які можуть бути використані як основи для стеганографічних систем, що є складовими частинами комплексної системи захисту інформації будь-якої установи, підприємства; при організації електронного документообігу.

Розроблені стеганографічні алгоритми SA_B, SA_M, що є поліноміальними ступеня 2, при забезпеченні надійності сприйняття формованого стеганоповідомлення (середнє значення $PSNR$ для SA_B / SA_M при стеганоперетворенні становить $49/53\,dB$ відповідно) підвищують стійкість стеганографічної системи при атаках проти вбудованого повідомлення, у порівнянні із системами, побудованими на основі їх сучасних аналогів. Так в умовах накладання гауссівського/мультиплікативного шуму максимально стійкість, у порівнянні з найкращим з аналогів, була підвищена на 4% / 1.5% відповідно; при накладанні пуасонівського шуму стійкість близька до одиниці; при атаці фільтрацією максимально стійкість підвищена на 13% (усереднюючий фільтр: маска 7×7, порівняння з кращим з аналогів), для гауссівського й медіанного фільтрів стійкість SA_B близька до 1; стійкість SA_B до атаки стиском перевищує стійкості всіх розглянутих аналогів, а при коефіцієнті якості $QF > 80$ близька до 1; розроблені стеганоалгоритми є стійкими до комплексних атак проти вбудованого повідомлення, зокрема, у випадку атаки дворазовим стиском при комбінації коефіцієнтів якості $QF = 80{,}90$, які є найбільш часто використовуваними при стиску, $NC = 0.99$ для SA_B.

Використання SA_B, SA_M для вбудови цифрових водяних знаків, що містять інформацію про автора, власника інформаційного контенту, дозволяє

забезпечити можливість аутентифікації зображення-контейнера в умовах атак проти вбудованого повідомлення.

Практична цінність отриманих у дисертаційній роботі результатів підтверджується актами впровадження: в діяльність Управління ДСНС України у Черкаській області; в навчальний процес в Черкаському інституті пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України та в Черкаському державному технологічному університеті.

Особистий внесок здобувача. Результати дисертаційної роботи отримані автором самостійно. Роботи [101,102,116,118] виконані без співавторів. У роботах, опублікованих у співавторстві, здобувачеві належать: аналіз відповідності збурення максимальних сингулярних чисел блоків матриці цифрового зображення (область перетворення) і збурень яскравості пікселів відповідного блоку (просторова область), виявлення причин порушення теоретичної відповідності зазначених величин в [106,108]; розробка стеганографічного методу, отримання оцінок збурень блоків матриці ЦЗ в результаті накладання шумів, розробка рекомендації для розмірів блоку при організації СПр в [115]; розробка стійкого СА в просторовій області ЦЗ-контейнера в [117]; дослідження ефективності СА в умовах одноразового й дворазового стиску із втратами стеганоповідомлення, порівняльний аналіз ефективності розробленого СА із сучасними аналогами в [117,153]; формальне співвідношення між розмірами маски для однорідного усереднюючого фільтра й блоку ОП, використовуваного при СПр, що забезпечує високу ефективність СА, практичне підтвердження стійкості розробленого СА в [122,124]; встановлення залежності ефективності стеганоаналітичних комплексів від значення коефіцієнта якості, використаного при стиску із втратами ЦЗ [161,162]; виявлення внутрішнього паралелізму розробленого СА на етапі обробки окремого блоку матриці ЦЗ [114]; отримання рекомендацій з вибору розміру блоку ОП, який задіюється при стеганоперетворенні в просторовій області [107].

Апробація результатів дисертації. Результати досліджень, які становлять основний зміст роботи, доповідалися й обговорювалися на Міжнародних і Всеукраїнських наукових конференціях і семінарах, у тому числі:

- семінар при вченій раді НАН України «Технічні засоби захисту інформації» (Одеса, 2013);
- 15-а міжнародна науково-практична конференція «Сучасні інформаційні й електронні технології» СИЕТ–2014 (Одеса, 2014);
- 11 Всеукраїнська конференція студентів і молодих науковців «Інформатика, інформаційні системи та технології» (Одеса,2014);
- VI Міжнародна науково-практична конференція «Проблеми й перспективи розвитку IT-індустрії» (Харків, 2014);
- Міжнародна науково-практична інтернет-конференція «Інформаційна й економічна безпека (INFECO–2014)» (Харків, 2014);
- 3-я науково-практична конференція «Проблеми інформатики та комп'ютерної техніки (ПІКТ–2014)» (Чернівці, 2014);
- V науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 2014).

Публікації. Основні результати дисертації знайшли своє відображення в 15 наукових працях, з яких: 7 статей у журналах, які включені в перелік наукових фахових видань України (2 статті написані без співавторів), 1 стаття і 1 монографія — у зарубіжних виданнях, 6 тез доповідей на наукових конференціях.

РОЗДІЛ 1
СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СТЕГАНОАЛГОРИТМІВ ДО АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

1.1 Стійкість стеганографічної системи до атак проти вбудованого повідомлення як одна з основних вимог при її розробці

Розвиток і вдосконалення системи захисту інформації, яка сьогодні обов'язково повинна мати комплексний характер, є неможливим без наявності в її складі ефективної стеганографічної системи, що ґрунтується на сучасних стеганографічних алгоритмах [1-4], загальний вид якої представлений на рис.1.1 [2].

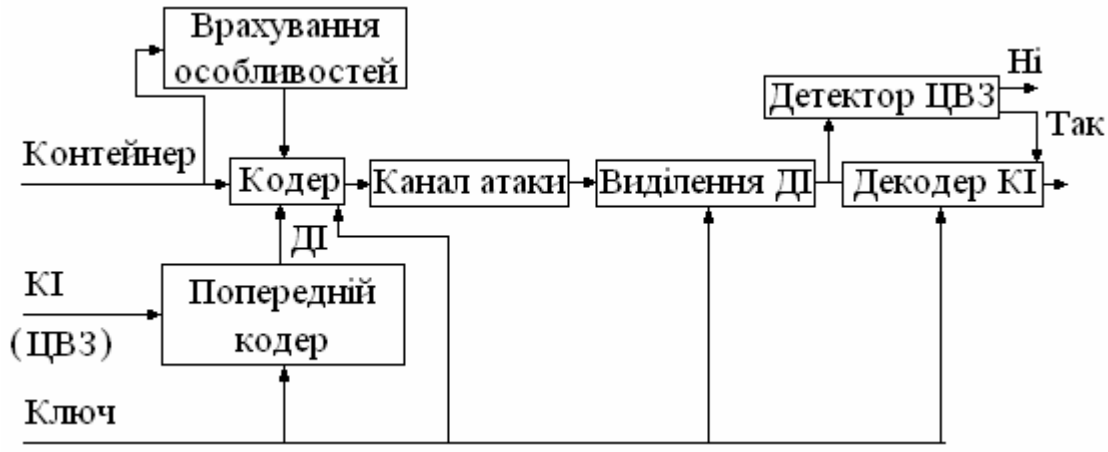


Рисунок 1.1 — Основні елементи стеганосистеми

Стеганографія — один з найбільш прадавніх напрямків рішення задачі захисту інформації від несанкціонованого доступу [2,5,6]. Стеганографія використовується не тільки для прихованої передачі даних (у цьому випадку до стеганоповідомлення висувається вимога надійності сприйняття: зміни, внесені в контейнер у результаті вбудови додаткової інформації, не повинні бути помітні [2,5,7-9]), але й для захисту від несанкціонованого використання інформаційного контенту шляхом вбудовування в контейнер, або основне повідомлення (ОП), цифрових водяних знаків (ЦВЗ) (watermarking) [1,4,5,10],

які, на відміну від звичайних водяних знаків, можуть бути як видимими, так і невидимими. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, про контент, що захищається, або яку-небудь керуючу інформацію.

У даний момент стеганографія переживає етап свого бурхливого розвитку, пов'язаний з багатьма об'єктивними й суб'єктивними причинами [2,5,11]. Цей розвиток є важливим для вдосконалювання системи захисту інформації в цілому.

При розробці будь-якого стеганометоду, стеганоалгоритму для прихованої передачі даних до нього висуваються певні вимоги, зокрема [2,5,8]:

- стійкості до різного роду збурних дій – атак проти вбудованого повідомлення;
- стійкості до стеганоаналізу;
- забезпечення надійності сприйняття формованого стеганоповідомлення;
- забезпечення достатньої (в умовах конкретної задачі) прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується;
- враховуючи те, що особливістю сьогоднішньої стеганографії є її «комп'ютерний характер», велике значення набуває забезпечення малої обчислювальної складності стеганоалгоритмів, а також контроль накопичення обчислювальної похибки при організації вбудови/декодування ДІ.

Таким чином, одною з основних є вимога забезпечення стійкості стеганографічного алгоритму до атак проти вбудованого повідомлення (фільтрації СП, атаки стиском, накладанню шумів на СП і т.і.). Забезпечення її разом з іншими є задачею, яка залишається сьогодні невирішеною до кінця [2,5,8].

Математичні підходи при організації стійких до збурних дій стеганоперетворень різні. Так останнім часом почала розвиватися стеганографічна техніка, заснована на встановлених особливостях головного

мозку людини. Зокрема, для підвищення стійкості розроблюваних стеганоалгоритмів сучасними вченими використовується підхід, заснований на нейронних мережах [12-15].

Для вбудови ДІ в контейнер-зображення можуть використовуватися як просторова [16,17], так і область перетворення ЦЗ. Як область перетворення може, зокрема, виступати частотна область ЦЗ [18,19], області різних розкладань матриці: сингулярного, спектрального [20,21], і ін. [15].

Протягом довгого часу вважалося, що для забезпечення стійкості стеганографічних методів і алгоритмів до збурних дій кращою для вбудови додаткової інформації є область перетворення зображення [15,22-30], зокрема, частотна область. Це відбувалося завдяки тому, що в частотній області найпростіше задовольнити умовам забезпечення стійкості: достатньо виконувати вбудову додаткової інформації шляхом збурення низькочастотних коефіцієнтів цифрового зображення, виділення яких з усієї множини частотних коефіцієнтів не представляє труднощів [2,5]. Тому велика кількість розробок стійких стеганометодів і алгоритмів відповідала саме частотній області для проведення стеганоперетворення [31-33]. Але твердження про переваги частотної області, враховуючи [8,34], є помилковим, оскільки в [8,34] показано, що не має значення, у якій області контейнера відбувається вбудова ДІ, важливо, до яких збурень сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) матриці контейнера це приведе, де ці збурення будуть локалізовані.

Очевидно, що гадана перевага стеганоалгоритмів, що вбудовують ДІ в області перетворення, заснована на тому, що реалізувати наявні достатні умови стійкості стеганоалгоритму до збурних дій у просторовій області складніше, чим в області перетворення, але принципово можливо. Дійсно, будь-які зміни, що відбуваються при вбудові додаткової інформації в будь-якій області контейнера (просторовій, області перетворення) однозначно відображаються у вигляді певних змін в інших областях (перетворення, просторовій), що приводять до тих самих результатів стосовно стійкості стеганографічного

алгоритму. Необхідно лише чітко визначити відповідності між збуреннями параметрів у різних областях ЦЗ (просторовій, області перетворення). Використовуючи виявлені відповідності, можна забезпечити стійкість стеганоалгоритму при організації стеганоперетворення в будь-якій області контейнера. При цьому процес вбудови/декодування додаткової інформації в просторовій області цифрового зображення дозволяє зменшити обчислювальну складність та обчислювальну похибку, що накопичується в процесі стеганоперетворення і декодування, в порівнянні з аналогічною організацією цих процесів в області перетворення, за рахунок відсутності переходів ПО – ОПр, ОПр – ПО. Це говорить про принципову можливість забезпечення більш високої ефективності для стеганографічних алгоритмів, що працюють у просторовій області, у порівнянні зі стеганоалгоритмами, що працюють в областях перетворення контейнера.

Таким чином, просторова область зображення-контейнера при розробці нових стеганоалгоритмів і використанні вже існуючих на сьогоднішній день незаслужено відійшла на другий план (виключенням є, мабуть, лише метод модифікації найменшого значущого біта, що здійснює вбудову додаткової інформації в просторовій області, широко використовуваний до цього моменту, але й він зазнає останнім часом модифікації, пов'язані з організацією стеганоперетворення в області дискретного косинусного перетворення (ДКП)), хоча, звичайно, спроби розробок стійких стеганометодів, що працюють у просторовій області ЦЗ-контейнера, робилися й робляться зараз [35,36]. Це гальмує процес підвищення ефективності в умовах атак проти вбудованого повідомлення для розроблюваних стеганографічних алгоритмів, які мають незначну обчислювальну складність за рахунок відсутності додаткових операцій для переходу із одної області зображення в іншу при організації стеганоперетворення в просторовій області контейнера.

1.2 Стійкі до атак проти вбудованого повідомлення стеганометоди й алгоритми, що здійснюють вбудову додаткової інформації в області перетворення контейнера

Розглянемо докладно особливості, переваги й недоліки сучасних стійких до атак проти вбудованого повідомлення стеганоалгоритмів, що працюють у різних областях ЦЗ-контейнера.

Як вже відзначалося, більшість розробок в цій галузі орієнтована на здійснення вбудови ДІ в області перетворення контейнера [37]. У якості таких областей перетворення використовуються: область дискретного вейвлет-перетворення (ДВП), ДКП, область перетворення Фур'є, область сингулярного розкладання матриці (матриць) контейнера й ін.

1.2.1 Стійкі до збурних дій стеганоалгоритми, що використовують для стеганоперетворення область дискретного вейвлет-перетворення. Серед областей перетворення ЦЗ, що використовуються для стійкого до збурних дій стеганоперетворення, найбільш відповідною задачі, що розглядається, вважається область ДВП [37-40]. Основним питанням при розробці стеганоалгоритмів тут є питання вибору вейвлет-коефіцієнтів для організації стеганоперетворення.

В [41-47] запропоновані алгоритми, в яких в значущі вейвлет-коефіцієнти вбудовується ЦВЗ, що гарантує стійкість стеганоалгоритмів, але не гарантує надійність сприйняття одержуваного стеганоповідомлення, а тому ці алгоритми не можуть використовуватися для організації прихованого каналу зв'язку. Аналогічний недолік має місце також для алгоритму, розробленого в [48], відповідно до якого оригінальне ЦЗ-контейнер розбивається на блоки фіксованого розміру $l \times l$ пікселів, після чого кожний блок піддається вейвлет-перетворенню, ЦВЗ вбудовується у вейвлет-коефіцієнти із середнього й нижнього піддиапазону.

Спроба відійти від збурення винятково значущих вейвлет-коефіцієнтів при стеганоперетворенні для забезпечення надійності сприйняття

стеганоповідомлення робилася в [49-53], однак закономірною «платою» [8] за використовуваний підхід стало те, що хоча при розробці стеганоалгоритмів висувалася вимога їх стійкості до атак проти вбудованого повідомлення, вони не гарантовано задовольняють їй: зокрема, виявляються нестійкими до однієї з найбільш часто використовуваних атак — атаки фільтрацією.

В [54] пропонується нова стійка до збурних дій схема вбудови ЦВЗ у ЦЗ для забезпечення захисту авторських прав. Тут вбудова біт ДІ відбувається в синю компоненту кольорового ЦЗ (в кольоровій схемі RGB) або в компоненту яскравості (в кольоровій схемі YUV) в області ДВП. Для забезпечення стійкості стеганоалгоритму кожний біт ЦВЗ вбудовується в три позиції виділеної матриці контейнера, які визначаються секретним ключем. При цьому процес стеганоперетворення відбувається шляхом модифікації двох найбільших коефіцієнтів ДВП в обраних непересічних блоках фіксованого розміру $l \times l$ в $\{LH_L, HL_L, HH_L\}$ стрічках [55]. Запропонована схема, як випливає з матеріалів публікації, є стійкою до найбільш часто використовуваних атак проти вбудованого повідомлення: стиску стеганоповідомлення, його фільтрації, накладанню шумів, у силу чого відповідний стеганоалгоритм використовується в розділі 4 при проведенні порівняльного аналізу стеганоалгоритмів.

В [56] пропонується стійкий до збурних дій метод приховування секретної інформації без втрат в медіа-контейнері (ЦЗ, відео, аудіо) (так звані оборотні ЦВЗ), який дає можливість маркірованому медіа бути відновленим у його оригінальну форму без яких-небудь спотворень (необхідно відзначити, що різні методи оборотних ЦВЗ, стійких до збурних дій, пропонувалися в областях перетворення контейнера і раніше[57-60]; основним недоліком цих методів є їхня орієнтованість на зображення-контейнери в градаціях сірого). Метод, розроблений в [56], ґрунтується на цілочисельному вейвлет-перетворенні (integer wavelet transform). Результати порівняльного аналізу останнього, що наведені в роботі [56], хоча й говорять про його перевагу над розглянутими трьома аналогами [49,52,61] в умовах атак проти вбудованого повідомлення, але за абсолютним значенням «змушують бажати кращого». Так в умовах атаки

фільтрацією для гауссова й медіанного фільтрів, розглянутих у роботі для маски 3*3, значення $NC < 0.87$; при атаці стиском шляхом збереження стеганоповідомлення у формат Jpeg з різними коефіцієнтами якості QF коефіцієнт кореляції для ДІ склав $NC = 0.79$ і $NC = 0.93$ для $QF = 30, 50$ відповідно, що значно уступає існуючим сучасним аналогам, наприклад, тим, що проводять стеганоперетворення в області сингулярного розкладання матриці [62,63].

Область вейвлет-перетворення використовується також у запропонованому в [64] стійкому до атак проти вбудованого повідомлення стеганометоді. Розроблений метод використовує два найменші вейвлет-коефіцієнти в дереві вейвлет-аналізу, які є основою для отримання вектора відстані. Використання найменших коефіцієнтів дозволяє зменшити спотворення зображення при стеганоперетворенні. Дерево розбивається на два кластери, які мають великі статистичні відмінності, засновані на використанні вектора відстаней. Ці відмінності використовуються для наступного декодування ЦВЗ. Результати тестування методу говорять про його високу ефективність, у силу чого він розглядається в розділі 4 для порівняння з розробленими у роботі стеганоалгоритмами, однак треба відзначити, що тестування в [64] проводилося лише на трьох ЦЗ, що змушує сумніватися в об'єктивності наведених високих результатів.

В [37] за основу взяте контурне перетворення (Contourlet transform), яке зберігає основні характеристики ДВП, але й має певні переваги, що дозволяє збільшити ефективність заснованих на ньому стеганоалгоритмів у порівнянні з використанням для стеганоперетворення області тільки «класичного» ДВП [37]. Контурне перетворення для організації стеганоперетворення поки не має значного поширення, хоча й не є новим [65]. Переваги контурного перетворення засновані на тому, що воно дозволяє зробити довільним напрямок декомпозиції при кожному масштабі, у порівнянні з вейвлет-перетворенням, яке проводить декомпозицію тільки в трьох напрямках. Контурне перетворення використовує подібність базової структури контурного сегмента для

апроксимації зображення (частини зображення). Носієм для базової структури виступає прямокутник, у якому можлива зміна співвідношення «довжина – ширина» при зміні масштабу, крім того, прямокутник має такі характеристики, як направленість і асиметричність властивостей залежно від напрямку їх виміру. Розроблений в [37] стеганографічний алгоритм є стійким до атак проти вбудованого повідомлення, а його основа — контурне перетворення виглядає перспективним з погляду можливості використання для розробки нових ефективних стеганоалгоритмів, що працюють в області перетворення. У силу цього згаданий алгоритм використовується в розділі 4 для проведення порівняльного аналізу, як і сліпий стеганографічний алгоритм, заснований на квантуванні максимального вейвлет-коефіцієнта, запропонований в [38], який позиціонується авторами як стійкий до атак проти вбудованого повідомлення, зокрема, до атаки фільтрацією й стиском, що підтверджується наведеними в [38] результатами обчислювального експерименту.

В [66] розроблений стійкий до фільтрації, накладання шуму, стиску метод, заснований на використанні величини відмінності між двома найбільшими вейвлет-коефіцієнтами, використовуваний у розділі 4 у процесі порівняльного аналізу. Кожний біт ЦВЗ вбудовується в кожний блок, який створюється чотирма LH_3-коефіцієнтами й одним LH_4-коефіцієнтом [67]. При декодуванні біта ЦВЗ згадана вище величина відмінності порівнюється в кожному блоці з адаптивним порогом. Якість декодованого ЦВЗ залежить від значення порога, що визначається в ході декодування.

Для організації стеганоперетворення часто використовуються вейвлет-дерева, як, наприклад, у методі, запропонованому в [68], і в методі, що поліпшує його з погляду візуальної якості стеганоповідомлення, запропонованому в [50], однак забезпечення надійності сприйняття стеганоповідомлення тут не дає можливості забезпечити стійкість відповідних алгоритмів до атак проти вбудованого повідомлення, зокрема, до атаки фільтрацією з використанням медіанного фільтра. Висока ефективність в умовах фільтрації стеганоповідомлення забезпечується в методі,

запропонованому в [69], за рахунок масштабування амплітуди значення різниці між двома найбільшими вейвлет-коефіцієнтами у вейвлет-дереві, однак цей метод виявився нестійким до атаки стиском.

В [70] запропонований метод, заснований на техніці квантування різниці між значущими вейвлет-коефіцієнтами: кожні сім вейвлет-коефіцієнтів в 3-му рівні ДВП групуються в блоки, вбудова біта ДІ відбувається шляхом квантування різниці між двома максимальними коефіцієнтами. Не дивлячись на використання значущих вейвлет-коефіцієнтів, запропонований метод не може забезпечити високу ефективність в умовах атак. Його поліпшенням є метод, розроблений в [71], що базується на частковій оптимізації (particle swarm optimization). Цей метод частково розв'язує конфлікт між вимогами забезпечення надійності сприйняття стеганоповідомлення й стійкості стеганоалгоритма й використовується в силу його високої ефективності в розділі 4 при проведенні порівняльного аналізу.

Таким чином, як випливає з результатів огляду сучасних стеганоалгоритмів, що працюють в області ДВП, задача одночасного забезпечення двох з основних вимог до СА: надійності сприйняття стеганоповідомлення й стійкості до атак проти вбудованого повідомлення залишається тут невирішеною до кінця. Спроби її рішення часто приводять до того, що розроблені СА не є одночасно стійкими навіть до найпоширеніших збурних дій. Стійкість алгоритму до однієї з атак проти вбудованого повідомлення й нестійкість до іншої говорить про недосконалість того математичного базису, який покладений в основу методу. Дійсно, результатом будь-якої атаки проти вбудованого повідомлення є збурення параметрів ЦЗ-стеганоповідомлення. Стійкість стеганоалгоритму повинна забезпечуватися незалежно від того, як відбулися ці збурення, визначатися лише величиною збурної дії, інакше алгоритм не можна вважати стійким до атак проти вбудованого повідомлення.

1.2.2 Стеганоалгоритми, що використовують для вбудови додаткової інформації область дискретного косинусного перетворення. Другою за частотою використання (після області ДВП) при розробці стеганоалгоритмів, стійких до збурних дій, є область дискретного косинусного перетворення [38,72,73]; область дискретного перетворення Фур'є уступає області ДКП [18,19].

Головним питанням при розробках стійких стеганоалгоритмів, що працюють в області ДКП, є питання визначення коефіцієнтів ДКП, що будуть задіяні в процесі вбудови ДІ.

В [72,74] вбудова ДІ здійснюється в частину значущих коефіцієнтів ДКП усього ЦЗ, де заздалегідь встановлюється область низькочастотних компонентів, крім dc-коефіцієнта, що приводить до стійкого до збурних дій стеганоалгоритму, однак, у загальному випадку, не виключає порушення надійності сприйняття стеганоповідомлення.

При організації стеганоперетворення частіше за все воно проводиться поблоково після попередньої розбивки матриці контейнера на блоки. Так в [75] вбудова ДІ здійснюється в коефіцієнти ДКП блоків контейнера, що мають різний розмір, де розмір блоку визначається з врахуванням характеристик відповідної підобласті в просторовій області ЦЗ-контейнера; в [76] запропонована так звана техніка диференціальної енергії для вбудови ЦВЗ (differential energy watermarking), відповідно до якої попередньо отримана множина 8*8-блоків ДКП-коефіцієнтів матриці контейнера для вбудови ЦВЗ розділяється на дві частини: високочастотні ДКП-коефіцієнти в Jpeg/Mpeg потоці вибірково відкидаються для забезпечення відмінностей енергії двох частин множини блоків.

Велику частину сучасних розроблюваних стеганоалгоритмів, що працюють в області ДКП (і інших областях ЦЗ), складають алгоритми, що є стійкими до якихось певних атак проти вбудованого повідомлення. Актуальність таких алгоритмів визначається певними областями їх застосування з передбачуваними збурними діями. Прикладами таких

алгоритмів є: стеганоалгоритм, запропонований в [77], заснований на сегментації ЦЗ; стеганометод з [78], заснований на теоремі лишків, та багато інших.

Необхідність забезпечення надійності сприйняття стеганоповідомлення (з одночасним забезпеченням стійкості СА до збурних дій) при організації прихованого каналу зв'язку приводить до використання в процесі стеганоперетворення середньої частини частотного спектру контейнеру. В [79] основна ідея методів полягає у вбудові ДІ в середньочастотний діапазон оригінального ЦЗ-контейнера після попереднього переведення його в область ДКП. Використання середньочастотних коефіцієнтів ДКП очікувано не дозволяє забезпечити алгоритму високу стійкість до атак проти вбудованого повідомлення, наприклад, до стиску з малими коефіцієнтами якості ($QF \le 50$), шумам (гауссівському, мультиплікативному) з значною дисперсією.

Для стеганоалгоритмів, що працюють в області ДКП (перетворення Фур'є) мають місце недоліки, аналогічні зазначеним у попередньому підрозділі для СА, що здійснюють стеганоперетворення в області ДВП: використання низькочастотних коефіцієнтів у процесі вбудови ДІ для забезпечення стійкості до збурних дій часто приводить до порушення надійності сприйняття відповідного стеганоповідомлення; компромісний варіант — використання середньочастотних коефіцієнтів не дозволяє забезпечити гарантовану стійкість навіть до найпоширеніших атак проти вбудованого повідомлення. Така ситуація очевидно відбувається в силу того, що в частотній області розподіл коефіцієнтів на складові: низько-, середньо-, високочастотні є чітко визначеним. Залучення певної групи коефіцієнтів дає можливість задовольнити конкретній вимозі, заважаючи задоволенню іншої: стійкість СА до збурних дій гарантована при використанні при стеганоперетворенні саме низькочастотних коефіцієнтів, надійність сприйняття стеганоповідомлення гарантується залученням при вбудові ДІ високочастотних коефіцієнтів. Такого чіткого розподілу формальних параметрів ЦЗ в сенсі їх відповідності певним частотним складовим не існує в областях сингулярного, спектрального розкладання

відповідної матриці, що дає можливість для забезпечення стійкості СА при менш вираженому збуренні низькочастотної складової ЦЗ при стеганоперетворенні [34]. Області сингулярного й спектрального розкладання є кращими для організації стеганоперетворення, в порівнянні з частотною областю, для одночасного забезпечення надійності сприйняття стеганоповідомлення й стійкості СА до атак проти вбудованого повідомлення.

1.2.3 Стеганоалгоритми, що використовують для вбудови додаткової інформації область сингулярного розкладання матриці зображення-контейнера. Ще одною традиційною областю ЦЗ-контейнера, використовуваною при організації стійкого стеганоперетворення, є область сингулярного розкладання (singular value decomposition (SVD)) відповідної матриці/матриць, яке може використовуватися самостійно [20,21,62,63,80,81], чи в комбінації з іншими перетвореннями контейнеру [28,82-87].

Одним з найбільш значущих СА, що працюють в області сингулярного розкладання матриці контейнера, який став основою для численних модифікацій і вдосконалень, є алгоритм, запропонований в [20]. Вбудова ДІ тут відбувається шляхом зміни знаків деяких компонент сингулярних векторів матриць $8\times8-$блоків ЦЗ-контейнера (незмінними залишаються лише два вектори, що відповідають двом найбільшим сингулярним числам), отриманих шляхом нормального сингулярного розкладання. Локалізація збурень, що є результатом стеганоперетворення, дозволяє забезпечити надійність сприйняття отримуваного стеганоповідомлення при значній прихованій пропускній спроможності каналу зв'язку, що організується за допомогою обговорюваного алгоритму, — 15/64 біт/піксель, однак залишає недостатньою стійкість алгоритму до збурних дій, причиною чого є невирішені в [20] теоретичні питання при організації стеганоперетворення. Удосконалення цього алгоритму проведено в [80], однак і тут використання СНВ, що відповідають середній частині сингулярного спектра матриць блоків контейнера, не дало можливості для забезпечення стійкості стеганоалгоритму до значних збурних дій, як і

стеганоалгоритму, запропонованому в [88], де вбудова ДІ відбувається в середню частину сингулярного спектра матриці контейнера, що залишає можливим порушення надійності сприйняття відповідного стеганоповідомлення.

Область сингулярного розкладання матриці ЦЗ дає можливість використання при організації стеганоперетворення ефективних комбінацій з різними іншими математичними техніками й інструментами.

В [85] запропонований метод, заснований на аналізі головних компонентів (Principal Component Analysis (PCA)) і сингулярному розкладанні матриці ЦЗ. Вбудова ЦВЗ у сингулярний вектор PCA-компоненти забезпечує стійкість розробленого методу до атаки стиском.

В [28] представлена гібридна стійка схема стеганоперетворення, що заснована на ДВП і сингулярному розкладанні. Експериментальні результати показують, що запропонована техніка, яка використовує частотну локалізацію у ДВП і SVD, ефективно представляє внутрішню алгебраїчну структуру зображення. Експериментальні результати говорять про стійкість розробленого методу до атак проти вбудованого повідомлення з одночасним дотриманням надійності сприйняття відповідного стеганоповідомлення. Усе це послужило причиною для використання алгоритму, розробленого в [28], у розділі 4 при проведенні порівняльного аналізу.

В [89] запропонована стійка до збурних дій стеганографічна техніка, заснована на сингулярному розкладанні блоків в області радіального симетричного перетворення (Radial symmetry transform) матриці синьої складової контейнера. Розроблений алгоритм забезпечує надійність сприйняття формованого стеганоповідомлення. Однак запропонований підхід потребує проведення різноманітних досліджень, більш представницьких обчислювальних експериментів (у роботі розглянуті тільки 3 ЦЗ) і порівнянь із іншими підходами для того, щоб оцінка ступеня його стійкості була об'єктивною.

Неможливість остаточного рішення задачі одночасного забезпечення надійності сприйняття стеганоповідомлення й стійкості до атак проти вбудованого повідомлення розглянутих стеганоалгоритмів пояснюється недостатньою розробкою теоретичних основ цих методів, відсутністю достатніх умов гарантованого забезпечення стійкості до збурних дій СА в області сингулярного розкладання матриці ЦЗ.

В [34,90] були отримані формальні достатні умови забезпечення стійкості стеганоалгоритму до атаки стиском, у тому числі, з малими коефіцієнтами якості, при формалізації стеганоперетворення в області сингулярного розкладання відповідних матриць. У результаті були розроблені нові, стійкі до атак стиском стеганоалгоритми, що здійснюють стеганоперетворення в області сингулярного розкладання відповідних матриць, для яких була показана їхня стійкість до значних збурних дій, у тому числі, до атак, що відрізняються від стиску, із збереженням надійності сприйняття стеганоповідомлення [62,63,91]. Стеганоперетворення тут проводилося за рахунок збурення максимального сингулярного числа $8\times8-$блоків матриці контейнера [62]; сингулярних векторів, що відповідають максимальним сингулярним числам, з урахуванням близькості цих векторів до *n*-оптимального вектору простору R^8 [91].

Таким чином, методи, засновані на сингулярному розкладанні матриці (матриць) цифрового зображення, є більш перспективними з погляду можливості забезпечення ними двох основних вимог до стеганографічного алгоритму, що використовуються для організації прихованого каналу зв’язку: стійкості до збурних дій і надійності сприйняття стеганоповідомлення, у порівнянні з алгоритмами, що працюють у частотній області ЦЗ. Однак, працюючи в області перетворення цифрового зображення, вони також не можуть уникнути додаткових обчислювальних витрат на переходи ПО – ОПр, ОПр – ПО й додаткового накопичення обчислювальної похибки, яке відбувається в ході цих переходів, у порівнянні з алгоритмами, що працюють у просторовій області.

1.3 Стеганографічні алгоритми, що здійснюють вбудову додаткової інформації в просторовій області зображення-контейнера

Як вже було відзначено, розробки стійких стеганоалгоритмів у просторовій області [16,17,30,92-95] є нечисленними, в порівнянні з використанням областей перетворення ЦЗ-контейнера. Це пов'язано, в першу чергу, з відсутністю загальних формальних достатніх умов забезпечення стійкості стеганографічного алгоритму в просторовій області ЦЗ. Як підтверджує проведений огляд літературних джерел, результати якого наведені нижче, розроблювані стеганоалгоритми не пов'язані загальними математичними принципами, їх стійкість до атак проти вбудованого повідомлення, у більшості випадків, не має строгого математичного обґрунтування, що, загалом кажучи, не гарантує їхню ефективну роботу для довільного контейнера, різних збурних дій.

В [96-99] запропоновані різні методи оборотних ЦВЗ, що здійснюють стеганоперетворення в просторовій області контейнера, стійкі до збурних дій. Однак, як і для їхніх аналогів, що працюють в областях перетворення, згаданих вище, область їх застосування обмежується зображеннями в градаціях сірого.

В [92] був запропонований стеганографічний алгоритм, який дотепер має значне поширення, зазнає численних модифікацій. У рамках алгоритму вбудовування ДІ відбувається в канал синього кольору ЦЗ, що має RGB-кодування. При цьому для вбудови 1 біта ДІ виконуються наступні операції. Нехай p_i — черговий біт ДІ, який підлягає вбудовуванню, $C=\{R,G,B\}$ — представлення ЦЗ-контейнера у вигляді трьох матриць, $p(x,y)$ — псевдовипадковий піксель контейнера, у який буде виконуватися вбудовування. Біт p_i вбудовується в канал синього кольору шляхом модифікації яскравості:

$$B'(x,y)=\begin{cases} B(x,y)-\nu\lambda(x,y), & при \quad p_i=0; \\ \\ B(x,y)+\nu\lambda(x,y), & при \quad p_i=1 \end{cases},$$

де $\lambda(x,y)=0.29890\cdot R(x,y)+0.58662\cdot G(x,y)+0.11448\cdot B(x,y)$, ν — константа, що визначає енергію ДІ, що вбудовується. Чим більше ν, тим вище стійкість інформації, що вбудовується, до збурень, тим більша ймовірність недотримання надійності сприйняття стеганоповідомлення. Безпосередня перевірка показує, що при дотриманні надійності сприйняття стеганоповідомлення, сформоване обговорюваним стеганоалгоритмом, витримує лише незначні атаки проти вбудованого повідомлення.

Пізніше в [16,100] були запропоновані просторові методи, що модифікують при вбудові ДІ піксель залежно й пропорційно його яскравості. Так в [16] у процесі вбудови ДІ біти ЦВЗ спочатку зазнають переставлення, використовуючи операцію «виключного АБО». Підвищення стійкості алгоритму досягається за рахунок балансування значень пікселів, що знаходяться в околі задіяних для вбудови ЦВЗ, шляхом регулювання довжини ЦВЗ, що вбудовується, відповідно до яскравості пікселів околу й скорочення відхилення оригінальних пікселів ЦЗ від сусідніх, задіяних у процесі стеганоперетворення.

Однак всі методи, запропоновані в [16,92,100], виявляються неефективними з погляду стійкості до збурних дій, коли ЦЗ має велику кількість високочастотних компонентів.

В [17] запропонований стійкий до збурних дій метод, заснований на модифікації пікселів ЦЗ, що використовує техніку кратних секцій (multiple sections technique), в основу якого покладений метод з [16]. Вбудова ДІ здійснюється тут у синю колірну складову ЦЗ. Судячи з наведених результатів обчислювального експерименту, метод має високу ефективність в умовах атак проти вбудованого повідомлення, тому результати його тестування [17]

використовуються в розділі 4 для організації порівняльного аналізу, однак сам метод у роботі [17] не наведений.

Таким чином, на підставі аналізу сучасних СА, стійких до атак проти вбудованого повідомлення, що працюють у просторовій області ЦЗ-контейнера, можна зробити висновок, що переваги просторової області зображення для організації стеганоперетворення практично не знаходять свого втілення в існуючих стеганографічних алгоритмах, розробки яких є безсистемними, математично строго необґрунтованими, а тому не несуть у собі показників явної переваги в ефективності, в порівнянні з СА, що працюють в областях перетворення ЦЗ.

Як видно із проведеного аналізу літературних джерел, у сучасних наукових публікаціях, присвячених питанням розробки стійких до атак проти вбудованого повідомлення стеганографічних алгоритмів, найбільша увага приділяється проблемам ЦВЗ, а питання організації стеганографічного каналу зв'язку обговорюються мало. Це пов'язано з багатьма причинами, однією з яких (найбільш вагомою) є те, що друга із зазначених задач є більш складною, оскільки в обов'язковому порядку вимагає забезпечення надійності сприйняття стеганоповідомлення, на відміну від першої. Складність рішення такої задачі виникає в силу відомого [2,8] протиріччя між вимогами стійкості СА до збурних дій (задоволення якої відбувається за рахунок залучення в процесі стеганоперетворення низькочастотної складової ЦЗ-контейнера) і вимогою надійності сприйняття стеганоповідомлення (що гарантовано задовольняється при організації стеганоперетворення шляхом збурення високочастотної складової контейнера).

Приділення основної уваги ЦВЗ (особливо в закордонних публікаціях) приводить до недостатньо представницьких експериментів, на підставі яких автори розроблюваних алгоритмів роблять висновки про їхні властивості. Часто такі обчислювальні експерименти проводяться на 3-7 ЦЗ, що не забезпечує об'єктивності висновків [64].

1.4 Висновки до розділу 1

Проведений аналіз сучасних відкритих літературних джерел по темі дисертаційної роботи дозволяє зробити наступні висновки:

1. Подальший розвиток комплексної системи захисту інформації неможливий без удосконалення її складової — стеганографічної системи за рахунок розробки нових ефективних стеганометодів і алгоритмів.
2. Одною з основних вимог, що висуваються до стеганоалгоритму при використанні його для організації прихованого каналу зв'язки, є вимога його стійкості до атак проти вбудованого повідомлення. Задача забезпечення такої стійкості не є повністю вирішеною, залишається на сьогоднішній день актуальною.
3. У сучасних наукових публікаціях більший розвиток отримали методи, що забезпечують стійкість до збурних дій ЦВЗ, у порівнянні зі стійкими до атак проти вбудованого повідомлення стеганометодами й алгоритмами, використовуваними для організації прихованого каналу зв'язку. Одною з основних причин цього є необхідна вимога забезпечення надійності сприйняття СП для останніх, що в сукупності з одночасною вимогою стійкості СА до збурних дій представляє невирішену до кінця задачу.
4. Найбільш часто використовуваними при організації стеганоперетворення для забезпечення стійкості стеганоалгоритма є області перетворення зображення-контейнера: область ДВП, ДКП, області різних розкладань матриці, а розробки стеганоалгоритмів у просторовій області є нечисленними, безсистемними. Це пов'язано, у першу чергу, з існуванням достатніх умов забезпечення стійкості до збурних дій СА в областях перетворення ЦЗ й відсутністю таких умов у ПО.
5. Для сучасних СА, що працюють в області ДВП, ДКП, дискретного перетворення Фур'є задача одночасного забезпечення двох вимог до СА: надійності сприйняття стеганоповідомлення й стійкості до атак проти вбудованого повідомлення залишається невирішеною до кінця. Спроби її

рішення часто приводять до того, що розроблювані СА не є одночасно стійкими навіть до найпоширеніших збурних дій. Це пов'язано з тим, що в частотній області ЦЗ використання відповідних коефіцієнтів у процесі стеганоперетворення дозволяє задіяти лише певні частотні складові зображення, які можуть гарантувати забезпечення лише одної із зазначених вимог; компромісні варіанти приводять до можливості порушення виконання якої-небудь із вимог до СА.

6. Більш перспективними з погляду забезпечення двох основних вимог до СА: стійкості до збурних дій і надійності сприйняття стеганоповідомлення, у порівнянні з алгоритмами, що працюють у частотній області, є методи, засновані на сингулярному розкладанні матриці (матриць) ЦЗ. Однак, працюючи в області перетворення ЦЗ, вони не можуть уникнути додаткових обчислювальних витрат на переходи ПО – ОПр, ОПр – ПО й додаткового накопичення обчислювальної похибки, що відбуваються в ході цих переходів, у порівнянні з алгоритмами, що працюють у просторовій області ЦЗ.
7. Враховуючи те, що збурення параметрів ЦЗ, що відбуваються при вбудові ДІ в будь-якій області контейнера (просторовій, області перетворення) приведуть до певних збурень в інших областях (перетворення, просторовій), стійкість стеганоалгоритму може бути забезпечена при проведенні стеганоперетворення в будь-якій області контейнера, у тому числі, просторовій. При цьому процес вбудови/декодування ДІ в просторовій області ЦЗ має переваги перед областями перетворення як в сенсі обчислювальної складності, так і в сенсі обчислювальної похибки. Це говорить про принципову можливість забезпечення більш високої стійкості для СА, що працюють у ПО, у порівнянні зі СА, що працюють в ОПр контейнера.
8. До цього моменту у відкритих наукових джерелах відсутні загальні формальні достатні умови забезпечення стійкості стеганометода (стеганоалгоритма) у ПО ЦЗ-контейнера; стійкість до атак проти вбудованого

повідомлення наявних СА, у більшості випадків, не забезпечена строгим математичним обґрунтуванням, що не гарантує їхню ефективну роботу для довільного контейнера, різних збурних дій. Це гальмує процес підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення.

Таким чином, у розділі 1 вирішена задача 1 з переліку задач дисертаційної роботи; показано, що задача підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення шляхом розробки стеганографічних методів і алгоритмів для організації прихованого каналу зв’язку, що працюють у просторовій області контейнера, стійких до збурних дій, є актуальною.

РОЗДІЛ 2
СТІЙКЕ СТЕГАНОПЕРЕТВОРЕННЯ ПРОСТОРОВОЇ ОБЛАСТІ ЗОБРАЖЕННЯ-КОНТЕЙНЕРА: ПЕРЕВАГИ ТА ТЕОРЕТИЧНЕ ОБГРУНТУВАННЯ

Як відзначалося в розділі 1, задача одночасного забезпечення стеганоалгоритмами, що використовуються для організації прихованого каналу зв’язку, вимог стійкості до атак проти вбудованого повідомлення і надійності сприйняття стеганоповідомлення не є повністю вирішеною. Одною з основних причин цього є відсутність належного теоретичного базису існуючих та розроблюваних стеганоалгоритмів, який передбачає обгрунтування переваг використання певних областей зображення для організації стеганоперетворення/декодування ДІ.

Метою розділу є розробка теоретичних основ забезпечення стійкості стеганографічних алгоритмів до атак проти вбудованого повідомлення, які дозволять підвищити стійкість відповідних стеганосистем завдяки використанню для стеганоперетворення області ЦЗ-контейнера, яка має переваги, в порівнянні з іншими областями.

Для досягнення мети необхідно розв'язати *задачі*:

1. Серед областей зображення (просторової, перетворення) обрати ту, яка має певні переваги для вбудови/декодування додаткової інформації, детально обґрунтувати ці переваги;
2. Отримати відповідності між формальними представленнями стійких стеганоперетворень в областях перетворень зображення й просторовій області;
3. Розробити формальну достатню умову забезпечення стійкості стеганоалгоритму до збурних дій в області контейнера-зображення, що має переваги для організації стеганоперетворення/декодування ДІ, забезпечення

якої не залежить від конкретного виду атаки проти вбудованого повідомлення;

4. Отримати рекомендації з вибору розміру блоку контейнера, задіяного в стеганоперетворенні.

Досягнення поставленої мети дозволить розробити на основі отриманої формальної достатньої умови стеганометоди та алгоритми, що їх реалізують, гарантовано стійкі до атак проти вбудованого повідомлення.

2.1 Аналіз переваг просторової області цифрового зображення-контейнера для організації стеганоперетворення/декодування додаткової інформації

Метою підрозділу є обгрунтування переваг використання для стеганоперетворення/декодування ДІ просторової області контейнера-зображення, у порівнянні з областями перетворення.

Для досягнення мети необхідно розв'язати наступні *задачі*:

1. Оцінити «накладні» обчислювальні витрати для переводу цифрового зображення із просторової області в області перетворення, які найчастіше використовуються в стеганографії;

2. Оцінити обчислювальну похибку, що виникає при виконанні прямого й зворотного перетворення зображення виду: ПО – ОПр, ОПр – ПО.

2.1.1 Обчислювальні витрати переходів «просторова область — область перетворення», «область перетворення — просторова область» у цифровому зображенні.

Одними з найчастіше використовуваних на сьогоднішній день перетворень ЦЗ, що передують вбудові ДІ, є:

- дискретне косинусне перетворення [2,6,27,32,73];
- дискретне вейвлет-перетворення [29,38,50,64,70];
- сингулярне/спектральне розкладання матриці/матриць ЦЗ [8,20,80,85].

Будь-яка попередня обробка ЦЗ вимагає додаткових обчислювальних витрат. Оцінимо ці витрати для перерахованих вище перетворень [101,102].

Нехай матриця контейнера F з елементами f_{ij} має розміри $m \times m$ пікселів ($i, j = \overline{0, m-1}$). З врахуванням того, що пряме ДКП із матрицею T, елементи якої нижче позначаються як t_{uv} , виражається у вигляді [55]:

$$t_{uv} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} f_{ij} \alpha(u) \alpha(v) cos\left(\frac{(2i+1)u\pi}{2m} \right) cos\left(\frac{(2j+1)v\pi}{2m} \right), \quad (2.1)$$

для $u, v = \overline{0, m-1}$, де

$$\alpha(u) = \begin{cases} \sqrt{1/m} & для \quad u = 0 \\ \\ \sqrt{2/m} & для \quad u = 1,2,...,m-1 \end{cases},$$

і аналогічно для $\alpha(v)$, а обернене може бути представлено як

$$f_{ij} = \sum_{u=0}^{m-1} \sum_{v=0}^{m-1} t_{uv} \alpha(u) \alpha(v) cos\left(\frac{(2i+1)u\pi}{2m} \right) cos\left(\frac{(2j+1)v\pi}{2m} \right), \quad (2.2)$$

то процеси переходів ПО – ОПр, ОПр – ПО в випадку ДКП в «класичному виді» вимагає

$$S = \underline{O}\left(m^4\right) \quad (2.3)$$

операцій. Використання алгоритму здвоювання (алгоритму Кьонига-Рунге [103]) при накопиченні суми в (2.1), (2.2) дозволить зменшити S до

$$S \approx \underline{O}\left(m^2 \log_2^2 m\right)$$

(швидке перетворення Фур'є) [103], однак все одно залишить цю кількість значущою при великих значеннях m. Крім того, для організації швидкого

перетворення Фур'є бажано, щоб m було цілим ступенем двійки, що для реальних ЦЗ зовсім не обов'язково. Якщо це не так, то єдиний спосіб зниження обчислювальних витрат полягає у відкиданні деяких даних або додаванні нульових (фіктивних) значень [103]. Ці дії змінюють очікувані результати, вносячи додаткову обчислювальну похибку у загальний процес, що є вкрай небажаним, зокрема при організації прихованого каналу зв’язку.

Організація процесів ДВП для матриці всього ЦЗ, отримання сингулярного/спектрального розкладання матриці F вимагає також відомих [55,103,104] значимих обчислювальних витрат.

Для більшості сучасних методів і алгоритмів обробки ЦЗ, у тому числі, стеганоалгоритмів, перед вбудовою ДІ матриця контейнера розбивається на блоки різного фіксованого розміру $n \times n$ (найчастіше — 8×8 пікселів), після чого кожний блок зазнає певної обробки. Доцільність такої розбивки обговорюється, наприклад, в [55], однак точно можна стверджувати, що однією з переслідуваних цілей тут є зменшення обчислювальної складності відповідних алгоритмів, у порівнянні з їхньою обчислювальною складністю при роботі з усім зображенням цілком.

Якщо передобробкою блоку є переведення його із просторової області в область перетворення, на це витрачається певна кількість операцій K, що не залежить від розміру матриці зображення (контейнера). Тоді загальне число операцій, яке буде потрібно для переведення всіх блоків ЦЗ в область перетворення, визначається кількістю блоків і становить:

$$S = K\left[\frac{m}{n}\right]\left[\frac{m}{n}\right] = \underline{O}\left(m^2\right), \tag{2.4}$$

операцій, де $[\bullet]$ — ціла частина аргументу. Така ж кількість операцій буде потрібна й для обов'язкового зворотного переходу з області перетворення в просторову область зображення.

З врахуванням того, що реальні ЦЗ мають значні розміри, значними виявляються й «накладні обчислювальні витрати» (2.3), (2.4) для процесів ПО – ОПр, ОПр – ПО, навіть коли ці переходи відбуваються поблоково, що дуже часто використовується в стеганографічних алгоритмах [2,5,6,101,102].

2.1.2 Обчислювальна похибка переходів «просторова область — область перетворення», «область перетворення — просторова область» для цифрового зображення. Особливості машинної арифметики накладають свої відбитки на обчислення, що робляться в системі з плаваючою точкою. Не можна не враховувати той факт, що обчислення, пов'язані з переходом в область перетворення ЦЗ, вносять додаткову похибку у будь-який процес, пов'язаний з поверненням у просторову область, що обов'язково відбувається при стеганоперетворенні.

Розглянемо в цьому зв'язку детально кожне з наведених вище перетворень, починаючи із ДКП.

У множині дійсних чисел послідовне виконання прямого й оберненого дискретного косинусного перетворення повертає матрицю до її первісного виду, але в системі чисел із плаваючою точкою, що допускає точне представлення лише скінченної множини дійсних чисел [105], накопичення обчислювальної похибки приводить до того, що результатом оберненого ДКП не є початкова матриця. Підтвердженням цьому є результати обчислювального експерименту [101,102], у якім було задіяно 200 цифрових зображень, збережених у різних форматах (із втратами, без втрат). В ході експерименту матриця кожного зображення розбивалася на блоки B розміром $n \times n$ пікселів. Для кожного блоку B виконувалося пряме (результат — B_{DCT}) і обернене дискретне косинусне перетворення (результат — B_{IDKT}), після чого визначалася абсолютна похибка для кожного елемента матриці вхідного блоку шляхом обчислення $abs(B_{IDKT} - B)$, де операція обчислення абсолютного значення $abs(\bullet)$ розглядається поелементно. Підсумком є обчислення середнього значення

похибки $\Delta_{ср}$ значення яскравості по всіх блоках усіх розглянутих цифрових зображень для кожного фіксованого n, $n \in \{8, 32, 128\}$. Результати експерименту відображені на рис.2.1.

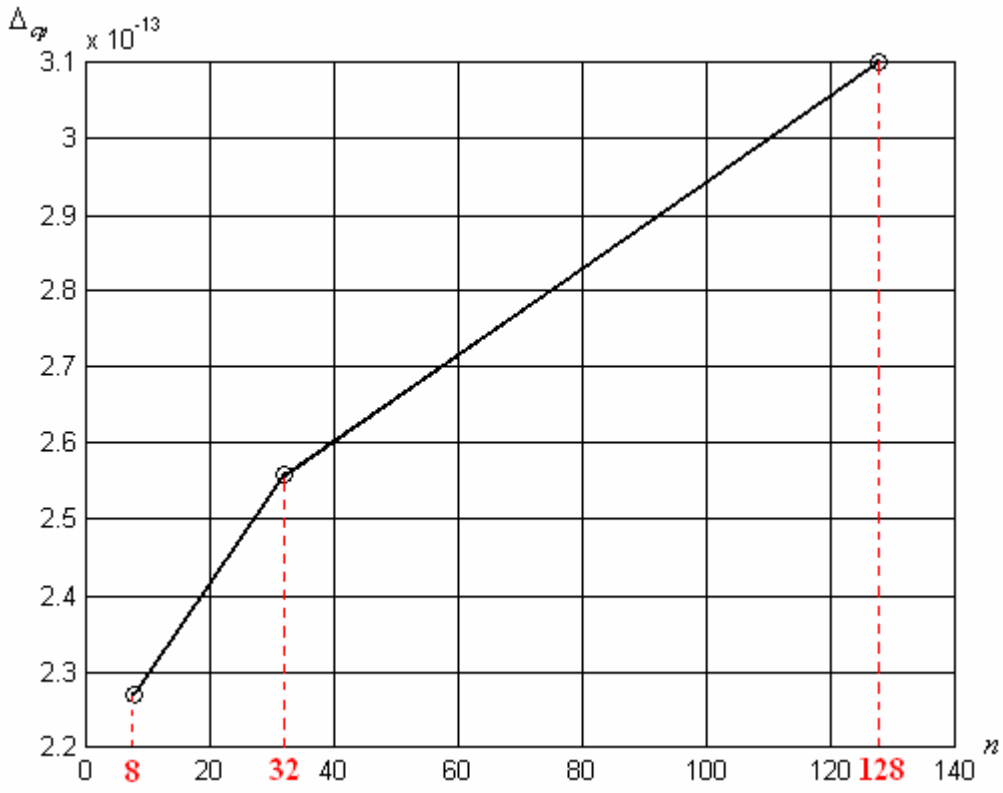


Рисунок 2.1 — Залежність середньої абсолютної похибки елементів цифрового зображення при проведенні поблокового прямого й оберненого дискретного косинусного перетворення від розміру блоку n

Для дискретного вейвлет-перетворення аналогічний експеримент дав результати, відображені на рис.2.2.

Однією з областей перетворення ЦЗ, яка, як уже було відзначено вище, останнім часом використовується для організації процесу вбудови ДІ, є область сингулярного розкладання матриці/матриць зображення:

$$B = U\Sigma V^T, \qquad (2.5)$$

де U, V — ортогональні матриці лівих, правих сингулярних векторів (СНВ) матриці B відповідно,

Σ — діагональна матриця сингулярних чисел,

а також область спектрального розкладання матриці (якщо ця матриця B є симетричною або приведена до симетричного виду): $B = U\Lambda U^T$, де U — ортогональна матриця власних векторів (ВВ) матриці B, Λ — діагональна матриця власних значень (ВЗ). Стеганоперетворення здійснюється тут шляхом модифікації СНЧ/ВЗ і/або СНВ/ВВ. У ході стеганоперетворення відбувається сингулярне/спектральне розкладання матриці блоку зображення-контейнера, після стеганоперетворення відновлюється блок $\overline{B}$ матриці стеганоповідомлення: $\overline{B} = \overline{U}\overline{\Sigma}\overline{V}^T$ / $\overline{B} = \overline{U}\overline{\Lambda}\overline{U}^T$, де $\overline{U}, \overline{\Sigma}, \overline{V}, \overline{\Lambda}$ — результати певних модифікацій СНВ, СНЧ, ВЗ, ВВ.

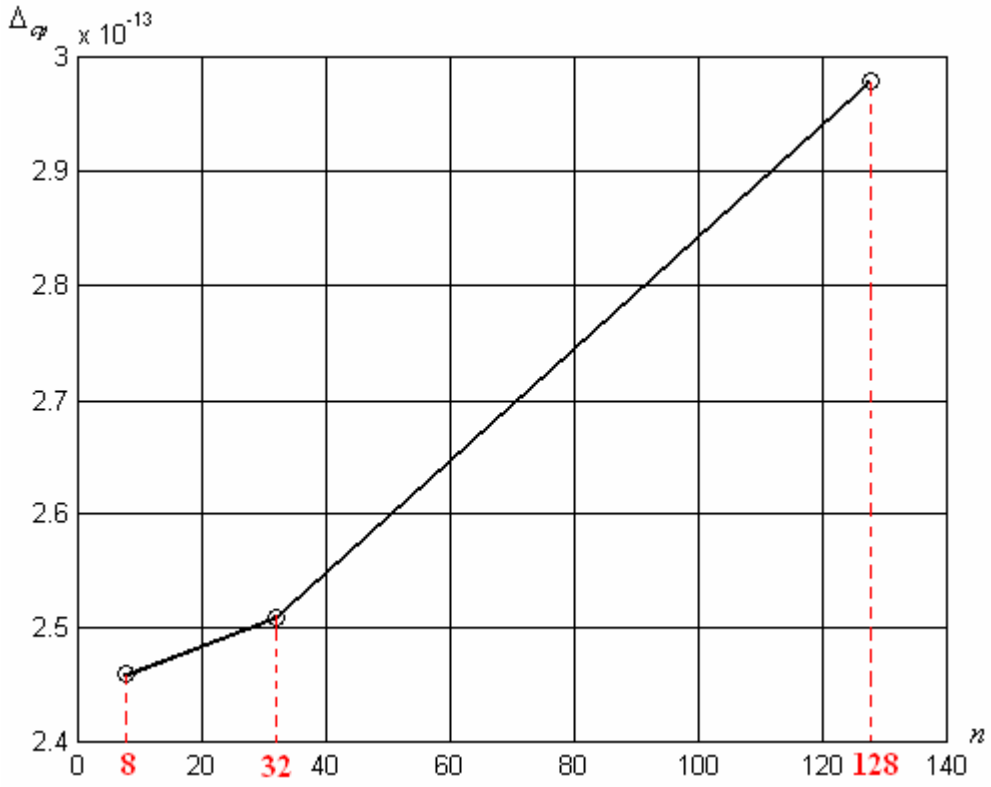


Рисунок 2.2 — Залежність середньої абсолютної похибки елементів цифрового зображення при проведенні поблокового прямого й оберненого дискретного вейвлет-перетворення від розміру блоку n

В області дійсних чисел при відсутності якої-небудь модифікації елементів сингулярних/спектральних множників U,Σ,V,Λ матриця $U\Sigma V^T$ $(U\Lambda U^T)$ співпадає з матрицею B, але в системі чисел із плаваючою точкою цього не відбувається через накопичення обчислювальної похибки. Результати обчислювального експерименту для сингулярного розкладання матриці, що наочно ілюструють зроблений висновок, представлені на рис.2.3; аналогічні результати отримані у випадку спектрального розкладання матриці [101,102].

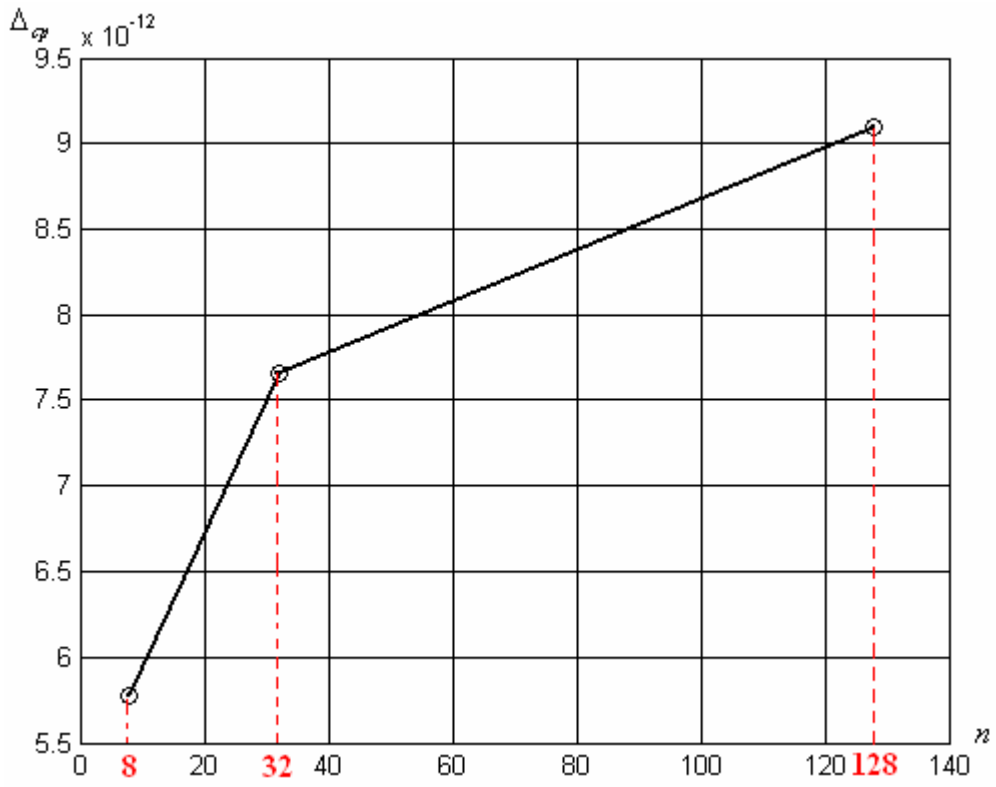


Рисунок 2.3 — Залежність середньої абсолютної похибки елементів цифрового зображення при його відновленні після проведення поблокового сингулярного розкладання від розміру блоку n

Як видно з отриманих результатів, абсолютна похибка елементів відновленої матриці не є нульовою, зростає з збільшенням розміру блоку. Це повністю відповідає очікуванням: зі збільшенням розміру блоку збільшується кількість операцій при обчисленнях його елементів у процесі переходів

«просторова область – область перетворення», «область перетворення – просторова область», відбувається накопичення похибки.

Зауважимо, що абсолютна середня похибка елементів відновленої матриці при переходах «просторова область – область перетворення», «область перетворення – просторова область», здійснюваних з використанням сингулярного/спектрального розкладання, на порядок більша, чим з використанням дискретного косинусного перетворення або дискретного вейвлет-перетворення [101,102].

Незважаючи на те, що значення абсолютних похибок малі, існує можливість накопичення цих похибок. Крім того, їх ненульові значення можуть бути збільшені збуреннями, яких будуть зазнавати елементи області перетворення цифрового зображення, наприклад, у процесі вбудови додаткової інформації, що, як свідчать матеріали деяких публікацій [8], може привести в підсумку навіть до виходу елементів матриці ЦЗ при поверненні в просторову область за межі $[0, 255]$, що приведе до виникнення похибки, що перевищує значення похибки округлення, і як наслідок, до зниження ефективності стеганоалгоритму.

Таким чином, просторова область зображення є кращою для вбудови додаткової інформації, у порівнянні з областями перетворення:

- у сенсі обчислювальної складності процесів стеганоперетворення й декодування додаткової інформації (з урахуванням переходів «просторова область – область перетворення», «область перетворення – просторова область»),
- в сенсі обчислювальної похибки, накопичення якої є необхідною частиною переходів «просторова область – область перетворення», «область перетворення – просторова область» в системі чисел із плаваючою точкою [101,102].

2.2 Теоретичні основи забезпечення стійкості стеганоперетворення, що реалізуються в просторовій області зображення-контейнера

Метою підрозділу є розробка умов забезпечення стійкості стеганоалгоритму до збурних дій при організації стеганоперетворення в просторовій області контейнера-зображення.

Для досягнення поставленої мети в підрозділі необхідно розв'язати наступні *задачі*:

1. Формалізувати процес стійкого до атак проти вбудованого повідомлення стеганоперетворення в просторовій області зображення-контейнера;
2. Отримати достатню умову стійкості стеганоалгоритму при організації стеганоперетворення в просторовій області.

2.2.1 Відповідності між збуреннями параметрів цифрового зображення в областях перетворення. Достатні умови забезпечення стійкості до збурних дій стеганометодів і алгоритмів вже обговорювалися у відкритих джерелах [8,34,90]. Однак ці достатні умови були отримані в областях перетворення матриці ЦЗ-контейнера. Так в [34] була отримана достатня умова забезпечення стійкості стеганоалгоритму до атаки стиском, у тому числі, зі значними коефіцієнтами, відповідно з якою для забезпечення стійкості стеганоперетворення достатньо проводити таким чином, щоб його формальним представленням була сукупність S збурень максимальних сингулярних чисел блоків матриці контейнера. Отримана достатня умова [34,62] забезпечує стійкість і до інших збурних дій, а з врахуванням тієї математичної бази, яка була покладена в її основу, — загальний підхід до аналізу стану й технології функціонування інформаційних систем [8], отримана достатня умова може розглядатися для збурних дій, незалежно від їхнього конкретного виду. Практичною реалізацією цієї достатньої умови, стали стеганометод і відповідний йому алгоритм $A1$, представлені в роботі [62], де вбудова ДІ, що представляє випадково сформовану бінарну послідовність, проводилася

шляхом збурення максимальних СНЧ блоків матриці ЦЗ-контейнера, отриманих у результаті її стандартної розбивки [55]. Обчислювальний експеримент підтвердив високу ефективність $A1$, що перевищує ефективність сучасних аналогів, при декодуванні ДІ в умовах збурних дій, спрямованих на стеганоповідомлення, у тому числі тих, що відрізняються від стиску. Однак згадана достатня умова розглядає область перетворення контейнера — область сингулярного розкладання матриць блоків основного повідомлення. А задача отримання її аналога в просторовій області залишається невирішеною до цього моменту.

Завдяки однозначності нормального сингулярного розкладання, дискретного перетворення Фур'є, однозначного визначення матриці ЦЗ в просторовій області своїми елементами існує взаємно однозначна відповідність між змінами параметрів, що визначають ЦЗ, у різних областях перетворення, а також відповідність між змінами параметрів в області перетворення й параметрів у просторовій області зображення [106,107].

Дійсно, нехай B — $l \times l$ – блок матриці зображення-контейнера. Для B існує сингулярне розкладання (2.5) [104], яке представляється більш детально:

$$B = U\Sigma V^T = (u_1,...,u_l)\begin{pmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma_l \end{pmatrix}(v_1,...,v_l)^T, \qquad (2.6)$$

де U, V — ортогональні $l \times l$ – матриці, стовпці яких u_i, v_i, $i = \overline{1,l}$, — ліві й праві сингулярні вектори B відповідно, $\Sigma = diag(\sigma_1,...,\sigma_l)$, $\sigma_1 \geq ... \geq \sigma_l \geq 0$ — СНЧ.

Нехай формально вбудова чергових біт ДІ виражається в збуренні СНЧ блоку. Тоді результатом стеганоперетворення буде блок $\overline{B}$ стеганоповідомлення, що відповідає з врахуванням (2.6) матричному виразу:

$$\overline{B} = U(\Sigma + \Delta\Sigma)V^T, \qquad (2.7)$$

де $\Delta\Sigma = diag(\Delta\sigma_1,...,\Delta\sigma_l)$ — діагональна матриця збурень $\Delta\sigma_i$ СНЧ σ_i, $i=\overline{1,l}$, матриці B в процесі стеганоперетворення.

Збурення найбільшого СНЧ блоку з врахуванням (2.7) формально виразиться наступним чином:

$$\overline{B} = (u_1,...,u_l)\begin{pmatrix} \sigma_1+\Delta\sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma_l \end{pmatrix}(v_1,...,v_l)^T = (u_1,...,u_l)\begin{pmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma_l \end{pmatrix}(v_1,...,v_l)^T +$$

$$+(u_1,...,u_l)\begin{pmatrix} \Delta\sigma_1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}(v_1,...,v_l)^T, \qquad (2.8)$$

тобто [106,108]

$$\overline{B} = B + \Delta\sigma_1 u_1 v_1^T. \qquad (2.9)$$

Визначимо, як відобразиться на коефіцієнтах ДКП блоку B збурення його максимального СНЧ. Блок, не обмежуючи спільності міркувань, для визначеності й спрощення викладу на даному етапі будемо вважати розміром 8×8.

Позначимо B_{DCT} і $\overline{B}_{DCT}$ — результати ДКП для B і $\overline{B}$ відповідно. B і B_{DCT} пов'язані співвідношенням [109]:

$$B_{DCT} = PBP^T, \qquad (2.10)$$

де матриця P — ортогональна з елементами p_{ij}, що визначаються відповідно до формули [109]:

$$p_{ij} = \begin{cases} \frac{1}{\sqrt{8}}, \ i = 1, \ 1 \le j \le 8, \\ \\ \frac{1}{2} cos \frac{\pi(2j-1)(i-1)}{16}, \ 2 \le i \le 8, \ 1 \le j \le 8 \end{cases} . \qquad (2.11)$$

Підставимо (2.6) в (2.10):

$$B_{DCT} = PU\Sigma V^T P^T = (PU)\Sigma(PV)^T . \qquad (2.12)$$

Формула (2.12) визначає сингулярне розкладання матриці B_{DCT} [110], для якої, очевидно, множина СНЧ співпадає з множиною СНЧ матриці B, але СНВ для B і B_{DCT} різні.

Відповідно до (2.10)

$$\overline{B}_{DCT} = P\overline{B}P^T . \qquad (2.13)$$

Підставляючи в (2.13) вираз (2.9), отримаємо:

$$\overline{B}_{DCT} = P(B + \Delta\sigma_1 u_1 v_1^T)P^T = PBP^T + \Delta\sigma_1 Pu_1 v_1^T P^T = B_{DCT} + \Delta\sigma_1 (Pu_1)(Pv_1)^T . \qquad (2.14)$$

Шукані зміни коефіцієнтів ДКП визначаються елементами матриці $\Delta\sigma_1 (Pu_1)(Pv_1)^T$ з (2.14). Розглянемо докладно матрицю $\Delta\sigma_1 (Pu_1)(Pv_1)^T$.

В [91] показано, що СНВ u_1, v_1 $8\times 8-$блоків матриці ЦЗ, що відповідають максимальним СНЧ, у випадку нормального сингулярного розкладання [8], яке додатково в (2.6) вимагає лексикографічну додатність [20] лівих СНВ і визначається однозначно, у переважній більшості блоків зображення близькі до n-оптимального вектору n^O простору R^8:

$$u_1 \approx n^O , \ v_1 \approx n^O , \qquad (2.15)$$

де *n*-оптимальний вектор в R^8 має вид:

$$n^O = \left(\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \ldots, \frac{1}{\sqrt{8}}\right)^T \in R^8. \qquad (2.16)$$

Тоді

$$Pu_1 = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{18} \\ p_{21} & p_{22} & \cdots & p_{28} \\ \cdots & \cdots & \cdots & \cdots \\ p_{81} & p_{82} & \cdots & p_{88} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{8}} \\ \frac{1}{\sqrt{8}} \\ \vdots \\ \frac{1}{\sqrt{8}} \end{pmatrix} = \frac{1}{\sqrt{8}} \begin{pmatrix} \sum_{j=1}^{8} p_{1j} \\ \sum_{j=1}^{8} p_{2j} \\ \vdots \\ \sum_{j=1}^{8} p_{8j} \end{pmatrix}, \quad Pv_1 = \frac{1}{\sqrt{8}} \begin{pmatrix} \sum_{j=1}^{8} p_{1j} \\ \sum_{j=1}^{8} p_{2j} \\ \vdots \\ \sum_{j=1}^{8} p_{8j} \end{pmatrix},$$

а

$$(Pu_1)(Pv_1)^T = \frac{1}{8} \begin{pmatrix} \sum_{j=1}^{8} p_{1j} \\ \sum_{j=1}^{8} p_{2j} \\ \vdots \\ \sum_{j=1}^{8} p_{8j} \end{pmatrix} \begin{pmatrix} \sum_{j=1}^{8} p_{1j} & \sum_{j=1}^{8} p_{2j} & \cdots & \sum_{j=1}^{8} p_{8j} \end{pmatrix} =$$

$$= \frac{1}{8} \begin{pmatrix} \left(\sum_{j=1}^{8} p_{1j}\right)\left(\sum_{j=1}^{8} p_{1j}\right) & \left(\sum_{j=1}^{8} p_{1j}\right)\left(\sum_{j=1}^{8} p_{2j}\right) & \cdots & \left(\sum_{j=1}^{8} p_{1j}\right)\left(\sum_{j=1}^{8} p_{8j}\right) \\ \left(\sum_{j=1}^{8} p_{2j}\right)\left(\sum_{j=1}^{8} p_{1j}\right) & \left(\sum_{j=1}^{8} p_{2j}\right)\left(\sum_{j=1}^{8} p_{2j}\right) & \cdots & \left(\sum_{j=1}^{8} p_{2j}\right)\left(\sum_{j=1}^{8} p_{8j}\right) \\ \cdots & \cdots & \cdots & \cdots \\ \left(\sum_{j=1}^{8} p_{8j}\right)\left(\sum_{j=1}^{8} p_{1j}\right) & \left(\sum_{j=1}^{8} p_{8j}\right)\left(\sum_{j=1}^{8} p_{2j}\right) & \cdots & \left(\sum_{j=1}^{8} p_{8j}\right)\left(\sum_{j=1}^{8} p_{8j}\right) \end{pmatrix}.$$

Враховуючи (2.11), маємо:

$$\left(\sum_{j=1}^{8} p_{1j}\right)\left(\sum_{j=1}^{8} p_{1j}\right) = 8,$$

для $k \neq 1$:

$$\sum_{j=1}^{8} p_{kj} = \frac{1}{2}\left(cos\frac{\pi(k-1)}{16} + cos\frac{\pi(k-1)\cdot 3}{16} + cos\frac{\pi(k-1)\cdot 5}{16} + \ldots + cos\frac{\pi(k-1)\cdot 15}{16} \right) \qquad (2.17)$$

Для зручності позначимо:

$$\alpha = \frac{\pi(k-1)}{16}. \qquad (2.18)$$

Тоді формула (2.17) буде мати вигляд:

$$\sum_{j=1}^{8} p_{kj} = \frac{1}{2}\sum_{j=1}^{8} cos(2j-1)\alpha .$$

Використовуючи відомі формули тригонометричних перетворень [111], з останньої рівності отримаємо:

$$\sum_{j=1}^{8} p_{kj} = \frac{sin16\alpha}{4sin\alpha},$$

а з врахуванням (2.18):

$$\sum_{j=1}^{8} p_{kj} = \frac{sin16\alpha}{4sin\alpha} = \frac{sin\left(16\frac{\pi(k-1)}{16}\right)}{4sin\frac{\pi(k-1)}{16}} = \frac{sin\pi(k-1)}{4sin\frac{\pi(k-1)}{16}} = 0 .$$

Таким чином

$$\Delta\sigma_1 (Pu_1)(Pv_1)^T = \frac{\Delta\sigma_1}{8}\begin{pmatrix} 8 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{pmatrix} = \begin{pmatrix} \Delta\sigma_1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Таким чином, збурення максимального сингулярного числа блоку B, що проведене в області сингулярного розкладання його матриці, у частотній

області блоку виразиться в збуренні dc-коефіцієнта [55] дискретного косинусного перетворення на $\Delta\sigma_1$, що взагалі може бути використаним при побудові нових стійких до атак проти вбудованого повідомлення стеганографічних алгоритмів, що діють у частотній області зображення-контейнера.

2.2.2 Формальне представлення стійкого стеганоперетворення в просторовій області контейнера-зображення. Знайдемо тепер відповідний формальний вираз для збурення максимального СНЧ блоку в просторовій області ЦЗ [106-108].

У просторовій області формула (2.9), може бути записана як:

$$\overline{B} = B + \Delta B, \tag{2.19}$$

де $\Delta B = \Delta\sigma_1 u_1 v_1^T$ — матриця збурення блоку B.

Формула (2.19) дає загальне формальне представлення процесу стеганоперетворення, що відбулося в області сингулярного розкладання шляхом збурення максимального СНЧ блоку, в просторовій області блоку контейнера.

Розглядаються блоки матриці ЦЗ довільного розміру $l \times l$. В загальному випадку *n*-оптимальний вектор арифметичного простору R^l має вид [91]:

$$n^O = \left(\frac{1}{\sqrt{l}}, \frac{1}{\sqrt{l}}, \ldots, \frac{1}{\sqrt{l}} \right)^T \in R^l. \tag{2.20}$$

В [91] показано, що середні значення кутів між лексикографічно додатним лівим СНВ u_1 і n^O, а також між відповідним правим СНВ v_1 і n^O порівнянні для різних форматів зображення (із втратами, без втрат) і різної якості стиску й незначно відрізняються від нуля при $l = 8$. З врахуванням [90,91], відмінності u_1,

v_1 від n-оптимального вектора повинні бути незначними при будь-якому розмірі l блоку. Для практичної перевірки висунутої гіпотези був проведений обчислювальний експеримент, у якому було задіяно по 200 цифрових зображень у форматах Jpeg і Tif. У ході експерименту для ЦЗ його матриця розбивалася на $l \times l$-блоки, $l \in \{4,8,16\}$, для кожного блоку будувалися нормальні СНР, визначалися кути між u_1 і n^O, v_1 і n^O. Для кожного зображення обчислювалися середні значення згаданих кутів. Для отриманих середніх (по зображенню) значень обчислювалися середні по всім тестованим зображенням. Ці значення далі позначені UN_{cp} (середній кут між u_1 і n^O), VN_{cp} (середній кут між v_1 і n^O).

Результати експерименту, що повністю підтверджують висунуту гіпотезу, відображені в табл.2.1, де кути представлені в градусах (для $l = 8$ результати взяті з [91]), тобто формула (2.15) має місце не тільки для простору R^8, а для R^l, де l може відрізнятися від 8.

Розглянемо докладно матрицю ΔB, що фігурує в (2.19). Якщо $u_1 = (u_{11}, u_{21}, u_{31}, ..., u_{l1})^T$, $v_1 = (v_{11}, v_{21}, v_{31} ..., v_{l1})^T$, то ця матриця має одиничний ранг і наступний вид:

$$\Delta B = \Delta\sigma_1 u_1 v_1^T = \Delta\sigma_1 \begin{pmatrix} u_{11} \\ u_{21} \\ u_{31} \\ \dots \\ u_{l1} \end{pmatrix} (v_{11}, v_{21}, v_{31} ..., v_{l1}) =$$

$$= \begin{pmatrix} \Delta\sigma_1 u_{11} v_{11} & \Delta\sigma_1 u_{11} v_{21} & \Delta\sigma_1 u_{11} v_{31} & \dots & \Delta\sigma_1 u_{11} v_{l1} \\ \Delta\sigma_1 u_{21} v_{11} & \Delta\sigma_1 u_{21} v_{21} & \Delta\sigma_1 u_{21} v_{31} & \dots & \Delta\sigma_1 u_{21} v_{l1} \\ \Delta\sigma_1 u_{31} v_{11} & \Delta\sigma_1 u_{31} v_{21} & \Delta\sigma_1 u_{31} v_{31} & \dots & \Delta\sigma_1 u_{31} v_{l1} \\ \dots & \dots & \dots & \dots & \dots \\ \Delta\sigma_1 u_{l1} v_{11} & \Delta\sigma_1 u_{l1} v_{21} & \Delta\sigma_1 u_{l1} v_{31} & \dots & \Delta\sigma_1 u_{l1} v_{l1} \end{pmatrix}. \qquad (2.21)$$

Таблиця 2.1 — Характеристики взаємного розташування сингулярних векторів u_1, v_1 і n- оптимального вектора при різних форматах зберігання цифрового зображення й різних розмірах блоків матриці

	$l=4$		$l=8$		$l=16$	
	Jpeg	Tif	Jpeg	Tif	Jpeg	Tif
$UN_{ср}$	4.29	4.33	4.31	4.41	5.87	5.76
$VN_{ср}$	4.17	4.11	3.80	3.87	5.88	5.69

З врахуванням (2.15) і (2.20) формула (2.21) набуває вид:

$$\Delta B \approx \begin{pmatrix} \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \dots & \frac{\Delta\sigma_1}{l} \\ \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \dots & \frac{\Delta\sigma_1}{l} \\ \dots & \dots & \dots & \dots \\ \frac{\Delta\sigma_1}{l} & \frac{\Delta\sigma_1}{l} & \dots & \frac{\Delta\sigma_1}{l} \end{pmatrix} = \begin{pmatrix} \Delta b & \Delta b & \dots & \Delta b \\ \Delta b & \Delta b & \dots & \Delta b \\ \dots & \dots & \dots & \dots \\ \Delta b & \Delta b & \dots & \Delta b \end{pmatrix}. \qquad (2.22)$$

Таким чином, стійке стеганоперетворення, яке реалізується шляхом збурення максимальних СНЧ блоків матриці ОП в області СНР блоків, у просторовій області ЦЗ-контейнера принципово може бути реалізоване шляхом корекції яскравості всіх пікселів відповідних блоків на одне й те саме значення, що дорівнює

$$\Delta b = \frac{\Delta\sigma_1}{l}. \qquad (2.23)$$

Основне питання при розробці конкретних стеганографічних методів і алгоритмів тут буде полягати у визначенні значень $\Delta\sigma_1, l$, що забезпечують стійкість алгоритмів до різних збурних дій з врахуванням дотримання надійності сприйняття формованого стеганоповідомлення.

2.2.3 Розмір блоку як один з визначальних обчислювальну похибку у стеганоповідомленні параметрів. Величина блоку l при організації стеганоперетворення важлива з врахуванням можливості виникнення/накопичення обчислювальної похибки при формуванні стеганоповідомлення, яка, у свою чергу, може вплинути на ефективність розроблюваних стеганографічних алгоритмів.

Зауваження 2.1. Хоча з врахуванням особливостей машинної арифметики, а також (2.15), у більшості блоків матриці зображення після операції (2.8) точна рівність в (2.22) досягатися не буде, відхилення від точної рівності в переважній більшості блоків буде незначним.

Для ілюстрації зробленого зауваження спочатку розглянемо приклад. З оригінального цифрового зображення випадково виділений $8\times 8-$ блок, матриця якого має вид:

$$B=\begin{pmatrix} 172 & 170 & 166 & 165 & 165 & 161 & 155 & 151 \\ 181 & 177 & 172 & 167 & 164 & 161 & 155 & 153 \\ 181 & 177 & 173 & 171 & 167 & 165 & 154 & 153 \\ 185 & 181 & 177 & 175 & 170 & 169 & 155 & 153 \\ 188 & 184 & 178 & 175 & 168 & 166 & 157 & 155 \\ 189 & 184 & 177 & 176 & 170 & 165 & 157 & 154 \\ 189 & 184 & 179 & 179 & 171 & 163 & 158 & 154 \\ 189 & 186 & 180 & 179 & 167 & 160 & 159 & 154 \end{pmatrix}.$$

Цей блок піддався нормальному сингулярному розкладанню (2.6), при цьому

$$u_1=(0.3402\ \ 0.3470\ \ 0.3499\ \ 0.3563\ \ 0.3579\ \ 0.3582\ \ 0.3596\ \ 0.3588)^T,$$

$$v_1=(0.3841\ \ 0.3760\ \ 0.3653\ \ 0.3615\ \ 0.3496\ \ 0.3413\ \ 0.3256\ \ 0.3196)^T.$$

Для порівняння: в просторі R^8 n-оптимальний вектор (2.16) виглядає:

$$n^O = \left(\frac{1}{\sqrt{8}},...,\frac{1}{\sqrt{8}}\right)^T \approx (0.3536,...,0.3536)^T .$$

Після операції (2.8) з $\Delta\sigma_1 = 80$ матриця $\Delta B = \overline{B} - B$ набула вид:

$$\Delta B = \begin{pmatrix} 10.4540 & 10.2336 & 9.9423 & 9.8365 & 9.5145 & 9.2868 & 8.8616 & 8.6984 \\ 10.6645 & 10.4396 & 10.1425 & 10.0345 & 9.7060 & 9.4738 & 9.0400 & 8.8735 \\ 10.7528 & 10.5261 & 10.2265 & 10.1176 & 9.7864 & 9.5522 & 9.1149 & 8.9470 \\ 10.9495 & 10.7187 & 10.4136 & 10.3027 & 9.9654 & 9.7270 & 9.2816 & 9.1107 \\ 10.9996 & 10.7677 & 10.4612 & 10.3499 & 10.0110 & 9.7715 & 9.3241 & 9.1524 \\ 11.0091 & 10.7770 & 10.4703 & 10.3588 & 10.0197 & 9.7799 & 9.3321 & 9.1603 \\ 11.0500 & 10.8171 & 10.5092 & 10.3973 & 10.0569 & 9.8163 & 9.3669 & 9.1943 \\ 11.0279 & 10.7954 & 10.4881 & 10.3764 & 10.0367 & 9.7966 & 9.3481 & 9.1759 \end{pmatrix}.$$

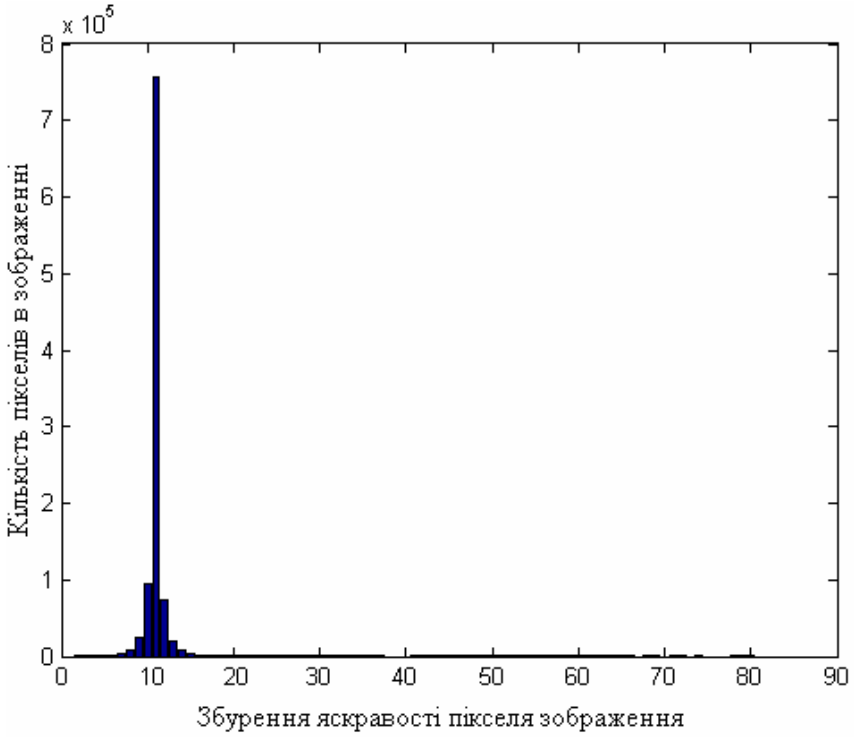
Відмітимо, що хоча елементи ΔB і відрізняються від значення $\frac{\Delta\sigma_1}{l} = \frac{80}{8} = 10$, але вони всі знаходяться у малому околі 10, середнє значення елементів матриці ΔB дорівнює 9.98, тобто відносна похибка середнього значення складає 0.2%.

Для більш ґрунтовної перевірки висновку зауваження 2.1 у середовищі Matlab був проведений обчислювальний експеримент, у якім було задіяно 200 цифрових зображень різних форматів (із втратами, без втрат). Для визначеності зображення бралися в градаціях сірого. У ході експерименту матриця ЦЗ розбивалася на $l \times l -$ блоки B, для кожного з яких будувалося розкладання (2.6), після чого σ_1 в кожному блоці збурювалось на $\Delta\sigma_1$ (однаково для всіх блоків). Після збурення сингулярного числа блок $\overline{B}$ ($\overline{B}$ — збурений блок B) відновлювався відповідно до (2.8). Коли описана операція була проведена з усіма блоками цифрового зображення, воно переводилося у формат uint8, що забезпечує введення значень яскравості пікселів у множину $\{0,1,2,...,255\}$. Після чого в просторовій області цифрового зображення визначалося середнє збурення яскравості пікселів по всьому ЦЗ. Типовий приклад у вигляді гістограм збурень яскравості пікселів для конкретно взятих обраних випадково

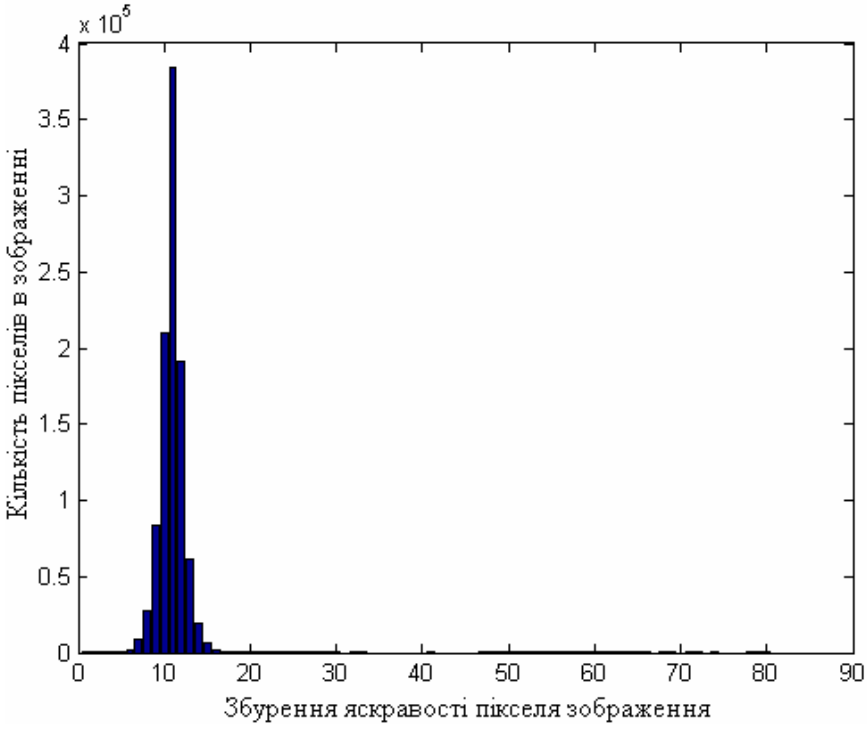
ЦЗ у форматі із втратами й без втрат предствленний на рис.2.4 (середнє значення збурення по зображенню склало для варіанта (а) – 9.96; для (б) – 9.91). Поведінка не залежить від формату зображення. Середнє значення по всім цифровим зображенням модуля збурення тут склало 9.65 (при очікуваному 10). Таким чином, відносна похибка середнього по всім ЦЗ збурення склала: 3.5%. При цьому середні значення по абсолютній більшості зображень, що брали участь в експерименті, виявилися близькими до 10 (рис.2.5).

Очікуваним тут є те, що при фіксованому $\Delta\sigma_1$ відносна похибка отримуваного по формулі (2.23) Δb буде зростати з зменшенням l. Дійсно, чим менше l, тим більше значення Δb корекції яскравості пікселів, тим більше ймовірність того, що результат такої корекції приведе до виходу нових значень яскравості за межі множини $\{0,1,...,255\}$, тобто до додаткового росту обчислювальної похибки й, як наслідок, до росту ймовірності збільшення помилок при декодуванні додаткової інформації.

Для перевірки висунутої гіпотези описаний вище експеримент (200 ЦЗ) був повторений для $\Delta\sigma_1 = 80$, $l = 4,16$. Результати експерименту, що підтверджують на практиці істинність висунутої гіпотези, відображені на рис.2.6. Відзначимо, що якщо при переході від $l = 16$ до $l = 8$ відносна похибка середнього значення Δb зростає незначно, то при переході від $l = 8$ до $l = 4$ ріст суттєвий, що вже на цьому етапі досліджень дозволяє говорити про переваги блоків розміру 8×8 пікселів над блоками 4×4. Перевага 8×8-блоків в порівнянні з блоками розміру 16×16 випливає зі зменшення в 4 рази прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується, у випадку використання останніх при поблоковому стеганоперетворенні.



а



б

Рисунок 2.4 — Гістограма збурень значень яскравості пікселів ЦЗ при збуренні найбільшого СНЧ у кожному 8×8 – блоці на $\Delta\sigma_1 = 80$: а – ЦЗ в форматі Jpeg; б – в форматі Tif

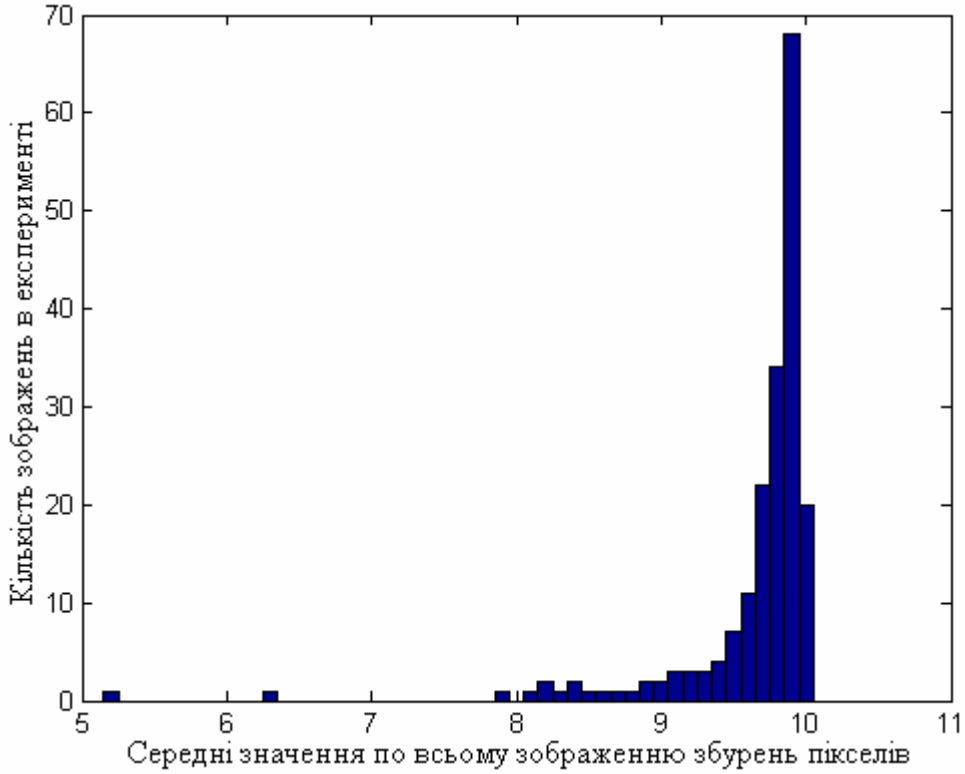


Рисунок 2.5 — Гістограма середніх по зображенню значень збурень яскравості пікселів ($l = 8$, $\Delta\sigma_1 = 80$)

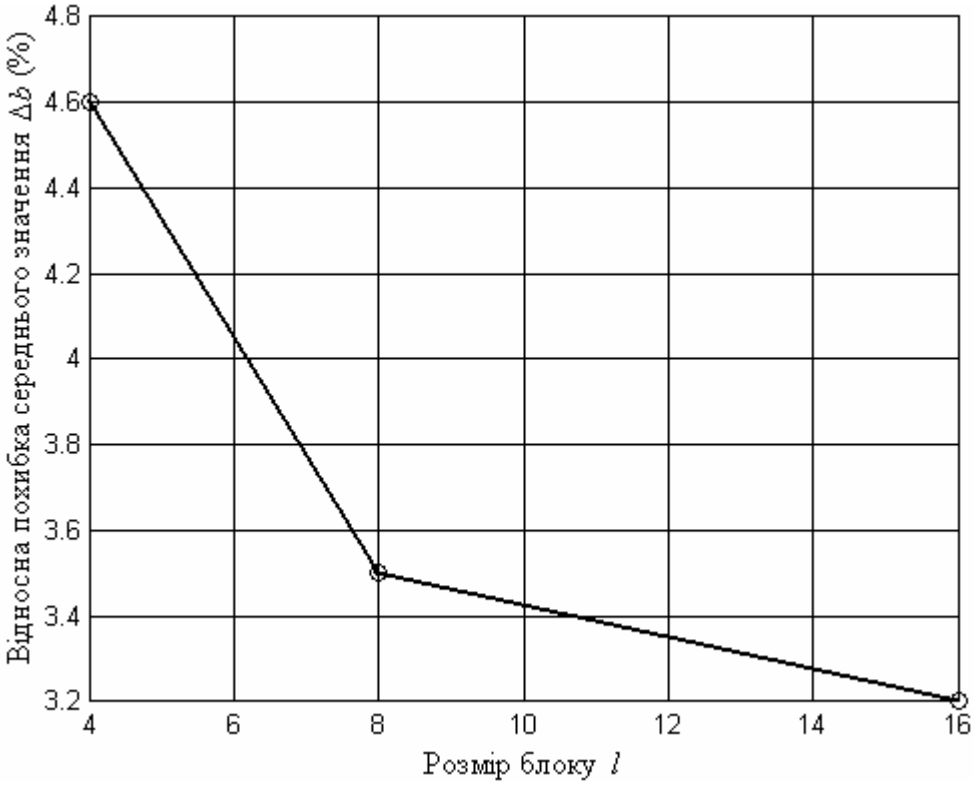


Рисунок 2.6 — Залежність відносної похибки середнього по експерименту значення Δb від розміру блоку зображення

2.2.4 Достатня умова стійкості стеганоалгоритму до атак проти вбудованого повідомлення в просторовій області зображення-контейнера. В [34] показано, що для принципової можливості декодування ДІ зі стеганоповідомлення, що зазнало збурних дій, сукупний результат збурення блоку основного повідомлення при вбудові ДІ повинен перевищувати збурення, яке буде зазнавати блок стеганоповідомлення у процесі збурної дії у каналі атаки (рис.1.1).

Нехай передбачуване збурення блоку $\overline{B}$ стеганоповідомлення при атаці визначається матрицею $\Delta\overline{B}$, тоді відповідно до співвідношення [104]:

$$\max_{1\le j\le l}\left|\sigma_j\left(\overline{B}\right)-\sigma_j\left(\overline{B}+\Delta\overline{B}\right)\right|\le\left\|\Delta\overline{B}\right\|_2,$$

де $\sigma_j\left(\overline{B}\right)$, $\sigma_j\left(\overline{B}+\Delta\overline{B}\right)$ — СНЧ матриць $\overline{B}$ і $\overline{B}+\Delta\overline{B}$ відповідно,

$\left\|\Delta\overline{B}\right\|_2$ — спектральна матрична норма $\Delta\overline{B}$,

кожне сингулярне число блоку $\overline{B}$, в тому числі і максимальне, збуриться на величину, меншу або рівну $\left\|\Delta\overline{B}\right\|_2$. Тоді, відповідно до вищесказаного, збурення $\Delta\sigma_1$ максимального сингулярного числа σ_1 блоку B при стеганоперетворенні, що організується в області сингулярного розкладання, повинне бути більше, чим передбачуване $\left\|\Delta\overline{B}\right\|_2$: $\Delta\sigma_1>\left\|\Delta\overline{B}\right\|_2$, а тоді збурення Δb (2.23) значень яскравості пікселів блоку B основного повідомлення при вбудові додаткової інформації для забезпечення стійкості в просторовій області повинні задовольняти співвідношенню:

$$|\Delta b|>\frac{\left\|\Delta\overline{B}\right\|_2}{l}. \qquad (2.24)$$

Таким чином, із усього вищесказаного випливає істинність наступного твердження.

Твердження 2.1 (*достатня умова стійкості стеганоалгоритму до збурних дій, яка реалізується в просторовій області ЦЗ-контейнера)*. Для того, щоб стеганографічний алгоритм був стійким до збурної дії, результат впливу якої на $l \times l$ – блок стеганоповідомлення $\overline{B}$ оцінюється як $\left\| \Delta \overline{B} \right\|_2$, достатньо, щоб стеганоперетворення, що організується в просторовій області ЦЗ-контейнера, формально представлялося у вигляді збурень яскравості всіх пікселів кожного блоку, задіяного в СПр, на величину Δb, для якої має місце співвідношення (2.24).

Зауваження 2.2. Отримана достатня умова забезпечує стійкість стеганографічного алгоритму до атак проти вбудованого повідомлення незалежно від того, у якому форматі зберігається ЦЗ-контейнер (із втратами, без втрат).

Зауваження 2.3. Забезпечення стійкості стеганографічного алгоритму відповідно до отриманої достатньої умови визначається не конкретним видом збурної дії, а величиною спотворення стеганоповідомлення. Це означає, що стеганоалгоритми, побудовані на основі отриманої достатньої умови, будуть ефективними в умовах атак проти вбудованого повідомлення, незалежно від конкретного виду атаки, на відміну від переважної більшості існуючих аналогів.

На практиці істинність зауважень 2.2, 2.3 буде підтверджено в розділі 4.

2.3 Висновки до розділу 2

У другому розділі розроблений теоретичний базис для стеганометодів і алгоритмів, стійких до атак проти вбудованого повідомлення, які здійснюють стеганоперетворення в просторовій області контейнера-зображення, що забезпечує принципову можливість підвищення ефективності відповідної стеганосистеми завдяки відсутності переходів ПО – ОПр, ОПр – ПО.

Отримані наступні результати:

1. Обґрунтовані переваги ПО ЦЗ-контейнера для організації СПр. Показано, що ПО зображення є кращою, у порівнянні з областями перетворення, як у сенсі обчислювальної складності процесів стеганоперетворення й декодування ДІ (з врахуванням переходів ПО – ОПр, ОПр – ПО, на які мінімально витрачається $\underline{O}(m^2)$ операцій, де $m \times m$ — розмір матриці контейнера), так і в сенсі обчислювальної похибки, додаткове накопичення якої відбувається при побудові СП та при декодуванні ДІ за рахунок переходів ПО – ОПр, ОПр – ПО, що викликає зниження ефективності стеганоалгоритмів.

2. Встановлено: абсолютна похибка елементів відновленого після перетворення блоку матриці росте з зростанням його розміру, що необхідно враховувати при виборі розмірів блоків ОП, що використовуються при стеганоперетворенні.

3. Отримані відповідності між формальними представленнями стійких СПр в областях перетворень ЦЗ й ПО. Показано, що стійкість СА, що забезпечується організацією СПр за рахунок збурення максимального СНЧ блоку ОП, може бути досягнута в частотній області за рахунок рівнозначного збурення dc-коефіцієнта ДКП, а в ПО — за рахунок однакового збурення яскравості пікселів блоку.

4. На основі отриманих відповідностей між збуреннями параметрів у різних областях зображення (просторовій, областях перетворення) отримана формальна достатня умова забезпечення стійкості СА до атак проти вбудованого повідомлення при організації стеганоперетворення в ПО контейнера-зображення. Ця умова дає можливість кількісної оцінки достатнього збурення яскравості пікселів блоку контейнера при СПр для забезпечення стійкості СА до передбачуваної збурної дії.

5. Отримана достатня умова забезпечує стійкість СА до атак проти вбудованого повідомлення незалежно від того, у якому форматі зберігається ЦЗ-контейнер (із втратами, без втрат), незалежно від конкретного виду збурної дії.

6. Отримані рекомендації з вибору розміру блоку контейнера, задіяного в стеганоперетворенні, як одного з параметрів, що визначають величину обчислювальної похибки в стеганоповідомленні. Для зменшення накопичення обчислювальної похибки при формуванні стеганоповідомлення відповідно до отриманої достатньої умови стійкості стеганоалгоритму, а також з врахуванням відповідності між величинами прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується, й розміром блоку l на цьому етапі дослідження рекомендовано $l = 8$.

Таким чином, задачі, поставлені в розділі 2, вирішені, мета розділу досягнута.

У розділі 2 вирішені задачі 2, 3 з переліку задач дисертаційної роботи. Основні результати даного розділу опубліковані в роботах [101,102,106-108].

РОЗДІЛ 3
РОЗРОБКА СТІЙКИХ ДО ЗБУРНИХ ДІЙ СТЕГАНОГРАФІЧНИХ МЕТОДА ТА АЛГОРИТМА, ЩО ДІЮТЬ У ПРОСТОРОВІЙ ОБЛАСТІ ЗОБРАЖЕННЯ

При розробці будь-якого стеганоалгоритму для прихованої передачі даних до нього висуваються певні вимоги, які вже були згадані в розділі 1: стійкості до різного роду збурних дій; стійкості до стеганоаналізу; забезпечення надійності сприйняття стеганоповідомлення; забезпечення достатньої прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується; забезпечення малої обчислювальної складності стеганоалгоритмів, а також контролю накопичення обчислювальної похибки при організації вбудови/декодування додаткової інформації.

Стійкість будь-якого стеганоалгоритма до збурних дій у роботі оцінюється стандартним чином за значенням коефіцієнта кореляції (NC) для вбудованої ДІ, який визначається відповідно до формули [38]:

$$NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p}_i'}{t}, \qquad (3.1)$$

де $p_1, p_2, ..., p_t$ — ДІ, що вбудовується в контейнер, $p_i \in \{0,1\}, i = \overline{1,t}$;

$\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$ — декодована ДІ, де $\overline{p}_i \in \{0,1\}, i = \overline{1,t}$;

$p_i' = 1, \overline{p}_i' = 1$, якщо $p_i = 1, \overline{p}_i = 1$;

$p_i' = -1, \overline{p}_i' = -1$, якщо $p_i = 0, \overline{p}_i = 0$.

Таким чином, значення $p_i' \times \overline{p}_i' \in \{1,-1\}$.

Спотворення контейнеру-зображення в результаті стеганоперетворення (збереження/незбереження надійності сприйняття стеганоповідомлення), збурення стеганоповідомлення в результаті атакуючих дій, і взагалі будь-які

спотворення ЦЗ в роботі будуть оцінюватися за допомогою значення *PSNR* — пікового відношення «сигнал–шум», що отримується в децибелах (dB) і є традиційним при оцінці спотворень ЦЗ [6]:

$$PSNR = 10 \cdot lg\left(255^2 \Big/ \left(\frac{1}{m^2} \sum_{i,j} \left(F(i,j) - (F + \Delta F)(i,j) \right)^2 \right) \right), \qquad (3.2)$$

де $F(i,j)$, $(F + \Delta F)(i,j)$, $i,j = \overline{1,m}$, — значення яскравості пікселів вхідного зображення з $m \times m$ – матрицею F і спотвореного з $m \times m$ – матрицею $F + \Delta F$ відповідно.

Необхідно відмітити, що оцінка візуального спотворення ЦЗ за допомогою *PSNR* в загальному випадку не завжди є придатною для оцінки надійності сприйняття СП у стеганографії, яка носить суб'єктивний характер [2,9]. Оскільки основною задачею будь-якого стеганометоду є збереження в секреті наявності прихованого каналу передачі інформації, що досягається, у тому числі, і за рахунок забезпечення надійності сприйняття СП, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги. У силу цього поряд з *PSNR* оцінка спотворень ЦЗ в роботі проводиться також шляхом суб'єктивного ранжирування.

Мала обчислювальна складність стеганоалгоритму має велике значення при організації процесу вбудови/декодування додаткової інформації в режимі реального часу. Прискорити процесс, враховуючи сучасний розвиток інформаційних технологій та комп’ютерної техніки, можливо за допомогою розпаралелювання відповідного стеганографічного алгоритму, яке можливо зробити лише за умови наявності в алгоритмі внутрішнього паралелизму [112,113,114]. Таким чином, відповідь на питання про те, чи присутній у тому чи іншому стеганоалгоритмі внутрішній паралелизм, є на сьогоднішній день важливою і своєчасною.

Звичайно, залежно від конкретної задачі й конкретних умов її рішення для використовуваного стеганоалгоритма деякі з вимог, перерахованих вище, можуть вважатися пріоритетними. Надзвичайно важливою у будь-яких умовах є вимога стійкості стеганоалгоритму до атак проти вбудованого повідомлення — збурних дій.

У зв'язку з вищевикладеним

Метою розділу є розробка стійких до збурних дій стеганометода й поліноміального стеганоалгоритма, що його реалізує, для організації прихованого каналу зв’язку, які діють в просторовій області зображення-контейнера, на основі отриманої в розділі 2 достатньої умови стійкості.

Серед збурних дій розглядаються найбільш часто використовувані атаки проти вбудованого повідомлення: накладання шуму на СП, фільтрація СП, атака стиском на СП.

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

1. Оцінити значення збурення $\left\|\Delta\overline{B}\right\|_2$ блоку стеганоповідомлення при різних очікуваних збурних діях, спрямованих на стеганоповідомлення, дослідити залежність $\left\|\Delta\overline{B}\right\|_2$ від розміру блоку l;
2. Визначити розмір блоків l, на які розбивається матриця основного повідомлення при поблоковому стеганоперетворенні, який, з врахуванням результатів рішення задачі 1, дозволить забезпечити: стійкість стеганоалгоритму до збурних дій; надійність сприйняття стеганоповідомлення; уникнути зменшення прихованої пропускної спроможності відповідного стеганографічного каналу зв'язку за рахунок величини l;
3. Визначити значення Δb елементів матриці збурення блоку контейнера в процесі стеганоперетворення з урахуванням обраного розміру блоку l і отриманої оцінки очікуваного збурення блоку стеганоповідомлення $\left\|\Delta\overline{B}\right\|_2$, що забезпечить стійкість стеганоалгоритму до збурних дій, надійність сприйняття стеганоповідомлення;

4. Використовуючи результати рішення задач 1–3, визначити параметри, що задіяні в розроблюваному стеганометоді і стеганоалгоритмі, що його реалізує, таким чином, щоб забезпечити стійкість до атак проти вбудованого повідомлення;
5. Оцінити обчислювальну складність розробленого стеганоалгоритму;
6. Дослідити розроблений стеганографічний алгоритм на наявність внутрішнього паралелізму.

3.1 Розробка стеганографічного методу, заснованого на достатній умові стійкості стеганоперетворення в просторовій області зображення-контейнера

Нехай F, $\overline{F}$ — $m \times m$ – матриці контейнера і стеганоповідомлення відповідно. У результаті пересилання й/або зберігання сформоване СП може зазнати збурень, після яких його матриця, у загальному випадку, буде відрізнятися від $\overline{F}$, а тому далі позначається $\overline{\overline{F}}$.

Для кольорового зображення його формальним представленням буде не одна, а три (чотири) матриці. Однак, з врахуванням того, що вбудова ДІ часто відбувається лише в одну матрицю ЦЗ (при моделі RGB — у синю складову, як правило [2,54,89]), представлення ОП, СП у вигляді однієї матриці ніяк не обмежує область застосування запропонованого нижче стеганометоду.

Припустимо, що оцінка $\left\|\Delta\overline{B}\right\|_2$ результату передбачуваної збурної дії на блок СП відома. Основні кроки пропонованого стеганометоду наступні [115].

Вбудова ДІ.

1. Матриця F ОП розбивається стандартним чином [55] на непересічні $l \times l$ – блоки. Кожний блок контейнера використовується для вбудови $k+1$ $(k \geq 0)$ біт ДІ.

2. (*Вбудова чергових біт ДІ в черговий блок контейнера*). Нехай B — черговий блок ОП, що використовується для СПр, а $p_i, ..., p_{i+k}$ — чергові біти ДІ. Вбудова ДІ проводиться шляхом збурення значень яскравості пікселів блоку

B на одне й те саме значення Δb, що задовольняє умові (2.24). Кількість різних варіантів коректування яскравості визначається кількістю S різних варіантів упорядкованих бінарних послідовностей $p_i,..., p_{i+k}$:

$$S = 2^{k+1}, \tag{3.3}$$

(наприклад, якщо в блок B контейнера вбудовується один біт додаткової інформації p_i ($k = 0$), то кількість різних варіантів бінарної послідовності, яка містить один елемент p_i, відповідно до (3.3) дорівнює 2. Таким чином, при стеганоперетворенні необхідно забезпечити два можливі варіанти коректування значень яскравості пікселів блоку B. Це можна зробити, наприклад, використовуючи як величини збурення $+\Delta b$, $-\Delta b$). Результат – блок $\overline{B}$ матриці $\overline{F}$ стеганоповідомлення.

Декодування ДІ.

1. Матриці F контейнера і $\overline{\overline{F}}$ можливо збуреного СП розбиваються на $l \times l$ – блоки. Кожний блок СП використовується для декодування $k+1$ ($k \geq 0$) біт ДІ.

2. Нехай $\overline{\overline{B}}$ — черговий блок СП, з якого декодуються біти $\overline{p}_i,..., \overline{p}_{i+k}$ ДІ, а B — відповідний йому блок ОП.

2.1. Визначити:

$$\Delta\overline{\overline{B}} = \overline{\overline{B}} - B.$$

2.2. Визначити по матриці $\Delta\overline{\overline{B}}$ значення Δb, відповідно до якого цілком декодувати бінарну послідовність $\overline{p}_i,..., \overline{p}_{i+k}$.

Конкретний спосіб реалізації кроків 2 при вбудові й декодуванні ДІ буде визначати конкретний стеганоалгоритм, що реалізує метод.

Ключовим моментом у запропонованому стеганометоді є оцінка значення $\left\|\Delta\overline{B}\right\|_2$ передбачуваної збурної дії.

3.2 Розробка стеганографічного алгоритму, що реалізує запропонований стеганометод

Метою підрозділу є розробка стеганоалгоритму, що реалізує запропонований вище метод, і задовольняє наступним вимогам:

— є стійким до атак (найпоширеніших) проти вбудованого повідомлення;

— забезпечує надійність сприйняття СП;

— є поліноміальним.

Оскільки теоретичною основою розроблюваного СА є отримана достатня умова стійкості до збурних дій, то відповідно до зауважень 2.2, 2.3, характеристика стійкості алгоритму (коефіцієнт NC) буде залежати не від виду збурної дії (накладання шуму, фільтрація СП і т.д.), якій піддається стеганоповідомлення, а визначатися, головним чином, величиною збурної дії, що зазнає матриця стеганоповідомлення під час атаки; крім того, характеристики алгоритму не будуть залежати від формату (з втратами, без втрат) використовуваного зображення-контейнера.

В позначеннях попереднього підрозділу основні кроки алгоритму, що реалізує запропонований метод (для $k = 0$), який будемо далі називати базовим і позначати SA_B, виглядають наступним чином [116,117,118].

Вбудова ДІ.

1. Матриця F ЦЗ-контейнера розбивається стандартним чином на непересічні $l \times l$ – блоки.

2. (*Вбудова ДІ – реалізація двох різних варіантів коректування значень яскравості пікселів блоку* B). Нехай B — черговий блок ОП, що використовується для СПр, а p_i — черговий біт ДІ, $\overline{B}$ — відповідний блок стеганоповідомлення.

Якщо

$$p_i = 1$$

то

$$\overline{B} = B + \Delta b \cdot \overline{E} \qquad (3.4)$$

інакше

$$\overline{B} = B - \Delta b \cdot \overline{E} \qquad (3.5)$$

де $\overline{E}$ — $l \times l$ – матриця, всі елементи якої дорівнюють 1, $\Delta b > 0$ задовольняє (2.24).

Декодування ДІ

1. Матриці F контейнера і $\overline{\overline{F}}$ можливо збуреного СП розбиваються стандартним чином на неперетинні $l \times l$ – блоки. Кожний блок СП використовується для декодування 1 біта ДІ.

2. Нехай $\overline{\overline{B}}$ — черговий блок СП, з якого декодується біт $\overline{p}_i$ ДІ, а B — відповідний йому блок ОП.

2.1. Визначити:

$$\Delta\overline{\overline{B}} = \overline{\overline{B}} - B. \qquad (3.6)$$

2.2. Визначити кількості додатних k_p і від'ємних k_n елементів в матриці $\Delta\overline{\overline{B}}$.

якщо

$$k_p > k_n,$$

то

$$\overline{p}_i = 1,$$

інакше

$$\overline{p}_i = 0.$$

Зауваження 3.1. Реалізація процесів СПр і декодування в SA_B відбувається в припущенні, що формальним представленням ЦЗ-контейнера є одна матриця

(що має місце в випадку зображення в градаціях сірого). Це ніяк не обмежує область застосування розробленого алгоритму: якщо як ОП використовується кольорове зображення, то алгоритм, по-перше, може застосовуватися для вбудови ДІ лише в одну із множини матриць, що використовуються для представлення ЦЗ (як вже було зазначено для розробленого вище методу); по-друге, він може застосовуватися для кожної з матриць окремо.

Зауваження 3.2. На даному етапі роботи в стеганоалгоритмі SA_B залишається невизначеним параметр l — розмір блоку зображення, Δb — значення збурення яскравості пікселів блоку при стеганоперетворенні. Ці параметри повинні забезпечувати високу ефективність роботи стеганоалгоритму незалежно від конкретики збурної дії, якій піддається стеганоповідомлення. Завдяки цьому визначення l, Δb буде остаточно проведене після аналізу передбачуваних атак на вбудоване повідомлення, який (аналіз), у свою чергу не міг би бути проведеним без уточнення кроків, виконуваних при вбудові/декодуванні ДІ, тобто вимагає їхньої конкретизації (розробки алгоритму, що реалізує запропонований метод) вже на цьому етапі роботи.

Зауваження 3.3. При розробці стеганоалгоритму реалізація двох різних варіантів коректування значень яскравості пікселів блоку B при СПр може бути реалізована шляхом тільки збільшення/зменшення значень яскравості. У цьому випадку для організації декодування ДІ значення Δb_1 і Δb_2 — двох варіантів коректування повинні задовольняти співвідношенням:

$$\begin{cases} |\Delta b_1| \geq |\Delta b|, \\ |\Delta b_1 - \Delta b_2| \geq |\Delta b| \end{cases},$$

де Δb визначається відповідно до (2.24).

Зауваження 3.4. Обчислювальна складність стеганоалгоритму SA_B визначається кількістю блоків, на які розбивається матриця контейнера/стеганоновідомлення, і становить

$$\left[\frac{m}{l}\right]\left[\frac{m}{l}\right] = \underline{O}\left(m^2\right)$$

операцій.

З врахуванням специфіки організації стеганоперетворення і декодування ДІ в SA_B для нього має місце наступне твердження.

Твердження 3.1. Для того, щоб атака на стеганоповідомлення, що сформоване стеганоалгоритмом SA_B, спрямована проти вбудованого повідомлення, виявилася неефективною (тобто щоб в умовах атаки можливо було декодування всієї вбудованої ДІ ($NC = 1$)) необхідно й достатньо, щоб у результаті цієї атаки зміна знаків елементів матриці $\Delta\overline{\overline{B}}$ відносно матриці $\Delta B = \Delta b \cdot \overline{E}$ торкнулася не більше, ніж s елементів у межах кожного блоку матриці стеганоповідомлення, де

$$s = \begin{cases} \left[l^2/2\right] - 1, \textit{ якщо } l - \textit{парне} \\ \left[l^2/2\right], \textit{ якщо } l - \textit{непарне} \end{cases}$$

де $[\bullet]$ — ціла частина аргументу.

Ключовим моментом у запропонованому стеганоалгоритмі SA_B залишається оцінка значення $\left\|\Delta\overline{B}\right\|_2$ передбачуваної збурної дії для визначення Δb відповідно до (2.24).

Виконання всіх висунутих до алгоритму вимог з врахування встановленого нижче значення l буде перевірено в розділі 4.

3.3 Визначення величини збурення яскравості пікселів при стеганоперетворенні, що забезпечує стійкість стеганоалгоритма SA_B

3.3.1 Оцінка величини збурної дії на стеганоповідомлення, що є накладанням шуму. Як збурну дію для визначення значення Δb збурення яскравості пікселів при стеганоперетворенні в алгоритмі SA_B розглянемо спочатку накладання різних шумів з різними параметрами на цифрове зображення.

Найбільш часто використовуваними шумами, що накладаються на ЦЗ при моделюванні атакуючих дій, як свідчать відкриті джерела [17,40,119], є гауссівський та мультиплікативний. На деякі шуми, наприклад, «сіль–перець», зображення дуже сильно реагує наочним спотворенням, тому такі шуми, враховуючи специфіку задачі, що розглядається, досліджуватися не будуть. Крім гауссівського та мультиплікативного розгянемо ще один тип шуму, який є поширеним – пуассонівський.

Метою підрозділу є оцінка збурень блоку зображення (величини $\left\|\Delta\overline{B}\right\|_2$), які виникають внаслідок накладання на цифрове зображення різних шумів з урахуванням параметрів (зокрема розміру блоку l) стеганоперетворення для подальшого визначення Δb.

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

1. Отримати оцінки значень $\left\|\Delta\overline{B}\right\|_2$ матриці збурення блоку зображення при накладанні на ЦЗ: гауссівського, мультиплікативного, пуассонівського шумів для різних розмірів блоку l;
2. Дослідити залежність $\left\|\Delta\overline{B}\right\|_2$ від розміру блоку l;
3. З урахуванням рішень задач 1, 2 визначити можливі значення Δb коректування яскравості пікселів блоку при стеганоперетворенні для різних l відповідно до (2.24);
4. Отримати рекомендації для розміру блоку l при організації стеганоперетворення відповідно до алгоритму SA_B.

Як вже згадувалося, оцінка значення $\left\|\Delta\overline{B}\right\|_2$ передбачуваної збурної дії, у якості якої зараз розглядається накладання шуму, є важливою кількісною характеристикою у запропонованому стеганографічному методі, алгоритмі SA_B.

Для рішення цієї задачі був проведений обчислювальний експеримент [115], у якому було задіяно 300 кольорових цифрових зображень (модель RGB) у форматах як з втратами (Jpeg), так і без втрат (Tif) з бази NRCS [120], яка є традиційною при тестуванні алгоритмів, що працюють з ЦЗ, а також зображення, отримані непрофесійними фотографами.

В ході експерименту на ЦЗ накладалися різні шуми (гауссівський, мультиплікативний, пуассонівський) з різними параметрами (варіанти значень параметрів шумів підбиралися, по можливості, так, щоб накладання шуму зберігало/не зберігало надійність сприйняття цифрового зображення), після чого зображення аналізувалося. Для цього одна з колірних матриць зашумленого ЦЗ й відповідна матриця вхідного зображення аналогічним чином розбивалися на $l\times l-$блоки ($l\in\{4,8,10,12\}$), для кожного з яких визначалася спектральна норма матриці збурення $\left\|\Delta\overline{B}\right\|_2$, що відбулося в результаті накладання шуму. Для кожного $i-$го ЦЗ, $i=\overline{1,300}$, для аналізованої колірної матриці обчислювалися: максимальне $M^{(i)}$, мінімальне $m^{(i)}$, середнє $S^{(i)}$ значення $\left\|\Delta\overline{B}\right\|_2$ по всім блокам, а також значення $PSNR$. Потім по всім зображенням обчислювалися середні значення $M^{(i)}$, $m^{(i)}$, $S^{(i)}$ і $PSNR$, що позначаються відповідно: M_c, m_c, S_c і $PSNR_c$. Результати експерименту відображені в табл.3.1 – 3.3 для гауссівського, мультиплікативного й пуассонівського шумів відповідно.

Таблиця 3.1 — Результати накладання на ЦЗ гауссівського шуму з нульовим математичним очікуванням

Дисперсія	l	Середні знач-я по всім протестованим цифровим зображенням				Збереження надійності сприйняття
		M_c	m_c	S_c	$PSNR_c$ (dB)	
$D = 0.001$	4	46	4	24	30	–
	8	58	21	39		
	10	63	23	44		
	12	67	32	49		
$D = 0.0001$	4	15	2	8	40	+
	8	19	7	13		
	10	20	8	14		
	12	22	11	16		
$D = 0.0005$	4	35	3	18	33	±
	8	41	15	27		
	10	45	18	31		
	12	48	23	35		

Оскільки, як було зазначено вище, оцінка візуального спотворення цифрового зображення за допомогою *PSNR* в загальному випадку не завжди є придатною для оцінки надійності сприйняття стеганоповідомлення у стеганографії, поряд з *PSNR* оцінка спотворень зображень в роботі проводиться також шляхом суб'єктивного ранжирування, відображенням якого є останні стовпці таблиць 3.1–3.3.

У ході обчислювального експерименту фіксувалися максимальні значення $\left\|\Delta\overline{B}\right\|_2$ при кожному розмірі l блоку для кожного виду розглянутого шуму. Результати знайшли своє відображення на графіках, представлених на рис.3.1.

Таблиця 3.2 — Результати накладання на цифрове зображення мультиплікативного шуму

Дисперсія	l	Середні знач-я по всім протестованим цифровим зображенням				Збереження надійності сприйняття
		M_c	m_c	S_c	$PSNR_c$ (dB)	
$v = 0.00005$	4	8	1	2	49	+
	8	10	1	4		
	10	12	2	5		
	12	13	3	6		
$v = 0.0001$	4	11	1	3	46	±
	8	15	2	6		
	10	17	2	7		
	12	18	3	8		
$v = 0.001$	4	35	2	9	37	–
	8	42	4	15		
	10	53	4	17		
	12	57	5	21		

Таблиця 3.3 — Результати накладання на цифрове зображення пуассонівського шуму

l	Середні знач-я по всім протестованим цифровим зображенням				Збереження надійності сприйняття
	M_c	m_c	S_c	$PSNR_c$ (dB)	
4	78	4	26	28	–
8	95	14	42		
10	102	16	47		
12	111	19	54		

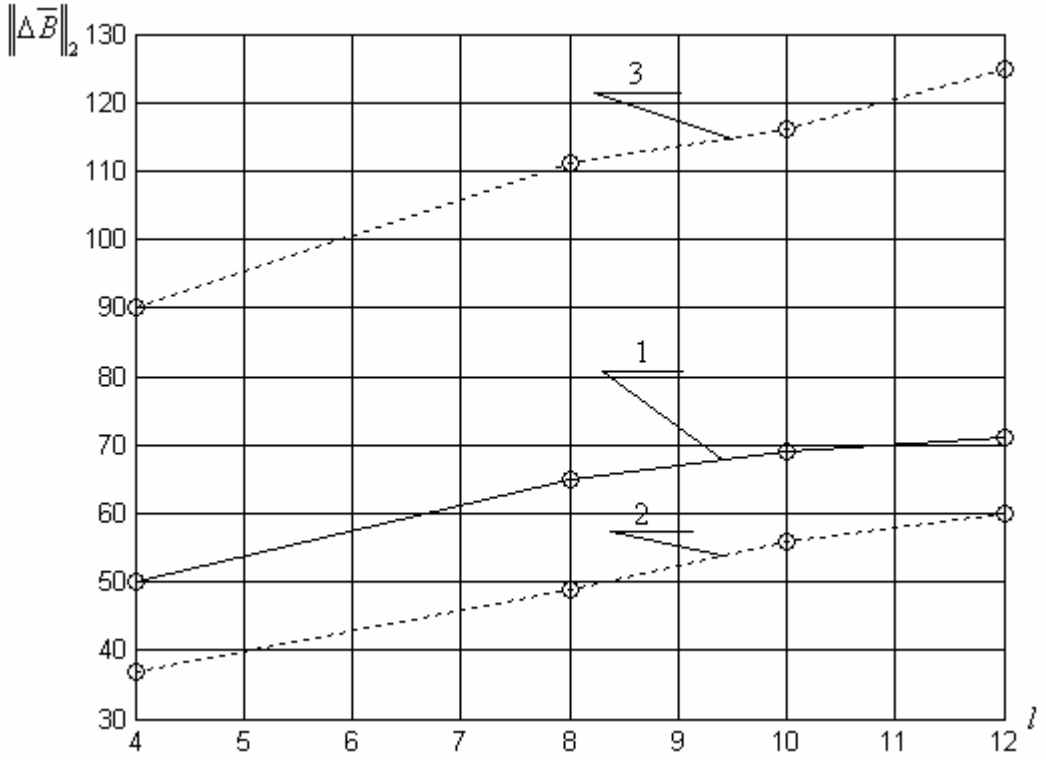


Рисунок 3.1 — Залежність максимального значення $\|\Delta\overline{B}\|_2$, що мало місце в експерименті, від l при різних шумах: 1 – гауссівський; 2 – мультиплікативний; 3 – пуассонівський шум

Аналіз отриманих результатів (табл.3.1–3.3, рис.3.1), на перший погляд, говорять про перевагу блоків малого розміру l для організації СПр, оскільки $\|\Delta\overline{B}\|_2$ для таких блоків має найменше значення. Однак, з врахуванням (2.24), для стійкості запропонованого стеганометоду і стеганоалгоритму до накладання гауссівського/мультиплікативного/пуассонівського шуму з розглянутими варіантами параметрів при $l \in \{4,8,10,12\}$ має сенс брати $|\Delta b|$, які задовольняють умовам, представленим в таблиці 3.4, тобто, наприклад, ті значення, які відображені на рис.3.2, що, враховуючи необхідність збереження надійності сприйняття СП (зацікавленість в можливості зменшення значення $|\Delta b|$), а також результати, що відображені на рис.2.6 і обговорювалися в розділі 2, надає переваги блокам більшого розміру.

Таблиця 3.4 — Значення $|\Delta b|$, що пропонуються для стійкості стеганоалгоритму до накладання шумів з розглянутими варіантами параметрів

Шум / l	гауссівський	мультиплікативний	пуассонівський
4	$\|\Delta b\| > 50/4$	$\|\Delta b\| > 37/4$	$\|\Delta b\| > 37/4$
8	$\|\Delta b\| > 65/8$	$\|\Delta b\| > 49/8$	$\|\Delta b\| > 111/8$
10	$\|\Delta b\| > 69/10$	$\|\Delta b\| > 56/10$	$\|\Delta b\| > 116/10$
12	$\|\Delta b\| > 71/12$	$\|\Delta b\| > 60/12$	$\|\Delta b\| > 125/12$

Однак, збільшення розміру блоку приведе до зменшення прихованої пропускної спроможності стеганографічного каналу зв'язку, що відповідно з вимогою 4 до стеганографічного алгоритму (розділ 1) є небажаним. Таким чином, з врахуванням усього вищесказаного можна зробити висновок, що компромісними варіантами розміру блоку l тут є величини 8,10 [115].

Треба зазначити, що основну увагу при аналізі результатів дослідження треба приділити гауссівському шуму, оскільки саме він найчастіше в наукових статтях виступає як модель атакуючої дії на стеганоповідомлення [17,40]. Для гауссівського шуму при $l = 8$ значення $\Delta b = 9$, а при $l = 10$ значення $\Delta b = 7$ (рис.3.2). Збільшення розміру блоку дозволило зменшити величину збурної дії для кожного пікселя блоку на 22%, але ж зменшилася й прихована пропускна спроможність: з $1/64$ біт/піксель (для $l = 8$) до $1/100$ біт/піксель (для $l = 10$), тобто на 36%. Таким чином, на цьому етапі дослідження рекомендованими значеннями параметрів стеганографічного алгоритму SA_B є: $l = 8$, $\Delta b = 9$.

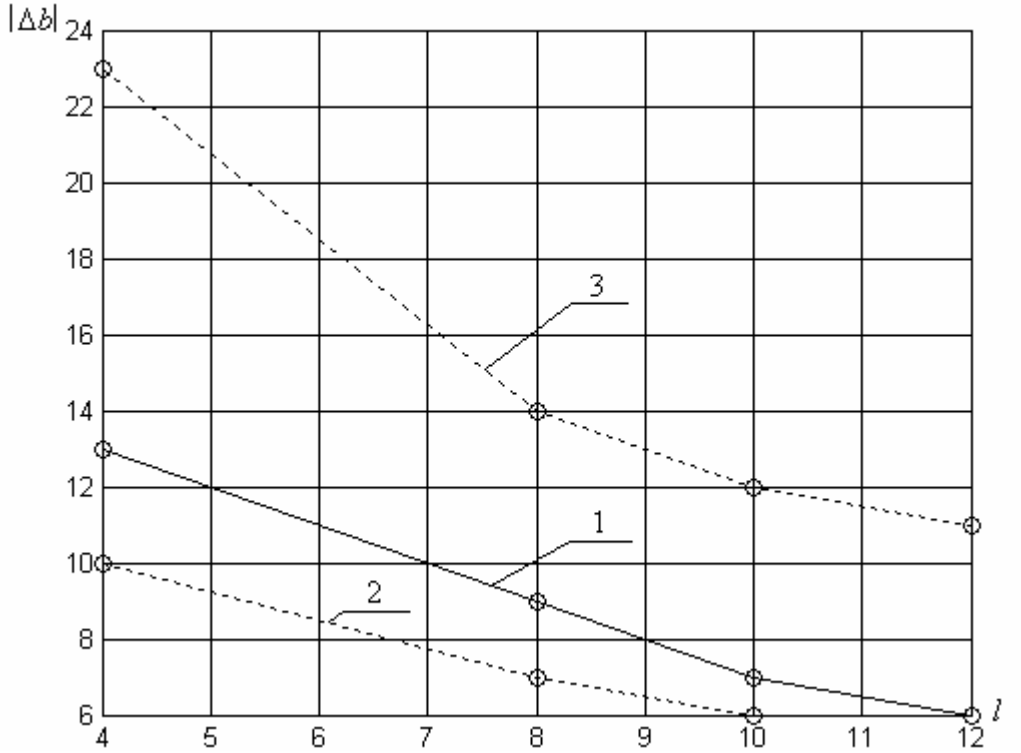


Рисунок 3.2 — Залежність пропонованих значень Δb від l при різних шумах: 1 – гауссівський; 2 – мультиплікативний; 3 – пуассонівський шум

3.3.2 Оцінка збурної дії при фільтрації стеганоповідомлення. Оскільки стеганоперетворення й декодування ДІ в розробленому стеганоалгоритмі відбувається в просторовій області контейнера-зображення, то й аналіз результатів усіх збурних дій доцільно проводити також у просторовій області (звичайно, якщо така можливість є, і вона є ефективною). Це дасть можливість уникнути небажаного накопичення обчислювальної похибки й зайвих обчислювальних витрат, пов'язаних з переходом в область перетворення зображення.

Як свідчать відкриті джерела, найбільш часто використовуваними видами просторових фільтрів при моделюванні атаки на стеганоповідомлення є: лінійні фільтри — прямокутний усереднюючий, низькочастотний гауссов [121,37,66]; нелінійний — медіанний фільтр [56,89].

Розглянемо послідовно кожний з них [122,124].

Процес лінійної просторової фільтрації полягає в переміщенні центру фільтруючої маски h, де h — $p \times n$-матриця коефіцієнтів, від пікселя до пікселя

ЦЗ з матрицею F. В кожному пікселі (i, j) відгуком фільтра є сума добутків коефіцієнтів фільтра й відповідних значень яскравості пікселів околу, які накриваються h. Найбільш часто використовуються фільтри, для яких p,n — непарні, оскільки в цьому випадку в маски є виражена центральна точка [55], тому скрізь нижче в роботі p,n беруться непарними.

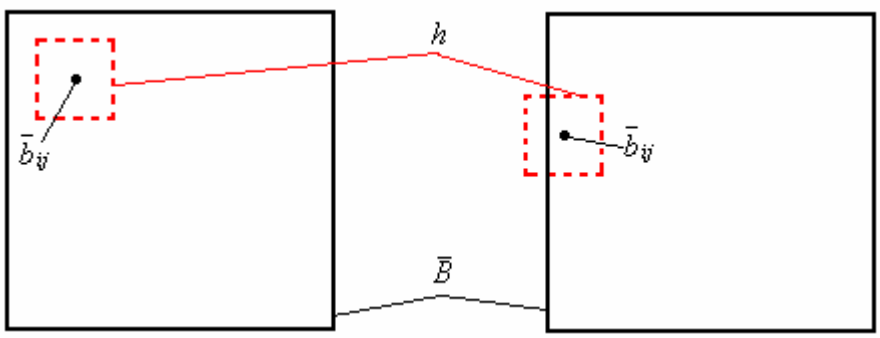
Розглянемо, з врахуванням твердження 3.1, прямокутний усереднюючий фільтр з квадратною $p\times p-$маскою $h=\frac{1}{p^2}\overline{E}$, де $\overline{E}$ — $p\times p-$ матриця, усі елементи якої дорівнюють 1. У процесі стеганоперетворення відповідно до алгоритму SA_B елементи b_{ij} $l\times l-$блоку B отримають приріст $\pm\Delta b$ (додатний або від'ємний, залежно від вбудовуваного біта додаткової інформації). Нехай для визначеності й спрощення подальшого викладу приріст додатний, елементи блоку $\overline{B}$ стегоноповідомлення — $\overline{b}_{ij}=b_{ij}+\Delta b$, $\Delta b>0$. Якщо елемент $b_{ij}+\Delta b$ блоку $\overline{B}$ розташований при фільтрації так, як показано на рис.3.3(а), то його нове значення $\overline{\overline{b}}_{ij}$ (елемент блоку $\overline{\overline{B}}$ збуреного фільтрацією стеганоповідомлення) буде дорівнювати:

$$\overline{\overline{b}}_{ij}=\frac{\sum\limits_{x=-\left[\frac{p}{2}\right]}^{\left[\frac{p}{2}\right]}\sum\limits_{y=-\left[\frac{p}{2}\right]}^{\left[\frac{p}{2}\right]}\left(b_{i+x,j+y}+\Delta b\right)}{p^2}=\frac{\sum\limits_{x=-\left[\frac{p}{2}\right]}^{\left[\frac{p}{2}\right]}\sum\limits_{y=-\left[\frac{p}{2}\right]}^{\left[\frac{p}{2}\right]}b_{i+x,j+y}}{p^2}+\Delta b. \qquad (3.7)$$

У чисельнику в правій частині формули (3.7) знаходиться середнє арифметичне значень яскравості пікселів блоку основного повідомлення, покритих маскою. У силу коррельованості значень яскравості сусідніх пікселів в оригінальному ЦЗ [55], можна стверджувати, що b_{ij} близько за значенням до значень $b_{i+x,j+y}$, $x,y=-\left[\frac{p}{2}\right],...,0,...,\left[\frac{p}{2}\right]$, коли p невелике: $p=3{,}5$, тобто

$$\overline{\overline{b}}_{ij} = \frac{\sum_{x=-\left[\frac{p}{2}\right]}^{\left[\frac{p}{2}\right]} \sum_{y=-\left[\frac{p}{2}\right]}^{\left[\frac{p}{2}\right]} b_{i+x,j+y}}{p^2} + \Delta b \approx b_{ij} + \Delta b. \qquad (3.8)$$

Формула (3.8) говорить про те, що при фільтрації усереднюючим фільтром з маскою незначних розмірів елементи матриці $\Delta\overline{\overline{B}}$ (3.6), що знаходяться у положенні, зазначеному на рис.3.3(а), не змінять знаки щодо елементів ΔB.



а б

Рисунок 3.3 — Можливі розташування маски фільтра h відносно блоку $\overline{B}$ стеганоповідомлення

Принципово можлива (хоча необов'язково) зміна знаків для елементів $\Delta\overline{\overline{B}}$ щодо елементів ΔB, що відповідають в блоці $\overline{\overline{B}}$ позиціям, зображеним на рис.3.3(б), коли частина маски виходить за межі $\overline{\overline{B}}$. Це елементи, що відстоять від границі блоку на відстань, меншу за $[p/2]$. Кількість таких елементів визначається відповідно до формули, яка доводиться методом математичної індукції:

$$4 \cdot \sum_{x=1}^{\left[\frac{p}{2}\right]} (l - 2(x-1) - 1). \qquad (3.9)$$

Тоді кількість елементів, що займають в $\overline{\overline{B}}$ положення рис.3.3(а) буде визначатися як:

$$l^2 - 4 \cdot \sum_{x=1}^{\left\lceil \frac{p}{2} \right\rceil} (l - 2(x-1) - 1). \qquad (3.10)$$

Тоді з врахуванням (3.9), (3.10) і твердження 3.1 для гарантованого забезпечення ефективної роботи стеганоалгоритму SA_B ($NC \approx 1$) в умовах атаки фільтрацією із прямокутним усереднюючим фільтром розміри l і p повинні забезпечувати виконання нерівності:

$$l^2 - 4 \cdot \sum_{x=1}^{\left\lceil \frac{p}{2} \right\rceil} (l - 2(x-1) - 1) > 4 \cdot \sum_{x=1}^{\left\lceil \frac{p}{2} \right\rceil} (l - 2(x-1) - 1),$$

звідки

$$l^2 - 8 \cdot \sum_{x=1}^{\left\lceil \frac{p}{2} \right\rceil} (l - 2(x-1) - 1) > 0. \qquad (3.11)$$

Співвідношення (3.11) дає кількісну відповідність між розмірами l (блоку основного повідомлення при стеганоперетворенні) і p (маски усереднюючого фільтру), що забезпечує високу ($NC \approx 1$) ефективність розробленого стеганоалгоритму SA_B (табл.3.5) [122].

Таблиця 3.5 — Відповідність між розміром l блоку ЦЗ, що використовується при стеганоперетворенні, і розміром p квадратної маски усереднюючого фільтра, що забезпечує стійкість ($NC \approx 1$) стеганоалгоритма SA_B

l	8	16	32
p	3	3; 5	3; 5; 7; 9

Розглянемо докладно процес просторової фільтрації з одним з найбільш часто використовуваних лінійних фільтрів — гауссовим фільтром. Матриця h гауссова фільтра для чергового елемента (i, j) при будь-яких лінійних розмірах у центрі має найбільше значення, тим самим даючи «вагову перевагу» при

побудові відгуку самому значенню (i, j). Всі інші елементи h, як мінімум, на порядок менші за значенням центрального елемента, що приводить до несуттєвості внеску відповідних значень яскравості сусідніх з (i, j) пікселів у значення відгуку. Для наочної ілюстрації сказаного нижче наведені приклади для $p \times p -$матриць h при $p = 3,5$ відповідно зі стандартним (додатним) відхиленням $sig = 0.5$ [123]:

$$h = \begin{pmatrix} 0.0113 & 0.0838 & 0.0113 \\ 0.0838 & 0.6193 & 0.0838 \\ 0.0113 & 0.0838 & 0.0113 \end{pmatrix}; \quad h = \begin{pmatrix} 0.0000 & 0.0000 & 0.0002 & 0.0000 & 0.0000 \\ 0.0000 & 0.0113 & 0.0837 & 0.0113 & 0.0000 \\ 0.0002 & 0.0837 & 0.6187 & 0.0837 & 0.0002 \\ 0.0000 & 0.0113 & 0.0837 & 0.0113 & 0.0000 \\ 0.0000 & 0.0000 & 0.0002 & 0.0000 & 0.0000 \end{pmatrix}.$$

У зв'язку з вищесказаним можна зробити наступний висновок: гауссова фільтрація в переважній більшості елементів матриці $\Delta\overline{\overline{B}}$ не приведе до зміни знаків щодо елементів ΔB (незалежно від розміру блоку l), а тому повинна забезпечити високу ефективність розробленого стеганоалгоритма незалежно від розміру маски.

Найвідомішим нелінійним фільтром у цифровій обробці зображень є медіанний фільтр [55], який замінює значення пікселя на значення медіани розподілу яскравостей усіх пікселів в околі, включаючи й поданий. Враховуючи коррельованість значень яскравості сусідніх пікселів, яка вже згадувалася вище, можна стверджувати, що для маски малих розмірів значення яскравостей усіх пікселів, що покриваються нею, будуть близькими, а тому вибір середнього з них значення замість пікселя (i, j) не зможе змінити його значно, а це означає, що в такому випадку такі зміни не зможуть привести до змін знаків елементів $\Delta\overline{\overline{B}}$ відносно елементів ΔB у переважній більшості пікселів, що забезпечить в умовах такої фільтрації стеганоповідомлення високу ефективність ($NC \approx 1$). Зі збільшенням розмірів маски значення NC будуть

зменьшуватися, оскільки зі збільшенням відстані між пікселями коррельованість їх значень слабшає.

Таким чином, для забезпечення стійкості стеганоалгоритму SA_B до атаки фільтрацією з відомими/передбачуваними параметрами рекомендується використовувати розмір блоку l відповідно до даних, наведених у табл.3.5 [122,124].

3.3.3 Атака стиском на стеганоповідомлення. Розглянемо як збурну дію атаку стиском на стеганоповідомлення, яка є надзвичайно розповсюдженою завдяки популярності використання форматів із втратами для зберігання й передачі цифрових контентів (зокрема, ЦЗ), а тому не привертає до себе уваги. Більше того, можна сказати, що додаткову увагу в сучасному мультимедійному просторі привертає пересилання ЦЗ, цифрового відео у форматах без втрат. У силу цього для додаткової прихованості стеганографічного каналу зв'язку, що організується, доцільним сьогодні є використання стеганоалгоритмів, необхідно стійких до стиску, що дають можливість ще на етапі формування стеганоповідомлення зберігати його у форматі із втратами.

Величина розміру блока l є суттєвою при організації стеганоперетворення розробленими стеганометодом і відповідним стеганоалгоритмом. Розроблюваний алгоритм націлений на стійкість до стиску із втратами. Найпоширенішим форматом із втратами на сьогоднішній день є Jpeg, менш розповсюдженим, але також використовуваним — формат Jpeg2000. І в тому, і в іншому випадку в процесі стиску ЦЗ розбивається на блоки розміру 8×8 [55]. У силу цього для можливості найбільш ретельного контролю й аналізу змін яскравості пікселів, що відбуваються в процесі стиску стеганоповідомлення, для забезпечення стійкості до стиску розробленого стеганоалгоритма доцільно в SA_B покласти $l = 8$ [117].

В [62] була отримана оцінка величини збурної дії блоку при стиску ЦЗ з коефіцієнтами якості $QF \geq 60$: $\left\|\Delta\overline{B}\right\|_2 < 72$. Використання цього результату з

врахуванням (2.24) визначає значення $\Delta b = 9$ для SA_B, яке повинне гарантувати високу ефективність розроблюваного алгоритму в умовах атаки стиском.

Таким чином, враховуючи результати досліджень, отримані в підрозділах 3.3.1 – 3.3.3, для одночасного забезпечення стійкості SA_B до атак проти вбудованого повідомлення: накладанню шумів, фільтрації, атаки стиском рекомендується в розробленому стеганоалгоритмі використовувати $l = 8$, $\Delta b = 9$. Висока стійкість стеганоалгоритма SA_B в умовах атакуючих дій буде практично підтверджена в розділі 4.

3.4 Аналіз внутрішнього паралелізму розробленого стеганографічного алгоритму

Однією з можливих форм запису алгоритмів, зручною для аналізу на наявність у них внутрішнього паралелізму, є їх представлення у вигляді графів, зокрема, графів інформаційної залежності реалізації алгоритму [112,113], які нижче для зручності називаються графами алгоритмів.

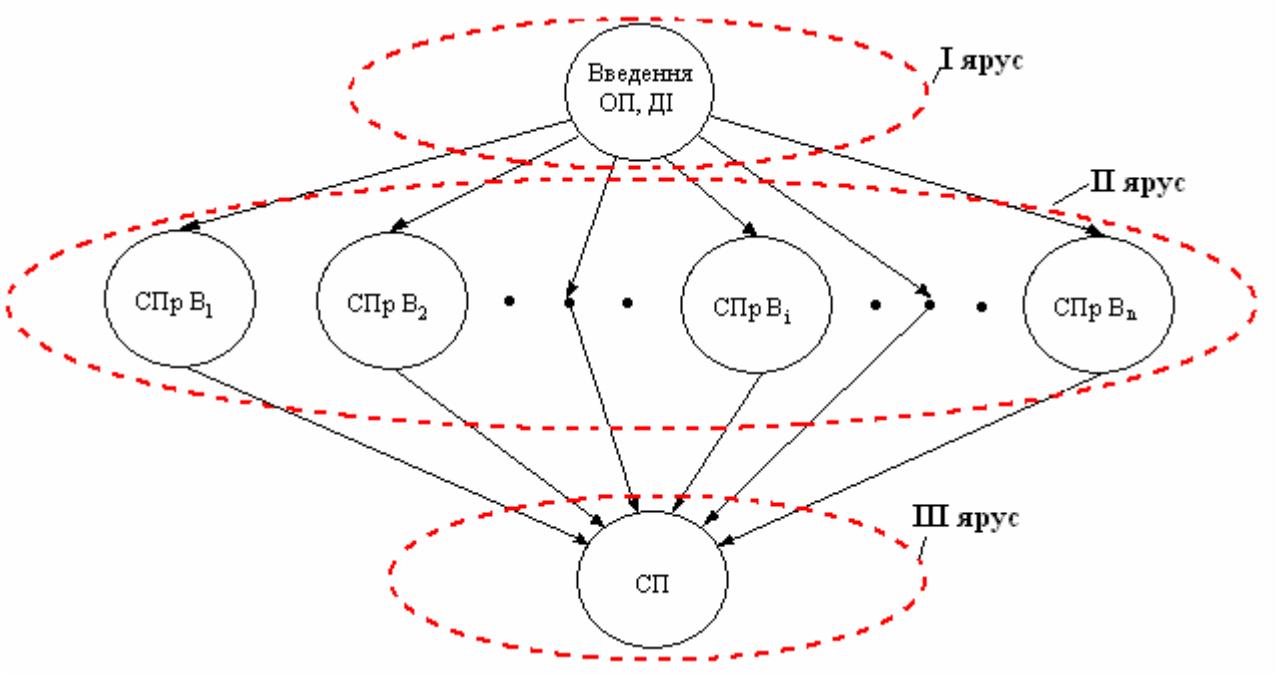
Множині операцій алгоритму, що реально виконуються при заданих вхідних даних, ставиться у взаємно однозначну відповідність множина вершин графа. Якщо аргумент однієї операції є результатом виконання іншої операції, то відповідні вершини утворюють ребро, спрямоване з тієї вершини, звідки береться результат. Необхідно відзначити, що з метою зменшення розмірів графа алгоритму, спрощення процедури його аналізу часто вершина графа відповідає не одній, а множині виконуваних операцій алгоритму, називаючись при цьому макровершиною.

Граф алгоритму $G(V,E)$, де V — множина вершин графа, а E — множина його ребер, визначає всю сукупність можливих реалізацій алгоритму, показуючи, як при цих реалізаціях відбувається поширення інформації.

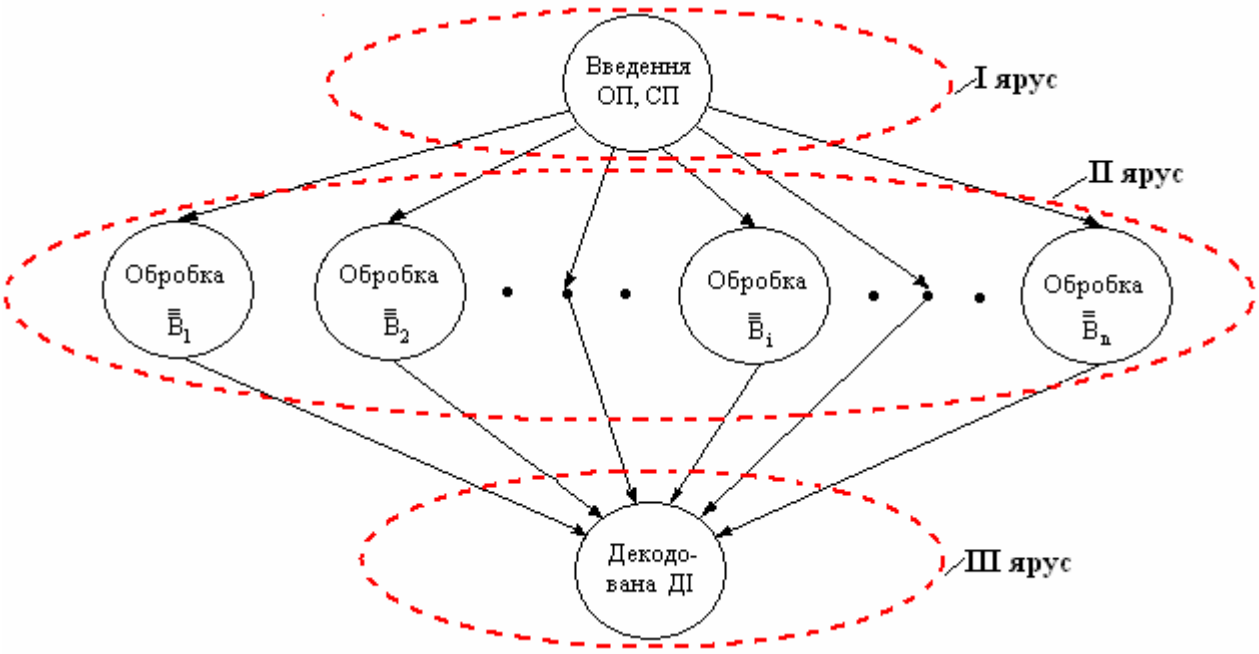
Реалізація алгоритму породжує певну розбивку його операцій на групи, які виконуються послідовно, а операції усередині кожної групи

можуть виконуватися паралельно (одночасно). Розбивка операцій алгоритму породжує відповідну розбивку вершин графа алгоритму (що називається топологічним сортуванням, або паралельною формою) і навпаки.

Для аналізу внутрішнього паралелізму розробленого теганографічного алгоритму SA_B побудуємо його граф, враховуючи логіку роботи алгоритму, а також для зручності дослідження розглянемо окремо графи, що відповідають логічним складовим частинам алгоритму: процесам вбудови ДІ і її декодування [114]. Загальні види таких графів — макрографи [112,113] представлені на рис.3.4, де макровершини, що є результатами гомоморфних згорток [112] підграфів, що відповідають операціям обробки окремих блоків $B_1, B_2, ..., B_n$ основного повідомлення при стеганоперетвореннi і блоків $\overline{\overline{B}}_1, \overline{\overline{B}}_2, ..., \overline{\overline{B}}_n$ стеганоповідомлення при виділенні додаткової інформації з можливо збуреного стеганоповідомлення, де $n = \left[\frac{m}{8}\right]\left[\frac{m}{8}\right]$, належать одному ярусу топологічного сортування [112,113] (на рис.3.4 ці яруси виділені штриховою лінією), тобто є інформаційно незалежними, а тому можуть виконуватися одночасно, або паралельно. Таким чином, вже на етапі аналізу макрографів можна стверджувати, що розроблений стеганоалгоритм SA_B має внутрішній паралелізм як у частині стеганоперетворення, так і в частині декодування ДІ. Однак, оскільки в загальному випадку топологічне сортування макрографа (який є результатом гомоморфної згортки графа алгоритму) породжує лише узагальнене топологічне сортування [112,113] вхідного графа алгоритму, розглянемо підграфи вхідного графа, що відповідають макровершинам макрографа, докладно з метою виявлення внутрішнього паралелізму й у цих частинах алгоритму [114].



а



б

Рисунок 3.4 — Паралельна форма макрографів складових частин розробленого стеганоалгоритму: а – процес стеганоперетворення; б – процес декодування додаткової інформації зі стеганоповідомлення

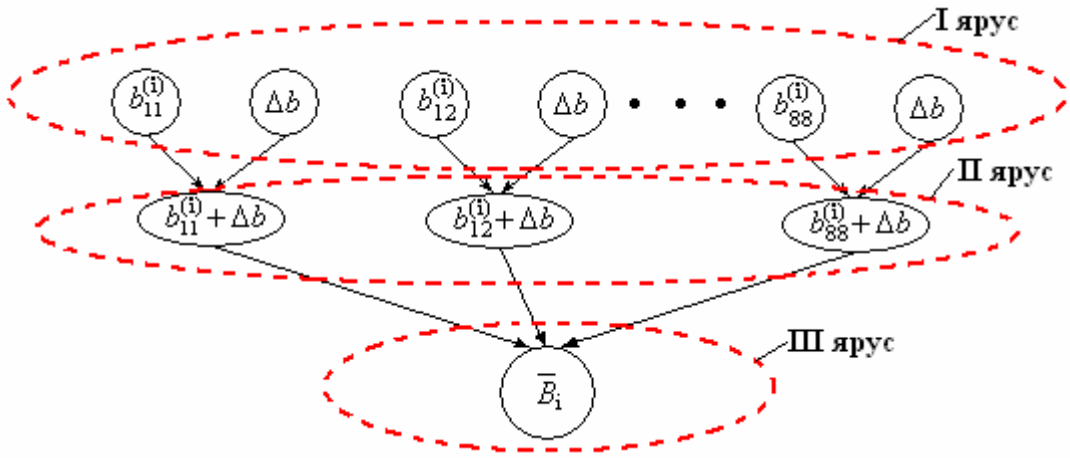
Оскільки як етап вбудови, так і етап декодування додаткової інформації містить умовні оператори, то розробленому стеганографічному алгоритму SA_B буде відповідати сімейство «схожих» графів [112-114].

Для кожного окремо взятого блоку $B_i, i=\overline{1,n}$, з елементами $b_{kp}^{(i)}, k, p=\overline{1,8}$, при вбудові ДІ (результат – блок $\overline{B}_i, i=\overline{1,n}$, з елементами $\bar{b}_{kp}^{(i)}, k, p=\overline{1,8}$) це сімейство складається із двох графів — підграфів графа алгоритму (рис.3.5(а,б)). У цьому випадку замість того, щоб окремо досліджувати топологічні сортування кожного із графів сімейства, аналізується топологічне сортування їх об'єднання (рис.3.5(в)), оскільки будь-яке топологічне сортування графа-об'єднання породжує топологічне сортування кожного графа сімейства [112].

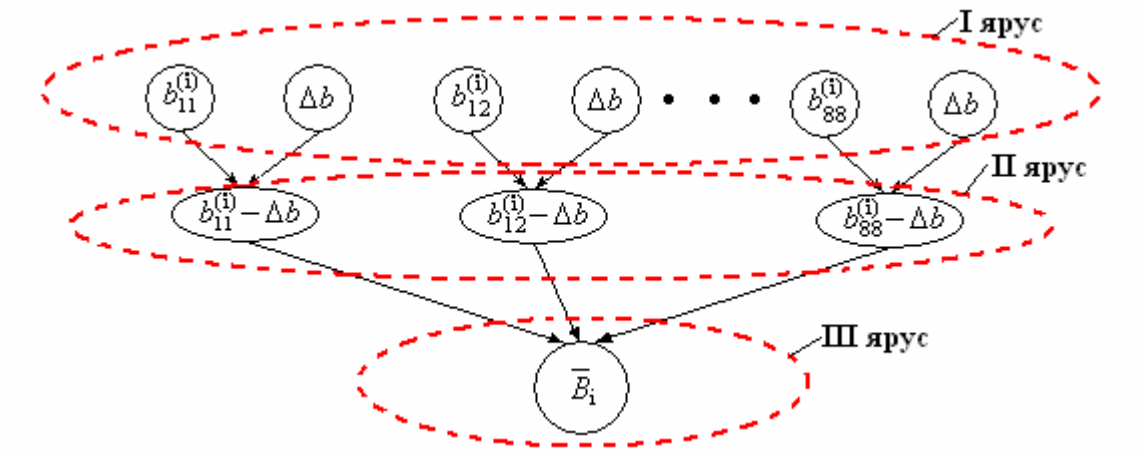
Такий спосіб аналізу алгоритму є кращим, оскільки для конкретних вхідних даних можна навіть не знати, з яким конкретно графом із сімейства «схожих» графів прийдется мати справа.

При декодуванні додаткової інформації для визначення кількості додатних і від'ємних елементів у матриці $\Delta\overline{\overline{B}}$ при стандартній організації процесу накопичення сум k_p і k_n буде використано в загальному випадку 64 умовних оператори (по кількості елементів в $8\times 8-$блоці), що вже на цій стадії побудови тієї частини графа алгоритму, яка відповідає за обробку одного блоку матриці стеганоповідомлення, приведе до сімейства з 2^{64} «схожих» графів. Для отримання топологічного сортування кожного з них має сенс відразу розглянути об'єднання сімейства (рис.3.6) [114].

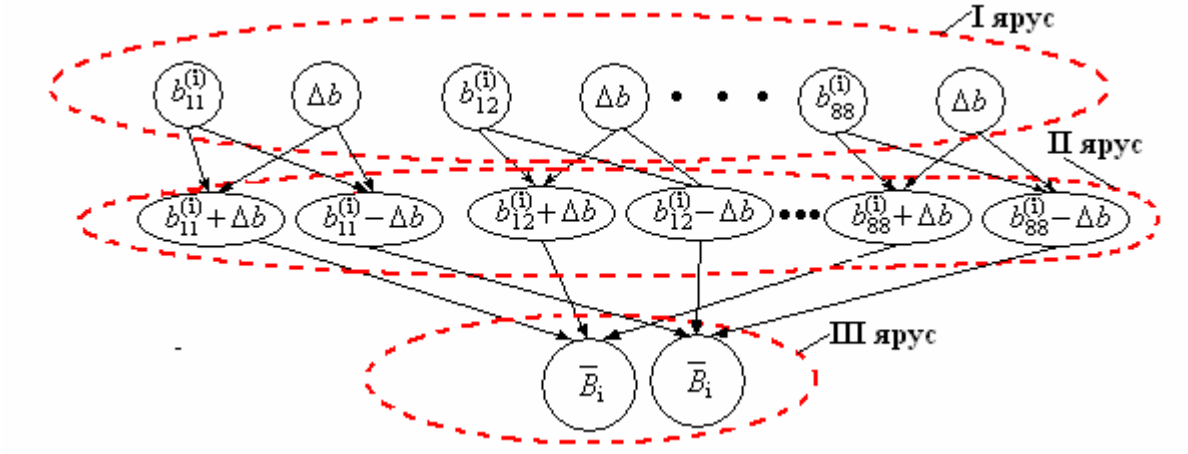
Таким чином, аналіз підграфів графа розробленого стеганоалгоритма, що відповідають обробці окремих блоків матриці контейнера/стеганоповідомлення, яка здійснюється при вбудові/декодуванні ДІ, виявив наявність внутрішнього паралелізму й у цих частинах алгоритму: кожний ярус топологічного сортування містить більше, ніж одну вершину.



а



б



в

Рисунок 3.5 — Паралельні форми підграфів, що відповідають стеганоперетворенню блока B_i, $i=\overline{1,n}$: а,б – графів, що становлять сімейство «схожих» графів; в – графа-об’єднання сімейства «схожих» графів

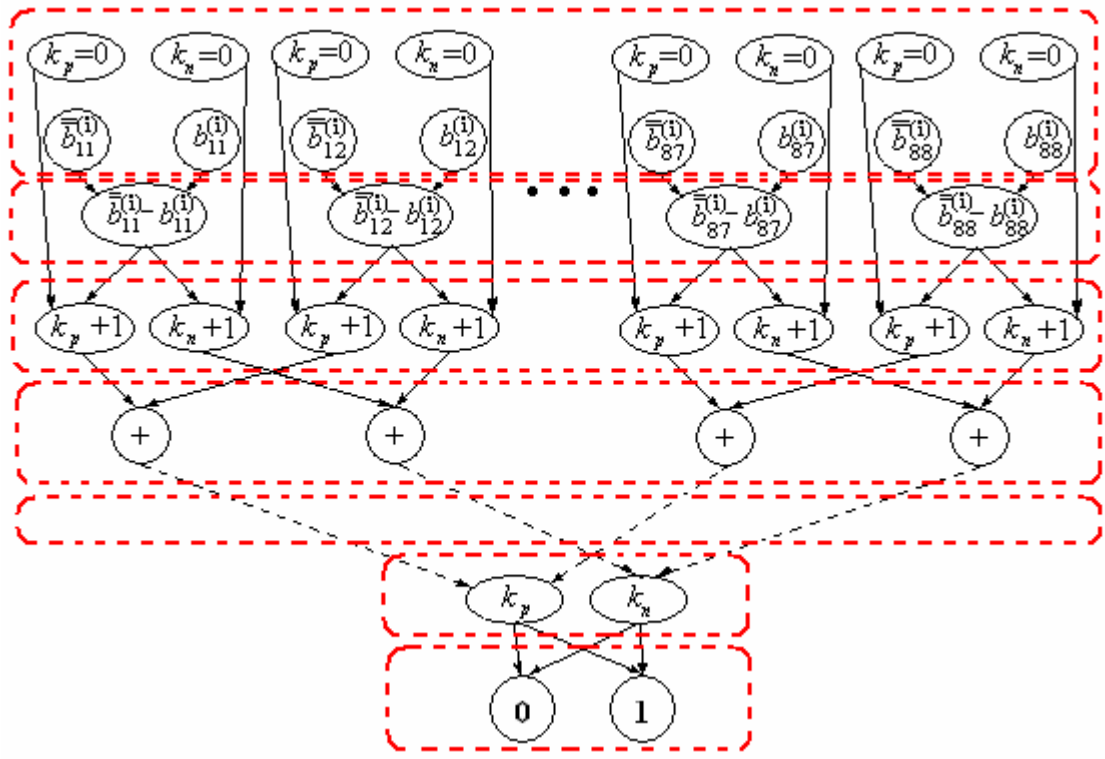


Рисунок 3.6 — Топологічне сортування об'єднання «схожих» підграфів, що відповідають процесу декодування ДІ з одного блоку $\overline{\overline{B}}_i$ можливо збуреного стеганоповідомлення

У результаті встановлено [114], що розроблений стеганографічний алгоритм має внутрішній паралелізм, що дає принципову можливість для зменшення часових витрат на його роботу при реалізації цього алгоритму в багатопроцесорній обчислювальній системі.

3.5 Висновки до розділу 3

У розділі 3 отримані наступні результати:

1. На основі отриманої достньої умови стійкости до збурних дій розроблені стеганометод і стеганографічний алгоритм SA_B, що його реалізує, які діють в просторовій області зображення-контейнера.
2. При дослідженні накладання різних шумів з різними параметрами: гауссівського, мультиплікативного, пуассонівського встановлена

залежність основного параметра розробленого методу/алгоритму — величини Δb збурення яскравості пікселів блоку контейнера при стеганоперетворенні, при якій забезпечується стійкість алгоритму до атак проти вбудованого повідомлення, від розміру l блока.

3. Для однорідного усереднюючого фільтра отримане співвідношення, що дозволяє визначати: розмір l блоку, що використовується при стеганоперетворенні, для забезпечення високої ефективності SA_B в умовах фільтрації залежно від можливого параметра p маски фільтра; розміри маски фільтра, які не приведуть до значущого погіршення ефективності SA_B при відомому використаному значенні l при стеганоперетворенні в умовах атаки фільтрацією, у порівнянні з умовами відсутності атакуючих дій.
4. Показано, що ефективність SA_B в умовах гауссової фільтрації стеганоповідомлення є високою й практично не залежить від розміру маски.
5. Обґрунтовано, що алгоритм SA_B є ефективним в умовах нелінійної (медіанної) фільтрації.
6. Отримані рекомендації для величини розміру блоку l, що дозволяють забезпечити: стійкість стеганоалгоритму до збурних дій, уникнути зменшення прихованої пропускної спроможності стеганографічного каналу зв'язку, що організується, за рахунок величини l, для кожної з розглянутих збурних дій (накладання шуму на стеганоповідомлення, фільтрації, атаки стиском стеганоповідомлення).
7. На основі отриманих оцінок значення збурення $\left\|\Delta\overline{B}\right\|_2$ блоку стеганоповідомлення при різних очікуваних збурних діях, спрямованих на стеганоповідомлення, встановлено, що для одночасного забезпечення стійкості розробленого стеганоалгоритму SA_B до атак проти вбудованого повідомлення: накладанню шумів, фільтрації, атаки стиском доцільно при

організації стеганоперетворення й декодування додаткової інформації використовувати $l = 8$, $\Delta b = 9$.

8. Встановлено, що розроблений стеганографічний алгоритм SA_B має внутрішній паралелізм, що дає принципову можливість для значного зменшення часових витрат на його роботу при реалізації цього алгоритму в багатопроцесорній обчислювальній системі.
9. Обчислювальна складність стеганоалгоритма SA_B становить $\underline{O}(m^2)$, де $m \times m$ — розмір матриці зображення-контейнера.

Таким чином, у розділі 3 вирішена задача 4 і частково вирішена задача 5 з переліку задач дисертаційної роботи.

Основні результати розділу знайшли своє відображення в роботах [114-118,122,124].

РОЗДІЛ 4
ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ

Ефективність стеганоалгоритму в роботі оцінюється його стійкістю до атак проти вбудованого повідомлення, у якості яких розглядаються: накладання різних шумів на стеганоповідомлення (гауссівського, мультиплікативного, пуассонівського), атака стиском СП, фільтрацією, а також комплексні атаки.

Метою розділу є аналіз і оцінка, в тому числі порівняльна (з сучасними аналогами), стійкості розроблених стеганографічних алгоритмів стосовно атак проти вбудованого повідомлення.

Стійкість алгоритму оцінюється стандартним чином за значенням коефіцієнта кореляції NC (3.1) для ДІ.

Для досягнення поставленої мети в розділі вирішуються наступні *задачі*:

1. Отримати кількісну оцінка спотворення контейнера-зображення в результаті розробленого в розділі 3 стеганографічного алгоритма SA_B;
2. Розробити стеганографічний метод і алгоритм, який його реалізує, що є модифікацією алгоритму SA_B, який зменшує спотворення контейнера під час стеганоперетворення, в порівнянні з SA_B;
3. Провести кількісний аналіз стійкості розроблених стеганоалгоритмів до накладання на стеганоповідомлення різних шумів з різними параметрами та порівняльну оцінку ефективності розроблених алгоритмів з найбільш ефективними сучасними аналогами в умовах накладання шуму;

4. Провести кількісний аналіз стійкості розроблених стеганографічних алгоритмів до атаки фільтрацією на стеганоповідомлення з використанням різних фільтрів з різними параметрами та порівняльну оцінку ефективності розроблених алгоритмів з найбільш ефективними сучасними аналогами в умовах фільтрації стеганоповідомлення;
5. Провести кількісний аналіз стійкості розроблених стеганоалгоритмів до атаки стиском з різними коефіцієнтами якості та порівняльну оцінку ефективності розроблених алгоритмів з найбільш ефективними сучасними аналогами;
6. Провести кількісний аналіз стійкості розроблених стеганоалгоритмів до комплексних атак;
7. Проаналізувати стійкість розроблених стеганоалгоритмів до стеганоаналітичних атак.

Для перевірки ефективності розроблених стеганоалгоритмів в середовищі Matlab була проведена серія обчислювальних експериментів, у яких було задіяно 300 цифрових зображень-контейнерів розміром 1000×1000 пікселів (колірна схема RGB) у форматах як з втратами (Jpeg), так і без втрат (Tif) з бази NRCS (яка є традиційною для тестування алгоритмів, що працюють із цифровими зображеннями), а також зображення, отримані непрофесійними фотографами. Далі цю множину зображень будемо називати експериментальною множиною. Вбудова додаткової інформації проводилася в синю колірну складову зображення.

При проведенні всіх обчислювальних експериментів спочатку експериментальна множина була розділена на дві підмножини, в одну з яких увійшли цифрові зображення, збережені без втрат, в іншу — зображення, збережені з втратами. Для кожної множини дослідження

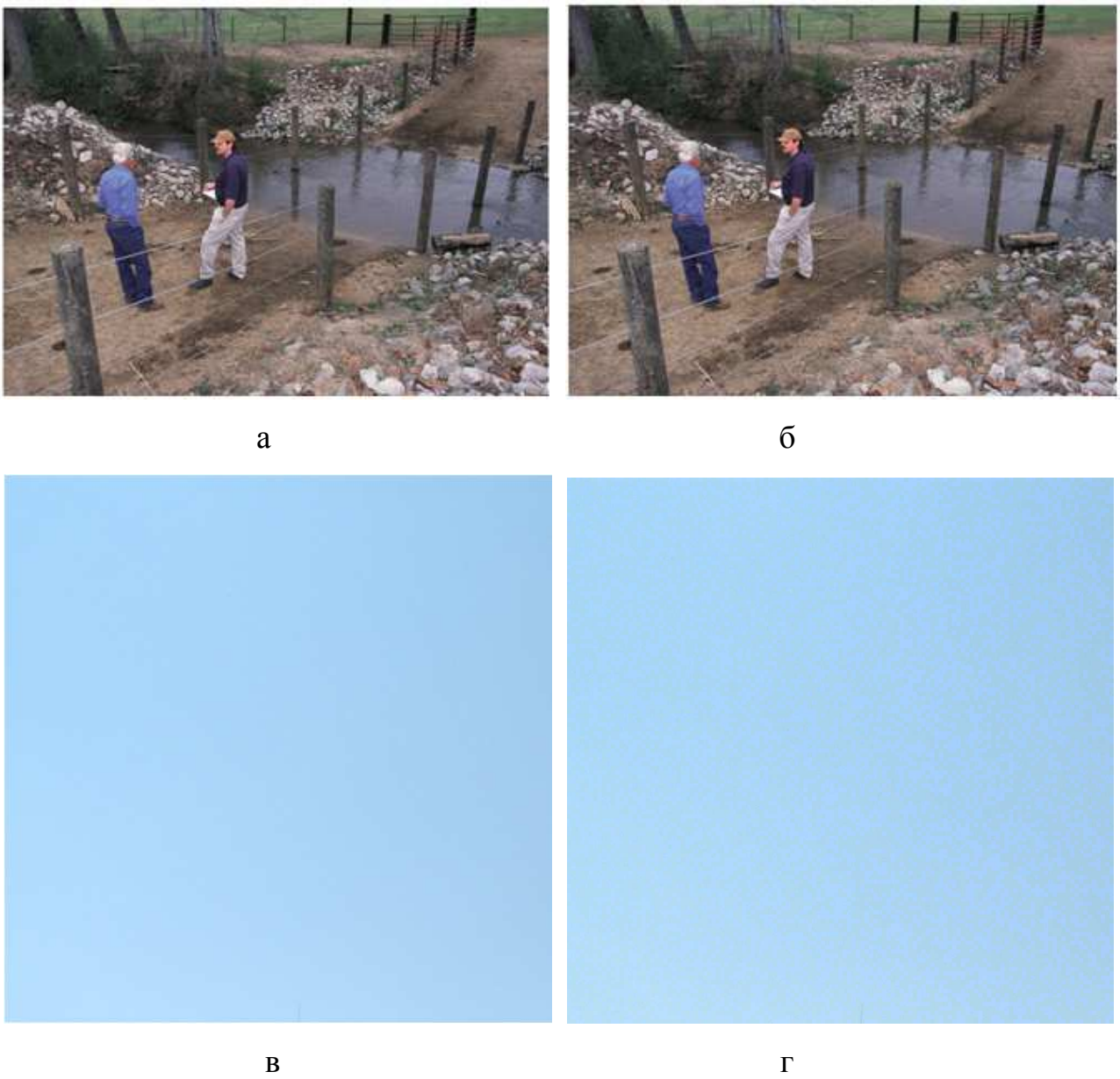
ефективності розроблених стеганографічних алгоритмів при різних атаках проти вбудованого повідомлення проводилися окремо. Однак, як і було передбачено вище в розділі 2, на практиці значення коефіцієнта NC для цих двох груп були настільки близькими (максимальна відмінність становила менш 1%), що розподіл експериментальної множини на зазначені підмножини виявився недоцільним. Тому скрізь нижче в роботі наведені результати по всій експериментальній множині цілком.

При проведенні порівняльного аналізу стійкості розроблених стеганографічних алгоритмів для кожної атаки проти вбудованого повідомлення обиралася своя множина сучасних аналогів, стійких саме до розглядаємої збурної дії, оскільки, як свідчать відкриті джерела (розділ 1), велика кількість існуючих стеганографічних алгоритмів, що позиціонуються як стійкі, не є одночасно стійкими навіть до найпоширеніших збурних дій, часто вони є націленими на конкретні атаки проти вбудованого повідомлення, що не гарантує їх ефективність для інших.

Кількісно оцінка спотворень цифрового зображення проводиться за допомогою значення $PSNR$ (3.2), але разом з цим, як вже відзначалося вище, ступінь забезпечення надійності сприйняття стеганоповідомлення оцінюється також за допомогою суб'єктивного ранжирування. У випадку кольорового цифрового зображення для обчислення $PSNR$ зображення переводиться в колірну схему YCbCr, де аналізується матриця Y – матриця яскравості [123].

4.1 Кількісна оцінка спотворення контейнера-зображення в результаті стеганоперетворення за допомогою розробленого базового стеганоалгоритму

Використання розробленого стеганографічного алгоритму SA_B для організації прихованого каналу зв'язку можливо лише в випадку забезпечення їм надійності сприйняття стеганоповідомлення. Для кількісної оцінки спотворення цифрового зображення при стеганоперетворенні за допомогою SA_B проведено обчислювальний експеримент, у ході якого в синю складову зображення вбудовувалася додаткова інформація, після чого стеганоповідомлення зберігалося у форматі без втрат (Tif). $PSNR$, що відображає спотворення контейнера у процесі стеганоперетворення, дорівнював тут у середньому 49 dB незалежно від формату контейнера, що розглядається в літературних джерелах як значення, яке характеризує прийнятну якість цифрового зображення при стеганоперетворенні [6,38]. Суб'єктивним ранжируванням було встановлено дотримання надійності сприйняття стеганоповідомлень, сформованих розробленим алгоритмом SA_B, для 98.3% зображень, підданих тестуванню (рис.4.1(а,б)). В 1.7% ЦЗ (ці зображення мали значні фонові області) спостерігалося виникнення артефактів на фонових областях, хоча $PSNR$ для них також мав прийнятне значення (рис.4.1(в,г), $PSNR = 49.56\ dB$). Таким чином, рекомендується не використовувати подібні цифрові зображення як контейнери для стеганоалгориту SA_B.



а б

в г

Рисунок 4.1 — Результат стеганоперетворення цифрового зображення розробленим стеганографичним алгоритмом SA_B : контейнери (а), (в); стеганоповідомлення (б), (г)

4.2 Стеганографічний алгоритм, що зменшує спотворення контейнера, в порівнянні з базовим

Щоб запобігти можливості виникнення артефактів на зображенні в результаті стеганоперетворення, розроблений базовий стеганографічний алгоритм SA_B піддається модифікації.

Зрозуміло, що артефакти виникають на фонових ділянках зображення завдяки перепаду значення яскравості пікселів на границі блоків, що використовуються при стеганоперетворенні за допомогою SA_B. Треба зменшити цей перепад на границі. Для цього змінимо вид (2.22) матриці ΔB збурення $l \times l$ – блоку наступним чином. Розіб'ємо ΔB на k ділянок, де k може приймати значення від 2 до $\left[\frac{l}{2}\right]$, як пропонує рис.4.2.

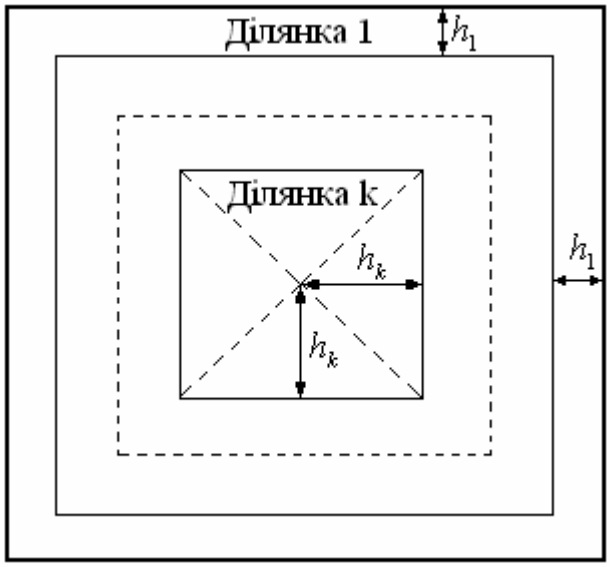


Рисунок 4.2 — Розбиття $l \times l$ – матриці збурення блоку ΔB при стеганоперетворенні на k ділянок

Значення елементів $b^{(\Delta)}{}_{rq}$, $r,q = 1,...,l$, матриці збурення блоку при стеганоперетворенні на i – ій ділянці, $i = \overline{1,k}$, буде визначатися як

$$\begin{cases} \left[\frac{\Delta b}{k}\right] \cdot i, & i = 1,2,...,k-1, \\ \Delta b, & i = k \end{cases} \tag{4.1}$$

при цьому ширина ділянок h_i для різних i може бути різною. Матрицю збурення блоку, елементи якої відповідають (4.1), для якої визначені конкретні значення k та h_i, $i=\overline{1,k}$, будемо позначати $\Delta B^{k,h}$.

Нехай F, $\overline{F}$ — $m\times m-$матриці ОП, СП відповідно. Основні кроки пропонуємого стеганографічного методу виглядають наступним чином

Вбудова ДІ.

1. Матриця F ЦЗ-контейнера розбивається стандартним чином на $l\times l-$блоки.

2. Визначити конкретні значення k та h_i, $i=\overline{1,k}$. Побудувати матрицю $\Delta B^{k,h}$ відповідно до (4.1).

3. Нехай B — черговий блок ОП, що використовується для стеганоперетворення, а p_i — черговий біт ДІ, $\overline{B}$ — відповідний блок СП.

Якщо

$$p_i=1$$

то

$$\overline{B}=B+\Delta B^{k,h} \qquad (4.2)$$

інакше

$$\overline{B}=B-\Delta B^{k,h}. \qquad (4.3)$$

Декодування ДІ відбувається аналогічно тому, як це робиться в базовому розробленому стеганоалгоритмі SA_B.

Треба зазначити, що означені вище кроки для вбудови додаткової інформації визначають конкретний алгоритм тоді, коли будуть визначені умовами вибору k та h_i, $i=\overline{1,k}$. Цей вибір може бути адаптивним: модифікація базового алгоритма і вбудова ДІ відповідно з (4.2), (4.3) (для обраних k та h_i, $i=\overline{1,k}$) може проводитися лише на деяких областях ЦЗ (фонових областях), а на всіх інших – стеганоперетворення може відповідати базовому алгоритму: (3.4), (3.5).

Враховуючи отриману в розділі 2 достатню умови стійкості стеганоперетворення в просторовій області зображення-контейнера, а також співвідношення (4.1), що визначають значення елементів матриці збурення блока основного повідомлення при стеганоперетворенні (тільки ділянка k матриці $\Delta B^{k,h}$ має значення елементів Δb (2.24)), очевидним є факт: для забезпечення стійкості модифікованого алгоритму, що реалізує запропонований вище метод, до збурних дій, доцільно робити розбивку ΔB на ділянки так, щоб кількість пікселів блоку матриці контейнера, що відповідають ділянці k в $\Delta B^{k,h}$, перевищувала $\left[l^2/2\right]$. Для $l=8$ (обраного в розділі 3) таке можливо лише в разі $k=2$, $h_1=1$, $h_2=3$. Тоді матриця $\Delta B^{k,h}$ буде мати вигляд:

$$\Delta B^{k,h}=\begin{pmatrix} \left[\frac{\Delta b}{2}\right] & \left[\frac{\Delta b}{2}\right] & \left[\frac{\Delta b}{2}\right] & \dots & \left[\frac{\Delta b}{2}\right] & \left[\frac{\Delta b}{2}\right] \\ \left[\frac{\Delta b}{2}\right] & \Delta b & \Delta b & \dots & \Delta b & \left[\frac{\Delta b}{2}\right] \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \left[\frac{\Delta b}{2}\right] & \Delta b & \Delta b & \dots & \Delta b & \left[\frac{\Delta b}{2}\right] \\ \left[\frac{\Delta b}{2}\right] & \left[\frac{\Delta b}{2}\right] & \left[\frac{\Delta b}{2}\right] & \dots & \left[\frac{\Delta b}{2}\right] & \left[\frac{\Delta b}{2}\right] \end{pmatrix}. \tag{4.4}$$

Стеганографічний алгоритм, для якого $k=2$, $h_1=1$, $h_2=3$, а матриця $\Delta B^{k,h}$ має вид (4.4**),** який реалізує запропонований вище метод і є модифікацією алгоритма SA_B, обчислювальна складність якого визначається кількістю $8\times8-$блоків в $m\times m-$матриці ЦЗ і становить $\underline{O}\left(m^2\right)$, будема далі позначати SA_M.

Для оцінки спотворень, які відбуваються в цифровому зображенні під час стеганоперетворення за допомогою алгоритма SA_M, було проведено обчислювальний експеримент, в ході якого в синю складову ЦЗ вбудовувалася додаткова інформація, після чого

стеганоповідомлення зберігалося у форматі без втрат (Tif). $PSNR$ в середньому дорівнював тут 53 dB (для SA_B — 49 dB) незалежно від формату контейнера, тобто SA_M зменшив спотворення контейнера під час стеганоперетворення, в порівнянні з SA_B, в середньому на 8.2%. До того ж суб'єктивним ранжируванням було встановлено дотримання надійності сприйняття стеганоповідомлення для абсолютної більшості тих контейнерів, для яких для алгоритму SA_B спостерігалося виникнення артефактів (рис.4.3).

а б

Рисунок 4.3 — Результат стеганоперетворення зображення алгоритмом SA_M : контейнер (а); стеганоповідомлення (б)

Заміна матриці ΔB (2.22) (алгоритм SA_B) на $\Delta B^{k,h}$ (4.4) (алгоритм SA_M) при організації стеганоперетворення може зменшити ефективність алгоритму SA_M в порівнянні з SA_B (що буде перевірятися нижче), але дає можливість використовувати будь-яке ЦЗ як контейнер.

4.3 Аналіз стійкості розроблених стеганоалгоритмів до накладання шуму

Збурні дії на стеганоповідомлення, сформовані на основі цифрових зображень з експериментальної множини розробленими стеганографічними алгоритмами та збережені без втрат, на цьому етапі роботи моделювалися в середовищі Matlab шляхом накладання на них різних шумів: гауссівського, мультиплікативного, пуассонівського з різними параметрами. Збурене стеганоповідомлення зберігалося у форматі без втрат (Tif). Необхідно відзначити, що хоча для повноти експерименту шуми бралися різні, але, виходячи з отриманої достатньої умови стійкості, покладеної в основу організації розроблених стеганоперетворень, зрозуміло, що ефективність стеганографічних алгоритмів SA_B, SA_M не буде залежати від характеру шуму, а буде визначатися величиною збурної дії, оцінюваною значенням $PSNR$, що буде практично підтверджено нижче.

Результати декодування додаткової інформації, що говорять про високу абсолютну ефективність розроблених стеганоалгоритмів, представлені в табл.4.1–4.3 ($PSNR$ тут відображає спотворення стеганоповідомлення при накладанні шуму).

Таблиця 4.1 — Результати декодування додаткової інформації в умовах накладання на стеганоповідомлення, сформовані SA_B, SA_M, гауссівського шуму з нульовим математичним очікуванням і дисперсією D

Дисперсія		$D = 0.0005$	$D = 0.001$	$D = 0.005$	$D = 0.01$	$D = 0.1$
NC	SA_B	0.994	0.993	0.988	0.962	0.524
	SA_M	0.994	0.992	0.979	0.951	0.508
$PSNR$ (dB)		38	35	28	25	16

Таблиця 4.2 — Результати декодування додаткової інформації в умовах накладання на стеганоповідомлення, сформовані SA_B, SA_M, мультиплікативного шуму

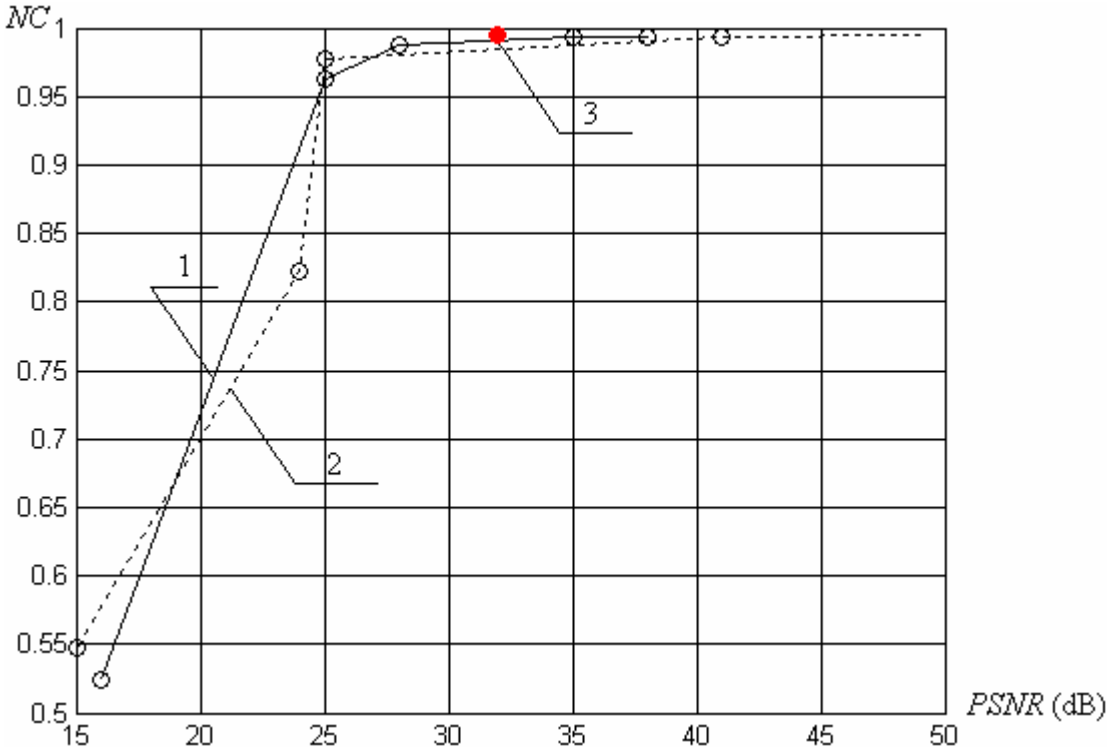
Дисперсія		$D = 0.0001$	$D = 0.001$	$D = 0.01$	$D = 0.08$	$D = 0.5$
NC	SA_B	0.995	0.993	0.977	0.822	0.548
	SA_M	0.995	0.993	0.967	0.810	0.533
$PSNR$ (dB)		49	41	25	24	15

Таблиця 4.3 — Результати декодування додаткової інформації в умовах накладання на стеганоповідомлення, сформовані SA_B, SA_M, пуассонівського шуму

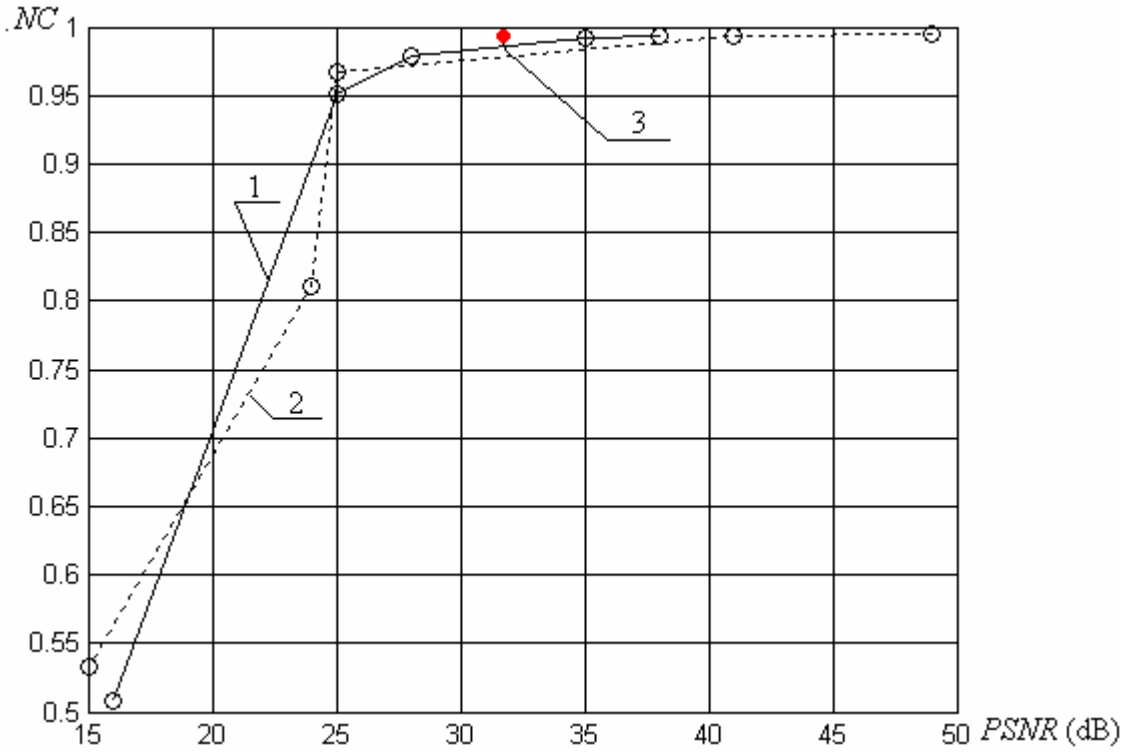
NC		$PSNR$ (dB)
SA_B	SA_M	
0.9977	0.9953	32

Представлення результатів експерименту у вигляді графіків залежності коефіцієнта NC від $PSNR$ (рис.4.4) для різних шумів наочно підтверджує, що ефективність SA_B, SA_M, як і передбачалося вище, визначається величиною спотворення ЦЗ, а не характером накладеного на стеганоповідомлення шуму (зауважимо, що для пуассонівського шуму значення $NC = 0.992$ для $PSNR = 32\ dB$ (табл.4.3) також знаходиться у відповідній області графіків на рис. 4.4) [116,118].

Результати обчислювального експерименту показують, що хоча стійкість алгоритму SA_B не меньша за стійкість SA_M, перевищення є дуже незначним, тому далі розглядається базовий алгоритм SA_B.



а



б

Рисунок 4.4 — Залежність *NC* від *PSNR* для SA_B (а), SA_M (б) при накладанні шуму: 1 – гауссівського; 2 – мультиплікативного; 3 – пуассонівського

Для порівняльної оцінки ефективності розроблених стеганоалгоритмів в умовах накладання гауссівського шуму були обрані 10 найбільш ефективних сучасних аналогів, що мають різні математичні основи та використовують різні області ЦЗ для стеганоперетворення: Surachat (2012) [17], Amornaksa et al. (2006) [16], Su and Chen (2013) [125], Al-Otum and N. Samara (2010) [126], Bazargani et al. (2012) [127], Zhu et al. (2009) [128], Fang et al. (2013) [40], Jiang et al. (2013) [129], Perwej et al. (2012) [130], Rawat et al (2013) [28]. Результати порівняння (для найчастіше використовуваних дисперсій), які говорять на користь розробленого в роботі алгоритма SA_B, відображені в табл. 4.4. Стеганоалгоритм SA_B за стійкістю до гауссівського шуму перевищує всі розглянуті алгоритми для всіх розглянутих значень D (винятком є лише Rawat et al. (2013) для $D = 0.01$, але при такій дисперсії, як відмічалося вище, порушується надійність сприйняття ЦЗ, тому для зловмисника є недоцільним використовувати таку атаку проти вбудованого повідомлення). Так для $D = 0.005$ стійкість SA_B більша за стійкість найкращого з аналогів (Su and Chen (2013)) на 4%.

Таблиця 4.4 — Ефективність стеганоалгоритмів в умовах накладання на стеганоповідомлення гаусівського шуму (значення NC)

D	SA_B	Surachat (2012)	Amornaksa et al. (2006)	Su and Chen (2013)	Al-Otum and N. Samara (2010)	Bazargani et al. (2012)	Zhu et al. (2009)	Fang et al. (2013)	Jiang et al. (2013)	Perwej et al. (2012)	Rawat et al (2013)
0,001	**0,993143**	0,87	0,79	-	-	0,99	0,968	-	-	-	-
0,005	**0,988105**	0,82	0,74	0,9514	0,9280	0,86	0,685	-	-	0,9276	-
0,01	**0,961855**	0,81	0,72	0,8994	0,8753	-	-	0,896	0,822	0,8714	0,9885

Для порівняльної оцінки ефективності розроблених стеганоалгоритмів в умовах накладання мультиплікативного шуму були обрані 7 найбільш ефективних сучасних аналогів, що мають різні математичні основи та

використовують різні області ЦЗ для СПр: Agarwal et al. (2012) [131], Isac et al. (2011) [132], Fadaeenia and Zarei (2011) [121], Xie and Wu (2007) [133], Kumar and Kumar (2011) [119], Alsaif et al. (2013) [134], Perwej (2012) [130]. Результати порівняння відображені в табл. 4.5 (для найчастіше вживаних дисперсій) та на рис.4.5.

Таблиця 4.5 — Ефективність стеганоалгоритмів в умовах накладання на стеганоповідомлення мультиплікативного шуму (значення NC)

D	SA_B	Agarwal et al. (2012)	Isac et al. (2011)	Fadaeenia and Zarei (2011)	Xie and Wu (2007)	Kumar and Kumar (2011)	Alsaif et al. (2013)
0,001	**0,993**	0,8699	0,94921	0,9765	0,9472	0,980	0,898524

Алгоритм SA_B за стійкістю до мультиплікативного шуму (табл.4.5) перевищує всі розглянуті сучасні алгоритми: для найчастіше вживаної дисперсії $D = 0.001$ стійкість SA_B більша за стійкість найкращого з аналогів (Kumar and Kumar (2011)) на 1.5%; при інших дисперсіях (рис.4.5) SA_B також перевищує за ефективністю аналоги (хоча крива, що відповідає алгоритму Perwej (2012), перетинає криву, що відповідає SA_B, алгоритм Perwej (2012), як свідчить [130], взагалі не тестувався для значної/малої дисперсії, на відміну від SA_B, що неявно говорить про його неспроможність ефективно працювати в таких умовах).

Для порівняльної оцінки ефективності розроблених СА в умовах накладання пуасонівського шуму були обрані 13 найбільш ефективних сучасних аналогів, що мають різні математичні основи та використовують різні області ЦЗ для СПр: Sulong et al. (2014) [95], Ali and Sulong (2013) [135], Wang and Li (2013) [136], Harish et al. (2013) [137], Rahman (2013) [138], Singh and Tayal (2012) [139] (4 алгоритми), Ali et al. (2012) [140], Vahedi et al. (2012) [141], Maheswari (2011) [142], Ramani et al. (2010) [143]. Результати порівняння

відображені в табл. 4.6, які показуть, що розроблений стеганогалгоритм не має рівних серед усіх аналогів, коефіцієнт кореляції для ДІ для SA_B є близьким до одиниці.

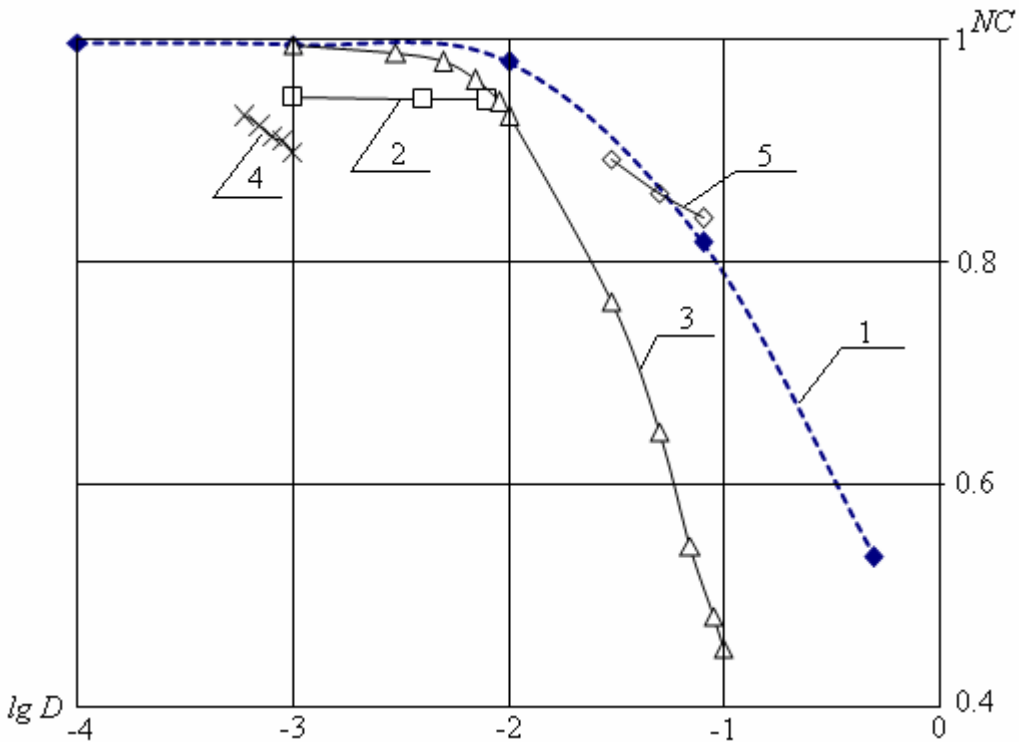


Рисунок 4.5 — Залежність NC від $lg\,D$ при накладанні мультиплікативного шуму: 1 — SA_B, 2 — Isac (2011), 3 — Kumar (2011), 4 — Alsaif (2013), 5 — Perwej (2012)

Таблиця 4.6 — Ефективність стеганоалгоритмів при накладанні на стеганоповідомлення пуассонівського шуму (значення NC)

SA_B	Sulong et al. (2014)	Ali and Sulong (2013)	Wang and Li (2013)	Harish et al. (2013)	Rahman (2013)	Singh and Tayal (2012)	Ali et al. (2012)	Vahedi et al. (2012)	Maheswari (2011)	Ramani et al. (2010)
0,997681	0,8126	0,9954	0,9963	0,939	0,9941	0,9754 0,978 0,996 0,9769	0,99	0,9562	0,9911	0,8567

Таким чином, проведений обчислювальний експеримент практично підтверджує високу ефективність розроблених СА в умовах накладання на СП шумів. Стійкість розроблених СА перевищує стійкість сучасних аналогів загалом.

4.4 Аналіз стійкості розроблених стеганоалгоритмів до атаки фільтрацією

Для практичної перевірки зроблених вище теоретичних висновків про стійкість розробленого СА до атаки фільтрацією в середовищі Matlab був проведений обчислювальний експеримент, у якому як контейнери були задіяні ЦЗ з експериментальної множини. Після вбудови ДІ ($l = 8$) СП зберігалося спочатку у форматі без втрат (Tif), піддавалося фільтрації й знову зберігалося без втрат, після чого проводилося декодування ДІ. Результати експерименту, усереднені по всім тестованим ЦЗ, наведені в табл.4.7, де в останньому рядку зазначена характеристика спотворення СП у результаті фільтрації ($PSNR$).

Таблиця 4.7 — Результати декодування ДІ стеганоалгоритмом SA_B в умовах фільтрації стеганоповідомлення

Вид фільтра	Усереднюючий фільтр розміру $p \times p$			Гауссов фільтр розміру $p \times p$ ($sig = 0.5$)			Медіанний фільтр 3×3
	$p = 3$	$p = 5$	$p = 7$	$p = 3$	$p = 5$	$p = 7$	
NC	0.994	0.962	0.881	0.997	0.997	0.997	0.997
$PSNR$	34	30	24	43	43	43	37

Експериментально підтверджено:

- для однорідного усереднюючого фільтра при виконанні умови (3.11) для p і l ефективність близька до 1 (при $p = 3$: NC =0.994);

- ефективність в умовах гауссової фільтрації стеганоповідомлення є високою й практично не залежить від розміру маски;
- алгоритм SA_B є ефективним в умовах нелінійної (медіанної) фільтрації.

Таким чином, результати експерименту знаходяться у повній відповідності з отриманими в розділі 3 теоретичними твердженнями й говорять про стійкість досліджуваного СА SA_B до атаки, що здійснюється шляхом фільтрації СП.

Результати порівняльної оцінки стійкості розробленого алгоритму із сучасними аналогами, що мають різні математичні основи і використовують різні області цифрового зображення для стеганоперетворення, (Elkhamssa et al. (2014) [89]; Lu et al (2014) [144], Vafaei et al. (2013) [145], T.H.The (2013) [66], Wang et al. (2011) [71]; Run et al. (2011) [69], Fadaeenia and Zarei (2011) [121], Soheili (2010) [146], W.-H.Lin et al. (2009) [38], Lin et al. (2009) [64], Qin and Wen (2014) [37], Lingamgunta et al. (2013) [56], Leung et al. (2012) [147], Ramanjaneyulu and Rajarajeswari (2010) [148], Lien and Lin (2006) [50], Li et al. (2006) [49], Cedillo-Hernandez, et al. (2013) [149], Hammouri et al. (2013) [150], Kalra et al. (2014) [151], Awwad (2013) [152]) до атак фільтрацією наведені в табл. 4.8–4.10.

Таблиця 4.8 — Ефективність стеганоалгоритмів в умовах фільтрації стеганоповідомлення усереднюючим фільтром (значення NC)

Маска	SA_B	Elkhamssa et al. (2014)	Lu et al (2014)	Vafaei et al. (2013)	T. H. The (2013)	Wang et al. (2011)	Run et al. (2011)	Fadaeenia and Zarei (2011)	Soheili (2010)	W.-H.Lin et al. (2009)	Lin et al. (2009)
3×3	**0,99393**	0,85	0,9665	0,98	0,95	0,98	0,95	0,9879	0,9933	0,95	0,93
5×5	**0,96214**	-	0,8687	-	0,8	0,89	0,8	0,9354	0,8433	0,8	0,87
7×7	**0,88048**	-	0,744	-	-	0,78	-	-	0,4866	0,48	-

З отриманих результатів випливає, що стійкість до атаки фільтрацією для SA_B перевищує стійкість усіх розглянутих сучасних аналогів. При цьому для усереднюючого фільтра максимально вдалося підвищити стійкість на 13%

(маска 7×7, порівняння з кращим з аналогів — Wang (2011)); для гауссова й медіанного фільтрів стійкість SA_B близька до одиниці: $NC=0.996568$, $NC=0.997177$.

Таблиця 4.9 — Ефективність стеганоалгоритмів в умовах фільтрації стеганоповідомлення гауссовим $3\times3-$фільтром (значення NC)

SA_B	Qin and Wen (2014)	T.H. The (2013)	Lingamgunta et al. (2013)	Leung et al. (2012)	Run et al. (2011)	Ramanjaneyulu and Rajarajeswari (2010)	Lin et al. (2009)	W.-H.Lin et al. (2009)	Lien and Lin (2006)	Li et al. (2006)
0,996568	0,9853	0,99	0,85	0,7262	0,95	0,8055	0,96	0,88	0,84	0,7

Таблиця 4.10 — Ефективність стеганоалгоритмів при фільтрації стеганоповідомлення медіанним $3\times3-$фільтром (значення NC)

SA_B	Elkhamsa et al. (2014)	Lu et al (2014)	Cedillo-Hernandez et al. (2013)	Hammouri et al. (2013)	Kalra et al. (2014)	Awwad (2013)	Lingamgunta et al. (2013)	Leung et al. (2012)	Ramanjaneyulu and Rajarajeswari (2010)	W.-H.Lin et al. (2009)
0,997177	0,9	0,9894	0,98	0,9841	0,929	0,98172	0,87	0,3328	0,7466	0,9

4.5 Аналіз стійкості розроблених алгоритмів до атаки стиском

Для перевірки ефективності розробленого СА SA_B в середовищі Matlab був проведений обчислювальний експеримент, у якому були задіяні ЦЗ з експериментальної множини. В якості матриці F при стеганоперетворенні використовувалася синя складова зображення-контейнера. Після вбудови додаткової інформації стеганоповідомлення зберігалося спочатку у форматі без втрат (Tif). Моделювання атаки стиском на стеганоповідомлення проводилося шляхом його перезбереження у формат із втратами (Jpeg, Jpeg2000) з різними коефіцієнтами якості $QF\in\{30,40,50,60,70,80,90\}$. Спотворення, які зазнавали стеганоповідомлення у процесі атак, оцінювалися за допомогою значення $PSNR$, що обчислювалося по матрицях

вхідного (формат Tif) і збуреного (формат Jpeg/Jpeg2000) стеганоповідомлення. Результати експерименту, що говорять про високу ефективність SA_B, наведені в табл.4.11,4.12. Результати, які представлені на рис.4.6, практично підтверджують, що основним параметром, від якого залежить ефективність розробленого алгоритму в умовах стиску із втратами, знову є величина збурної дії (оцінювана за значенням $PSNR$), яку зазнає стеганоповідомлення у процесі атаки. Дійсно, значення NC при близьких значеннях $PSNR$ також близькі для обох варіантів проведення атаки — збереження стеганоповідомлення в Jpeg, Jpeg2000, не зважаючи на різні математичні основи цих стисків — ДКП (Jpeg), ДВП (Jpeg2000) [117,153].

Таблиця 4.11 — Результати декодування ДІ алгоритмом SA_B в умовах атаки стиском на стеганоповідомлення шляхом його перезбереження у формат Jpeg

QF	30	40	50	60	70	80	90
NC	0.946	0.969	0.981	0.987	0.988	0.989	0.991
$PSNR$	35	37	38	39	41	43	45

Таблиця 4.12 — Результати декодування ДІ алгоритмом SA_B в умовах атаки стиском на стеганоповідомлення шляхом його перезбереження у формат Jpeg2000

QF	40	60	70	80	90
NC	0.782	0.947	0.980	0.990	0.992
$PSNR$	33	36	39	43	44

Для порівняльної оцінки ефективності розробленого алгоритму SA_B використовувалися 10 сучасних аналогів, що позиціонуються як стійкі до стиску, мають різні математичні основи та використовують різні області ЦЗ для

СПр: Elkhamssa et al. (2014) [89], A1 (2013) [62], Vafaei et al. (2013) [15], Lingamgunta et al. (2013) [56], Cedillo-Hernandez et al. (2013) [149], Fadaeenia and Zarei (2011) [121], W.-H.Lin et al. (2009) [38], Peng (2009) [154], Xiao et al. (2008) [155], Fanf Li et al. (2008) [156]. Результати, з яких випливає, що стійкість SA_B перевищує стійкості всіх розглянутих аналогів при всіх значеннях QF, відображені в табл.4.13 (для $QF = 30$ коефіцієнти кореляції ДІ для SA_B і найкращого з аналогів $A1$ (2013) з точністю до двох значущих цифр співпадають).

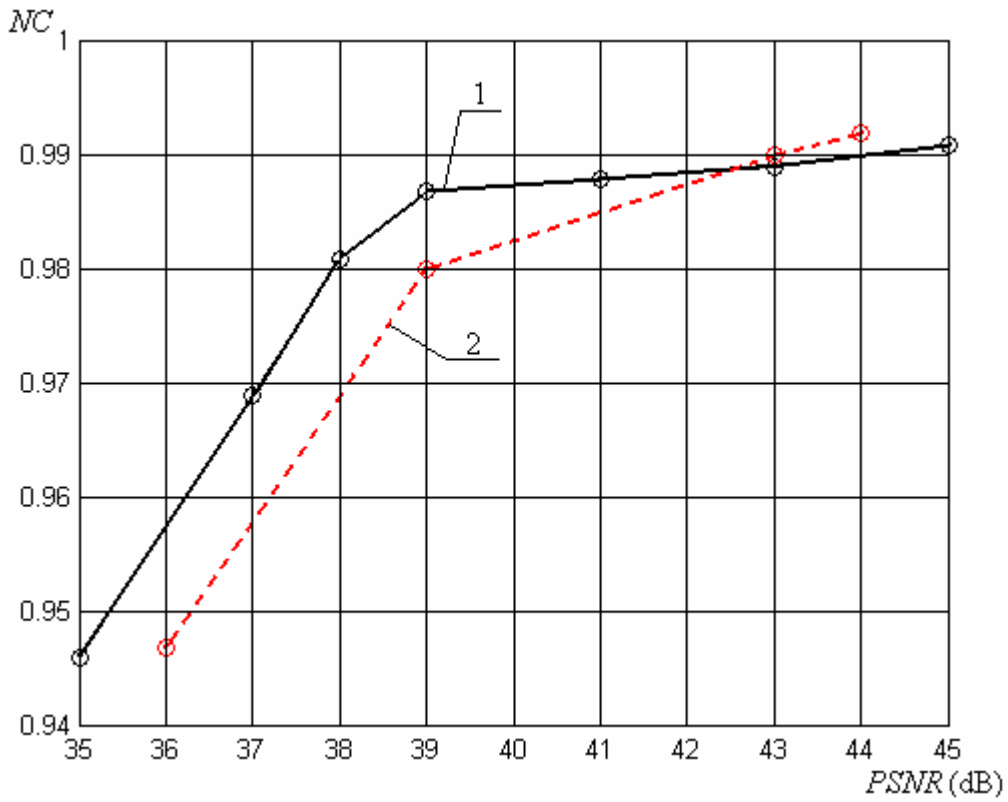


Рисунок 4.6 — Залежність ефективності алгоритму SA_B від $PSNR$ в умовах атаки стиском шляхом збереження СП у формат із втратами: 1 – Jpeg; 2 – Jpeg2000

Достатня умова стійкості стеганоалгоритма, отримана в області сингулярного розкладання матриці [34], яка згадувалася в розділі 2 і послужила відправним моментом для розробки достатньої умови, забезпечуваної в просторовій області ЦЗ-контейнера, є основою для СА

$A1$(2013) [62], стійкого до атаки стиском, тому порівняння SA_B з $A1$ (2013) викликає особливий інтерес. Результати порівняння наочно відображені на рис.4.7, з яких видно, що SA_B перевищує свій аналог по ефективності (необхідно відзначити, що ситуація, що має місце при $QF = 30$, обумовлена врахуванням різної кількості значущих цифр в NC). Причиною цьому очевидно є використання просторової області контейнера для вбудови ДІ, що спричинило зменшення накопичення обчислювальної похибки, яке передує процесу декодування [117].

Таблиця 4.13 — Значення NC для різних стеганоалгоритмів в умовах атаки стиском з різними коефіцієнтами якості QF

QF	SA_B	Elkhamssa et al. (2014)	A1 (2013)	Vafaei et al. (2013)	Lingamgunta et al. (2013)	Cedillo-Hernandez, et al. (2013)	Fadaeenia and Zarei (2011)	W.-H.Lin et al. (2009)	Peng (2009)	Xiao et al. (2008)	Fanf Li et al. (2008)
30	**0,9460**	-	0,95	-	0,79	0,93	0,915	0,83	-	0,7836	-
40	**0,9685**	-	0,96	0,949	-	-	0,946	0,903	0,828	0,9198	-
50	**0,9805**	-	0,98	-	0,93	0,95	0,955	0,94	0,916	-	0,79
60	**0,9873**	0,7775	0,98	0,957	-	-	-	0,953	-	0,9064	0,82
70	**0,9884**	-	0,98	-	-	0,96	-	0,966	0,928	-	0,86
80	**0,9894**	0,9425	0,98	0,983	-	-	0,965	0,983	0,945	0,9668	0,92
90	**0,9906**	-	0,98	0,989	0,99	-	-	0,986	-	-	0,97

Таким чином, розроблений алгоритм SA_B, здійснюючи вбудову додаткової інформації в просторовій області контейнера-зображення, є стійким до атаки стиском.

За рахунок відсутності необхідності переходів «просторова область – область перетворення», «область перетворення – просторова область» при організації вбудови/декодування ДІ ефективність розробленого алгоритму вище, чим у його «найближчого» аналога – алгоритма $A1$ (2013), що

забезпечує нечутливість СП в області сингулярного розкладання відповідних матриць контейнера.

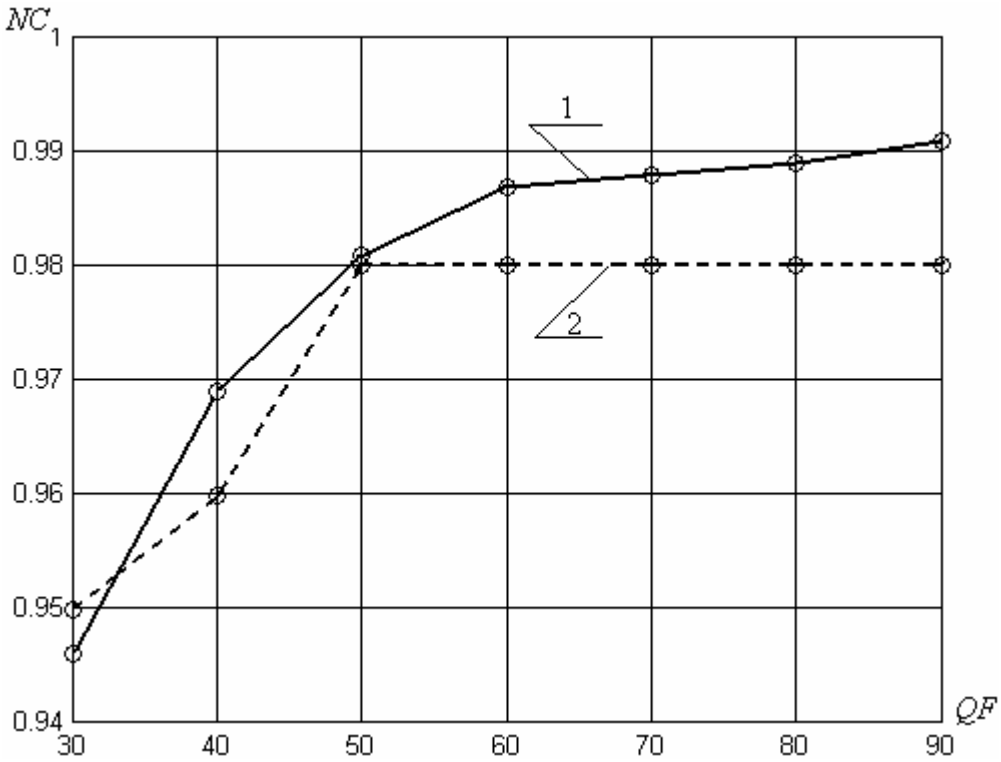


Рисунок 4.7 — Залежність ефективності від коефіцієнта якості стиску стеганоповідомлення: 1 – для стеганоалгоритму SA_B; 2 – для СА $A1$ (2013)

Результати проведених обчислювальних експериментів дали практичне підтвердження зауваженню 2.3, а саме тому, що стійкість стеганоалгоритмів, побудованих на основі твердження 2.1, визначається величиною спотворення матриці стеганоповідомлення при атаці ($PSNR$), а не конкретним видом збурної дії, що забезпечило високу ефективність розроблених стеганографічних алгоритмів незалежно від виду атаки (рис.4.8).

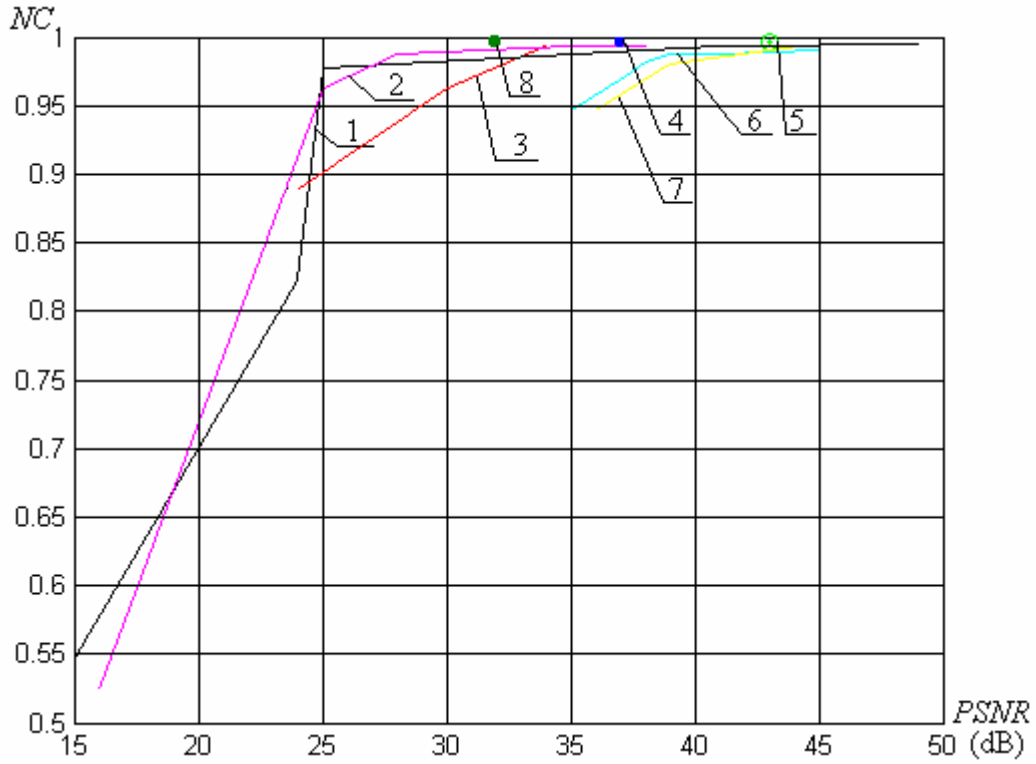


Рисунок 4.8 — Залежність NC від $PSNR$ для SA_B в умовах: 1— накладання мультиплікативного шуму, 2 — гауссівського шуму, 3 — фільтрація усереднюючим фільтром, 4 — медіанним фільтром, 5 — гауссовим фільтром, 6 — збереження СП у форматі Jpeg, 7 — збереження СП у форматі Jpeg2000, 8 — накладання пуассонівського шуму

4.6 Аналіз ефективності розробленого стеганоалгоритму в умовах комплексних атак проти вбудованого повідомлення

Назвемо атаку проти вбудованого повідомлення комплексною, якщо вона складається з декількох збурних дій на стеганоповідомлення.

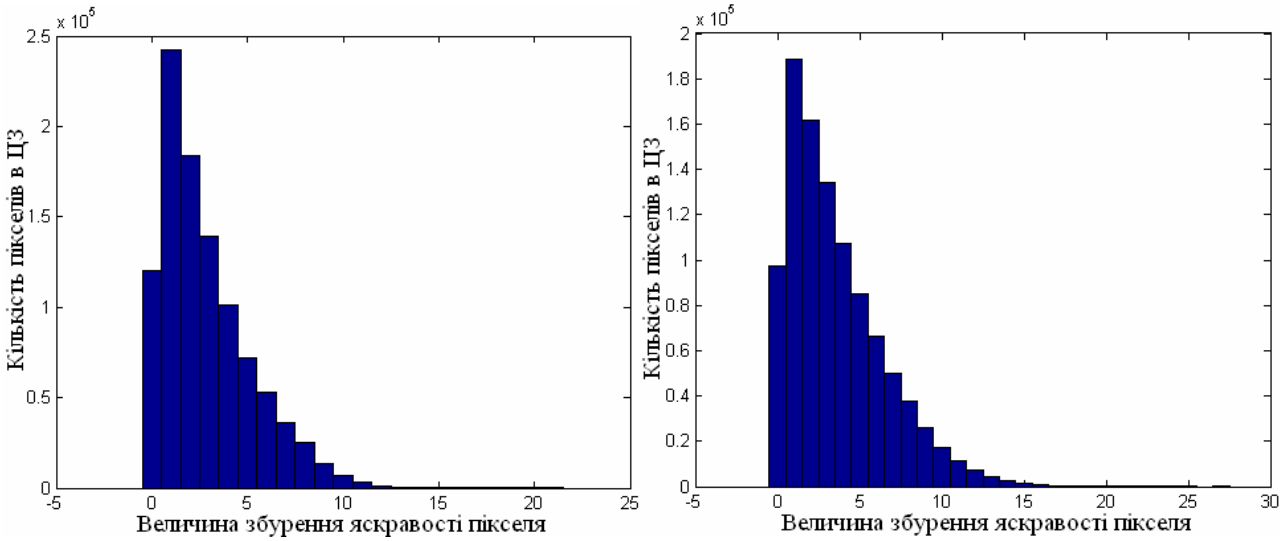
У роботі в якості комплексних розглядаються атаки двох видів: дворазовий стиск стеганоповідомлення; накладання на стеганоповідомлення шуму з наступним стиском, обґрунтування вибору яких наведено нижче.

У даний момент передача інформації, у тому числі ЦЗ, по каналах комунікацій відбувається, як правило, у форматах із стиском. Тому сама передача ЦЗ у форматах без втрат, у більшій або меншій мірі, привертає до себе увагу. Це говорить про те, що стеганоповідомлення ще на стадії його

формування для збільшення ймовірності нерозкриття стеганографічного каналу зв'язку має сенс зберігати у форматі із втратами (Jpeg), тобто для стеганоперетворення сьогодні доцільно завжди використовувати стеганоалгоритми, стійкі до стиску, якими є алгоритми SA_B, SA_M, розроблені у роботі, а обов'язковою складовою комплексної атаки має сенс розглядати стиск із втратами. Найчастіше ЦЗ зберігаються в Jpeg з $QF = 80,90$, що відповідає гарній візуальній якості зображення й порівняно малому об'єму пам'яті для зберігання. Якщо припустити в такій ситуації атаку стиском на стеганоповідомлення, проведену супротивником, то для вхідного стеганоповідомлення (збереженого без втрат) цей стиск буде повторним, тому використовуваний стеганоалгоритм повинен бути стійким не тільки до первинного, але й до повторного стиску. Перевіримо, на скільки збурюються пікселі ЦЗ (значення яскравості в колірній матриці синього кольору (схема RGB)) при стиску з $QF = 80,90$. Як показує обчислювальний експеримент для переважної більшості пікселів їх збурення не перевищують 4, і лише мала частина пікселів зазнає збурення, величина яких більше 9, що з врахуванням обраного значення $\Delta b = 9$ говорить про те, що навіть після первинного стиску стеганоповідомлення, сформоване SA_B, залишається малочутливим до повторного, оскільки для переважної більшості пікселів ЦЗ знак їх збурень, що відбулися в ході стеганоперетворення, при первинному стиску змінитися не міг. Типові картини кількісного розподілу різних значень збурень яскравості пікселів для $QF = 90,80$ відповідно представлені на рис.4.9(а),4.9(б) [117].

Таким чином, проведений обчислювальний експеримент дає можливість припустити високу ефективність розробленого стеганоалгоритму в умовах повторного стиску стеганоповідомлення супротивником. Для практичного підтвердження цієї гіпотези в середовищі Matlab був проведений обчислювальний експеримент, де стеганоповідомлення (спочатку збережені у форматі без втрат) піддавалися спочатку первинному стиску з $QF = 80,90$, а потім повторному з $QF = 50,70,90$. Результати, що повністю підтверджують

високу ефективність алгоритму SA_B в умовах дворазового стиску, наведені в табл.4.14 [117].



а б

Рисунок 4.9 — Типовий приклад гістограм значень збурень яскравості пікселів зображення при стиску: а — $QF = 90$; б — $QF = 80$

Таблиця 4.14 — Результати декодування ДІ (значення NC) розробленим стеганоалгоритмом SA_B в умовах дворазового стиску стеганоповідомлення

Повторний стиск / Первинний стиск	$QF = 50$	$QF = 70$	$QF = 90$
$QF = 90$	0.967	0.984	0.988
$QF = 80$	0.965	0.984	0.986

Таким чином, розроблений алгоритм SA_B, здійснюючи вбудову ДІ в просторовій області контейнера-зображення, є стійким не тільки до атаки стиском, але й до комплексної атаки, що полягає у дворазовому стиску.

Оскільки, як вже відзначалося вище, у даний момент для того, щоб уникнути небажаної уваги до інформації, що пересилається, доцільно пересилати ЦЗ у форматах із втратами, то при використанні в якості атаки на

вбудоване повідомлення накладання шуму, зашумлене стеганоповідомлення з великою ймовірністю буде збережено у форматі із втратами, що пояснює розгляд у роботі саме такої комплексної атаки.

В табл. 4.15 наведені результати при накладанні шумів с $D = 0.001$ (найбільш часто використовуване значення параметра D).

Таблиця 4.15 — Значення NC для SA_B в умовах комплексної атаки: накладання шума з $D = 0.001$ і наступний стиск із коефіцієнтом QF

QF / Шум	50	70	90
Мультиплікативний	0.969831	0.982947	0.985590
Гауссівський	0.971234	0.980201	0.991032

Таким чином, розроблений стеганоалгоритм SA_B є стійким до комплексних атак проти вбудованого повідомлення, складовою яких є стиск із втратами. Так при першій з розглянутих атак комбінація різних/однакових значень $QF = 50,70,80,90$ при первинному й повторному стиску забезпечила значення $NC > 0.96$, а при комбинації $QF = 80,90$, які є найбільш часто використовуваними при стиску, $NC = 0.99$. Комплексна атака накладання шуму й стиску для $QF = 70,90$ привела до показника $NC > 0.98$.

4.7 Аналіз стійкості розробленого стеганоалгоритму до стеганоаналітичних атак

Активізація наукової діяльності в області стеганографії, публікації нових результатів у відкритій пресі привели до зростання можливостей використання отримуваних розробок різними антидержавними, терористичними структурами. Симетричною відповіддю став розвиток розробок у напрямку підвищення ефективності стеганоаналізу.

На сьогоднішній день СА може позиціонуватися як ефективний тільки в тому випадку, якщо він є стійким до стеганоаналізу. У силу цього питання оцінки такої стійкості є актуальним для кожного стеганометоду й алгоритму.

Метою підрозділу є дослідження стійкості алгоритму SA_B до стеганоаналізу, здійснюваному сучасними програмними комплексами.

Головною задачею стеганоаналізу, якому піддаються ОП/СП, є визначення факту наявності прихованої інформації [2,5].

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

1. Для всебічного аналізу розглянутого алгоритму виділити серед сучасних стеганоаналітичних комплексів такі, які мають різні математичні основи, використовують різні математичні інструменти й принципи роботи;
2. Визначити слабкі місця в побудові й функціонуванні сучасних стеганоаналітичних комплексів;
3. Провести обчислювальний експеримент і отримати числові характеристики ефективності стеганоаналізу для досліджуваного СА SA_B.

Стеганоаналіз сьогодні розвивається у двох основних напрямках: розробка алгоритмів, що дозволяють детектувати результати роботи конкретних стеганографічних методів, і так званих, універсальних, або сліпих (blind), методів, що дозволяють шляхом виявлення або констатації відсутності певних характерних ознак в аналізованому контенті робити висновок про наявність конфіденційної інформації або її відсутність, не відштовхуючись від конкретики використаного стеганографічного алгоритму [7,11].

У процесі досягнення поставленої мети спочатку була проведена серія експериментів з використанням ЦЗ із експериментальної множини. Вбудова додаткової інформації відбувалася в синю складову зображення-контейнера. З врахуванням того, що алгоритм SA_B є стійким до стиску, стеганоповідомлення були збережені у форматі JPEG з різними коефіцієнтами якості QF: від 50 до 100 із кроком 10, після чого піддавалися стеганоаналізу.

Використані стеганоаналітичні комплекси представлені наступними продуктами:

1. CANVASS 1.0 (2009 р.);
2. StegAlyzerSS 3.0 (2007 р.);
3. Stegdetect 0.6.3 (2004 р.).

Обрані стеганоаналітичні комплекси є ефективними, широко використовуваними, у тому числі, при тестуванні нових стеганоалгоритмів, сучасними й доступними для вільного (неурядового) застосування, крім того, як показано нижче, вони відрізняються своїми математичними основами.

При проведенні обчислювального експерименту найгірші результати показав StegAlyzerSS [157], або Steganography Analyzer Signature Scanner, — даний комплекс не зміг здійснити детектування вкладень у жодній із груп зображень із різним коефіцієнтами якості QF .

Пояснення даного факту полягає в наступному. Представлений програмний продукт є сигнатурним сканером, тобто принцип його роботи базується на пошуку масок і сигнатур різних відомих на даний момент стеганографічних методів і алгоритмів, включених у його базу. Таким чином, будь-який новий СА може виявитися «невидимим» даним програмним комплексом, що й відбулося з SA_B .

Отриманий результат говорить про недоцільність подальших розробок сигнатурних сканерів для рішення задач стеганоаналізу. Майбутнє стеганоаналізу може бути пов'язане тільки з «сліпими» методами, сигнатурні ж методи приречені на вічну роль «наздоганяючого» у гонці з розроблювачами СА.

Наступною була проаналізована робота програмного комплексу Stegdetect, розробленого в 2000-х рр. Н. Провосом. Даний комплекс здатний виявляти приховану інформацію в зображеннях Jpeg-формату, вбудовану різними відомими алгоритмами стеганографії (наприклад, jsteg, jphide, F5 і т.д.), а також автоматично виявляти нові стеганографічні методи, використовуючи для цього можливості лінійного дискримінантного аналізу [158].

Результати роботи цього комплексу, як і інших, продемонстровані в табл.4.16. Ефективність детектування (тут і далі під ефективністю детектування буде розумітися частина вірно виявлених стеганоповідомлень від загального числа аналізованих стеганоповідомлень, виражена у відсотках) даного комплексу в жодній із груп не перевищила 14%.

Низький рівень детектування даним стеганоаналітичним комплексом розробленого алгоритму, очевидно, пов'язаний з використанням конкретного математичного апарата — лінійного дискримінантного аналізу для класифікації (ОП, СП) зображень.

Лінійний дискримінантний аналіз містить у собі методи статистики й машинного навчання, застосовувані для знаходження лінійних комбінацій ознак, що найкраще розділяють два або більш класів об'єктів або подій. Отримана комбінація може бути використана в якості лінійного класифікатора або для зменшення вимірності простору ознак перед наступною класифікацією.

Лінійний дискримінантний аналіз для випадку двох класів (а саме це й ставиться в задачу стеганоаналітичного комплексу — відокремити стеганоповідомлення від контейнерів) здійснюється в такий спосіб: для кожного зразка об'єкта або події з відомим класом y розглядається набір спостережень x (що називаються ще ознаками, змінними або вимірами). Набір таких зразків називається навчальною вибіркою. Завдання класифікації полягає в тому, щоб побудувати гарний прогноз класу y для всякого так само розподіленого об'єкта (що не обов'язково належить навчальній вибірці), маючи тільки спостереження x [159]. Таким чином, ефективна робота даного стеганоаналітичного програмного продукту буде забезпечуватися у випадку значної кількості спостережень, що є його недоліком, оскільки на практиці ця вимога не тільки часто не реалізована, але є й малоймовірною (з врахуванням вимоги підтримки прихованості й безпеки самого каналу).

Наступною була проаналізована робота програмного комплексу Canvass, заснованого на частково впорядкованих марківських моделях, які використані для методу опорних векторів [160]. Ефективність даного комплексу

максимальна з усіх розглянутих у роботі, однак варто відзначити, що як видно з табл. 4.16, максимум ефективності досягається при значеннях QF від 50 до 70, тобто можно сказати, що комплекс Canvass детектує наявність збурень ЦЗ, що відбуваються саме під час стиску (а не в результаті стеганоперетворення). При високій якості стеганоповідомлень даний програмний комплекс не особливо виділяється на фоні вище розглянутого Stegdetect. Ефективність детектування для групи $QF = 75$ буде приблизно на рівні 50%, що відповідає в бінарному класифікаторі випадковому віднесенню об'єкта до класу. Однак використання JPEG з низьким QF при організації стеганографічного каналу є невиправданим з кількох причин: через ненульову ймовірність порушення надійності сприйняття зображеня-стеганоповідомлення (на фоновій області ЦЗ); у випадку, якщо використовуваний стеганоалгоритм не є стійким до стиску; навіть для стійкого до стиску стеганоалгоритму ефективність (NC) знижується при малих значеннях QF, тому організатори стеганографічного каналу звязку не зацікавлені в пересиланні стеганоповідомлення з малим коефіцієнтом якості; пересилання ЦЗ в «поганій» якості також може привернути до себе небажану увагу.

Таблиця 4.16 — Ефективність детектування розробленого стеганографічного алгоритму SA_B сучасними стеганоаналітичними комплексами

Стеганоаналітичний комплекс	Ефективність детектування (%)					
	$QF = 50$	$QF = 60$	$QF = 70$	$QF = 80$	$QF = 90$	$QF = 100$
Canvass	83,6	83,1	72,6	37,2	9,1	1,8
Stegdetect	0	1,6	0,5	13,5	3,1	1
StegAlyzerSS	0					

Таким чином, хоча в роботі розглянуто три стеганоаналітичних комплекси, однак недоліки цих програмних продуктів можуть бути віднесені до роботи й інших комплексів, через те, що принципи функціонування залишаються

практично незмінними. У результаті проведених експериментів практично підтверджується стійкість стеганографічного алгоритму SA_B до стеганоаналітичних атак сучасними програмними комплексами [161,162].

Отримані результати свідчать про те, що

- Розроблений алгоритм не має аналогів у базах сигнатур стеганоаналітичних комплексів, що здійснюють визначення наявності вкладення по масці використовуваного алгоритму;
- Навченість стеганоаналітичних комплексів (будь то лінійний дискримінантний аналіз, або ж метод опорних векторів) вимагає для своєї реалізації наявності постійно діючого стеганографічного каналу, що на практиці не тільки часто не реалізовано, але і є малоймовірним (з урахуванням вимоги підтримки прихованості й безпеки самого каналу);
- Для високоякісних JPEG-зображень із QF вище 90 ефективність детектування не перевищує 10%.

4.6 Висновки до розділу 4

У розділі 4 проведений аналіз і оцінена ефективність розроблених стеганографічних алгоритмів стосовно атак проти вбудованого повідомлення.

Отримані наступні результати:

1. Розроблено стеганографічний алгоритм SA_M, що є модифікацією алгоритму SA_B, який зменшує спотворення контейнера під час стеганоперетворення, кількісною оцінкою якого є $PSNR$, в порівнянні з SA_B, в середньому на 8.2%.
2. Практично підтверджено, що стійкість SA_B, SA_M до накладання шумів визначається величиною спотворення СП ($PSNR$), а не характером накладеного шуму. Встановлена висока стійкість SA_B, SA_M до накладання шумів: загалом стійкість розроблених СА перевищує стійкість сучасних аналогів. Зокрема для найчастіше використовуваної при тестуванні СА

дисперсії гаусівського шуму $D = 0.005$ стійкість SA_B перевищує найкращий з аналогів на 4%; для найчастіше вживаної дисперсії $D = 0.001$ при накладанні мультиплікативного шуму стійкість SA_B більша за стійкість найкращого з аналогів на 1.5%; при накладанні пуасонівського шуму стійкість SA_B перевищує стійкість всіх аналогів і становить $NC = 0.9987$.

3. Встановлена висока стійкість до атаки фільтрацією для розробленого алгоритму SA_B, яка перевищує стійкість усіх розглянутих сучасних аналогів. При цьому для усереднюючого фільтра шляхом розробки SA_B максимально вдалося підвищити стійкість на 13%; для гауссівського й медіанного фільтрів стійкість SA_B близька до 1: $NC = 0.996568$, $NC = 0.997177$ відповідно.

4. Практично підтверджено, що стійкість SA_B до атаки стиском визначається величиною спотворення СП ($PSNR$), а не конткретним способом стиску. Встановлено, що стійкість SA_B до атаки стиском перевищує стійкості всіх розглянутих аналогів при всіх значеннях QF, при цьому для $QF > 80$ значення NC для SA_B близько до 1. Результати порівняння SA_B з аналогом, взятим за основу, практично підтвердили зроблені в розділі 1 висновки про перевагу ПО для вбудови ДІ, в порівнянні з ОПр контейнера. Встановлено, що SA_B є стійким до комплексних атак. Так при атаці дворазовим стиском: при комбінація різних/однакових значень $QF = 50,70,80,90$ при первинному й повторному стиску значення $NC > 0.96$, а при комбінації $QF = 80,90$, які є найбільш часто використовуваними при стиску, $NC = 0.99$; накладання шуму з найбільш часто використовуваними параметрами з наступним стиском забезпечило значення $NC > 0.98$ при $QF \geq 70$.

5. Практично підтверджена стійкість SA_B до стеганоаналітичних атак сучасними програмними комплексами. Для високоякісних ЦЗ, які, з урахуванням необхідного забезпечення надійності сприйняття СП, з великою ймовірністю використовуються в процесі стеганографічної передачі даних, ефективність детектування вкладення ДІ не перевищує 10%.

Таким чином, у розділі 4 практично підтверджена висока стійкість до атак проти вбудованого повідомлення розроблених на основі отриманої в розділі 2 формальної достатньої умови стеганоалгоритмів, яка перевищує стійкість сучасних аналогів завдяки використанню для стеганоперетворення/декодування ДІ просторової області ЦЗ; остаточно вирішена задача 5 з переліку задач дисертаційної роботи.

Основні результати розділу знайшли своє відображення в роботах [116,117,118,124,153,161,162].

ВИСНОВКИ

В роботі вирішена важлива науково-практична задача, що полягає в підвищенні ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення шляхом розробки стеганографічних методів й алгоритмів для організації прихованого каналу зв'язку, що працюють у просторовій області контейнера, стійких до збурних дій.

Практична цінність роботи полягає в доведенні отриманих наукових результатів до конкретних алгоритмів, які можуть бути використані як складові частини комплексних систем захисту інформації будь-якої установи, підприємства.

У роботі отримані наступні результати:

1. Вперше на основі встановленої відповідності між збуреннями максимального сингулярного числа, яскравості пікселів блоку матриці зображення отримана формальна достатня умова забезпечення стійкості стеганоалгоритму до атак проти вбудованного повідомлення у просторовій області зображення-контейнера, що дозволило розробити теоретичний базис гарантовано стійких до збурних дій стеганометодів і алгоритмів, які працюють в просторовій області.
2. Вперше на основі розробленого теоретичного базису, розроблені стеганографічні методи і поліноміальні (степеня 2) алгоритми, що їх реалізують, стійкість яких перевищує стійкість сучасних аналогів, що дало можливість підвищити ефективність стеганографічної системи в умовах накладання шуму максимально на 4%, при атаці фільтрацією – на 13%, забезпечити в умовах атаки стиском при $QF > 80$ ефективність, близьку до максимально можливої: $NC \approx 1$. Практично підтверджена стійкість розроблених алгоритмів до стеганоаналітичних атак.

3. Отримали подальший розвиток умови забезпечення стійкості стеганоалгоритмів до атак проти вбудованого повідомлення за рахунок забезпечення отриманою достатньою умовою залежності ефективності відповідних алгоритмів лише від величини спотворення стеганоповідомлення при збурній дії, що дало можливість для розробки стеганоалгоритмів, стійких: незалежно від формату (з/без втрат) використовуваного зображення-контейнера – максимальна відмінність у значеннях NC для контейнерів з/без втрат склала менше 1%; незалежно від конкретного виду збурної дії (значення NC визначаються значеннями $PSNR$ в результаті атаки на стеганоповідомлення); в умовах комплексних атак проти вбудованого повідомлення: мінімальне значення NC, що відповідає коефіцієнту якості стиску із втратами $QF = 50$, використаному при тестуванні комплексних атак, становить $NC = 0.97$.
4. Отримали подальший розвиток методи розробки стійких до атак проти вбудованого повідомлення стеганоалгоритмів за рахунок: встановлених переваг просторової області зображення в обчислювальній складності (мінімально – $\underline{O}(m^2)$ операцій, де $m \times m$ – розмір матриці контейнера) й обчислювальній похибці, у порівнянні з областями перетворення, для організації стеганоперетворення; отримання кількісних оцінок можливих збурень яскравості пікселів блоків контейнера для стійкого стеганоперетворення залежно від розміру блоку матриці зображення. З врахуванням: необхідності дотримання надійності сприйняття стеганоповідомлення, отримуваної прихованої пропускної спроможності каналу зв'язку, що організується, встановлено значення $\Delta b = 9$ для збурення пікселів 8×8 – блоку контейнера при стеганоперетворенні, що гарантує стійкість до збурних дій.
5. Розроблено стеганоалгоритм SA_M, що є модифікацією алгоритму SA_B, який зменшує спотворення контейнера під час стеганоперетворення, в порівнянні

з SA_B, в середньому на 8.2%, зберігаючи високу стійкість до атак проти вбудованого повідомлення, може бути застосований до будь-якого зображення-контейнера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хорошко, В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. — К. : ЮНИОР, 2003. — 505 с.
2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
3. Задирака, В.К. Анализ стойкости криптографических и стеганографических систем на основе общей теории оптимальных алгоритмов / В.К. Задирака, А.М. Кудин // Jornal of Qafqaz University. Mathematics and Computer Science. — 2010. — No. 30. — PP. 49–58.
4. Хорошко, В.О. Основи комп’ютерної стеганографії: Навч. посіб. для студ. і асп. / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук; Нац. авіац. ун-т. — Вінниця, 2003. — 143 с.
5. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
6. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
7. Рудницкий, В.Н. Стеганоаналитический алгоритм детектирования метода модификации наименьшего значащего бита для контейнеров, хранимых в форматах без потерь / В.Н. Рудницкий, И.А. Узун // Інформатика та математичні методи в моделюванні. – 2012. – Т.2,№3. – С. 238-245.

8. Кобозєва, А.А. Аналіз захищеності інформаційних систем [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напр. «Інформаційна безпека» та «Системні науки та кібернетика» / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко ; М-во трансп. та зв'язку України, Держ. ун-т інформ.-комунікац. технологій. — К. : ДУІКТ, 2010. — 316 с.

9. Кобозева, А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник НТУ «ХПИ». — 2007. — № 18. — С. 81–93.

10. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008 — . — Т.2: Информационная безопасность. — 2008. — 344 с.

11. Бобок, И.И. Детектирование наличия возмущений матрицы цифрового изображения как составная часть стеганоанализа / И.И. Бобок // Вісник Східноукр-го нац-го ун-ту ім. В. Даля. — 2011. — № 7(161). — С. 32–41.

12. Yang, Q.T. Novel Robust Watermarking Scheme Based on Neural Network / Q.T. Yang, T.G. Gao, L. Fan // International Conference on Intelligent Computing and Integrated Systems, 22–24 Oct. 2010, Guilin. — 2010. — PP. 71–75.

13. Mei,S.C. Decision of Image Watermarking Strength Based on Artificial Neural-networks / S.C.Mei, R.H. Li, H.M. Dang, Y.K. Wang // In Proceedings of the 9th International Conference on Neural Information Processing. — 2002. — P.2430-2434.

14. Davis, K.J. Maximizing Strength of Digital Watermarks Using Neural Networks / K.J.Davis, K. Najarian // International Joint Conference on Neural Networks, Washington DC. – 2001. – P. 2893-2898.

15. Vafaei, M. A Novel Digital Watermarking Scheme Using Neural Networks with Tamper Detection Capability/ M.Vafaei, H.Mahdavi-Nasab // J. Basic. Appl. Sci. Res. — 2013. — 3(4). — P. 577-587.

16. Amornaksa, T. Enhanced Images Watermarking Based on Amplitude Modulation / T.Amornaksa, K. Janthawongwilai // Journal of Image and Vision Computing. – 2006. – P.111 – 119.

17. Surachat, K. Pixel-wise based Digital Watermarking Using a Multiple Sections Embedding Technique / K.Surachat // International Journal of Future Computer and Communication. — 2012. — Vol. 1, No. 2. — P.124-127.

18. Doncel, V.R. An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics / V.R.Doncel, N. Nikolaidis, I. Pitas // IEEE Transactions on Visualization and Computer Graghics. — 2007. — 13(5). — P.851-863.

19. Rosa, A. D. Optimum Decoding of Non-additive Full Frame DFT Watermarks / A.D.Rosa, M.Barni, F.Bartolini *et al.* // In Proceedings of the International Conference on Information Hiding, Germany. — 1999. — P.159-171.

20. Bergman, C. Unitary Embedding for Data Hiding with the SVD / C. Bergman, J. Davidson // Proceedings of Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, CA, January 17, 2005. — Vol. 5681. — PP. 619–630.

21. Кобозева А.А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы / А.А.Кобозева // Праці УНДІРТ. — 2006. — №4(48). — С. 44-52.

22. Subhashini, D. Comparison analysis of spatial Domain and compressed Domain steganographic techniques / D. Subhashini, P. Nalini, G. Chandrasekhar // International Journal of Engineering Research and Technology. — 2012. — Vol. 1, Iss. 4. — PP. 1–6.

23. Прохожев, Н.Н. Влияние внешних воздействий на DC-коэффициент матрицы дискретно-косинусного преобразования в полутоновых изображениях / Н.Н. Прохожев, О.В. Михайличенко, А.Г. Коробейников // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. — 2008. — № 56. — С. 57–62.
24. Шумейко, А.А. Использование квантования Ллойда-Макса для внедрения цифровых водяных знаков / А.А. Шумейко, А.И. Пасько, Т.Н. Тищенко // Інформаційна безпека. — 2010. — № 2(4). — С. 101–108.
25. Корольов, В.Ю. Планування досліджень методів стеганографії та стеганоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л.Горінштейн // Вісник Хмельницького національного університету. — 2011. — № 4. — С. 187–196.
26. Королев, В.Ю. Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей / В.Ю. Королёв, В.В. Полиновский, В. А. Герасименко // Управляющие системы и машины. — 2011. — № 1(231).— С. 79–87.
27. Li, B. A Survey on Image Steganography and Steganalysis / B. Li *et al.* // Journal of Information Hiding and Multimedia Signal Processing. — 2011. — Vol.2, No.2. — PP.142–172.
28. Rawat, H. Robust Digital Image Watermarking Scheme for Copyright Protection / H.Rawat, A.Kumar, S.Kumar // International Journal of Computer Applications. — 2013. — Vol.75, No.18. — P.27-32.
29. Hsieh, M.S. Hiding Digital Watermarks Using Multiresolution Wavelet Transform / M.S.Hsieh, D.C. Tseng, Y.H. Huang // IEEE Transactions on Industrial Electronics. — 2001. — 48(5). — P.875-882.
30. Mukherjee, D.P. Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication / D.P.Mukherjee, S. Maitra, S.T. Acton // IEEE Transactions on Multimedia. — 2004. — 6(1). — P.1-15.

31. Shih, F.Y. Combinational image watermarking in the spatial and frequency domains / F.Y. Shih, S.Y.T. Wu // Pattern Recognition. — 2003. — Vol. 36, Iss. 4. — PP. 969–975.

32. Suhail, M.A. Digital watermarking based DCT and JPEG model / M.A. Suhail, M.S. Obaidat // IEEE Transactions on Instrumentation and Measurement. — 2003. — Vol. 52, Iss. 5. — PP. 1640–1647.

33. Fan, C.-H. A robust watermarking technique resistant Jpeg compression / C.-H. Fan, H.-Y. Huang, W.-H. Hsu // Journal of Information Science and Engineering. — 2011. — Vol. 27, Iss. 1. — PP. 163–180.

34. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию/ А.А.Кобозева, М.А.Мельник // Сучасна спеціальна техніка. — 2012. — №4(31) — С.60-69.

35. Lancini, R. A robust video watermarking technique in the spatial domain / R. Lancini, F. Mapelli, S. Tubaro // Proceedings of Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, Zadar, Croatia, 16–19 June 2002. — 2002. — P. 251–256.

36. Huang, H.Y. Robust technique for watermark embedding in a video stream based on block matching algorithm / H.Y. Huang, Y.R. Lin, W.H. Hsu // Optical Engineering. — 2008. — Vol. 47, Iss. 3. — P. 037402-1–037402-14.

37. Qin, C. A Novel Digital Watermarking Algorithm in Contourlet Domain / C. Qin, X. Wen // Journal of Information & Computational Science. — 2014. — 11(2). — P.519–526.

38. Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H.Lin, Y.-R.Wang, S.-J.Horng *et al*. // Expert Systems with Applications. — 2009. — No.36. — P.11509–11516.

39. Meerwald, P. A survey of watermark-domain watermarking algorithms / P.Meerwald, A.Uhl // In Proceedings of the SPIE, Electronic Imaging,

Security and Watermarking of Multimedia Contents III. — 2001. — P.505–516.

40. Fang, H. Robust Watermarking Scheme for Multispectral Images Using Discrete Wavelet Transform and Tucker Decomposition / H.Fang, Q.Zhou, K.Li // Journal of Computers. — 2013. — Vol. 8, No. 11. — P. 2844-2850.
41. Dugad, R. A new wavelet-based scheme for watermarking images / R.Dugad, K.Ratakonda, N.Ahuja // In IEEE ICIP, Chicago, IL. — 1998. — P. 419–423.
42. Kim, J. R. A robust wavelet-based digital watermarking using level-adaptive thresholding / J. R. Kim, Y.S. Moon // In Proceedings of the IEEE ICIP, Kobe. — 1999. — P. 226–230.
43. Kwon, S.G. Highly reliable digital watermarking using successive subband quantization and human visual system / S.G.Kwon,S.W.Ban, I.-S. Ha *et al*. // In Proceedings of IEEE ISIE, Pusan. — 2001. — P. 205–209.
44. Wang, Y.P. Robust image watermark with wavelet transform and spread spectrum techniques / Y.P.Wang, M.J.Chen, P.Y.Cheng // In Thirty-Fourth Asilomar Conference on Signals, Systems and Computers, Pacific Grove. — 2000. — P.1846–1850.
45. Wang, H.J. A multi-threshold wavelet coder (MTWC) for high fidelity image compression / H.J. Wang, C.C.J.Huo // In Proceedings of the IEEE ICIP, Santa Barbara. — 1997. — P.652–655.
46. Wang, H.J. Wavelet-based digital image watermarking / H.J.Wang, P.C.Su, C.C.J.Kuo // Optics Express. — 1998. — 3(12). — P. 491–496.
47. Davoine, F. Comparison of two wavelet based image watermarking schemes / F.Davoine // In International Conference on Image Processing, Vancouver. — 2000. — P.682–685.
48. Huang, J. Image digital watermarking algorithm using multiresolution wavelet transform / J. Huang, C. Yang // In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics. — 2004. — P. 2977–2982.

49. Li, E. An integer wavelet based multiple logowatermarking scheme / E.Li, H.Liang, X.Niu // In Proceedings of the IEEE WCICA. — 2006. — P.10256–10260.

50. Lien, B.K. A watermarking method based on maximum distance wavelet tree quantization / B.K.Lien, W.H. Lin // In 19th Conference on Computer Vision, Graphics and Image Processing. — 2006. — P.269–276.

51. Tsai, M.J. Constrained wavelet tree quantization for image watermarking / M.J.Tsai, C.L. Lin // In Proceedings of the IEEE ICC Glasgow, Scotland. — 2007. — P. 1350–1354.

52. Wang, S.H. Wavelet tree quantization for copyright protection watermarking / S.H.Wang, Y.P. Lin // IEEE Transactions on Image Processing. — 2004. — 13(2). — P.154–165.

53. Wu, G.D. Image watermarking using structure based wavelet tree quantization / G.D.Wu, P.H.Huang // In ICIS, Melbourne, Australia. — 2007. — P. 315–319.

54. Nasir, I.A. A Robust Color Image Watermarking Scheme Based on Image Normalization / I.A. Nasir, A.B. Abdurrman // Proceedings of the World Congress on Engineering, July 3 - 5, 2013, London, U.K. — 2013. — Vol III, WCE 2013.

55. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.

56. Lingamgunta, S. Reversible Watermarking for Image Authentication using IWT / S.Lingamgunta, V.K. Vakulabaranam, S.Thotakura // International Journal of Signal Processing, Image Processing and Pattern Recognition. — 2013. — Vol.6, No 1. — P.145-156.

57. Tian, J. Reversible data embedding using a difference expansion / J. Tian // IEEE Trans. Circuits Syst. Video Technol. — 2003. — Vol. 13, No. 8. — P. 890–896.

58.Chang, C.C. Reversible hiding in DCT-based compressed images / C.C.Chang, C.C.Lin,C.S.Tseng *et al*. // Information Sciences. — 2007. — Vol. 177, No. 13. — P. 2768-2786.

59.Kamstra, L. Reversible data embedding into images using wavelet techniques and sorting / L. Kamstra, H.J. Heijmans // IEEE Trans. Image Process Processing. — 2005. — Vol. 14, No. 12. — P. 2082-2090.

60.Lee, S. Reversible image watermarking based on integer to integer wavelet transform" / S.Lee, C.D.Yoo, T. Kalker // IEEE Trans. Information Forensics and Security. — 2007. — Vol. 2, No. 3. — P. 321-330.

61.Kumsawat, P. A Robust Image Watermarking Scheme Using Multiwavelet Tree / P. Kumsawat, K. Attakitmongcol, A. Srikaew // Proceedings of the World Congress on Engineering. — 2007. — Vol. 1,WCE 2007.

62. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. — 2012. — № 2(8). — С. 99–106.

63. Мельник, М.А. Стеганографический алгоритм для контейнеров-изображений, устойчивый к атаке сжатием / М.А. Мельник // Труды 14-й международной научно-практической конференции «Современные информационные и электронные технологии», 27–31 мая 2013 г. — Одесса, 2013. — С. 193–194.

64.Lin, W.-H. A wavelet-tree-based watermarking method using distance vector of binary cluster / W.-H. Lin, Y.-R.Wang, S.-J. Horng // Expert Systems with Applications. — 2009. — No. 36. — P. 9869–9878.

65.Jayalakshmi, M. Digital watermarking in contourlet domain [C] / M. Jayalakshmi, S.N. Merchant, U.B. Desai // The 18th International Conference on Pattern Recognition, ICPR'06. — 2006. — P. 861-864.

66.The, T.H. An Efficient Blind Watermarking Method based on Significant Difference of Wavelet Tree Quantization using Adaptive Threshold / T.H.The, T.L.Tien // International Journal of Electronics and Electrical Engineering. — 2013. — Vol. 1, No. 2. — P.98-103.

67. Уэлстид, С. Фракталы и вейвлеты для сжатия изображений в действии [Текст] : учебное пособие / С. Уэлстид. — М.: Издательство Триумф, 2003. — 320 с.

68. Hsiel, M. Hiding digital watermarks using multiresolution wavelet transform / M.Hsiel, D. Tseng, Y. Huang // IEEE Trans. Ind. Electron. — 2001. — Vol.48. — P.875–882.

69. Run, R.S. An efficient wavelet-tree-based watermarking method / R.S.Run,S.J.Horng, W.H.Lin *et al*. // Expert Systems with Applications. — 2011. — P. 14 357–14 366.

70. Lin, W.H. An efficient watermarking method based on significant difference of wavelet coefficient quantization / W.H.Lin, S.J.Horng, T.W. Kao *et al*. // IEEE Transactions on multimedia. — 2008. — P.746–757.

71. Wang, Y.R. An intelligent watermarking method based on particle swarm optimization / Y.R.Wang, W.H.Lin, L.Yang // Expert Systems with Applications. — 2011. — Vol.38. — P.8024–8029.

72. Cox, I.J. Secure Spread Spectrum Watermarking for Multimedia / I.J.Cox, J.Kilian, F.T.Leighton, T. Shamoon // IEEE Transactions on Image Processing. — 1997. — Vol.6, No.12. — P. 1673-1687.

73. Hernandez, J.R. DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure / J.R. Hernandez, A. Amado, F. Perez-Gonzalez // IEEE Transactions on Image Processing. — 2000. — Vol. 9, Iss. 1. — PP. 55–68.

74. Cox, I.J. Secure spread spectrum watermarking for images, audio and video / I.J.Cox, J.Kilian, T. Leighton *et al*. // In Proceedings of the IEEE ICIP, Lausanne. — 1996. — P. 243– 246.

75. Kwon, O. H. A variable block-size dot-based watermarking method / O.H.Kwon, Y.S. Kim, R.H. Park // IEEE Transactions on Consumer Electronics. — 1999. — 45(4). — P. 1221–1229.

76. Langelaar, G.C. Optimal ifferential energy watermarking of DCT encoded images and video / G.C. Langelaar, R.L. Lagendijk // IEEE Transactions on Image Processing. — 2001. — Vol. 10, Iss. 1. — P. 148–158.

77. Badran, E.F. DCT-Based Digital Image Watermarking Via Image Segmentation Techniques / E. F. Badran, A. Ghobashy, K. El-Shenawy // In Proc. of ITI 4th International Conference on Information and Communications Technology, Alaska. USA. — 2006.

78. Patra, J.C. Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital media authentication / J.C. Patra, A.K. Kishore, C. Bornand // In Proc. of 2011 IEEE International Conference on Systems, Man, and Cybernetics. — 2011. — P. 2940 – 2945.

79. Farid, M. Near-lossless spread spectrum watermarking for multispectral remote sensing images / M.Farid, B.Redha, F.G.B. De Natale // Journal of Applied Remote Sensing. — 2007. — Vol. 1, Iss. 1. — P. 3501-3517.

80. Кобозева, А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах / А.А.Кобозева // Вісник Східноукр-го нац-го ун-ту ім. В.Даля. — 2006. — №9(103), ч.1. — С.74—82.

81. Liu, R. A svd-based watermarking scheme for protecting right-ful ownership / R.Liu, T. Tan // IEEE Transactions on Multimedia. — 2002. — Vol. 4. — P. 121-128.

82. Loukhaoukha, K. Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective / K. Loukhaoukha // Phd thesis, Laval University. — 2010. — P. 115-126.

83. Huang, F. A hybrid SVD-DCT watermarking method based on LPSNR / F.Huang, Z.H. Guan // Pattern Recognition Letters. — 2004. — Vol. 25. — P.1769–1775.

84. Cai, Y.-M. An Audio Blind Watermarking Scheme Based on DWT-SVD / Y.-M.Cai, W.-Q. Guo, H.-Y. Ding // Journal of Software. — 2013. — Vol. 8, Iss. 7. — P. 1801-1808.

85. Ma, L. Digital watermarking of spectral images using PCA-SVD / L.Ma, C.Li, S.Song // Journal of Imaging Science and Technology. — 2007. — Vol. 51, Iss. 1. — P. 80-86.

86. Kumar, S. SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform / S. Kumar, N. Arora, J. Kishore // International Journal of Computer Applications. — 2012. — Vol. 57, No.11. — P.176-185.

87. Praful Saxena. DWT-SVD Semi-Blind Image Watermarking Using High Frequency Band / Praful Saxena, Shanon Garg and Arpita Srivastava // In Proceedings of the 2nd International Conference on Computer Science and Information Technology (ICCSIT'2011), April 28–29, Singapore. — 2011. — PP. 138–142.

88. Maheswari, S. A novel blind 3-D CDHWT-SVD based watermarking algorithm for hyper spectral images / S. Maheswari, K. Rameshwaran // European Journal of Scientific Research. — 2012. — Vol. 71, No. 2. — P. 163-173.

89. Elkhamssa, L. Robust content based watermarking algorithm using singular value decomposition of radial symmetry maps / L.Elkhamssa, B.Mohamed // Signal & Image Processing : An International Journal (SIPIJ). — 2014. — Vol.5, No.1. — P.13-28.

90. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А.Кобозева, М.А.Мельник // Збірник наукових праць Військового інституту Київського національного університету ім.Т.Г.Шевченка. — 2012. — Вип.38. — С.193-203.

91. Кобозева, А.А. Анализ чувствительности сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию /

А.А. Кобозева, М.А. Мельник // Захист інформації. — 2013. — Том 15, №2. — С. 88–96.

92. Kutter, M. Improved Digital Signature of Colour Images using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Journal of Electronic Imaging. — 1998. — P. 326 – 332.

93. Nasir, I. A New Robust Watermarking Scheme for Color Image in Spatial Domain / I. Nasir, Y. Weng, J. Jiang // In Proceedings of the 3rd International IEEE Conference on Signal-Image Technologies and Internet-Based System (SITIS'07), 16–18 Dec. 2007, Shanghai. — 2007. — PP. 942–947.

94. Viswanatham, V.M. Novel Technique for Embedding Data in Spatial Domain / V.M.Viswanatham, J.Manikonda // International Journal on Computer Science and Engineering. — 2010. — Vol. 2. — P.233-236.

95. Sulong, G.B. A New Watermarking Technique for Mammogram Images Copy Right Protection / G.B.Sulong, H.R.Hasan, T. Hajiabdollah *et al*. // Life Science Journal. — 2014. — Vol. 11, Iss.5. — P.102-108.

96. Alattar, A.M. Reversible watermark using the difference expansion of a generalized integer transform / A.M. Alattar // IEEE Trans. Image Processing. — 2004. — Vol. 13, No. 8. — P. 1147-1156.

97. Thodi, D.M. Expansion embedding techniques for reversible watermarking / D.M.Thodi, J.J. Rodríguez // IEEE Trans. Image Processing. — 2007. — Vol. 16, No. 3. — P. 721-730.

98. Celik, M.U. Lossless generalized-LSB data embedding / M.U. Celik, G. Sharma, A.M. Tekalp *et al*. // IEEE Trans. Image Processing. — 2005. — Vol. 14, No. 2. — P. 253-266.

99. Ni, Z. Reversible data hiding / Z. Ni, Y.-Q. Shi, N. Ansari *et al*. // IEEE Trans. Circuits Systems Video Technology. — 2006. — Vol. 16, No. 3. — P. 354-362.

100. Puertpun, R. Pixel Weighting Marks in amplitude Modulation of Colour Image Watermarking / R. Puertpun, T. Amornraksa // In Proceedings of the IEEE ISSPA, Kuala-Lumpur. — 2001. — P. 194 – 197.

101. Костырка, О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В.Костырка // Інформатика та математичні методи в моделюванні. — 2013. — Т.3, №3. — С.275-282.

102. Костырка, О.В. Преимущества пространственной области контейнера-изображения при организации стеганопреобразования / О.В.Костырка // Праці ІІІ-ї Міжнародної науково-практичної конференції «Проблеми інформатики та комп'ютерної техніки». Чернівці, 27-30 травня, 2014 р. — С.181-183.

103. Каханер, Д. Численные методы и программное обеспечение [Текст] / Д. Каханер, К. Моулер, С. Нэш ; Пер. с англ. под ред. Х.Д.Икрамова. — 2-е изд., стер. — М. : Мир, 2001. — 575 с.

104. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель ; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.

105. Бахвалов, Н.С. Численные методы [Текст] : учебное пособие для студ. физико-математических спец. вузов; Рекомендовано МО РФ / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — 6-е изд. — М. : БИНОМ. Лаборатория знаний, 2008. — 636 с.

106. Кобозева, А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А.Кобозева, О.В. Костырка // Інформаційна безпека. — 2013. — №3(11). – С.29-35.

107. Кобозева, А.А. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного

сообщения / А.А.Кобозева, О.В.Костырка, Е.Ю.Лебедева // Проблемы региональной энергетики. Электронный журнал Академии наук республики Молдова. — 2014. — №1(24). — С. 1-12.

108. Кобозева, А.А. Формальные достаточные условия устойчивости стеганоалгоритма в пространственной области контейнера-изображения / А.А.Кобозева, О.В.Костырка // Труды XV Международной научно-практической конференции «Современные информационные и электронные технологии». — 26-30 мая 2014 г. Украина. Одесса. Т.1. — С.129-130.

109. Кобозева, А.А. Повышение эффективности метода обнаружения фальсификации цифрового изображения, основанного на анализе сингулярных чисел матрицы / А.А.Кобозева, Е.А.Трифонова // Труды Одесского политехнического университета. — 2008. — №1(29). — С.183-190.

110. Бобок, И.И. Стеганоанализ как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева // Сучасна спеціальна техніка. — 2011. — №2. — С. 21–34.

111. Сборник задач по математике для поступающих во втузы [Текст] / ред. М.И. Сканави. — 6-е изд., стер. — М. : Высш. шк., 1992. — 528 с.

112. Воеводин, В.В. Математические основы параллельных вычислений [Текст] / В.В.Воеводин. — М.: Изд-во Моск. ун-та, 1991. — 345 с.

113. Воеводин, В.В. Параллельные вычисления [Текст] / В.В. Воеводин, Вл. В. Воеводин. — СПб.: БХВ-Петербург, 2002. — 608 с.

114. Бобок, И.И. Разработка устойчивого стеганографического алгоритма, обладающего внутренним параллелизмом / И.И.Бобок, А.А.Кобозева, О.В.Костырка // Криптографическое кодирование: коллективная монография. Под редакцией В.Н. Рудницкого, В.Я. Мильчевича. — Краснодар, 2014. — С. 98 – 119.

115. Костирка, О.В. Стійке стеганоперетворення в просторовій області зображення-контейнера / О.В.Костирка, В.М.Рудницький // Інформатика та математичні методи в моделюванні. — 2013. — Т.3, №4. — С.353-360.

116. Костирка, О.В. Стеганографічний алгоритм, стійкий до накладання шуму / О.В.Костирка // Безпека інформації. — 2014. — Т.20, №1. — С. 71-75.

117. Костырка, О.В. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к сжатию // О.В.Костырка, М.А.Мельник, В.Н.Рудницкий // Сучасна спеціальна техніка. — 2014. — №1(36). — С.75-84.

118. Костирка, О.В. Реалізація стеганоперетворення, стійкого до накладання шуму/ О.В.Костирка // Одинадцята Всеукраїнська конференція студентів і молодих науковців «Інформатика, інформаційні системи та технології». — Одеса, 2014. — С. 56-57.

119. Kumar, D. Contourlet transform based watermarking for colour images / D.Kumar,V.Kumar // The International Journal of Multimedia & Its Applications (IJMA). — 2011. — Vol.3, No.1. — P.122-131.

120. NRCS Photo Gallery: *[Електронний ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступу: http://photogallery.nrcs.usda.gov (Дата звернення: 26.07.2012).

121. Fadaeenia, B. Hybrid DCT-CT Digital Image Adaptive Watermarking / B.Fadaeenia, N. Zarei // DBKDA 2011: The Third International Conference on Advances in Databases, Knowledge, and Data Applications. — 2011. — P. 47-53.

122. Костырка, О.В. Анализ устойчивости стеганопреобразования пространственной области контейнера-изображения к атаке фильтрацией / О.В.Костырка, М.А.Мельник, В.Н.Рудницкий // Системи обробки інформації. — 2014. — Вип.2(118), том 2. — С. 91-95.

123. Гонсалес, Р. Цифровая обработка изображений в среде MATLAB / Р.Гонсалес, Р.Вудс, С.Эддинс; перев. с англ. В.В.Чепыжова. — М.: Техносфера, 2006. — 616 с.

124. Костырка, О.В. Устойчивость пространственного стеганопреобразования к атаке фильтрацией / О.В.Костырка, М.А.Мельник, В.Н.Рудницкий // Системи обробки інформації. VI Міжнародна НПК «Проблеми і перспективи розвитку IT-індустрії» — 2014. — Випуск 2(118), том 2. — С.256.

125. Su, C.-Y. A Robust Color Image Watermarking Using Maximum Wavelet-Tree Difference Scheme [*Електронний ресурс*] / C.-Y. Su, Y.-L. Chen // The 2013 World Congress in Computer Science, Computer Engineering, and Applied Computing. — 2013. — Режим доступу: http://worldcomp-proceedings.com/proc/p2013/IPC3490.pdf (Дата звернення: 11.03.2014).

126. Al-Otum, H. A robust blinds color image watermarking based on wavelet-tree bit host difference selection / H. Al-Otum, N. Samara // Signal Processing. — 2010. — Vol. 90. — P. 2498-2512.

127. Bazargani, M. Digital Image Watermarking in Wavelet, Contourlet and Curvelet Domains / M.Bazargani, H.Ebrahimi, R.Dianat // J. Basic. Appl. Sci. Res. — 2012. — Vol.2, No. 11. — P. 11296-11308.

128. Zhu, S.M. A Novel Blind Watermarking Scheme in Contourlet Domain Based on Singular Value Decomposition / S.M. Zhu, J.M. Liu // Proc. WKDD'09. — 2009. — Vol.1. — P. 672-675.

129. Jiang, J. An Image Watermarking Algorithm with Adaptively Determining the Number of Information Bits to Be Embedded / J.Jiang, Y.Zhu, Q.Su // Journal of Information & Computational Science. — 2013. — Vol. 10, No. 14. — P. 4555–4562.

130. Perwej, Y. Copyright Protection of Digital Images Using Robust Watermarking Based on Joint DLT and DWT / Y.Perwej, F.Parwej, A.Perwej //

International Journal of Scientific & Engineering Research. — 2012. — Vol. 3, Iss.6. — P. 1-9.

131. Agarwal, H. Highly Robust and Imperceptible Luminance Based Hybrid Digital Video Watermarking Scheme for Ownership Protection / H.Agarwal, R.Ahuja, S.S.Bedi // I.J. Image, Graphics and Signal Processing. — 2012. — Vol. 11. — P. 47-52.

132. Isac, B. Region of non-interest based digital image watermarking using neural networks / B.Isac, V. Santhi, A.Thangavelu // Ictact Journal on Image and Video Processing. — 2011. — Vol. 2, Iss. 2. — P. 287-293.

133. Xie, J. Fingerprint image watermarking algorithm using the quantization of parity based on contourlet transform / J. Xie, Y. Wu // Computer Applications. — 2007. — Vol. 6. — P. 1365–1367.

134. Alsaif, K.I. Studying The Noise Effect on Data Hiding Based on Contourlet Coefficients / K.I.Alsaif, N.S.Al-lella // Iraqi Journal of Statistical Sciences. The 6th Scientific Conference of the College of Computer Sciences & Mathematics. — 2013. — Vol. 25. — P. 165-180.

135. Ali, B.O. Semi-Blind RGB Color Image Watermarking Using DCT and Two Level SVD/ B.O.Ali, G.B.Sulong // Signal & Image Processing: An International Journal (SIPIJ). — 2013. — Vol.4, No.5. — P. 1-10.

136. Wang, T.-Y. A Novel Robust Color Image Digital Watermarking Algorithm Based on Discrete Cosine Transform / T.-Y.Wang, H.-W.Li // Journal of Computers. — 2013. — Vol. 8, No. 10. — P.2507-2511.

137. Harish, N.J. Hybrid Robust Watermarking Technique Based on DWT, DCT and SVD / N.J.Harish, B.B.S. Kumar, A. Kusagur // International Journal of Advanced Electrical and Electronics Engineering. — 2013. — Vol. 2, Iss. 5. — P.137-143.

138. Rahman, M.M. A DWT, DCT and SVD based watermarking technique to protect the image piracy/ M.M.Rahman // International Journal of Managing

Public Sector Information and Communication Technologies. — 2013. — Vol. 4, No. 2. — P. 21-32.

139. Singh, A. Choice of Wavelet from Wavelet Families for DWT-DCT-SVD Image Watermarking / A.Singh, A.Tayal // International Journal of Computer Applications. — 2012. — Vol. 48, No.17. — P. 9-14.

140. Ali, H.A. Robust Digital Image Watermarking Technique Based on Histogram Analysis / H.A. Ali, A. K. Khamis // World of Computer Science and Information Technology Journal. — 2012. — Vol. 2, No. 5. — P.163-168.

141. Vahedi, E. Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles / E.Vahedi, R.A.Zoroofi, M.Shiva // Digital Signal Processing. — 2012. — Vol. 22. — P. 153–162.

142. Maheswari, S. Robust Blind Complex Double Haar Wavelet Transform Based Watermarking Algorithm for Digital Images / S.Maheswari, K.Rameshwaran // IACSIT International Journal of Engineering and Technology. — 2011. — Vol. 3, No. 6. — P.638-645.

143. Ramani, K. Colour Image Watermarking using Bi-Orthogonal Wavelet Transform / K. Ramani, E.V. Prasad, V.L. Naidu *et al*. // International Journal of Computer Applications. — 2010. — Vol. 11, No.9. — P.25-29.

144. Lu, J. A Robust Fractal Color Image Watermarking Algorithm / J.Lu, Y.Zou, C. Yang *et al*. // Mathematical Problems in Engineering. — 2014. — Vol. I. — P.1-12.

145. Vafaei, M. A New Robust Blind Watermarking Method Based on Neural Networks in Wavelet Transform Domain / M. Vafaei, H. Mahdavi-Nasab, H.Pourghassem // World Applied Sciences Journal. — 2013. — Vol. 22, No. 11. — P.1572-1580.

146. Soheili, M.R. Blind Wavelet Based Logo Watermarking Resisting to Cropping // M.R. Soheili // In Proceedings of the 20th International Conference on Pattern Recognition (ICPR’2010), 23–26 Aug. 2010, Istanbul. — 2010. — PP. 1449–1452.

147. Leung, H.Y. Robust digital image watermarking scheme using wave atoms with multiple description coding [*Електронний ресурс*] / H.Y. Leung, L.M. Cheng, F. Liu // EURASIP Journal on Advances in Signal Processing. — 2012. — Vol. 2012. — Режим доступу: http://asp.eurasipjournals.com/content/2012/1/245 (Дата звернення: 11.03.2014).

148. Ramanjaneyulu, K. An oblivious and robust multiple image watermarking scheme using genetic algorithm / K. Ramanjaneyulu, K. Rajarajeswari // IJMA. — 2010. — Vol. 2, No. 3. — P. 19–38.

149. Cedillo-Hernandez, M. Robust Object-Based Watermarking Using SURF Feature Matching and DFT Domain / M. Cedillo-Hernandez, F. Garcia-Ugalde, M.Nakano-Miyatake *et al*. // Radioengineering. — 2013. — Vol. 22, No. 4. — P. 1057-1071.

150. Hammouri, A.I. An Intelligent Watermarking Approach Based Particle Swarm Optimization in Discrete Wavelet Domain / A.I. Hammouri, B.Alrifai, H.Al-Hiary // IJCSI International Journal of Computer Science. — 2013. — Vol. 10, Iss. 2, No. 1. — P.330-338.

151. Kalra, G.S. Digital Image Watermarking With Random Selection of Watermark Insertion Having Adaptive Strength / G.S. Kalra, R. Talwar, H.Sadawarti // Research Journal of Applied Sciences, Engineering and Technology. — 2014. — Vol.7, Iss. 8. — P. 1644-1655.

152. Aiman, M. A Color Watermarking Scheme Based on Conway Game / M.Aiman, A.Awwad // International Journal of Computer Science and Telecommunications. — 2013. — Vol. 4, Iss. 2. — P.15-19.

153. Костирка, О.В. Порівняльна оцінка стійкості стеганометодів, стеганоалгоритмів до стиску / О.В. Костирка, М.О. Мельник // Інформаційна та економічна безпека : матеріали Міжнародної наук.-практ. інтернет-конференції – Х. : ХІБС УБС НБУ, 2014. — 1 електрон. опт. диск (CD-ROM). — Систем. вимоги: Pentium ; 512 Mb RAM ; Windows XP, 7, 8; Adobe Acrobat

Reader 5.0 - 10.0;. — Назва з екрану. — Режим доступу: http://khibs.edu.ua/site_razdel/mizhnarodna_naukovo-praktichna_internet-konferencija_informaciina_ta_ekonomichna_bezpeka_%28infeco-2014%29.php

154. Peng, L. A blind image watermarking scheme based on wavelet tree quantization / L. Peng, D. Zhizhong // Second International Symposium on Electronic Commerce and Security (ISECS'09), 22–24 May 2009, Nanchang. — 2009. — Vol. 1. — PP. 218–222.

155. Xiao, Y. A robust image watermarking scheme based on a novel HVS model in curvelet domain / Y. Xiao, L.M. Cheng, L.L. Cheng // In International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China. — 2008. — P. 343–346.

156. Li, F. Multi-Bit Digital Watermarking Based on Bit Decomposition/ F. Li, X.Luo, F. Dai *et al*. // International Journal of Information and Systems Sciences. — Vol. 4, No. 4. — P. 548-559.

157. Steganography Analyzer Signature Scanner (StegAlyzerSS) : *[Электронный ресурс]* // SARC: Steganography Analysis and Research Center. Fairmont, USA. Режим доступа: http://www.sarc-wv.com/products/stegalyzerss/ (Дата обращения: 26.01.2014).

158. Steganography Detection with Stegdetect : *[Электронный ресурс]* // OutGuess.org by Niels Provos. Режим доступа: http://www.outguess.org/detection.php (Дата обращения: 26.01.2014).

159. Линейный дискриминантный анализ : *[Электронный ресурс]* // MachineLearning.ru — Профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных. Режим доступа: http://www.machinelearning.ru/wiki/index.php?title=Линейный_дискриминантный_анализ (Дата обращения: 26.01.2014).

160. Jalan, J. Feature selection, statistical modeling and its applications to universal JPEG steganalyzer : *[Электронный ресурс]* // Digital Repository @ Iowa State

University. USA. Режим доступа: http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2039&context=etd (Дата обращения: 26.01.2014).

161. Бобок, И.И. Анализ устойчивости нового стеганографического алгоритма к стеганоаналитическим атакам / И.И.Бобок, О.В.Костырка // Сучасний захист інформації. – 2014. – № 2. – С. 28-34.

162. Бобок, І.І. Дослідження стійкості нового стеганографічного методу до стеганоаналізу / І.І.Бобок, О.В.Костирка // Збірник матеріалів V науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави». — 2014. — Київ. — С.143-145.

Додаток А

АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ

ЗАТВЕРДЖУЮ

Начальник управління ДСНС України в Черкаській області
генерал-майор служби цивільного захисту
кандидат технічних наук, доцент

_____ В.М. Гвоздь

«20» _____12_____ 2013 р.

АКТ

про впровадження наукових результатів дисертаційного дослідження «Підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення»

Костирки Олесі Вікторівни

Дана робота виконувалась в рамках договору про співробітництво між Академією пожежної безпеки імені Героїв Чорнобиля і У ДСНС України в Черкаській області.

Комісія у складі:

голова комісії - Сташенко С.І., к.і.н., доцент, полковник с.ц.з., перший заступник начальника У ДСНС України в Черкаській області;

члени комісії:

1. Дубенець О.С., підполковник с.ц.з., начальник аварійно-рятувального загону спеціального призначення У ДСНС України в Черкаській області;

2. Вінніченко М.В., підполковник с.ц.з., начальник сектора телекомунікацій, інформаційних технологій та системи 112 У ДСНС України в Черкаській області;

Встановила, що розроблені стеганографічні алгоритми дозволяють підвищити стійкість цифрових водяних знаків, що вбудовуються в цифрові контенти для забезпечення їх автентичності, в умовах збереження їх у форматах із втратами, в тому числі, з великим коефіцієнтом стиску. Це дозволило зменшити об'єм файлів, що зберігаються, передаються по каналах зв'язку в процесі організації електронного документообігу, без спотворення інформації, що ідентифікує автора, власника, в середньому на 17.6%, шляхом збереження в форматах з втратами із значними коефіцієнтами стиску.

Голова комісії С.І. Сташенко

Члени комісії: О.С. Дубенець

М.В. Вінніченко

ЗАТВЕРДЖУЮ
Проректор
з навчальної роботи
к.т.н., доц.
О.О. Ситник
«10» 04 2014 р.

АКТ

про впровадження наукових результатів дисертаційного дослідження «Підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення»
Костирки Олесі Вікторівни

Комісія в складі: голови комісії – доцента кафедри комп'ютерних систем к.т.н., доц. Ланських Є.В., членів комісії – доцента кафедри системного програмування, к.ф-м.н., доц. Півень О.Б., доцента кафедри системного програмування, к.т.н., доц. Бабенко В.Г., склали цей акт про те, що результати дисертаційної роботи Костирки Олесі Вікторівни а саме – стеганографічні алгоритми, які дозволяють підвищити стійкість цифрових водяних знаків, що вбудовуються в цифрові контенти для забезпечення їх автентичності, в умовах збереження їх у форматах із втратами, в тому числі, з великим коефіцієнтом стиску використовуються в навчальному процесі Черкаського державного технологічного університету при викладанні дисципліни «Системи захисту інформації» студентами денної форми навчання за напрямом підготовки 050102 «Комп'ютерна інженерія».

Голова комісії: Є.В. Ланських

Члени комісії: О.Б. Півень

В.Г. Бабенко

ЗАТВЕРДЖУЮ
Заступник начальника інституту
з навчальної та наукової роботи
кандидат технічних наук, доцент
_____ О.М. Тищенко
«14» 05 2014 р.

АКТ
впровадження результатів дисертаційної роботи
Костирки Олесі Вікторівни

Комісія в складі: голови комісії – начальника навчально-методичного відділу, підполковника с.ц.з. Короля В.М., членів комісії – начальника факультету пожежної безпеки, к.т.н., доцента, підполковника с.ц.з. Джулая О.М., начальника кафедри вищої математики та інформаційних технологій к.ф-м.н., доцента, полковника с.ц.з Частоколенка І.П., професора кафедри вищої математики та інформаційних технологій д.ф-м.н., професора Акіньшина В.Д. склали цей акт про те, що основні практичні результати дисертаційної роботи Костирки О.В.: розроблені стеганографічні алгоритми, що працюють в просторовій області зображення-контейнера, є стійкими, незалежно від формату (з втратами, без втрат) контейнера, до атак проти вбудованого повідомлення (накладанню шумів на стеганоповідомлення, фільтрація, атака стиском з втратами стеганоповідомлення) впроваджені в навчальний процес Черкаського інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України та використовуються при викладанні дисципліни «Інформаційне забезпечення діяльності підрозділів цивільного захисту» курсантам і студентам денної форми навчання освітньо-кваліфікаційного рівня „бакалавр”.

Це дозволило підвищити якість викладання курсантам та студентам навчального закладу аспектів взаємозв'язку спеціальних дисциплін з майбутньою професією.

Слід зазначити, що розроблені автором і упроваджені в процес викладання дисципліни «Інформаційне забезпечення діяльності підрозділів цивільного захисту» матеріали дослідження, враховують специфіку професійної підготовки майбутніх фахівців інженерного профілю.

Даний акт не є підставою для одержання премій та інших винагород із фондів Черкаського інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України.

Голова комісії: В.М. Король

Члени комісії: О.М. Джулай

І.П. Частоколенко

В.Д. Акіньшин