МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

КОСТИРКА ОЛЕСЯ ВІКТОРІВНА

УДК 004.056.5

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ В УМОВАХ АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

05.13.21 — системи захисту інформації

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Одеса — 2014

Дисертацією є рукопис.
Робота виконана в Черкаському інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України

Науковий керівник: доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний університет,
завідувач кафедрою інформаційної безпеки та системного програмування

Офіційні опоненти: доктор технічних наук, доцент
Смірнов Олексій Анатолійович,
Кіровоградський національний технічний університет,
професор кафедри програмного забезпечення

кандидат технічних наук, доцент
Браіловський Микола Миколайович,
Державний університет телекомунікацій,
доцент кафедри комп'ютерних систем та мереж

Захист відбудеться « 11 » вересня 2014 р. о 14 годині на засіданні спеціалізованої вченої ради К 41.052.11 в Одеському національному політехнічному університеті за адресою: 65044, м. Одеса, пр. Шевченка, 1, ауд. 400-А.

З дисертацією можна ознайомитись у бібліотеці Одеського національного політехнічного університету за адресою: 65044, м. Одеса, пр. Шевченка, 1.

Автореферат розісланий « 21 » липня 2014 р.

Вчений секретар
спеціалізованої вченої ради В.Я. Чечельницький

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 неможливі без наявності в її складі ефективної стеганографічної системи, що ґрунтується на сучасних стеганографічних алгоритмах (СА).

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, И.Н.Окову, И.В.Туринцеву, В.А.Хорошку, М.Е.Шелесту та ін., а також їх закордонним колегам: C.Bergman, J.Davidson, J.Fridrich, W.-H.Lin, D. Kumar та ін.

У процесі стеганографування конфіденційна інформація після попереднього кодування, результатом якого є додаткова інформація (ДІ), вбудовується в контейнер, чи основне повідомлення (ОП), в якості якого в роботі виступає цифрове зображення (ЦЗ), результатом чого є стеганоповідомлення (СП). СП відкрито пересилається по каналу зв'язку.

При розробці і вдосконаленні 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 атак проти вбудованого повідомлення – збурних дій. До таких атак відносяться, зокрема, накладання шумів на СП, фільтрація, стиск СП із втратами та ін.

Протягом привалого часу вважалося, що для забезпечення стійкості СА кращою для вбудови ДІ є область перетворення (ОПр) ЦЗ, зокрема, частотна область. Завдяки цьому розробки стійких СА у просторовій області (ПО) ЦЗ були нечисленними, безсистемними, не мали потрібного математичного фундаменту. У результаті сучасних наукових досліджень показано, що забезпечення стійкості СА не залежить від того, у якій області контейнера (ПО, ОПр) відбувається вбудова ДІ. При цьому ПО має певні переваги при організації стеганоперетворення (СПр). Зокрема, процес вбудови/декодування ДІ в просторовій області ЦЗ дозволяє зменшити обчислювальні складність та похибку, що накопичується в процесі СПр і декодування ДІ, в порівнянні з аналогічною організацією цих процесів в ОПр. Це говорить про принципову можливість забезпечення більш високої ефективності для СА, що працюють у ПО, у порівнянні зі СА, що працюють в ОПр контейнера.

ПО ЦЗ-контейнера при розробці СА, стійких до збурних дій, на сьогоднішній день незаслужено відійшла на другий план. Серед причин цього: відсутність до цього моменту достатніх умов забезпечення такої стійкості для ПО ЦЗ; більш проста реалізації існуючих достатніх умов стійкості в ОПр контейнера. Усе це гальмує процес підвищення ефективності в умовах атакуючих дій розроблюваних СА, яка на сьогоднішній день, як свідчать відкриті джерела, залишається недостатньою при організації прихованого каналу зв’язку.

Таким чином, задача розробки стійких СА, що працюють у ПО ЦЗ-контейнера, є важливою, а тема дисертації «Підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення» *актуальною.*

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

Тема дисертаційної роботи 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 і задачі дослідження. Метою роботи є 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 ЦЗ, що формалізують процес СПр, які забезпечують стійкість СА до збурних дій, у ПО й областях перетворення, отримання формальної достатньої умови стійкості СА у ПО контейнера використовувалися матричний аналіз, методи цифрової

обробки зображень, обчислювальна лінійна алгебра, теорія збурень. Для отримання кількісних оцінок можливих збурень яскравості пікселів ЦЗ-контейнера в результаті СПр, оцінок збурень блоків матриць СП в процесі атак використовувалися методи обробки зображень, чисельні методи, методи обчислювальної лінійної алгебри. При розробці СА для оцінки їх обчислювальної складності й виявлення внутрішнього паралелізму використовувалися теорія алгоритмів, основи паралельних обчислень.

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 стеганосистем, що є складовими частинами комплексної системи захисту інформації будь-якої установи, підприємства; при організації електронного документообігу.

Розроблені СА SA_B, SA_M, що є поліноміальними степеня 2, при забезпеченні надійності сприйняття СП (середнє значення $PSNR$ для SA_B / SA_M при СПр становить $49/53\,dB$ відповідно) підвищують стійкість стеганосистеми, у порівнянні із системами, побудованими на основі їх сучасних аналогів: в умовах накладання гауссівського/мультиплікативного шуму стійкість максимально, у порівнянні з найкращим з аналогів, була підвищена на 4% / 1.5% відповідно; при накладанні пуасонівського

шуму $NC \approx 1$; при атаці фільтрацією максимально стійкість підвищена на 13% (усереднюючий фільтр, маска 7×7), для гауссова й медіанного фільтрів $NC \approx 1$; стійкість SA_B до атаки стиском перевищує стійкості аналогів, а при коефіцієнті якості $QF > 80$ близька до 1; розроблені СА є стійкими до комплексних атак, 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.

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 ім.Героїв Чорнобиля Національного університету цивільного захисту України та в Черкаському державному технологічному університеті.

Особистий внесок здобувача. Результати дисертаційної роботи отримані автором самостійно. Роботи [1,2,10,11] виконані без співавторів. У роботах, опублікованих у співавторстві, здобувачеві належать: аналіз відповідності збурення максимальних сингулярних чисел (СНЧ) блоків матриці ЦЗ (ОПр) і збурень яскравості пікселів відповідного блоку (ПО), виявлення причин порушення теоретичної відповідності зазначених величин в [3,14]; розробка стеганографічного методу, отримання оцінок збурень блоків матриці ЦЗ в результаті накладання шумів, розробка рекомендації для розмірів блоку при організації СПр в [4]; розробка стійкого СА в ПО ЦЗ-контейнера в [5], дослідження ефективності СА в умовах одноразового й дворазового стиску СП, порівняльний аналіз ефективності розробленого СА із сучасними аналогами в [5,13]; 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 [6,12]; встановлення залежності ефективності стеганоаналітичних комплексів від значення коефіцієнта якості, використаного при стиску із втратами ЦЗ [7,15]; отримання рекомендацій з вибору розміру блоку контейнера, який задіюється при СПр в ПО [8]; виявлення внутрішнього паралелізму розробленого СА на етапі обробки окремого блоку матриці ЦЗ [9].

Апробація результатів дисертації. Результати досліджень доповідалися й обговорювалися на Міжнародних і Всеукраїнських наукових конференціях і семінарах, у тому числі: Міжвідомчий міжрегіональний науковий семінар при Вченій раді НАН України «Технічні засоби захисту інформації» (Одеса, 2013,2014); 15-а Міжнародна науково-практична конференція «Сучасні інформаційні й електронні технології (СІЕТ– 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 ІТ-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 опубліковані в 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 конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, списку використаної літератури з 162 найменувань, 1

додатку, 21 рисунку і 22 таблиць – всього 151 сторінка. Основний текст дисертації складається з 126 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** розкрито сутність і стан наукової задачі та обґрунтовано її актуальність, визначена мета й завдання роботи, показано наукову новизну та практичну значущість отриманих результатів, наведено інформацію про особистий внесок здобувача, апробацію наукових результатів роботи.

В **першому розділі** на основі аналізу літературних джерел по темі дисертації встановлено, що задача забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення не є повністю вирішеною. Більшість СА, що позиціонуються як стійкі до збурних дій, роблять СПр у частотній області ЦЗ-контейнера, у рамках якої одночасне забезпечення стійкості СА до значних збурних дій, надійності сприйняття СП викликає значні труднощі. Велика кількість існуючих СА виявляються стійкими лише до певних атак. До цього моменту не існує формальних достатніх умов забезпечення стійкості СА, що реалізуються у ПО ЦЗ, яка має певні переваги над ОПр при організації СПр. Це уповільнює процес розробки просторових СА, потенційні можливості яких для забезпечення стійкості принципово вищі, в порівнянні з СА, що працюють в ОПр ЦЗ, а тому гальмує процес удосконалення стеганографічної системи і, як наслідок, комплексної системи захисту інформації в цілому.

Таким чином, у розділі 1 показано, що задача підвищення стійкості стеганосистеми до атак проти вбудованого повідомлення шляхом отримання достатньої умови стійкості і розробки на її основі СА, стійких до збурних дій, є актуальною.

У **другому розділі** обґрунтовані переваги ПО зображення для організації СПр в порівнянні з ОПр, розроблені теоретичні основи забезпечення стійкості СА до атак проти вбудованого повідомлення в ПО ЦЗ-контейнера. У ході розробки отримані: відповідності між формальними представленнями стійких СПр в областях перетворень зображення й ПО, формальна достатня умова забезпечення стійкості СА до збурних дій при організації СПр в ПО контейнера, рекомендації з вибору розміру блоку контейнера, задіяного в СПр, як одного з визначальних обчислювальну похибку параметрів у формованому СП.

Будь-яка обробка (перетворення) ЦЗ вимагає обчислювальних витрат. В роботі оцінені «накладні» обчислювальні витрати для переводу ЦЗ із ПО в ОПр, які найчастіше використовуються в стеганографії: дискретне вейвлет-перетворення (ДВП); дискретне косинусне перетворення (ДКП); сингулярне розкладання (СНР) матриці ЦЗ. Показано, що мінімально такі витрати (при організації поблокового СПр) становлять $\underline{O}\left(m^2\right)$операцій, де $m \times m$ – розмір матриці контейнера. Ці витрати можуть стати критичними при організації СПр в ОПр в режимі *on-line*, наприклад, коли як контейнер використовується відеопослідовність.

У множині дійсних чисел послідовне виконання прямого й оберненого ДКП, ДВП, СНР повертає матрицю до її первісного виду, але в системі чисел із плаваючою точкою накопичення обчислювальної похибки приводить до того, що результатом оберненого перетворення не є первинна матриця. На основі обчислювального експерименту, в якому було задіяно 300 ЦЗ, збережених у різних форматах (із втратами, без втрат), в ході якого матриця кожного ЦЗ розбивалася на $l \times l$-блоки B, $l \in \{8, 32, 128\}$ (всі перетворення проводилися поблоково), було встановлено, що середнє значення абсолютної похибки яскравості пікселів відновленого блоку по всіх блоках усіх розглянутих ЦЗ знаходиться в межах $2.2 * 10^{-13} ... 9.1 * 10^{-12}$, зростає з збільшенням розміру блоку, що відповідає очікуванням: зі збільшенням розміру блоку

збільшується кількість операцій при обчисленнях його елементів у процесі переходів ПО – ОПр, ОПр – ПО, збільшується накопичувана похибка. Ненульові значення похибки можуть бути збільшені збуреннями, яких будуть зазнавати елементи ОПр ЦЗ у процесі вбудови/декодуваня ДІ, що може привести в підсумку до виходу елементів матриці ЦЗ при поверненні в ПО за межі $[0, 255]$, що приведе до зростання похибки, і як наслідок, до зниження стійкості СА.

Таким чином, ПО зображення є кращою для організації СПр, у порівнянні з ОПр, як у сенсі остаточної обчислювальної складності процесів СПр й декодування ДІ, так і в сенсі обчислювальної похибки (з урахуванням переходів ПО – ОПр, ОПр – ПО).

Достатні умови забезпечення стійкості до збурних дій СА вже обговорювалися у відкритих джерелах, однак ці достатні умови, як правило, стосуються ОПр контейнера. Останнім часом було доведено, що для забезпечення високої стійкості до збурних дій разом з надійністю сприйняття СП стеганоперетворення достатньо проводити так, щоб його формальним представленням була сукупність збурень максимальних СНЧ (область СНР) блоків матриці ОП, отриманих в результаті її розбиття. Ці збурення відобразяться на параметрах (їх збуреннях) блоків ЦЗ в будь-якій іншій ОПр та ПО. Знаходження цієї відповідності дає змогу для побудови достатньої умови стійкості СА в ОПр ЦЗ, що відрізняються від області СНР, а також в ПО.

Показано, що збурення максимального СНЧ σ_1 (область СНР) блоку B матриці ЦЗ на $\Delta\sigma_1$ у частотній області блоку виражається в збуренні dc-коефіцієнта ДКП на $\Delta\sigma_1$, що може бути використаним при побудові нових стійких до атак проти вбудованого повідомлення СА, що діють у частотній області ЦЗ.

Знайдемо відповідний формальний вираз для збурення σ_1 в ПО ЦЗ. Для $l \times l$ – блоку B матриці ЦЗ-контейнера існує СНР:

$$B = U\Sigma V^T = (u_1,...,u_l)\begin{pmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma_l \end{pmatrix}(v_1,...,v_l)^T, \quad (1)$$

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

Збурення найбільшого СНЧ блоку формально виражається наступним чином:

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

$$+ (u_1,...,u_l)\begin{pmatrix} \Delta\sigma_1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}(v_1,...,v_l)^T, \quad (2)$$

де $\overline{B}$ – результат збурення B. Таким чином, у ПО формула (2), має вид:

$$\overline{B} = B + \Delta\sigma_1 u_1 v_1^T = B + \Delta B, \quad (3)$$

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

Відомо, що СНВ u_1, v_1 8×8 – блоків матриці ЦЗ, що відповідають σ_1, у випадку нормального СНР, яке додатково в (1) вимагає лексикографічну додатність лівих

СНВ і визначається однозначно, у переважній більшості блоків близькі до n-оптимального вектору $n^O \in R^8$. Показано, що відмінності u_1, v_1 від n^O, загальний вид якого в просторі R^l – $n^O = \left(1/\sqrt{l},\ldots,1/\sqrt{l}\right)^T$, є незначними при будь-якому розмірі l блоку:

$$u_1 \approx n^O,\; v_1 \approx n^O. \tag{4}$$

Якщо $u_1 = (u_{11}, u_{21}, \ldots, u_{l1})^T$, $v_1 = (v_{11}, v_{21}, \ldots, v_{l1})^T$, то матриця ΔB в (3) має вид:

$$\Delta B = \Delta\sigma_1 u_1 v_1^T = \Delta\sigma_1 \begin{pmatrix} u_{11} \\ u_{21} \\ \ldots \\ u_{l1} \end{pmatrix} (v_{11}, v_{21}, \ldots, v_{l1}) = \begin{pmatrix} \Delta\sigma_1 u_{11} v_{11} & \Delta\sigma_1 u_{11} v_{21} & \ldots & \Delta\sigma_1 u_{11} v_{l1} \\ \Delta\sigma_1 u_{21} v_{11} & \Delta\sigma_1 u_{21} v_{21} & \ldots & \Delta\sigma_1 u_{21} v_{l1} \\ \ldots & \ldots & \ldots & \ldots \\ \Delta\sigma_1 u_{l1} v_{11} & \Delta\sigma_1 u_{l1} v_{21} & \ldots & \Delta\sigma_1 u_{l1} v_{l1} \end{pmatrix}. \tag{5}$$

З врахуванням (4) формула (5) набуває вид:

$$\Delta B \approx \begin{pmatrix} \Delta\sigma_1/l & \ldots & \Delta\sigma_1/l \\ \ldots & \ldots & \ldots \\ \Delta\sigma_1/l & \ldots & \Delta\sigma_1/l \end{pmatrix} = \begin{pmatrix} \Delta b & \ldots & \Delta b \\ \ldots & \ldots & \ldots \\ \Delta b & \ldots & \Delta b \end{pmatrix}. \tag{6}$$

Таким чином, стійке СПр в області СНР блоку (2) у ПО ЦЗ-контейнера формально представляється у вигляді збурень яскравості всіх пікселів блоку на одне й те саме значення $\Delta b = \Delta\sigma_1/l$.

Відомо, що для принципової можливості декодування ДІ зі СП, що зазнало збурних дій, сукупний результат збурення блоку контейнера при вбудові ДІ повинен перевищувати збурення, яке буде зазнавати блок СП у процесі збурної дії. Нехай передбачуване збурення блоку $\overline{B}$ СП при атаці – це $\Delta\overline{B}$, тоді відповідно до співвідношення: $\max\limits_{1\le j\le l}\left|\sigma_j\left(\overline{B}\right) - \sigma_j\left(\overline{B}+\Delta\overline{B}\right)\right| \le \left\|\Delta\overline{B}\right\|_2$, 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 СНЧ $\sigma_j\left(\overline{B}\right)$ блоку $\overline{B}$ СП збуриться на величину, не більшу $\left\|\Delta\overline{B}\right\|_2$. Тоді збурення $\Delta\sigma_1$ СНЧ σ_1 блоку B ОП при СПр (що організується в області СНР), повинно бути більшим за $\left\|\Delta\overline{B}\right\|_2$, а збурення $\Delta b = \Delta\sigma_1/l$ значень яскравості пікселів блоку B контейнера при вбудові ДІ в ПО для забезпечення стійкості СА повинні задовольняти співвідношенню:

$$|\Delta b| > \left\|\Delta\overline{B}\right\|_2 / l. \tag{7}$$

Твердження 1 (*достатня умова стійкості СА до збурних дій, яка реалізується в ПО ЦЗ-контейнера*). Для того, щоб СА був стійким до збурної дії, результат впливу якої на $l\times l-$блок СП $\overline{B}$ оцінюється як $\left\|\Delta\overline{B}\right\|_2$, достатньо, щоб СПр, що організується в ПО ЦЗ-контейнера, формально представлялося у вигляді збурень яскравості всіх пікселів кожного блоку, задіяного в СПр, на величину Δb, для якої має місце співвідношення (7).

Зауваження 1. Отримана достатня умова забезпечує стійкість СА до атак проти вбудованого повідомлення незалежно від формату ЦЗ-контейнера (з/без втрат).

Зауваження 2. Забезпечення стійкості СА відповідно до отриманої достатньої умови визначається не конкретним видом збурної дії, а величиною спотворення СП. Це означає, що СА, 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.

Для зменшення накопичення обчислювальної похибки при формуванні СП відповідно до отриманої достатньої умови стійкості СА, а також з врахуванням

відповідності між величинами прихованої пропускної спроможності (ППС) стеганографічного каналу зв'язку, що організується, й розміром блоку l, який використовується для СПр, на цьому етапі роботи рекомендовано розмір блоку $l = 8$.

Таким чином, у розділі 2 розроблений теоретичний базис для стеганометодів і СА, стійких до атак проти вбудованого повідомлення, що здійснюють СПр в ПО ЦЗ.

У **третьому розділі** розроблені стійкі до збурних дій стеганометод й поліноміальний СА, що його реалізує, які діють в ПО ЦЗ-контейнера, на основі отриманої в розділі 2 достатньої умови стійкості, проведено аналіз результатів атак проти вбудованого повідомлення на блоки матриці зображення, отримані рекомендації щодо розмірів блоку та величини збурення пікселів при СПр.

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

Стійкість СА до збурних дій у роботі оцінюється за значенням коефіцієнта кореляції NC для ДІ: $NC = \left(\sum_{i=1}^{t} p_i' \times \overline{p}_i' \right) \Big/ t$, де $p_1, p_2, ..., p_t$ – ДІ, що вбудовується в контейнер, $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$ – декодована ДІ, де $p_i, \overline{p}_i \in \{0,1\}, i = \overline{1,t}$; $p_i' = 1, \overline{p}_i' = 1$, якщо $p_i = 1$, $\overline{p}_i = 1$; $p_i' = -1, \overline{p}_i' = -1$, якщо $p_i = 0, \overline{p}_i = 0$. Будь-які спотворення ЦЗ оцінюються за допомогою значення пікового відношення «сигнал–шум»: $PSNR = 10 \cdot lg\left(255^2 \Big/ \left(\frac{1}{m^2} \sum_{i,j} (F(i,j) - (F + \Delta F)(i,j))^2 \right) \right)$, де $F(i,j)$, $(F + \Delta F)(i,j)$, $i, j = \overline{1,m}$, — значення яскравості пікселів вхідного ЦЗ з $m \times m$–матрицею F і спотвореного з $m \times m$–матрицею $F + \Delta F$ відповідно. Оцінка візуального спотворення ЦЗ за допомогою $PSNR$ в загальному випадку не завжди є придатною для оцінки надійності сприйняття СП, яка носить суб'єктивний характер, тому поряд з $PSNR$ оцінка спотворень ЦЗ в роботі проводиться шляхом суб'єктивного ранжирування.

Нехай F, $\overline{F}$, $\overline{\overline{F}}$ – $m \times m$–матриці контейнера, СП, збуреного СП відповідно. Припустимо, що оцінка $\left\| \Delta \overline{B} \right\|_2$ результату передбачуваної збурної дії на блок СП відома. Основні кроки пропонованого стеганометоду наступні.

Вбудова ДІ.

1. Матриця F розбивається стандартним чином на непересічні $l \times l$–блоки. Блок контейнера використовується для вбудови $k+1$ ($k \geq 0$) біт ДІ.

2. Нехай B — черговий блок ОП, що використовується для СПр, $p_i, ..., p_{i+k}$ — чергові біти ДІ. Вбудова ДІ проводиться шляхом збурення яскравості пікселів блоку B на одне й те саме значення Δb, що задовольняє умові (7). Кількість варіантів коректування яскравості визначається кількістю S різних варіантів упорядкованих бінарних послідовностей $p_i, ..., p_{i+k}$: $S = 2^{k+1}$. Результат – блок $\overline{B}$ СП $\overline{F}$.

Декодування ДІ.

1. Матриці F і $\overline{\overline{F}}$ розбиваються стандартним чином на непересічні $l \times l$–блоки. Блок збуреного 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 контейнера.

2.1. Визначити: $\Delta \overline{\overline{B}} = \overline{\overline{B}} - B$.

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

Основні кроки алгоритму, що реалізує запропонований метод для $k=0$, який далі називається базовим і позначається SA_B, наступні.

Вбудова ДІ.

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

2. Нехай B — черговий блок контейнера, що використовується для СПр, а p_i — черговий біт ДІ, $\overline{B}$ – відповідний блок СП.

Якщо $p_i=1$, *то* $\overline{B}=B+\Delta b\cdot\overline{E}$, *інакше* $\overline{B}=B-\Delta b\cdot\overline{E}$,

де $\overline{E}$ – $l\times l$ – матриця, всі елементи якої дорівнюють 1, $\Delta b>0$ задовольняє (7).

Декодування ДІ

1. Матриці F і $\overline{\overline{F}}$ розбиваються стандартним чином на непересічні $l\times l$ – блоки.

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

2.1. Визначити: $\Delta\overline{\overline{B}}=\overline{\overline{B}}-B$.

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

Якщо $k_p>k_n$, *то* $\overline{p}_i=1$, *інакше* $\overline{p}_i=0$.

Зауваження 3. Обчислювальна складність СА SA_B визначається кількістю блоків, на які розбивається матриця контейнера/СП, і становить $[m/l][m/l]=\underline{O}(m^2)$ операцій, де $[\bullet]$ – ціла частина аргументу.

Твердження 2. Для того, щоб атака на СП, що сформоване СА SA_B, виявилася неефективною (в умовах атаки – $NC=1$) 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 менше половини елементів у межах кожного блоку матриці СП, задіяного в СПр.

Ключовим моментом у SA_B для визначення Δb відповідно до (7) є оцінка $\left\|\Delta\overline{B}\right\|_2$. В роботі проведено оцінку $\left\|\Delta\overline{B}\right\|_2$ для $l\times l$ – блоків ЦЗ ($l\in\{4,8,10,12\}$) при накладанні шумів з найбільш часто використовуваними при моделюванні атак на СП параметрами: гауссівського (з нульовим математичним очікуванням і значеннями дисперсії $D\in\{0.0001, 0.0005, 0.001\}$), мультиплікативного ($D\in\{0.00005, 0.0001, 0.001\}$), пуассонівського шуму за допомогою обчислювального експерименту, в якому було задіяно 300 кольорових ЦЗ (схема RGB) у форматах як з втратами (Jpeg), так і без втрат (Tif) з бази NRCS, яка є традиційною при тестуванні алгоритмів, що працюють з ЦЗ, а також отримані непрофесійними фотографами. Далі ця множина ЦЗ називається експериментальною множиною. В результаті експерименту для забезпечення стійкості SA_B до накладання шумів рекомендуються значення Δb, залежність яких від l відображена на рис.1, що, враховуючи зацікавленість в можливості зменшення $|\Delta b|$ для збереження надійності сприйняття СП, надає перевагу блокам більшого розміру. Однак, збіль-

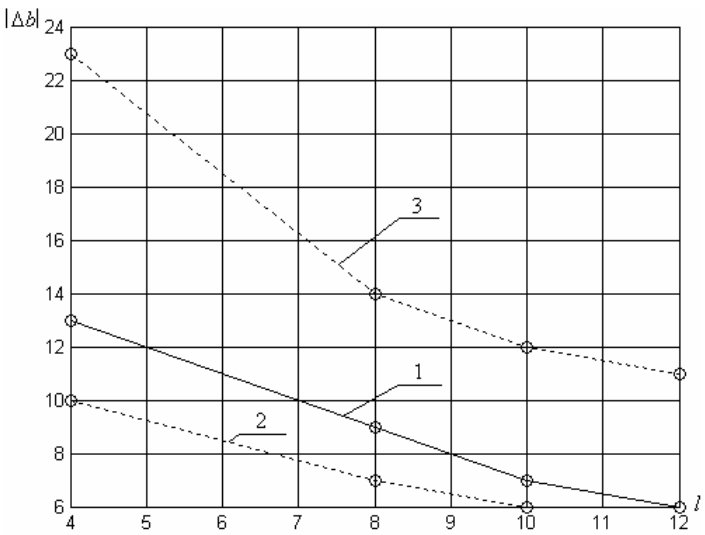

Рисунок 1 – Залежність пропонованих значень Δb від l при різних шумах: 1 – гауссівський; 2 – мультиплікативний; 3 – пуассонівський шум

шення розміру блоку приведе до змен- шення ППС стеганографічного каналу зв'язку, що є небажаним. Таким чином, «компромісними» варіантами розміру блоку l тут є величини 8,10. Основна увага при аналізі результатів дослідження приділяється гауссівському шуму, оскільки саме він найчастіше виступає як модель атакуючої дії на СП. Для гауссівського шуму збільшення розміру блоку з $l=8$ до $l=10$ дозволяє зменшити величину збурної дії Δb для кожного пікселя блоку на 22% (рис.1), але при цьому ППС зменшується на 36%: з $1/64$ до $1/100$ біт/ піксель, тому на цьому етапі дослідження рекомендовано для SA_B: $l=8$, $\Delta b=9$.

Найбільш часто використовуваними видами просторових фільтрів при моделюванні атаки на СП є: лінійні фільтри – прямокутний усереднюючий, гауссов; нелінійний – медіанний фільтр.

Показано, що при фільтрації СП усереднюючим фільтром з $p\times p-$маскою з врахуванням твердження 2 для забезпечення $NC\approx 1$ для SA_B розміри l і p повинні задовольняти співвідношенню: $l^2-8\cdot\sum_{x=1}^{[p/2]}\left(l-2(x-1)-1\right)>0$, результати врахування якого відображено в табл.1.

Таблиця 1 — Відповідність між l і p, що забезпечує ефективну роботу ($NC\approx 1$) SA_B

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

Дослідження процесу гауссової фільтрації, проведені в роботі, приводять до наступного висновку: в умовах гауссової фільтрації буде забезпечуватися висока ефективність SA_B незалежно від розміру $p\times p$ маски фільтру. Отриманий висновок кількісно підтверджується в розділі 4.

Найвідомішим нелінійним фільтром у цифровій обробці зображень є медіанний фільтр, відносно якого, враховуючи коррельованість значень яскравості сусідніх пікселів, робиться висновок, що для маски малих розмірів в умовах такої фільтрації СП буде забезпечуватися висока ефективність SA_B ($NC\approx 1$) при будь-якому розмірі l блоку. Зі збільшенням розмірів $p\times p$ маски значення NC будуть зменьшуватися, оскільки зі збільшенням відстані між пікселями коррельованість їх значень слабшає.

Таким чином, для забезпечення стійкості СА SA_B до атаки фільтрацією з відомими/передбачуваними параметрами маски рекомендується використовувати розмір блоку l відповідно до даних, наведених у табл.1.

Надзвичайно розповсюдженою завдяки популярності використання форматів із втратами для зберігання й передачі ЦЗ (найпоширеніші з яких – Jpeg, Jpeg2000) є сьогодні атака стиском, де в процесі стиску ЦЗ розбивається на блоки розміру 8×8. У силу цього для можливості найбільш ретельного контролю й аналізу змін яскравості пікселів, що відбуваються в процесі стиску СП, для забезпечення стійкості до стиску доцільно в SA_B покласти $l=8$.

Використання відомого з відкритих джерел результату оцінки величини збурної дії $8\times 8-$блоку при стиску ЦЗ з коефіцієнтами якості $QF\geq 60$: $\left\|\Delta\overline{B}\right\|_2<72$, визначає значення $\Delta b=9$ для SA_B, яке повинне гарантувати високу ефективність розроблюваного алгоритму в умовах атаки стиском.

Таким чином, враховуючи отримані результати досліджень, для одночасного забезпечення стійкості SA_B до атак проти вбудованого повідомлення: накладанню шумів, фільтрації, атаки стиском рекомендується в базовому СА використовувати

$l=8$, $\Delta b=9$. Висока стійкість СА SA_B з отриманими значенями параметрів в умовах атакуючих дій практично підтверджується в розділі 4.

Встановлено, що SA_B володіє внутрішнім паралелізмом, що дає принципову можливість для зменшення часових витрат на його роботу при реалізації в багатопроцесорній обчислювальній системі.

В **четвертому розділі** розроблено стеганометод і СА, що є модифікацією алгоритму SA_B, який зменшує спотворення контейнера під час СПр, в порівнянні з SA_B; проведена оцінка і порівняльний аналіз стійкості розроблених СА до атак проти вбудованого повідомлення; встановлено стійкість СА до стеганоаналітичних атак.

В результаті обчислювального експерименту встановлено, що спотворення ЦЗ у процесі СПр за допомогою SA_B у середньому оцінювалося $PSNR=49dB$ незалежно від формату ОП, що розглядається в літературних джерелах як значення, яке характеризує прийнятну якість СП, але для 1.7% ЦЗ з експериментальної множини суб'єктивним ранжируванням було встановлене порушення надійності сприйняття СП (на великих фонових ділянках ЦЗ). Виходячи з цього не рекомендується застосовувати SA_B для ЦЗ-контейнерів, що мають великі фонові ділянки. Для зменшення спотворення ЦЗ в результаті СПр було розроблено стеганометод і СА, що є модифікацією SA_B, де змінено вид (6) матриці ΔB збурення $l\times l$ – блоку ОП: $l\times l$ – матриця розбивається на k ділянок, k може приймати значення від 2 до $\lfloor l/2\rfloor$ (рис.2). Матриця збурення блоку в процесі СПр, для якої визначені значення k та h_i, $i=\overline{1,k}$, позначається $\Delta B^{k,h}$. Значення елементів $b^{(\Delta)}{}_{rq}$, $r,q=1,...,l$, матриці $\Delta B^{k,h}$ на i – ій ділянці:

$$\begin{cases}\lfloor \Delta b/k\rfloor \cdot i, & i=1,2,...,k-1,\\ \Delta b, & i=k\end{cases} \qquad (9)$$

де Δb задовольняє (7); при цьому h_i для різних i можуть бути різними.

Основні кроки пропонуємого методу виглядають наступним чином.

Вбудова ДІ.

1. Матрицю F розбити стандартним чином на непересічні $l\times l$ – блоки.

2. Визначити значення k, h_i, $i=\overline{1,k}$. Побудувати матрицю $\Delta B^{k,h}$ (9).

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

Якщо $p_i=1$, *то* $\overline{B}=B+\Delta B^{k,h}$, *інакше* $\overline{B}=B-\Delta B^{k,h}$.

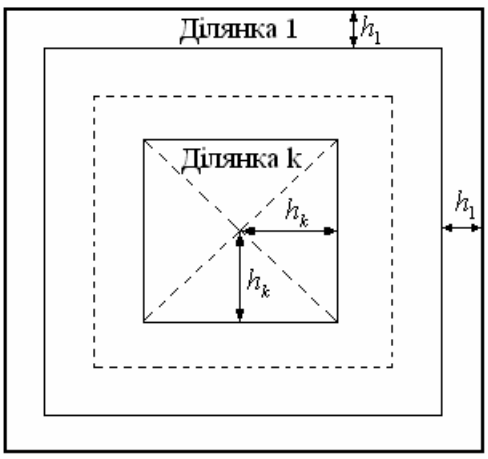

Рисунок 2 – Розбиття ΔB на k ділянок

Декодування ДІ відбувається аналогічно тому, як це робиться в SA_B ($\Delta b>0$).

Враховуючи отриману достатню умову стійкості СА, а також те, що відповідно до (9) тільки ділянка k матриці $\Delta B^{k,h}$ має значення елементів Δb (7), для того, щоб забезпечити стійкість СА, що реалізує запропонований вище метод, кількість пікселів блоку матриці контейнера, що відповідають ділянці k в $\Delta B^{k,h}$, доцільно зробити більшою за $\lfloor l^2/2\rfloor$. Для $l=8$ (обране в розділі 3) таке можливо лише в разі $k=2$, $h_1=1$, $h_2=3$, при цьому:

$$\Delta B^{k,h} = \begin{pmatrix} [\Delta b/2] & [\Delta b/2] & \dots & [\Delta b/2] & [\Delta b/2] \\ [\Delta b/2] & \Delta b & \dots & \Delta b & [\Delta b/2] \\ \dots & \dots & \dots & \dots & \dots \\ [\Delta b/2] & \Delta b & \dots & \Delta b & [\Delta b/2] \\ [\Delta b/2] & [\Delta b/2] & \dots & [\Delta b/2] & [\Delta b/2] \end{pmatrix}. \quad (10)$$

СА, для якого $k=2$, $h_1=1$, $h_2=3$, а матриця $\Delta B^{k,h}$ має вид (10), далі позначається SA_M і називається модифікованим. Для SA_M середнє значення $PSNR$ в результаті СПр дорівнює 53 dB, що на 8.2% більше, ніж для SA_B, при цьому суб'єктивним ранжируваням порушення надійності сприйняття для СП встановлено не було, тому СА SA_M може застосовуватися для будь-якого ЦЗ-контейнера. Обчислювальна складність SA_M складає $\underline{O}(m^2)$ операцій.

В роботі проводено оцінку і порівняльний аналіз стійкості розроблених СА стосовно атак проти вбудованого повідомлення. В обчислювальному експерименті були задіяні ЦЗ з експериментальної множини. Для практичного підтвердження істиності зауваження 1 спочатку при проведенні експериментів експериментальна множина була розділена на дві підмножини: ЦЗ в форматах з втратами і без втрат. Було встановлено, що стійкості розроблених алгоритмів (значення NC) на отриманих підмножинах скрізь відрізнялися менш, ніж на 1%, тому далі наведені результати, де експериментальна множина розглядається цілком.

При проведенні порівняльного аналізу стійкості розроблених СА для кожної атаки обиралася своя множина сучасних аналогів, що мають різні математичні основи та використовують різні області ЦЗ для СПр, стійких саме до розглядаємої збурної дії, оскільки велика кількість СА, що позиціонуються як стійкі, не є одночасно стійкими навіть до найпоширеніших збурних дій, часто вони є націленими на певні збурні дії, що не гарантує їх ефективність для інших.

Результати експерименту, що говорять про високу ефективність SA_B, SA_M в умовах накладання шуму представлені в табл.2,3; для пуасонівського шуму $NC=0.9977$ (для SA_B), $NC=0.9953$ (SA_M).

Таблиця 2 — Результати декодування ДІ в умовах накладання на СП 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
$PSNR$		38	35	28	25	16

Таблиця 3 — Результати декодування ДІ в умовах накладання на СП 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
$PSNR$		49	41	25	24	15

Результати проведених в роботі обчислювальних експериментів показують, що хоча стійкість алгоритму SA_B не меньша за стійкість SA_M, перевищення є дуже незначним, тому далі наводяться результати для базового алгоритму SA_B.

Для порівняльної оцінки стійкості SA_B в умовах накладання гаусівського шуму були обрані 10 найбільш ефективних сучасних аналогів. Результати порівняння (для найчастіше використовуваних дисперсій), які говорять на користь алгоритма SA_B, відображені в табл. 4. Стійкість SA_B тут перевищує стійкості всіх аналогів (винятком є лише Rawat et al. (2013) для $D = 0.01$, але при такій дисперсії порушується надійність сприйняття ЦЗ, що виявить зловмисника); для $D = 0.005$ стійкість SA_B більша за стійкість найкращого з аналогів (Su and Chen (2013)) на 4%.

Таблиця 4 — Оцінка ефективності СА в умовах гаусівського шуму (значення NC)

D	SA_B	Sura-chat (2012)	Amor-naksa et al. (2006)	Su and Chen (2013)	Al-Otum and N. Sam-ara (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	**0,9931**	0,87	0,79	-	-	0,99	0,968	-	-	-	-
0,005	**0,9881**	0,82	0,74	0,9514	0,9280	0,86	0,685	-	-	0,9276	-
0,01	**0,9619**	0,81	0,72	0,8994	0,8753	-	-	0,896	0,822	0,8714	0,9885

Результати порівняльної оцінки ефективності SA_B в умовах накладання мультиплікативного шуму з сучасними аналогами відображені на рис.3, в табл. 5 (для найчастіше вживаної дисперсії): SA_B за стійкістю перевищує аналоги в цілому; стійкість SA_B більша за стійкість найкращого (при $D = 0.001$) (Kumar and Kumar (2011)) на 1.5%.

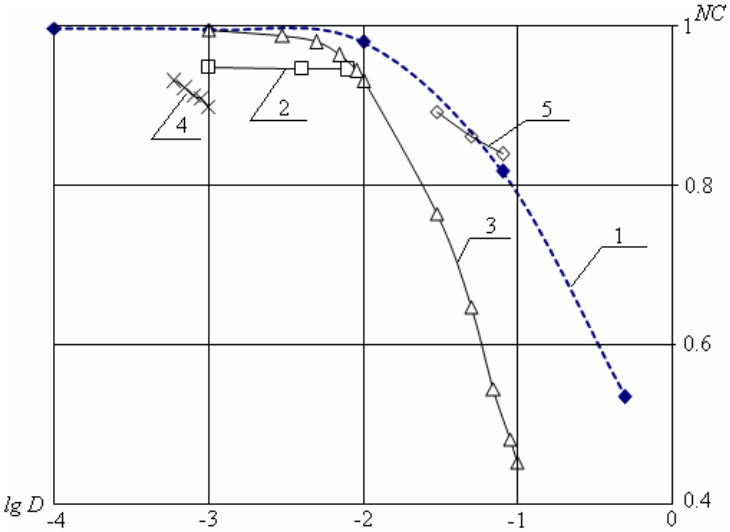

Рисунок 3 – Залежність NC від $lg\,D$ при накладанні мультиплікативного шуму: 1 - SA_B, 2 - Isac (2011), 3 - Kumar (2011), 4 - Alsaif (2013), 5 – Perwej (2012)

Для порівняльної оцінки стійкості SA_B до накладання пуасонівського шуму були обрані 13 найбільш ефективних сучасних аналогів. Результати порівняння, що відображені в табл.6, показуть, що SA_B не має рівних серед усіх аналогів, $NC \approx 1$.

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

Для практичної перевірки зроблених теоретичних висновків про стійкість розробленого СА до атаки фільтрацією був проведений обчислювальний експеримент, результати якого відображені в табл.7, у якому як контейнери були задіяні ЦЗ з експериментальної множини. Результати експерименту знаходяться у повній відповідності з отриманими в розділі 3 теоретичними твердженнями й говорять про стійкість досліджуваного СА до атаки фільтрацією.

Результати порівняльної оцінки стійкості SA_B із сучасними аналогами до атак фільтрацією наведені в табл. 8–10. 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 1.

Таблиця 5 — Стійкість СА до накладання 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	0,8985

Таблиця 6 — Стійкість СА до накладання 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)	Ra-mani et al. (2010)
0,9977	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

Таблиця 7 — Результати декодування ДІ SA_B в умовах фільтрації СП

Вид фільтра	Усереднюючий фільтр розміру $p \times p$			Гауссов фільтр розміру $p \times p$ ($sig = 0.5$)			Медіан-ний 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

Таблиця 8 — Значення NC в умовах фільтрації СП усереднюючим фільтром

Маска	SA_B	Elkhamssa et al. (2014)	Lu et al (2014)	Vafaei et al. (2013)	Thien Huynh 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	**0,994**	0,85	0,9665	0,98	0,95	0,98	0,95	0,9879	0,9933	0,95	0,93
5×5	**0,962**	-	0,8687	-	0,8	0,89	0,8	0,9354	0,8433	0,8	0,87
7×7	**0,881**	-	0,744	-	-	0,78	-	-	0,4866	0,48	-

Таблиця 9 — Значення NC в умовах фільтрації СП гауссовим 3×3 – фільтром

SA_B	Qin and Wen (2014)	T.H.The (2013)	Lingam-gunta et al. (2013)	Leung et al. (2012)	Run et al. (2011)	Ramanjaneyulu and Rajarajes-wari (2010)	Lin et al. (2009)	W.-H. Lin et al. (2009)	Lien and Lin (2006)	Li et al. (2006)
0,997	0,9853	0,99	0,85	0,7262	0,95	0,8055	0,96	0,88	0,84	0,7

Моделювання атаки стиском на СП проводилося шляхом його перезбереження у формат із втратами (Jpeg, Jpeg2000) з різними коефіцієнтами якості $QF \in \{30,40,50,60,70,80,90\}$. Результати експерименту, що говорять про високу ефективність SA_B, наведені в табл.11,12. Результати наочно підтверджують, що основним параметром, від якого залежить ефективність розробленого СА, зокрема в умовах стиску, є величина збурної дії, оцінювана за значенням $PSNR$, яку зазнає СП у процесі атаки: значення NC при близьких значеннях $PSNR$ також близькі для обох варіантів проведення атаки – збереження СП в Jpeg, Jpeg2000, не зважаючи на різні математичні основи цих стисків.

Таблиця 10 — Значення NC в умовах фільтрації СП медіанним 3×3 – фільтром

SA_B	Elkhamssa et al. (2014)	Lu et al (2014)	Cedillo-Hernandez, et al. (2013)	Hammouri et al. (2013)	Kalra et al. (2014)	Awwad (2013)	Lingam-gunta et al. (2013)	Leung et al. (2012)	Ramanjaneyulu and Rajarajes-wari (2010)	W.-H. Lin et al. (2009)
0,997	0,9	0,9894	0,98	0,9841	0,929	0,98172	0,87	0,3328	0,7466	0,9

Для порівняльної оцінки ефективності SA_B використовувалися 10 сучасних аналогів, стійких до стиску. Результати обчислювального експерименту (табл.13) показали, що стійкість SA_B не менша за стійкість всіх розглянутих аналогів.

Таблиця 11 — Результати декодування ДІ 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

Таблица 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

Таблиця 13 — Значення *NC* для SA_B в умовах атаки стиском

QF	SA_B	Elkham-ssa et al. (2014)	A1 (2013)	Vafaei et al. (2013)	Lingam-gunta 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

Результати проведених обчислювальних експериментів дали практичне підтвердження зауваженню 2, а саме тому, що стійкість СА, побудованих на основі твердження 1, визначається величиною спотворення матриці СП при атаці (*PSNR*), а не конкретним видом збурної дії, що забезпечило високу ефективність розроблених СА незалежно від виду атаки (рис.4).

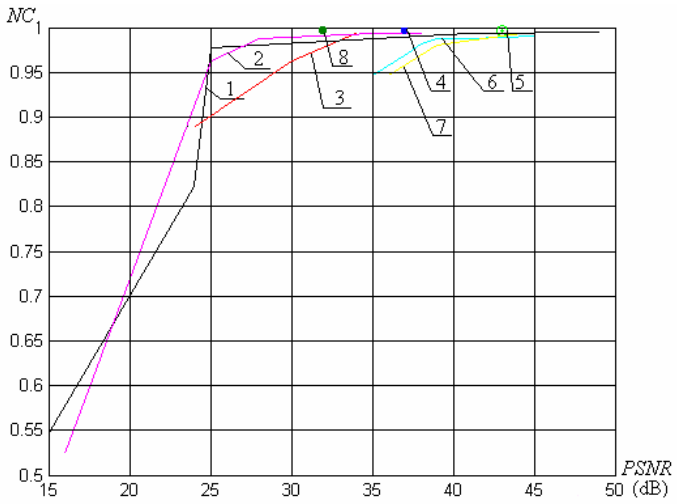

Рисунок 4 — Залежність *NC* від *PSNR* для SA_B в умовах: 1— накладання мультиплікативного шуму, 2 — гауссівського шуму, 3 — фільтрація усереднюючим фільтром, 4 — медіанним фільтром, 5 — гауссовим фільтром, 6 — збереження СП у форматі Jpeg, 7 — Jpeg2000, 8 — накладання пуассонівського шуму

Назвемо атаку проти вбудованого повідомлення комплексною, якщо вона складається з декількох збурних дій на СП. У роботі як комплексні розглядаються атаки двох видів: дворазовий стиск СП; накладання на СП шуму з наступним стиском, вибір яких обгрунтований.

Про високу ефективність розробленого СА в умовах комплексних атак свідчать результати обчислювального експерименту, в якому брали участь ЦЗ з експериментальної множини, результати якого відображені в табл. 14,15.

В роботі проведено дослідження стійкості SA_B до стеганоаналізу, здійснюваному сучасними програмними комплексами: CANVASS 1.0 (2009), StegAlyzerSS 3.0 (2007), Stegdetect 0.6.3 (2004), які мають різні математичні основи, використовують різні математичні інструменти й принципи роботи. Практично підтверджена стійкість SA_B до стеганоаналітичних атак.

Встановлено, що SA_B не має аналогів у базах сигнатур стеганоаналітичних комплексів, що здійснюють визначення наявності ДІ по масці використовуваного СА. 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%.

Таблиця 14 — Значення NC для СА SA_B в умовах дворазового стиску СП

Вторинний 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

Таблиця 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, у розділі 4 встановлена висока стійкість до атак проти вбудованого повідомлення розроблених на основі отриманої формальної достатньої умови СА, яка перевищує стійкість сучасних аналогів завдяки використанню для стеганоперетворення/декодування ДІ просторової області ЦЗ.

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 зна-

ченнях NC для контейнерів з/без втрат склала менше 1%; незалежно від конкретного виду збурної дії (значення NC визначаються значеннями $PSNR$ в результаті атаки на СП); 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 ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. 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. (Ulrich, EBSCO, РИНЦ).
2. Костирка, О.В. Стеганографічний алгоритм, стійкий до накладання шуму / О.В. Костирка // Безпека інформації. – 2014. – Т. 20, № 1. – С. 71-75. (Ulrich, EBSCO, РИНЦ, Google Scholar, WorldCat, BASE)
3. 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.
4. Рудницький, В.М. Стійке стеганоперетворення в просторовій області зображення-контейнера / В.М. Рудницький, О.В. Костирка // Інформатика та математичні методи в моделюванні. – 2013. – Т. 3, № 4. – С. 353-360. (Ulrich, EBSCO, РИНЦ)
5. 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.
6. 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), Т. 2. – С. 91-95.
7. 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.
8. Кобозева, А.А. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного сообщения / А.А. Кобозева,

О.В.Костырка, Е.Ю. Лебедева // Про- блемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2014. – № 1(24). – С. 1-12. (Google Scholar).
9. Бобок, И.И. Разработка устойчивого стеганографического алгоритма, обладающего внутренним параллелизмом / И.И. Бобок, А.А. Кобозева, О.В. Костырка // Криптографическое кодирование: коллективная монография; Под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Краснодар, 2014. – С. 98-119.
10. Костирка, О.В. Реалізація стеганоперетворення, стійкого до накладання шуму / О.В. Костирка // 11-а Всеукраїнська конференція студентів і молодих науковців «Інформатика, інформаційні системи та технології». – Одеса, 2014. – С. 56-57.
11. Костырка, О.В. Преимущества пространственной области контейнера-изображения при организации стеганопреобразования / О.В. Костырка // 3-я науково-практична конференція «Проблеми інформатики та комп'ютерної техніки ПІКТ-2014». – Чернівці, 2014. – С. 181-183.
12. 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 ІТ-індустрії». – 2014. – Вип. 2(118), Т. 2. – С. 256.
13. 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
14. Кобозева, А.А. Формальные достаточные условия устойчивости стеганоалгоритма в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // 15-я Міжнародна науково-практична конференція «Сучасні інформаційні й електронні технології». – Одеса, 2014. – Т. І. – С. 129-130.
15. Бобок, І.І. Дослідження стійкості нового стеганографічного методу до стеганоаналізу / І.І. Бобок, О.В. Костирка // V науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави». – Киев, 2014. – С. 143-145.

АНОТАЦІЯ

Костирка О.В. Підвищення ефективності стеганографічної системи в умовах атак проти вбудованого повідомлення. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Одеський національний політехнічний університет, МОНУ, Одеса, 2014.

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, що працюють у просторовій області зображення-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.

Отримана формальна достатня умова забезпечення стійкості стеганоалгоритму до збурних дій у просторовій області зображення-контейнера, для якої встановлені й кількісно оцінені її переваги для організації стеганоперетворення. На основі отриманої достатньої умови розроблені стеганографічні методи і поліноміальні (степеня 2) алгоритми, стійкість яких перевищує стійкість існуючих сучасних аналогів, що дало можливість підвищити ефективність стеганографічної системи, в порівнянні з сучасними аналогами, в умовах накладання шуму максимально на 4%, при атаці фільтрацією - на 13%, забезпечити в умовах атаки стиском та комплексних атак проти вбудованого повідомлення ефективність, близьку до максимально можливої.

Ключові слова: стеганоалгоритм, стеганосистема, стійкість стеганоалгоритма, атака проти вбудованого повідомлення, просторова область зображення.

АННОТАЦИЯ

Костырка О.В. Повышение эффективности стеганографической системы в условиях атак против встроенного сообщения. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 - системы защиты информации. - Одесский национальный политехнический университет, МОНУ, Одесса, 2014.

В работе решена важная научно-практическая задача, которая состоит в повышении эффективности стеганографической системы, являющейся необходимой составной частью современной комплексной системы защиты информации, в условиях атак против встроенного сообщения путем разработки стеганографических методов и алгоритмов для организации скрытого канала связи, которые работают в пространственной области изображения, устойчивых к возмущающим воздействиям.

Практическая ценность работы состоит в доведении полученных научных результатов до конкретных алгоритмов, которые могут быть использованы при разработках систем защиты информации любого учреждения, предприятия.

Объектом исследования являются процессы организации скрытого канала связи; предметом исследования - устойчивые к атакам против встроенного сообщения стеганографические системы.

На основе установленного соответствия между возмущениями формальных параметров, определяющих цифровое изображение в областях преобразования, - максимальных сингулярных чисел, коэффициентов дискретного косинусного преобразования, значений яркости пикселей блока матрицы изображения впервые получено формальное достаточное условие обеспечения устойчивости стеганоалгоритма к возмущающим воздействиям в пространственной области изображения-контейнера. Для пространственной области установлены и количественно оценены ее преимущества в смысле вычислительной сложности (минимально - $\underline{O}(m^2)$ операций, где $m \times m$ - размер матрицы контейнера) и вычислительной погрешности, по сравнению с областями преобразования. Полученное достаточное условие позволило построить теоретические основы устойчивых к атакам против встроенного сообщения стеганометодов и алгоритмов, разработанных в работе.

Устойчивость разработанных стеганографических алгоритмов, являющихся полиномиальными степени 2, превышает устойчивость современных аналогов, что дало возможность повысить эффективность стеганографической системы в условиях наложения шума максимально на 4%, при атаке фильтрацией - на 13%, обеспечить в условиях атаки сжатием эффективность, близкую к максимально возможной.

Дальнейшее развитие условий обеспечения утойчивости стеганоалгоритмов к атакам против встроенного сообщения за счет независимости требований, выдвигаемых полученным достаточным условием к стеганопреобразованию, от формата контейнера и конкретного вида возмущающего воздействия (устойчивость соответствующих алгоритмов определяется величиной возмущения матрицы стеганосообщения при атаке), обеспечило высокую эффективность разработанных стеганоалгоритмов независимо от вида атаки и формата изображения-контейнера (с/ без потерь), в том числе, в условиях комплексных атак, в отличие от существующих аналогов, устойчивость большинства которых обеспечивается в условиях лишь конкретных атак.

Получение количественных оценок возможных возмущений параметров стеганосообщения в процессе атак против встроенного сообщения обеспечили дальнейшее развитие методов разработки устойчивых стеганоалгоритмов, позволило получить оценки возможных возмущений яркости пикселей блоков контейнера для устойчивого стеганопреобразования в пространственной области в зависимости от размера блока матрицы изображения с учетом необходимости соблюдения надежности восприятия стеганосообщения и величины скрытой пропускной способности организуемого канала связи, которые могут быть использованы для разработки устойчивых стеганоалгоритмов.

Разработанные стеганографические алгоритмы позволяют при их использовании для внедрения цифровых водяных знаков, содержащих информацию об авторе информационного контента, обеспечить возможность аутентификации контейнера после возмущающих воздействий, направленных на стеганосообщение.

Ключевые слова: стеганоалгоритм, стеганосистема, устойчивость алгоритма, атака против встроенного сообщения, пространственная область изображения.

ABSTRACT

Kostyrka O.V. Increase in efficiency of a stego system under attacks against the embedded message. – Manuscript.

Thesis for degree the candidate in technical sciences, speciality 05.13.21 - Information Security Systems – Odessa National Polytechnic University, Odessa, 2014.

In this paper, the following important theoretical and practical task was solved: to increase the efficiency of a stego system under attacks against the embedded message by developing robust-to-disturbing-influence stego methods and algorithms for operation in the spatial domain of cover image. The practical value of the paper is that its scientific findings were reduced to specific algorithms which can be used to develop information security systems for any institution or enterprise.

A sufficient condition to ensure the robustness of a stego algorithm to disturbing influences in the spatial domain of cover image was obtained; moreover, the benefits of the spatial domain for organization of stego transformation were identified and quantitatively evaluated. Based on the sufficient condition obtained, stego methods and second degree polynomial algorithms were developed, with their robustness being higher than that of modern analogs. This made it possible to (1) get an up-to-4% and 13% increase in the effectiveness of a stego system under application of noise and filtering attack, respectively, and (2) ensure the effectiveness approaching that of the highest possible value under compression attacks and complex attacks against the embedded message.

Key words: stego algorithm, stego system, stego algorithm robustness, attack against the embedded message, spatial domain of cover image.